



Cisco Desk, Board, and Room Series Wireless LAN Deployment Guide



The Cisco RoomOS Series are industry-first, next-generation IP endpoints purpose-built for an employee's primary place of work, that combines compelling, powerfully integrated, always-on and secure, mission-critical unified communications, collaboration including HD video and cloud-computing experiences, with the interactive ease-of-use, customizable personalization and workflow options that are made available from an enterprise-grade platform.

The Cisco RoomOS Series introduce a new era in employee productivity, spawning new opportunities to collaboration-enable business processes and workflows, to advance business results.

The Cisco RoomOS Series meet the evolving needs of business, across industries and geographies, at the campus or at home, for both today and tomorrow.

This guide provides information and guidance to help the network administrator deploy the Cisco RoomOS Series into a wireless LAN environment.

Revision History

Date	Comments
07/14/21	10.5(1) Release
10/19/21	10.8(1) Release
01/17/22	10.11(1) Release
03/25/22	10.13(1) Release
02/15/24	11.13(1) Release

Contents

Cisco RoomOS Series Overview	6
<i>Models</i>	6
<i>Requirements</i>	8
Site Survey	8
Call Control	9
Wireless LAN	10
<i>Protocols</i>	15
<i>Wi-Fi</i>	15
Regulatory	27
<i>Bluetooth</i>	28
<i>Languages</i>	29
<i>Video Calls</i>	29
<i>Device Care</i>	29
Wireless LAN Design	31
<i>802.11 Network</i>	31
5 GHz (802.11a/n/ac/ax)	31
2.4 GHz (802.11b/g/n/ax).....	32
Signal Strength and Coverage	33
Data Rates	36
Rugged Environments	37
<i>Security</i>	39
Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)	40
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)	41
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS)	41
Protected Extensible Authentication Protocol (PEAP)	41
<i>Quality of Service (QoS)</i>	42
Call Admission Control (CAC).....	43
Wired QoS.....	43
<i>Roaming</i>	44
Interband Roaming	44
<i>Power Management</i>	44
<i>Call Capacity</i>	45
<i>Multicast</i>	46
Configuring the Cisco Wireless LAN	47
<i>Cisco AireOS Wireless LAN Controller and Lightweight Access Points</i>	47
802.11 Network Settings	47
WLAN Settings	58
Controller Settings.....	66
Call Admission Control (CAC).....	68
RF Profiles.....	71
FlexConnect Groups.....	73
Multicast Direct.....	75
QoS Profiles	77
Advanced Settings.....	81
<i>Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points</i>	84
802.11 Network Settings	85

WLAN Settings	93
Controller Settings.....	108
Mobility Settings.....	109
Call Admission Control (CAC).....	110
Multicast.....	110
Advanced Settings.....	113
Sample Configuration	115
<i>Cisco Mobility Express and Lightweight Access Points</i>	122
Controller Settings.....	123
802.11 Network Settings	124
WLAN Settings.....	127
RF Profiles.....	134
Multicast Direct.....	136
<i>Cisco Autonomous Access Points</i>	137
802.11 Network Settings	137
WLAN Settings.....	141
Call Admission Control (CAC).....	151
QoS Policies	152
Power Management.....	155
Sample Configuration	156
<i>Cisco Meraki Access Points</i>	161
Creating the Wireless Network	161
SSID Configuration.....	164
Radio Settings	167
Firewall and Traffic Shaping.....	169
Configuring Cisco Call Control.....	171
<i>Webex</i>	171
Personal Usage	171
Shared Usage.....	173
<i>Cisco Unified Communications Manager</i>	176
Device Enablement	176
Device Pools.....	177
Phone Button Templates	177
Security Profiles	178
SIP Profiles.....	179
QoS Parameters	182
Audio and Video Bit Rates.....	183
Product Specific Configuration Options	184
Configuring the Cisco RoomOS Series	241
<i>Wi-Fi Profile Configuration</i>	241
<i>Certificate Management</i>	252
Installing Certificates	252
Removing Certificates.....	254
<i>Call Control Configuration</i>	255
<i>Bluetooth Settings</i>	258
<i>Upgrading Firmware</i>	259
Using the Cisco RoomOS Series	261
Troubleshooting	263
<i>About Device</i>	263
<i>Network Connection Status</i>	264

<i>Advanced Wi-Fi Details</i>	264
<i>Issues and Diagnostics</i>	266
<i>Device Webpages</i>	267
System Information	267
Setup.....	268
Customization.....	271
System Maintenance	274
<i>Restoring Factory Defaults</i>	276
<i>Capturing a Screenshot of the Device Display</i>	277
Additional Documentation	279

Cisco RoomOS Series Overview

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

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

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

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

Models

The following Cisco RoomOS Series models are available.

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

Cisco RoomOS Series 1

Model	Part Number	Peak Antenna Gain	Frequency Ranges	Channel Set (# of channels)
Cisco Board 55	CS-BOARD55	2.4 GHz = 4.23 dBi 5 GHz = 6.00 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz	1-13 (13) 36,40,44,48 (4)
Cisco Board 55s	CS-BOARD55S	2.4 GHz = 4.50 dBi 5 GHz = 5.80 dBi	5.260 - 5.320 GHz 5.500 - 5.720 GHz	52,56,60,64 (4) 100-144 (12)
Cisco Board 70	CS-BOARD70	2.4 GHz = 4.23 dBi 5 GHz = 6.00 dBi	5.745 - 5.825 GHz	149,153,157,161,165 (5)
Cisco Board 70s	CS-BOARD70S	2.4 GHz = 4.40 dBi 5 GHz = 5.50 dBi		
Cisco Board 85s	CS-BOARD85S	2.4 GHz = 4.40 dBi 5 GHz = 4.40 dBi		
Cisco Board Pro 55	CS-BRD55P	2.4 GHz = 5.91 dBi 5 GHz = 5.72 dBi		

Cisco Board Pro 75	CS-BRD75P	2.4 GHz = 6.17 dBi 5 GHz = 4.95 dBi		
Cisco Codec Plus	CS-CODEC-PLUS	2.4 GHz = 3.28 dBi 5 GHz = 5.12 dBi		
Cisco Codec Pro	CS-CODEC-PRO	2.4 GHz = 4.58 dBi 5 GHz = 4.48 dBi		
Cisco Desk Limited Edition	CS-DESK-LE	2.4 GHz = 4.13 dBi 5 GHz = 5.95 dBi		
Cisco Desk Pro	CS-DESKPRO	2.4 GHz = 4.13 dBi 5 GHz = 5.95 dBi		
Cisco Room 55	CS-ROOM55	2.4 GHz = 4.00 dBi 5 GHz = 7.10 dBi		
Cisco Room 55 Dual	CS-ROOM55D	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Single	CS-ROOM70S	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Dual	CS-ROOM70D	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Single G2	CS-ROOM70SG2	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Dual G2	CS-ROOM70DG2	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room 70 Panorama	CS-ROOM70-PANO	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room Panorama	CS-ROOM-PANO85	2.4 GHz = 7.00 dBi 5 GHz = 7.18 dBi		
Cisco Room Kit	CS-KIT	2.4 GHz = 4.30 dBi 5 GHz = 5.70 dBi		
Cisco Room Kit Mini	CS-KITMINI	2.4 GHz = 3.70 dBi 5 GHz = 5.30 dBi		
Cisco Room USB	CS-ROOM-USB	2.4 GHz = 3.70 dBi 5 GHz = 5.30 dBi		

Cisco RoomOS Series 2

Model	Part Number	Peak Antenna Gain	Frequency Ranges	Channel Set (# of channels)
Cisco Desk	CS-DESK	2.4 GHz = 3.40 dBi 5 GHz = 6.10 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz	1-13 (13) 36,40,44,48 (4)
Cisco Desk Mini	CS-DESKMINI	2.4 GHz = 5.00 dBi 5 GHz = 4.90 dBi	5.260 - 5.320 GHz 5.500 - 5.720 GHz	52,56,60,64 (4) 100-144 (12)
Cisco Room Bar	CS-BAR	2.4 GHz = 4.96 dBi 5 GHz = 7.85 dBi	5.745 - 5.825 GHz	149,153,157,161,165 (5)

Cisco RoomOS Series 3

Model	Part Number	Peak Antenna Gain	Frequency Ranges	Channel Set (# of channels)
Cisco Codec EQ	CS-CODEC-EQ	2.4 GHz = 3.50 dBi 5 GHz = 3.40 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz	1-13 (13) 36,40,44,48 (4)
Cisco Room Bar Pro	CS-BARPRO	2.4 GHz = 6.70 dBi 5 GHz = 5.70 dBi	5.260 - 5.320 GHz 5.500 - 5.720 GHz 5.745 - 5.825 GHz	52,56,60,64 (4) 100-144 (12) 149,153,157,161,165 (5)

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 RoomOS Series are IEEE 802.11a/b/g/n/ac/ax collaboration devices that provides voice, video, and data communications.

The wireless LAN must be validated to ensure it meets the requirements to deploy the Cisco RoomOS Series.

Site Survey

Before deploying the Cisco RoomOS Series 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 RoomOS Series 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 RoomOS Series.

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 RoomOS Series always has 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 RoomOS Series 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 RoomOS Series can hold a signal for at least 5 seconds.

Channel Utilization

Channel Utilization levels should be kept under 40%.

Noise

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

Also need to ensure that the upstream signal from the Cisco RoomOS Series 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 RoomOS Series are supported on the following call control platforms.

- **Cisco RoomOS Series 1**
 - Webex
 - Cisco Unified Communications Manager (CUCM)
 - Minimum = 10.5(2)
 - Recommended = 11.5(1), 12.0(1), 12.5(1), 14.0(1) and later

- **Cisco RoomOS Series 2**
 - Webex
 - Cisco Unified Communications Manager (CUCM)
 - Minimum = 11.5(1)
 - Recommended = 12.5(1), 14.0(1) and later

- **Cisco RoomOS Series 3**
 - Webex
 - Cisco Unified Communications Manager (CUCM)
 - Minimum = 12.5(1)
 - Recommended = 14.0(1) and later

Note: Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable Cisco RoomOS Series device support.

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

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

Wireless LAN

The Cisco RoomOS Series are supported on the following Cisco Wireless LAN solutions.

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

Access Points

Below are the Cisco access points that are supported.

Any access point model that is not listed below is not supported.

The Cisco RoomOS Series are supported on the following Cisco Aironet access point platforms.



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

Cisco AP Series	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	Lightweight	Mobility Express	Autonomous

1700	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
1810	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
1810W	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
1815	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (not 1815t)	No
1830	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1840	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1850	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
2700	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
2800	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
3700	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
3800	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
4800	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
9105	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9115	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9117	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9120	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9124	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9130	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9136	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9162	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9164	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9166	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

The Cisco RoomOS Series are supported on the following Cisco Meraki access point platforms.



MR20



MR28



MR30H



MR32



MR33



MR34



MR36



MR36H



MR42



MR44



MR45



MR46



MR52



MR53



MR55



MR56



MR57



9162



9164



9166



MX64W



MX65W



MX67W



MX68W



Z3

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

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

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

Meraki AP Series	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
9162	Yes	Yes	Yes	Yes	Yes	Yes
9164	Yes	Yes	Yes	Yes	Yes	Yes
9166	Yes	Yes	Yes	Yes	Yes	Yes
MR20	Yes	Yes	Yes	Yes	Yes	No
MR28	Yes	Yes	Yes	Yes	Yes	Yes
MR30H	Yes	Yes	Yes	Yes	Yes	No
MR32	Yes	Yes	Yes	Yes	Yes	No
MR33	Yes	Yes	Yes	Yes	Yes	No
MR34	Yes	Yes	Yes	Yes	Yes	No
MR36	Yes	Yes	Yes	Yes	Yes	Yes
MR36H	Yes	Yes	Yes	Yes	Yes	Yes
MR42	Yes	Yes	Yes	Yes	Yes	No
MR44	Yes	Yes	Yes	Yes	Yes	Yes
MR45	Yes	Yes	Yes	Yes	Yes	Yes
MR46	Yes	Yes	Yes	Yes	Yes	Yes
MR52	Yes	Yes	Yes	Yes	Yes	No
MR53	Yes	Yes	Yes	Yes	Yes	No
MR55	Yes	Yes	Yes	Yes	Yes	Yes
MR56	Yes	Yes	Yes	Yes	Yes	Yes
MR57	Yes	Yes	Yes	Yes	Yes	Yes
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.

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

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/ax)
- Wi-Fi Protected Access v3 (WPA3+AES)
- Wi-Fi Multimedia (WMM)
- Differentiated Services Code Point (DSCP)
- Class of Service (CoS / 802.1p)

Antenna Systems

Some Cisco access points require or allow external antennas.

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

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

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

Protocols

Supported voice and wireless LAN protocols include the following:

- 802.11a,b,d,e,g,h,i,n,ac,ax
- Wi-Fi MultiMedia (WMM)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
 - AAC-LD, Opus, G.722, G.711, G.722.1, G.729
 - H.264, H.263
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- HyperText Transfer Protocol (HTTP)

Wi-Fi

The following table lists the maximum tx power and receiver sensitivity info for each data rate per 802.11 mode utilized by the Cisco RoomOS Series.

Cisco RoomOS Series 1

5 GHz Specifications

Model	5 GHz - 802.11a	Data Rate	Spatial Streams	Modulation		
Cisco Board 55 Cisco Board 55s Cisco Board 70 Cisco Board 70s Cisco Board 85s Cisco Board Pro 55 Cisco Board Pro 75 Cisco Codec Plus Cisco Codec Pro	Max Tx Power = 20 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK		
		9 Mbps	1	OFDM - BPSK		
		12 Mbps	1	OFDM - QPSK		
		18 Mbps	1	OFDM - QPSK		
		24 Mbps	1	OFDM - 16 QAM		
		36 Mbps	1	OFDM - 16 QAM		
		48 Mbps	1	OFDM - 64 QAM		
		54 Mbps	1	OFDM - 64 QAM		
		Cisco Desk Limited Edition Cisco Desk Pro	5 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
Cisco Room 55 Cisco Room 55 Dual Cisco Room 70 Single Cisco Room 70 Dual Cisco Room 70 Single G2 Cisco Room 70 Dual G2 Cisco Room 70 Panorama Cisco Room Panorama Cisco Room Kit Cisco Room Kit Mini Cisco Room USB	Max Tx Power = 19 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK		
		14 Mbps (MCS 1)	1	OFDM - QPSK		
		21 Mbps (MCS 2)	1	OFDM - QPSK		
		29 Mbps (MCS 3)	1	OFDM - 16 QAM		
		43 Mbps (MCS 4)	1	OFDM - 16 QAM		
		58 Mbps (MCS 5)	1	OFDM - 64 QAM		
		65 Mbps (MCS 6)	1	OFDM - 64 QAM		
		72 Mbps (MCS 7)	1	OFDM - 64 QAM		
		14 Mbps (MCS 8)	2	OFDM - BPSK		
		28 Mbps (MCS 9)	2	OFDM - QPSK		
		43 Mbps (MCS 10)	2	OFDM - QPSK		
		58 Mbps (MCS 11)	2	OFDM - 16 QAM		
		87 Mbps (MCS 12)	2	OFDM - 16 QAM		
		116 Mbps (MCS 13)	2	OFDM - 64 QAM		
		130 Mbps (MCS 14)	2	OFDM - 64 QAM		
144 Mbps (MCS 15)	2	OFDM - 64 QAM				
	5 GHz - 802.11n (HT40)	Data Rate	Spatial Streams	Modulation		
		Max Tx Power = 18 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK	
			30 Mbps (MCS 1)	1	OFDM - QPSK	
			45 Mbps (MCS 2)	1	OFDM - QPSK	
60 Mbps (MCS 3)	1		OFDM - 16 QAM			

		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		30 Mbps (MCS 8)	2	OFDM - BPSK
		60 Mbps (MCS 9)	2	OFDM - QPSK
		90 Mbps (MCS 10)	2	OFDM - QPSK
		120 Mbps (MCS 11)	2	OFDM - 16 QAM
		180 Mbps (MCS 12)	2	OFDM - 16 QAM
		240 Mbps (MCS 13)	2	OFDM - 64 QAM
		270 Mbps (MCS 14)	2	OFDM - 64 QAM
		300 Mbps (MCS 15)	2	OFDM - 64 QAM
	5 GHz - 802.11ac (VHT20)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 19 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		87 Mbps (MCS 8)	1	OFDM - 256 QAM
		14 Mbps (MCS 0)	2	OFDM - BPSK
		28 Mbps (MCS 1)	2	OFDM - QPSK
		43 Mbps (MCS 2)	2	OFDM - QPSK
		58 Mbps (MCS 3)	2	OFDM - 16 QAM
		87 Mbps (MCS 4)	2	OFDM - 16 QAM
		116 Mbps (MCS 5)	2	OFDM - 64 QAM
		130 Mbps (MCS 6)	2	OFDM - 64 QAM
		144 Mbps (MCS 7)	2	OFDM - 64 QAM
		173 Mbps (MCS 8)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT40)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 18 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
30 Mbps (MCS 1)		1	OFDM - QPSK	
45 Mbps (MCS 2)		1	OFDM - QPSK	
60 Mbps (MCS 3)		1	OFDM - 16 QAM	
90 Mbps (MCS 4)		1	OFDM - 16 QAM	
120 Mbps (MCS 5)		1	OFDM - 64 QAM	
135 Mbps (MCS 6)		1	OFDM - 64 QAM	
150 Mbps (MCS 7)		1	OFDM - 64 QAM	

		180 Mbps (MCS 8)	1	OFDM - 256 QAM
		200 Mbps (MCS 9)	1	OFDM - 256 QAM
		30 Mbps (MCS 0)	2	OFDM - BPSK
		60 Mbps (MCS 1)	2	OFDM - QPSK
		90 Mbps (MCS 2)	2	OFDM - QPSK
		120 Mbps (MCS 3)	2	OFDM - 16 QAM
		180 Mbps (MCS 4)	2	OFDM - 16 QAM
		240 Mbps (MCS 5)	2	OFDM - 64 QAM
		270 Mbps (MCS 6)	2	OFDM - 64 QAM
		300 Mbps (MCS 7)	2	OFDM - 64 QAM
		360 Mbps (MCS 8)	2	OFDM - 256 QAM
		400 Mbps (MCS 9)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT80)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 18 dBm (Depends on region)	33 Mbps (MCS 0)	1	OFDM - BPSK
		65 Mbps (MCS 1)	1	OFDM - QPSK
		98 Mbps (MCS 2)	1	OFDM - QPSK
		130 Mbps (MCS 3)	1	OFDM - 16 QAM
		195 Mbps (MCS 4)	1	OFDM - 16 QAM
		260 Mbps (MCS 5)	1	OFDM - 64 QAM
		293 Mbps (MCS 6)	1	OFDM - 64 QAM
		325 Mbps (MCS 7)	1	OFDM - 64 QAM
		390 Mbps (MCS 8)	1	OFDM - 256 QAM
		433 Mbps (MCS 9)	1	OFDM - 256 QAM
		65 Mbps (MCS 0)	2	OFDM - BPSK
		130 Mbps (MCS 1)	2	OFDM - QPSK
		195Mbps (MCS 2)	2	OFDM - QPSK
		260 Mbps (MCS 3)	2	OFDM - 16 QAM
390 Mbps (MCS 4)		2	OFDM - 16 QAM	
520 Mbps (MCS 5)	2	OFDM - 64 QAM		
585 Mbps (MCS 6)	2	OFDM - 64 QAM		
650 Mbps (MCS 7)	2	OFDM - 64 QAM		
780 Mbps (MCS 8)	2	OFDM - 256 QAM		
867 Mbps (MCS 9)	2	OFDM - 256 QAM		

2.4 GHz Specifications

Model	2.4 GHz - 802.11b	Data Rate	Spatial Streams	Modulation
Cisco Board 55 Cisco Board 55s	Max Tx Power = 19 dBm (Depends on region)	1 Mbps	1	DSSS - BPSK
		2 Mbps	1	DSSS - QPSK

Cisco Board 70 Cisco Board 70s Cisco Board 85s Cisco Board Pro 55 Cisco Board Pro 75 Cisco Desk Pro Cisco Desk Limited Edition Cisco Room 55 Cisco Room 55 Dual Cisco Room 70 Single Cisco Room 70 Dual Cisco Room 70 Single G2 Cisco Room 70 Dual G2 Cisco Room 70 Panorama Cisco Room Panorama Cisco Room Kit Cisco Room Kit Mini Cisco Room Kit Plus Cisco Room Kit Pro Cisco Room USB		5.5 Mbps	1	DSSS - CCK
		11 Mbps	1	DSSS - CCK
	2.4 GHz - 802.11g	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 19 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
		36 Mbps	1	OFDM - 16 QAM
		48 Mbps	1	OFDM - 64 QAM
		54 Mbps	1	OFDM - 64 QAM
	2.4 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 19 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		14 Mbps (MCS 8)	2	OFDM - BPSK
		28 Mbps (MCS 9)	2	OFDM - QPSK
		43 Mbps (MCS 10)	2	OFDM - QPSK
		58 Mbps (MCS 11)	2	OFDM - 16 QAM
		87 Mbps (MCS 12)	2	OFDM - 16 QAM
		116 Mbps (MCS 13)	2	OFDM - 64 QAM
		130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM	

Cisco RoomOS Series 2

5 GHz Specifications

Model	5 GHz - 802.11a	Data Rate	Spatial Streams	Modulation
Cisco Desk Cisco Desk Mini Cisco Room Bar	Max Tx Power = 19 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK

		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
		36 Mbps	1	OFDM - 16 QAM
		48 Mbps	1	OFDM - 64 QAM
		54 Mbps	1	OFDM - 64 QAM
	5 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 19 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		14 Mbps (MCS 8)	2	OFDM - BPSK
		28 Mbps (MCS 9)	2	OFDM - QPSK
		43 Mbps (MCS 10)	2	OFDM - QPSK
		58 Mbps (MCS 11)	2	OFDM - 16 QAM
		87 Mbps (MCS 12)	2	OFDM - 16 QAM
		116 Mbps (MCS 13)	2	OFDM - 64 QAM
		130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM	
	5 GHz - 802.11n (HT40)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 18 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
		30 Mbps (MCS 1)	1	OFDM - QPSK
		45 Mbps (MCS 2)	1	OFDM - QPSK
		60 Mbps (MCS 3)	1	OFDM - 16 QAM
		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		30 Mbps (MCS 8)	2	OFDM - BPSK
		60 Mbps (MCS 9)	2	OFDM - QPSK
		90 Mbps (MCS 10)	2	OFDM - QPSK
		120 Mbps (MCS 11)	2	OFDM - 16 QAM
		180 Mbps (MCS 12)	2	OFDM - 16 QAM
	240 Mbps (MCS 13)	2	OFDM - 64 QAM	

		270 Mbps (MCS 14)	2	OFDM - 64 QAM
		300 Mbps (MCS 15)	2	OFDM - 64 QAM
	5 GHz - 802.11ac (VHT20)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 19 dBm (Depends on region)		7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		87 Mbps (MCS 8)	1	OFDM - 256 QAM
		14 Mbps (MCS 0)	2	OFDM - BPSK
		28 Mbps (MCS 1)	2	OFDM - QPSK
		43 Mbps (MCS 2)	2	OFDM - QPSK
		58 Mbps (MCS 3)	2	OFDM - 16 QAM
		87 Mbps (MCS 4)	2	OFDM - 16 QAM
		116 Mbps (MCS 5)	2	OFDM - 64 QAM
		130 Mbps (MCS 6)	2	OFDM - 64 QAM
		144 Mbps (MCS 7)	2	OFDM - 64 QAM
		173 Mbps (MCS 8)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT40)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 18 dBm (Depends on region)		15 Mbps (MCS 0)	1	OFDM - BPSK
		30 Mbps (MCS 1)	1	OFDM - QPSK
		45 Mbps (MCS 2)	1	OFDM - QPSK
		60 Mbps (MCS 3)	1	OFDM - 16 QAM
		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		180 Mbps (MCS 8)	1	OFDM - 256 QAM
		200 Mbps (MCS 9)	1	OFDM - 256 QAM
		30 Mbps (MCS 0)	2	OFDM - BPSK
		60 Mbps (MCS 1)	2	OFDM - QPSK
		90 Mbps (MCS 2)	2	OFDM - QPSK
		120 Mbps (MCS 3)	2	OFDM - 16 QAM
		180 Mbps (MCS 4)	2	OFDM - 16 QAM
		240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM	
	300 Mbps (MCS 7)	2	OFDM - 64 QAM	

		360 Mbps (MCS 8)	2	OFDM - 256 QAM
		400 Mbps (MCS 9)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT80)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 17 dBm (Depends on region)	33 Mbps (MCS 0)	1	OFDM - BPSK
		65 Mbps (MCS 1)	1	OFDM - QPSK
		98 Mbps (MCS 2)	1	OFDM - QPSK
		130 Mbps (MCS 3)	1	OFDM - 16 QAM
		195 Mbps (MCS 4)	1	OFDM - 16 QAM
		260 Mbps (MCS 5)	1	OFDM - 64 QAM
		293 Mbps (MCS 6)	1	OFDM - 64 QAM
		325 Mbps (MCS 7)	1	OFDM - 64 QAM
		390 Mbps (MCS 8)	1	OFDM - 256 QAM
		433 Mbps (MCS 9)	1	OFDM - 256 QAM
		65 Mbps (MCS 0)	2	OFDM - BPSK
		130 Mbps (MCS 1)	2	OFDM - QPSK
		195Mbps (MCS 2)	2	OFDM - QPSK
		260 Mbps (MCS 3)	2	OFDM - 16 QAM
		390 Mbps (MCS 4)	2	OFDM - 16 QAM
		520 Mbps (MCS 5)	2	OFDM - 64 QAM
		585 Mbps (MCS 6)	2	OFDM - 64 QAM
650 Mbps (MCS 7)		2	OFDM - 64 QAM	
780 Mbps (MCS 8)		2	OFDM - 256 QAM	
867 Mbps (MCS 9)	2	OFDM - 256 QAM		

2.4 GHz Specifications

Model	2.4 GHz - 802.11b	Data Rate	Spatial Streams	Modulation
Cisco Desk Cisco Desk Mini Cisco Room Bar	Max Tx Power = 22 dBm (Depends on region)	1 Mbps	1	DSSS - BPSK
		2 Mbps	1	DSSS - QPSK
		5.5 Mbps	1	DSSS - CCK
		11 Mbps	1	DSSS - CCK
	2.4 GHz - 802.11g	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 21 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
36 Mbps		1	OFDM - 16 QAM	
48 Mbps	1	OFDM - 64 QAM		

	2.4 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
		54 Mbps	1	OFDM - 64 QAM
Max Tx Power = 20 dBm (Depends on region)		7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		14 Mbps (MCS 8)	2	OFDM - BPSK
		28 Mbps (MCS 9)	2	OFDM - QPSK
		43 Mbps (MCS 10)	2	OFDM - QPSK
		58 Mbps (MCS 11)	2	OFDM - 16 QAM
		87 Mbps (MCS 12)	2	OFDM - 16 QAM
		116 Mbps (MCS 13)	2	OFDM - 64 QAM
		130 Mbps (MCS 14)	2	OFDM - 64 QAM
		144 Mbps (MCS 15)	2	OFDM - 64 QAM

Cisco RoomOS Series 3

5 GHz Specifications

Model	5 GHz - 802.11a	Data Rate	Spatial Streams	Modulation
Cisco Codec EQ Cisco Room Bar Pro	Max Tx Power = 19 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
		36 Mbps	1	OFDM - 16 QAM
		48 Mbps	1	OFDM - 64 QAM
		54 Mbps	1	OFDM - 64 QAM
	5 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 19 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM

		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM
		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		14 Mbps (MCS 8)	2	OFDM - BPSK
		28 Mbps (MCS 9)	2	OFDM - QPSK
		43 Mbps (MCS 10)	2	OFDM - QPSK
		58 Mbps (MCS 11)	2	OFDM - 16 QAM
		87 Mbps (MCS 12)	2	OFDM - 16 QAM
		116 Mbps (MCS 13)	2	OFDM - 64 QAM
		130 Mbps (MCS 14)	2	OFDM - 64 QAM
		144 Mbps (MCS 15)	2	OFDM - 64 QAM
	5 GHz - 802.11n (HT40)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 18 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
		30 Mbps (MCS 1)	1	OFDM - QPSK
		45 Mbps (MCS 2)	1	OFDM - QPSK
		60 Mbps (MCS 3)	1	OFDM - 16 QAM
		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		30 Mbps (MCS 8)	2	OFDM - BPSK
		60 Mbps (MCS 9)	2	OFDM - QPSK
		90 Mbps (MCS 10)	2	OFDM - QPSK
		120 Mbps (MCS 11)	2	OFDM - 16 QAM
		180 Mbps (MCS 12)	2	OFDM - 16 QAM
		240 Mbps (MCS 13)	2	OFDM - 64 QAM
		270 Mbps (MCS 14)	2	OFDM - 64 QAM
		300 Mbps (MCS 15)	2	OFDM - 64 QAM
	5 GHz - 802.11ac (VHT20)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 19 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
		21 Mbps (MCS 2)	1	OFDM - QPSK
		29 Mbps (MCS 3)	1	OFDM - 16 QAM
		43 Mbps (MCS 4)	1	OFDM - 16 QAM
		58 Mbps (MCS 5)	1	OFDM - 64 QAM
		65 Mbps (MCS 6)	1	OFDM - 64 QAM

		72 Mbps (MCS 7)	1	OFDM - 64 QAM
		87 Mbps (MCS 8)	1	OFDM - 256 QAM
		14 Mbps (MCS 0)	2	OFDM - BPSK
		28 Mbps (MCS 1)	2	OFDM - QPSK
		43 Mbps (MCS 2)	2	OFDM - QPSK
		58 Mbps (MCS 3)	2	OFDM - 16 QAM
		87 Mbps (MCS 4)	2	OFDM - 16 QAM
		116 Mbps (MCS 5)	2	OFDM - 64 QAM
		130 Mbps (MCS 6)	2	OFDM - 64 QAM
		144 Mbps (MCS 7)	2	OFDM - 64 QAM
		173 Mbps (MCS 8)	2	OFDM - 256 QAM
	5 GHz - 802.11ac (VHT40)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 18 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
		30 Mbps (MCS 1)	1	OFDM - QPSK
		45 Mbps (MCS 2)	1	OFDM - QPSK
		60 Mbps (MCS 3)	1	OFDM - 16 QAM
		90 Mbps (MCS 4)	1	OFDM - 16 QAM
		120 Mbps (MCS 5)	1	OFDM - 64 QAM
		135 Mbps (MCS 6)	1	OFDM - 64 QAM
		150 Mbps (MCS 7)	1	OFDM - 64 QAM
		180 Mbps (MCS 8)	1	OFDM - 256 QAM
		200 Mbps (MCS 9)	1	OFDM - 256 QAM
		30 Mbps (MCS 0)	2	OFDM - BPSK
		60 Mbps (MCS 1)	2	OFDM - QPSK
		90 Mbps (MCS 2)	2	OFDM - QPSK
		120 Mbps (MCS 3)	2	OFDM - 16 QAM
		180 Mbps (MCS 4)	2	OFDM - 16 QAM
		240 Mbps (MCS 5)	2	OFDM - 64 QAM
		270 Mbps (MCS 6)	2	OFDM - 64 QAM
		300 Mbps (MCS 7)	2	OFDM - 64 QAM
		360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM	
	5 GHz - 802.11ac (VHT80)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 17 dBm (Depends on region)	33 Mbps (MCS 0)	1	OFDM - BPSK
		65 Mbps (MCS 1)	1	OFDM - QPSK
		98 Mbps (MCS 2)	1	OFDM - QPSK
		130 Mbps (MCS 3)	1	OFDM - 16 QAM
		195 Mbps (MCS 4)	1	OFDM - 16 QAM
		260 Mbps (MCS 5)	1	OFDM - 64 QAM
		293 Mbps (MCS 6)	1	OFDM - 64 QAM

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

2.4 GHz Specifications

Model	2.4 GHz - 802.11b	Data Rate	Spatial Streams	Modulation
Cisco Codec EQ Cisco Room Bar Pro	Max Tx Power = 22 dBm (Depends on region)	1 Mbps	1	DSSS - BPSK
		2 Mbps	1	DSSS - QPSK
		5.5 Mbps	1	DSSS - CCK
		11 Mbps	1	DSSS - CCK
	2.4 GHz - 802.11g	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 21 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
		9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
		24 Mbps	1	OFDM - 16 QAM
		36 Mbps	1	OFDM - 16 QAM
		48 Mbps	1	OFDM - 64 QAM
		54 Mbps	1	OFDM - 64 QAM
	2.4 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
	Max Tx Power = 20 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
		14 Mbps (MCS 1)	1	OFDM - QPSK
21 Mbps (MCS 2)		1	OFDM - QPSK	
29 Mbps (MCS 3)		1	OFDM - 16 QAM	
43 Mbps (MCS 4)		1	OFDM - 16 QAM	
58 Mbps (MCS 5)		1	OFDM - 64 QAM	
65 Mbps (MCS 6)		1	OFDM - 64 QAM	
72 Mbps (MCS 7)		1	OFDM - 64 QAM	

		14 Mbps (MCS 8)	2	OFDM - BPSK
		28 Mbps (MCS 9)	2	OFDM - QPSK
		43 Mbps (MCS 10)	2	OFDM - QPSK
		58 Mbps (MCS 11)	2	OFDM - 16 QAM
		87 Mbps (MCS 12)	2	OFDM - 16 QAM
		116 Mbps (MCS 13)	2	OFDM - 64 QAM
		130 Mbps (MCS 14)	2	OFDM - 64 QAM
		144 Mbps (MCS 15)	2	OFDM - 64 QAM

Note: 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 dual integrated antennas.

To achieve 802.11n/ac/ax connectivity, it is recommended that the Cisco RoomOS Series 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 RoomOS Series operates 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 RoomOS Series will passively scan DFS channels first before engaging in active scans of those channels.

If 802.11d is not enabled, then the Cisco RoomOS Series 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 RoomOS Series.

Australia (AU)	Hungary (HU)	Philippines (PH)
Austria (AT)	Iceland (IS)	Poland (PL)
Bahrain (BH)	India (IN)	Portugal (PT)
Belgium (BE)	Ireland (IE)	Puerto Rico (PR)
Brazil (BR)	Israel (IL)	Romania (RO)
Bulgaria (BG)	Italy (IT)	Russian Federation (RU)
Canada (CA)	Japan (JP)	Saudi Arabia (SA)
Chile (CL)	Korea (KR)	Serbia (RS)
China (CN)	Latvia (LV)	Singapore (SG)
Colombia (CO)	Liechtenstein (LI)	Slovakia (SK)
Costa Rica (CR)	Lithuania (LT)	Slovenia (SI)
Croatia (HR)	Luxembourg (LU)	South Africa (ZA)
Cyprus (CY)	Macedonia (MK)	Spain (ES)
Czech Republic (CZ)	Malaysia (MY)	Sweden (SE)
Denmark (DK)	Malta (MT)	Switzerland (CH)
Dominican Republic (DO)	Mexico (MX)	Taiwan (TW)

Ecuador (EC)	Monaco (MC)	Thailand (TH)
Egypt (EG)	Montenegro (ME)	Turkey (TR)
Estonia (EE)	Netherlands (NL)	Ukraine (UA)
Finland (FI)	New Zealand (NZ)	United Arab Emirates (AE)
France (FR)	Nigeria (NG)	United Kingdom (GB)
Germany (DE)	Norway (NO)	United States (US)
Gibraltar (GI)	Panama (PA)	Uruguay (UY)
Greece (GR)	Paraguay (PY)	Vietnam (VN)
Hong Kong (HK)	Peru (PE)	

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

<https://cae-cnc-prd.cisco.com/pdtenc>

Bluetooth

The Cisco RoomOS Series supports 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 RoomOS Series.

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/ax 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 RoomOS Series supports the following Bluetooth profiles.

- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Generic Access Profile (GAP)
- Generic Audio/Video Distribution Profile (GAVDP)
- Hands-Free Profile (HFP)

Coexistence (802.11b/g/n/ax + Bluetooth)

If using Coexistence where 802.11b/g/n/ax 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/ax + Bluetooth), call capacity is reduced due to the utilization of CTS to protect the 802.11g/n/ax 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/ax if using Bluetooth due to 802.11b/g/n/ax and Bluetooth both utilizing 2.4 GHz, but also due to the above limitations.

Languages

The Cisco RoomOS Series supports the following languages.

Arabic	French	Polish
Catalan	German	Portuguese
Chinese	Hebrew	Russian
Czech	Hungarian	Spanish
Danish	Italian	Swedish
Dutch	Japanese	Turkish
English	Korean	
Finnish	Norwegian	

Video Calls

The Cisco RoomOS Series supports video calling via a high-resolution multi-touch color LCD and an integrated camera.

The Cisco RoomOS Series is able to establish video calls with other Cisco RoomOS Series endpoints, Cisco TelePresence Systems, and other video enabled endpoints.

H.264 is the protocol used for the video stream, where up to 30 fps (frames per second) are supported.

There is a separate stream for the audio session that utilizes one of the support audio codecs.

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

The following video formats are supported:

- QnHD 180p (320 x 180)
- CIF 288p (512 x 288)
- nHD 360p (640 x 360)
- SD 448p (768 x 448)
- WSVGA 576p (1024 x 576)
- HD 720p (1280 x 720)
- FHD 1080p (1920 x 1080)

Device Care

To clean the Cisco RoomOS Series, use a soft, moist cloth to wipe the device.
Do not apply liquids or powders directly to the device as it can damage the device.
Do not use bleach or other caustic products to clean the device.
Do not use compressed air to clean the device as it can also damage the device.

For more information, refer to the **Cisco RoomOS Series User Guide** at this URL:

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-user-guide-list.html>

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 RoomOS Series.

802.11 Network

Use the following guidelines to plan channel usage for these wireless environments.

5 GHz (802.11a/n/ac/ax)

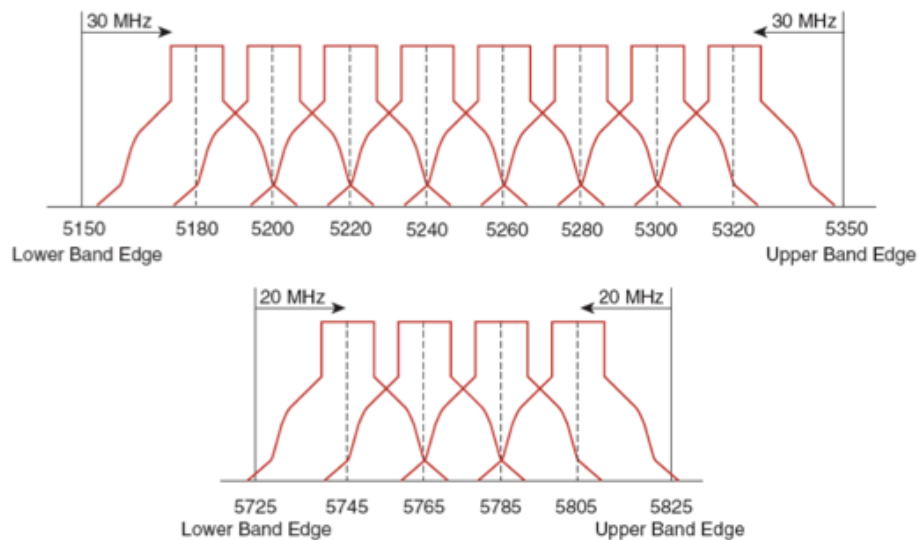
5 GHz is the recommended frequency band to utilize for operation of the Cisco RoomOS Series.

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 RoomOS Series supports 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 RoomOS Series in the 802.11a/n/ac/ax 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 a signal of -67 dBm or higher, while the Cisco RoomOS Series also meets 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																UNII-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.

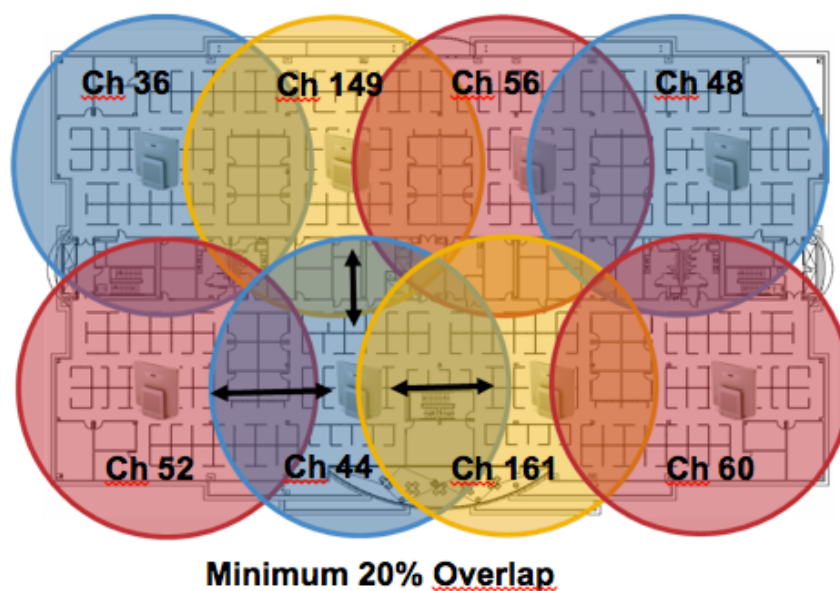
If there are repeated radar events detected by the access point (just or falsely), determine if the radar signals are impacting a single channel (narrowband) or multiple channels (wideband), then potentially disable use of that channel or channels in the wireless LAN.

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/ax)

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

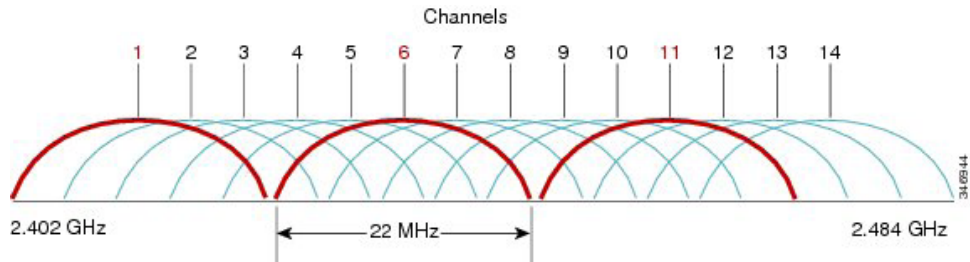
If there is an intermittent interferer, then the access point or access points serving that area may need to have a channel statically assigned.

In a 2.4 GHz (802.11b/g/n/ax) 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.

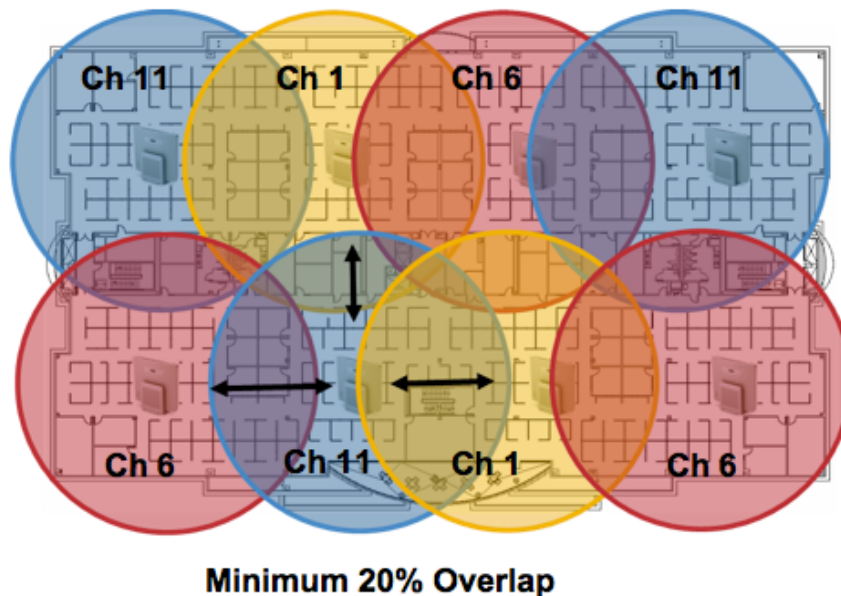
There are only 3 non-overlapping channels in the 2.4 GHz frequency range (channels 1, 6, 11).

Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying the Cisco RoomOS Series in an 802.11b/g/n/ax 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 RoomOS Series should always have a signal of -67 dBm or higher when using 5 GHz or 2.4 GHz, while the Cisco RoomOS Series also meets 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%.

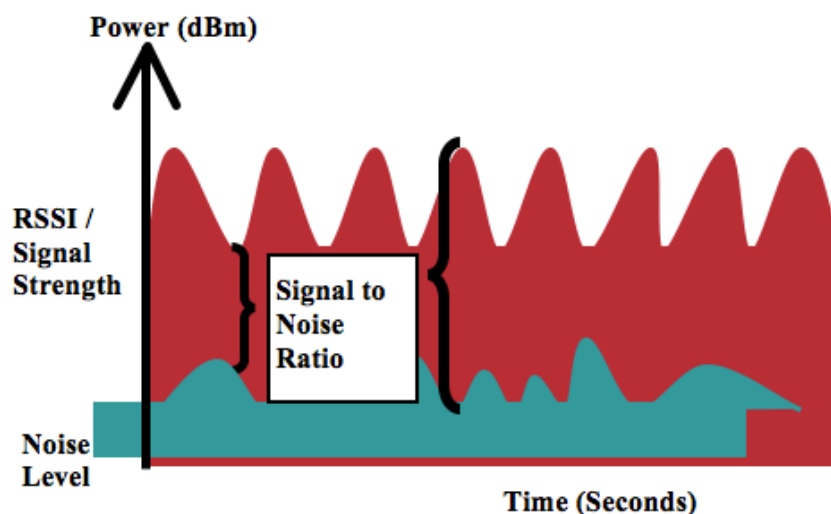
A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal should be maintained.

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).

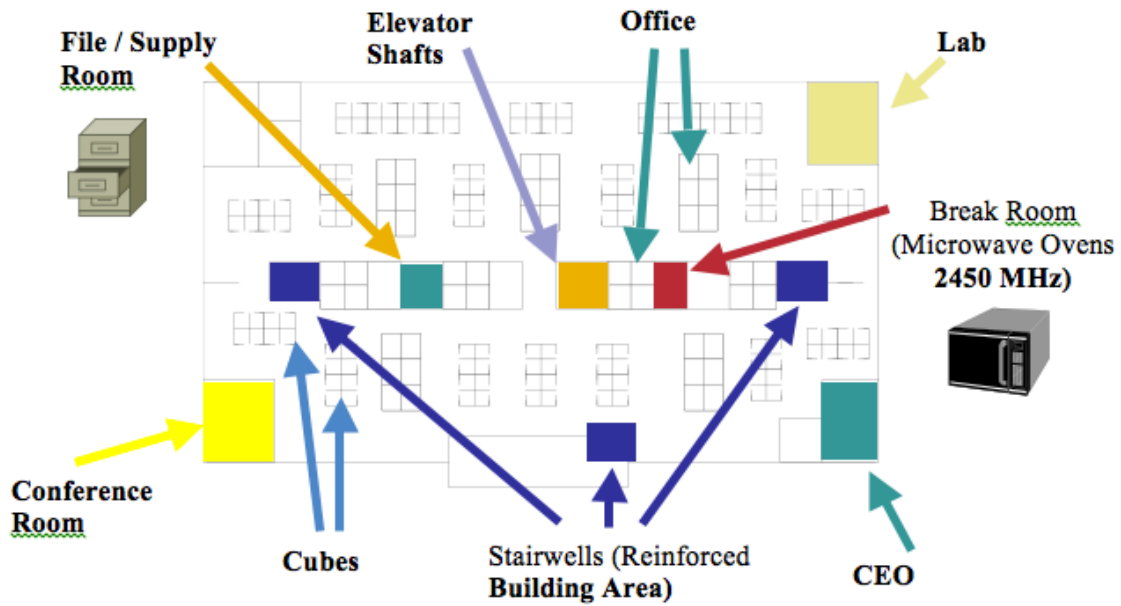
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

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/ax. 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/ax technology provides more non-overlapping channels and typically lower initial RF utilization. For voice deployments, it is suggested to use 802.11a/n/ac/ax for voice and use 802.11b/g/n/ax for data.

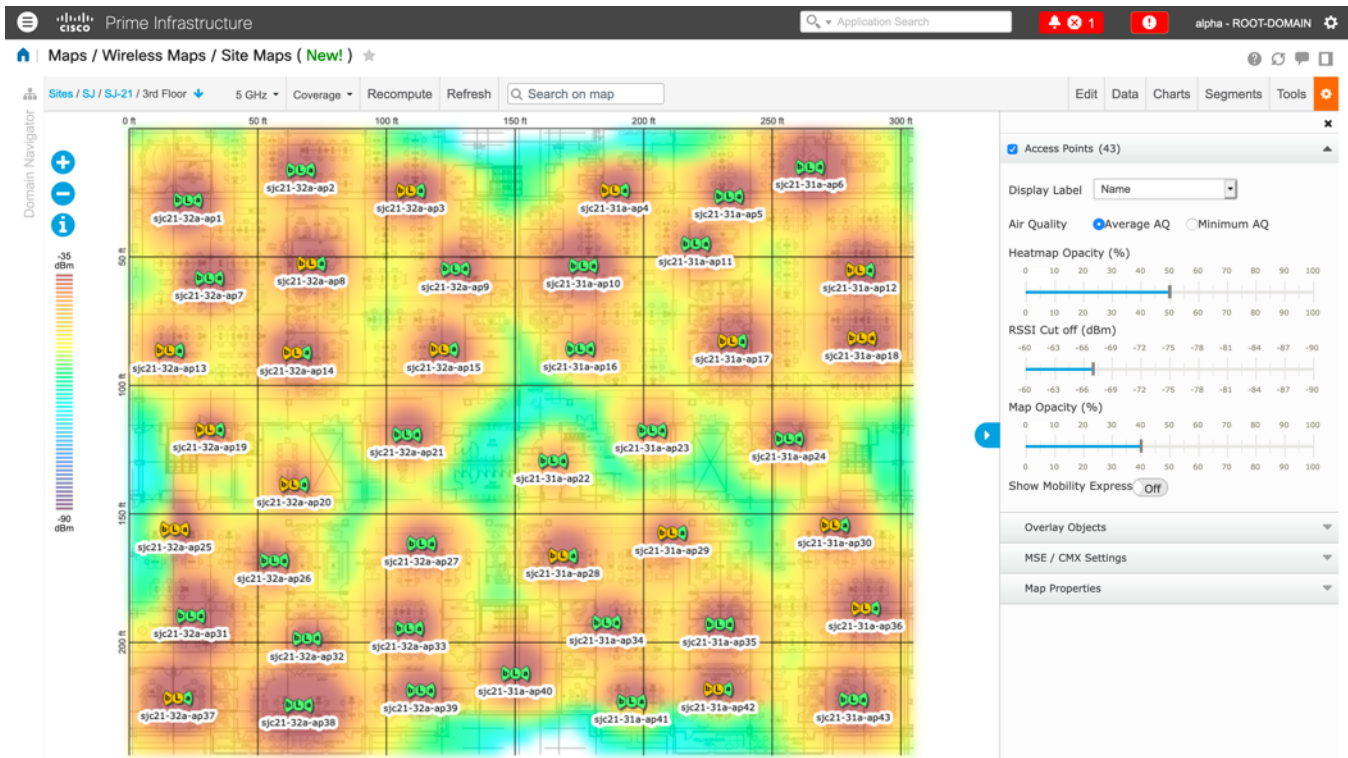
However there are products that also utilize the non-licensed 5 GHz frequency (e.g. 5.8 GHz cordless phones, which can impact UNII-3 channels).



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 RoomOS Series has dual antennas, therefore they support up to MCS 15 data rates for 802.11n (up to 300 Mbps).

For 802.11ac, the Cisco RoomOS Series supports up to VHT80 MCS 9 2SS (up to 867 Mbps).

For 802.11ax, the capable Cisco RoomOS Series supports up to HE80 MCS 11 (up to 1200 Mbps).

Higher MCS rates can be left enabled for other 802.11n/ac/ax 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/ax 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:

5 GHz

802.11 Mode	Mandatory Data Rates	Supported Data Rates	Disabled Data Rates
802.11ax	12 Mbps	18-54 Mbps, HE MCS 0 - MCS 11 1SS, HE MCS 0 - MCS 11 2SS	6, 9 Mbps
802.11ac	12 Mbps	18-54 Mbps,	6, 9 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)	
802.11n	12 Mbps	18-54 Mbps, HT MCS 0 - MCS 15, (HT MCS 16 - MCS 31)	6, 9 Mbps
802.11a	12 Mbps	18-54 Mbps	6, 9 Mbps

2.4 GHz

802.11 Mode	Mandatory Data Rates	Supported Data Rates	Disabled Data Rates
802.11ax	12 Mbps	18-54 Mbps, HE MCS 0 - MCS 11 1SS, HE MCS 0 - MCS 11 2SS	1, 2, 5.5, 6, 9, 11 Mbps
802.11n	12 Mbps	18-54 Mbps, HT MCS 0 - MCS 15, (HT MCS 16 - MCS 31)	1, 2, 5.5, 6, 9, 11 Mbps
802.11g	12 Mbps	18-54 Mbps	1, 2, 5.5, 6, 9, 11 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 RoomOS Series 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 RoomOS Series 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 RoomOS Series 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 RoomOS Series will utilize the access point's current transmit power setting to determine what transmit power it uses for transmitted frames when DTPC is enabled in the access point's configuration.

Fast Roaming

It is recommended to utilize 802.11r / Fast Transition (FT) for fast roaming. Enabling 802.11r (FT) also reduces the number of frames in the handshake when roaming to only two frames. Reducing the number of frames during a roam, increases the chances of roam success.

When using 802.1x authentication, it is important to use the recommended EAPOL key settings.

Quality of Service (QoS)

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

Beamforming

If using Cisco 802.11n/ac/ax 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

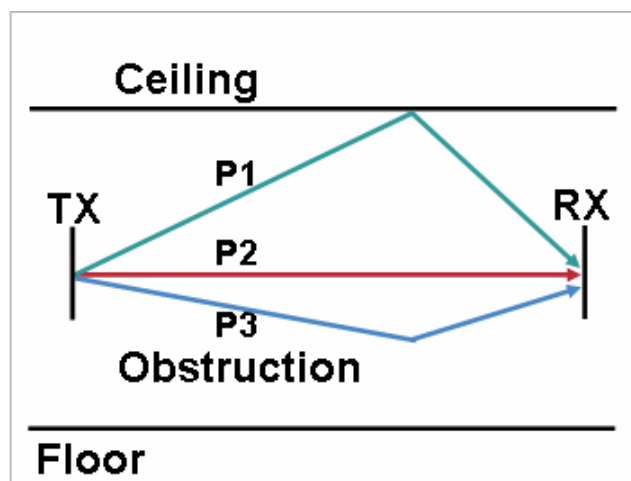
Occurs when the reflected waves arrive exactly out of phase with the main signal and cancel the main signal completely.

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/ax and 802.11g/n/ax, 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 RoomOS Series supports the following wireless security features.

WLAN Authentication

- Enterprise
 - WPA3 802.1x
 - EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
 - EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
 - EAP-TTLS (Extensible Authentication Protocol – Tunneled Transport Layer Security)
 - PEAP (Protected Extensible Authentication Protocol)
 - WPA2 802.1x
 - EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
 - EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
 - EAP-TTLS (Extensible Authentication Protocol – Tunneled Transport Layer Security)
 - PEAP (Protected Extensible Authentication Protocol)
- Personal
 - WPA3-SAE (Simultaneous Authentication of Equals)
 - WPA2-PSK (Pre-Shared key)
- None

WLAN Encryption

- AES (Advanced Encryption Standard)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)

Note: The access point must support AES (CCMP128) as TKIP can only be used as the broadcast/multicast cipher. CCMP256, GCMP128, and GCMP256 encryption ciphers are not supported.

The Cisco RoomOS Series also supports the following additional security features.

- Image authentication
- Device authentication
- File authentication
- Signaling authentication
- Media encryption (SRTP)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)
- Secure profiles
- Encrypted configuration files

Extensible Authentication Protocol - 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 RoomOS Series) and the RADIUS server. The server sends an Authority ID (AID) to the client, which in turn selects the appropriate PAC. The client returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both endpoints now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must enable don the RADIUS server.

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

The Cisco RoomOS Series currently supports 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 RoomOS Series.

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

Ensure the production master EAP-FAST RADIUS server is setup to send the EAP-FAST master keys and policies to the staging slave EAP-FAST RADIUS server, which will then allow the Cisco RoomOS Series 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 RoomOS Series has connected to the network during the grace period to ensure it can use its existing PAC created either using the active or retired master key in order to get issued a new PAC.

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

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

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

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

A certificate is required to be installed.

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

EAP-TLS may also require a user account to be created on the authentication server matching the common name of the certificate imported into the Cisco RoomOS Series.

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

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

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

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

The authentication server can be validated via importing a certificate into the Cisco RoomOS Series.

Protected Extensible Authentication Protocol (PEAP)

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

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

PEAP-NONE, PEAP-GTC and PEAP-MSCHAPv2 are supported inner authentication protocols.

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

The authentication server can be validated via importing a certificate into the Cisco RoomOS Series.

Quality of Service (QoS)

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

To enable proper queuing for voice, interactive video, 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, interactive video, and call control traffic.

Traffic Type	Call Server	DSCP	802.1p	WMM UP	Protocol
Voice	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
	Webex	EF (46)	5	6	RTP (UDP 5004)
TelePresence Voice	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
	Webex	EF (46)	5	6	RTP (UDP 5004)
TelePresence Video	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
	Webex	AF41 (34)	4	5	RTP (UDP 5004)
Call Control	CUCM	CS3 (24)	3	4	SIP (TCP/UDP 5060 - 5061)
	Webex	Default (0)	0	0	HTTPS (TCP 443)

- Be sure that voice, interactive video, 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 IP Phone 8861 and 8865 and the Cisco Unified Communications Manager, refer to the **Cisco Unified Communications Manager TCP and UDP Port Usage** document at this URL:

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

For information on network requirements for Webex, refer to the **Network Requirements for Webex Services** document at this URL:

<https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services>

Call Admission Control (CAC)

The Cisco RoomOS Series currently does not support Call Admission Control of voice or video streams.

If TSPEC is enabled for voice or video in the access point, then the priority of voice and video frames will be downgraded.

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 RoomOS Series enables both sets of frequencies, which allows the Cisco RoomOS Series to connect to either 5 GHz or 2.4 GHz and enables interband roaming support.

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

If 802.11r (FT) 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.

Security Type	Roaming Time
Personal	150 ms
Enterprise	300 ms

The Cisco RoomOS Series manages 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).

Note: The Cisco RoomOS Series does not currently support 802.11r (FT).

Interband Roaming

The Cisco RoomOS Series enables both sets of frequencies, 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 RoomOS Series will scan all 2.4 and 5 GHz channels, then attempt to associate to an access point for the configured network if available.

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

Power Management

The power supply is required to enable the Cisco RoomOS Series for wireless LAN mode, as there is no internal battery.

Wireless LAN is automatically disabled temporarily when Ethernet is connected to the Cisco RoomOS Series, but will be automatically re-enabled once Ethernet is disconnected if Wireless LAN was enabled previously.

The Cisco RoomOS Series primarily uses active mode (no Wi-Fi power save) when in idle or on call.

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

Delivery Traffic Indicator Message (DTIM)

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

Since the Cisco RoomOS Series uses active mode, the DTIM period will not be used to schedule wake up periods to check for broadcast and multicast packets as well as any unicast packets.

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

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

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/ax and 802.11g/n/ax at a data rate of 24 Mbps or higher. To achieve this capacity, there must be minimal wireless LAN background traffic and initial radio frequency (RF) utilization.

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

Audio Only Calls

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

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

Video Calls

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

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

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

Max # of Video Calls	802.11 Mode	Audio Codec	Audio Bit Rate	Video Type	Video Resolution	Video Bit Rate
2-11+	5 GHz or 2.4 GHz	G.722 / G.711	64 Kbps	HD 720p	1280 x 720	1000 Kbps

1-7+	5 GHz or 2.4 GHz	G.722 / G.711	64 Kbps	FHD 1080p	1920 x 1080	2500 Kbps
------	------------------	---------------	---------	-----------	-------------	-----------

Note: Currently there is no Call Admission Control support.

Multicast

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

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

The Cisco RoomOS Series utilizes active mode primarily, but if there is an associated client that is in power save mode, then all multicast packets will be queued until the DTIM period.

With multicast, there is no guarantee that the packet will be received 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 RoomOS Series supports 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/ax 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)** and **CCKM** are not configured as mandatory
- 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**
- 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, Required, or Disabled**
- Set **MFP Client Protection** to **Optional, Required, 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/ac/ax capable Access Points
- Configure the **Data Rates** as necessary
- Configure **Auto RF** as necessary
- 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 RoomOS Series 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/ax network status is **Enabled**.

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

If using Cisco 802.11n/ac/ax 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.

The screenshot shows the Cisco RoomOS configuration interface for 802.11a Global Parameters. The interface is divided into several sections:

- General:** 802.11a Network Status (Enabled), Beacon Period (100), Fragmentation Threshold (2346), DTPC Support (Enabled), Maximum Allowed Clients (100), RSSI Low Check (Disabled), and RSSI Threshold (-80).
- 802.11a Band Status:** Low Band (Enabled), Mid Band (Enabled), High Band (Enabled).
- Data Rates:**:** 6 Mbps (Disabled), 9 Mbps (Disabled), 12 Mbps (Mandatory), 18 Mbps (Supported), 24 Mbps (Supported), 36 Mbps (Supported), 48 Mbps (Supported), 54 Mbps (Supported).
- CCX Location Measurement:** Mode (Enabled), Interval (60 seconds).
- TWT Configuration ***:** Target Waketime (Enabled), Broadcast TWT Support (Enabled).

If wanting to use 2.4 GHz, ensure the 802.11b/g/n/ax 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.

If using Cisco 802.11n/ac/ax 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).

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS (selected), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the 'Wireless' menu with options like Access Points, Radios, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, and Network Lists. The main content area is titled '802.11b/g Global Parameters' and is divided into three sections:

- General:**
 - 802.11b/g Network Status: Enabled
 - 802.11g Support: Enabled
 - Beacon Period (milliseconds):
 - Short Preamble: Enabled
 - Fragmentation Threshold (bytes):
 - DTPC Support: Enabled
 - Maximum Allowed Clients:
 - RSSI Low Check: Enabled
 - RSSI Threshold (-60 to -90 dBm):
- CCX Location Measurement:**
 - Mode: Enabled
 - Interval (seconds):
- Data Rates**:**
 - 1 Mbps: Disabled
 - 2 Mbps: Disabled
 - 5.5 Mbps: Disabled
 - 6 Mbps: Disabled
 - 9 Mbps: Disabled
 - 11 Mbps: Disabled
 - 12 Mbps: Mandatory
 - 18 Mbps: Supported
 - 24 Mbps: Supported
 - 36 Mbps: Supported
 - 48 Mbps: Supported
 - 54 Mbps: Supported
- TWT Configuration ***:**
 - Target Waketime: Enabled
 - Broadcast TWT Support: Enabled

Beamforming (ClientLink)

Enable **ClientLink** if using Cisco 802.11n/ac/ax 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**

802.11a/n/ac/ax Cisco APs > Configure

General

AP Name: rtp9-31a-ap1
 Admin Status: Enable
 Operational Status: UP
 Slot #: 1

11n Parameters

11n Supported: Yes

CleanAir

CleanAir Capable: Yes
 CleanAir Admin Status: Enable
 * CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections: 0

Antenna Parameters

Antenna Type: Internal
 Antenna: A, B, C, D (all checked)

RF Channel Assignment

Current Channel: (48,44)
 Channel Width: 40 MHz
 * Channel width can be configured only when channel configuration is in custom mode
 Assignment Method: Global

Radar Information

Channel: Last Heard(Seecs)
 No radar detected channels

Tx Power Level Assignment

Current Tx Power Level: 1
 Assignment Method: Global

Performance Profile

View and edit Performance Profile for this AP
 Performance Profile

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

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.

802.11a > RRM > Tx Power Control(TPC)

TPC Version

Interference Optimal Mode (TPCv2)
 Coverage Optimal Mode (TPCv1)

Tx Power Level Assignment Algorithm

Power Level Assignment Method: Automatic (Every 600 sec)
 On Demand (Invoke Power Update Once)
 Fixed (1)

Maximum Power Level Assignment (-10 to 30 dBm): 17
 Minimum Power Level Assignment (-10 to 30 dBm): 11
 Power Assignment Leader: RTP9-32A-WLC3 (10.81.6.70)
 Last Power Level Assignment: 463 secs ago
 Power Threshold (-80 to -50 dBm): -65
 Channel Aware: Enabled
 Power Neighbor Count: 3

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 or 802.11ax Access Points.

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

The screenshot shows the Cisco Wireless LAN Controller configuration interface for Dynamic Channel Assignment (DCA). The left sidebar contains navigation options like 'Access Points', 'Advanced', 'Mesh', 'AP Group NTP', 'ATF', 'RF Profiles', 'FlexConnect Groups', 'FlexConnect ACLs', 'FlexConnect VLAN Templates', and 'Network Lists'. The main content area is titled '802.11a > RRM > Dynamic Channel Assignment (DCA)'. Under the 'Dynamic Channel Assignment Algorithm' section, the following settings are visible:

- Channel Assignment Method: Automatic, Freeze, OFF
- Interval: 10 minutes, AnchorTime: 0
- Invoke Channel Update Once: [Button]
- Avoid Foreign AP interference: Enabled, Disabled
- Avoid Cisco AP load: Enabled, Disabled
- Avoid non-802.11a noise: Enabled, Disabled
- Avoid Persistent Non-WiFi Interference: Enabled, Disabled
- Channel Assignment Leader: RTP9-32A-WLC3 (10.81.6.70)
- Last Auto Channel Assignment: 556 secs ago
- DCA Channel Sensitivity: Medium (15 dB)
- Channel Width: 20 MHz, 40 MHz, 80 MHz, 160 MHz, 80+80 MHz, Best
- Avoid check for non-DFS channel: Enabled, Disabled

The 'DCA Channel List' is shown as a text box containing the following channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 153, 157, 161.

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/ax Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.

The screenshot displays the Cisco RoomOS configuration interface for Dynamic Channel Assignment (DCA). The breadcrumb navigation shows the path: 802.11b > RRM > Dynamic Channel Assignment (DCA). The left sidebar contains a navigation menu with categories like Access Points, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, and 802.11a/n/ac/ax. The main content area is titled 'Dynamic Channel Assignment Algorithm' and includes the following settings:

- Channel Assignment Method: Automatic, Freeze, OFF
- Interval: 10 minutes, AnchorTime: 0
- Invoke Channel Update Once: [Button]
- Avoid Foreign AP interference: Enabled
- Avoid Cisco AP load: Enabled
- Avoid non-802.11b noise: Enabled
- Avoid Persistent Non-WiFi Interference: Enabled
- Channel Assignment Leader: RTP9-32A-WLC3 (10.81.6.70)
- Last Auto Channel Assignment: 75 secs ago
- DCA Channel Sensitivity: Medium (10 dB)

Below the settings is a 'DCA Channel List' section with a text area containing the channels: 1, 6, 11.

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 or 802.11ax 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.

802.11a/n/ac/ax Cisco APs > Configure

General

AP Name: rtp9-31a-ap1
 Admin Status:
 Operational Status: UP
 Slot #: 1

11n Parameters

11n Supported: Yes

CleanAir

CleanAir Capable: Yes
 CleanAir Admin Status:
** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections: 0

Antenna Parameters

Antenna Type:
 A
 B
 C
 D

RF Channel Assignment

Current Channel: (48,44)
 Channel Width:
** Channel width can be configured only when channel configuration is in custom mode*
 Assignment Method: Global
 Custom

Radar Information

Channel	Last Heard (Secs)
No radar detected channels	

Tx Power Level Assignment

Current Tx Power Level: 1
 Assignment Method: Global
 Custom

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Client Roaming

The Cisco RoomOS Series does 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 device 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/ax Access Points.

802.11a/n/ac/ax Cisco APs > Configure

General

EDCA Profile:
 Enable Low Latency MAC:

Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled.

DFS (802.11h)

Power Constraint should be left un-configured or set to 0 dB.

Cisco RoomOS Series Wireless LAN Deployment Guide

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

The screenshot shows the Cisco RoomOS configuration interface for Wireless LANs. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS (selected), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the 'Wireless' menu with options like Access Points, Radios, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, and FlexConnect ACLs. The main content area is titled '802.11h Global Parameters' and contains three sections: 'Power Constraint' with a 'Local Power Constraint(0-30)' field set to 0 dB; 'Channel Switch Announcement' with 'Channel Announcement' checked, 'Channel Switch Count' set to 0, and 'Channel Quiet Mode' checked; and 'Radar Blacklist' with 'Smart DFS' checked.

High Throughput (802.11n/ac/ax)

The 802.11n and 802.11ax 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 **WPA3 (AES)** or **WPA2(AES)** is configured in order to utilize 802.11n/ac/ax data rates.

The Cisco RoomOS Series supports HT MCS 0 – MCS 15 and VHT MCS 0 – MCS 9 1SS and 2SS data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n/ac/ax 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 RoomOS Series.

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 RoomOS Series 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.

The screenshot shows the Cisco RoomOS configuration page for CleanAir. The left sidebar contains a navigation menu with categories like Access Points, 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, and QoS. The main content area is titled '802.11a > CleanAir' and is divided into several sections:

- CleanAir/Spectrum Intelligence Parameters:**
 - CleanAir: Enabled
 - Spectrum Intelligence³: Enabled
 - Report Interferers¹: Enabled
 - Persistent Device Propagation: Enabled
- Interferences to Ignore:** Canopy, WiMax Fixed, SI_FHSS
- Interferences to Detect:** TDD Transmitter, Jammer, Continuous Transmitter, DECT-like Phone, Video Camera
- Trap Configurations:**
 - Enable AQI(Air Quality Index) Trap: Enabled
 - AQI Alarm Threshold (1 to 100)²: 35
 - Enable trap for Unclassified Interferences: Enabled
 - Threshold for Unclassified category trap (1 to 99): 20
 - Enable trap for Classified Interferences: Enabled
 - Threshold for Classified category trap (1 to 99): 0
 - Enable Interference For Security Alarm: Enabled
- Do not trap on these types:** TDD Transmitter, Continuous Transmitter, DECT-like Phone, Video Camera, SuperAG
- Trap on these types:** Jammer, WiFi Inverted, WiFi Invalid Channel
- Event Driven RRM (Change Settings):**
 - EDRRM: Disabled
 - Sensitivity Threshold: N/A
 - Rogue Contribution: N/A
 - Rogue Duty-Cycle: N/A

Footnotes at the bottom of the page:

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

802.11a/n/ac/ax Cisco APs > Configure

General

AP Name: rtp9-31a-ap1
 Admin Status: Enable
 Operational Status: UP
 Slot #: 1

11n Parameters

11n Supported: Yes

CleanAir

CleanAir Capable: Yes
 CleanAir Admin Status: Enable
 * CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections: 0

Antenna Parameters

Antenna Type: Internal
 Antenna: A, B, C, D (all checked)

RF Channel Assignment

Current Channel: (48,44)
 Channel Width: 40 MHz
 * Channel width can be configured only when channel configuration is in custom mode
 Assignment Method: Global

Radar Information

Channel: Last Heard (Secs)
 No radar detected channels

Tx Power Level Assignment

Current Tx Power Level: 1
 Assignment Method: Global

Performance Profile

View and edit Performance Profile for this AP
 Performance Profile

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Rx Sop Threshold

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

Rx Sop Threshold

Rx Sop Threshold 802.11a: Default (0) Custom
 Rx Sop Threshold 802.11b: Default (0) Custom

1 Rxsop only supported in Local, Flex, Bridge and Flex+Bridge mode Aps.

WLAN Settings

It is recommended to have a separate SSID for the Cisco RoomOS Series.

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 RoomOS Series can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

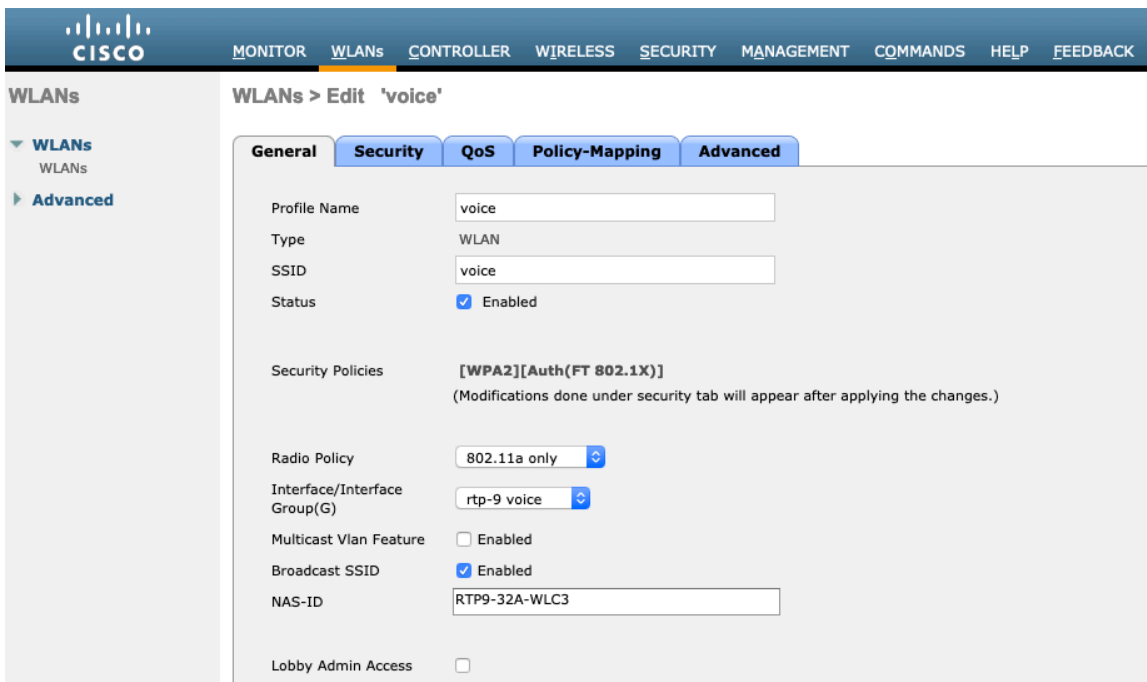
It is recommended to have the Cisco RoomOS Series operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

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.



The screenshot shows the 'WLANs > New' configuration page in the Cisco RoomOS interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > New' and contains the following fields:

Type	WLAN
Profile Name	voice
SSID	voice
ID	6



The screenshot shows the 'WLANs > Edit 'voice'' configuration page in the Cisco RoomOS interface. The top navigation bar is the same as the previous page. The left sidebar is also the same. The main content area is titled 'WLANs > Edit 'voice'' and has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is selected, showing the following configuration details:

Profile Name	voice
Type	WLAN
SSID	voice
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(FT 802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	802.11a only
Interface/Interface Group(G)	rtp-9 voice
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	RTP9-32A-WLC3
Lobby Admin Access	<input type="checkbox"/>

Protected Management Frame can be set to **Optional**, **Required**, or **Disabled**.

Enable WPA2 policy with AES encryption then 802.1x-SHA2, 802.1x-SHA1 or PSK for authenticated key management type depending on whether 802.1x or PSK is to be utilized.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security ⁶ WPA+WPA2

Security Type Enterprise

MAC Filtering ²

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

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

Protected Management Frame

PMF Disabled

Authentication Key Management ¹²

802.1X-SHA1 Enable

802.1X-SHA2 Enable

FT 802.1X Enable

CCKM Enable

WPA GTK-randomize State ¹⁴ Disable

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'voice'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security ⁶ WPA+WPA2

Security Type Personal

MAC Filtering ²

AutoConfig IPSK Enable

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

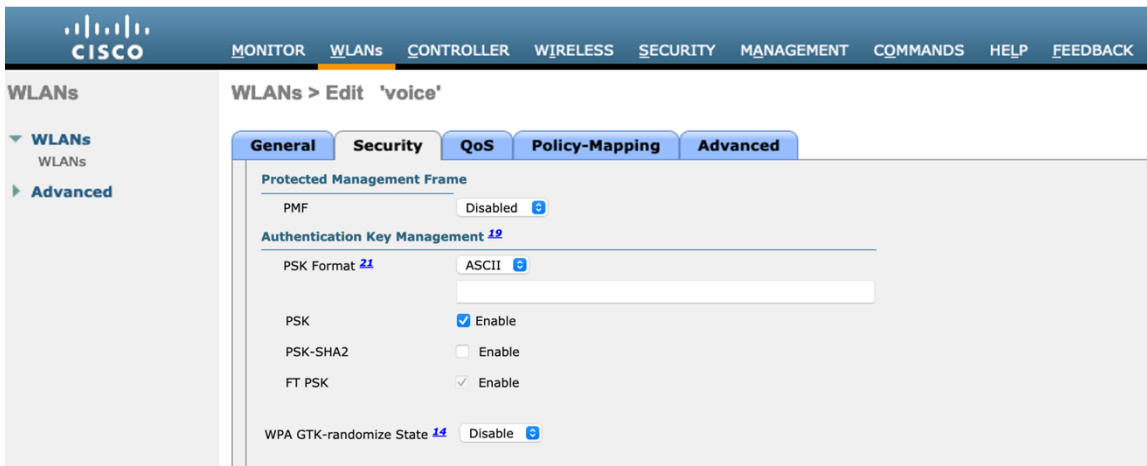
WPA2 Encryption CCMP128(AES) TKIP

Fast Transition

Fast Transition Enable

Over the DS

Reassociation Timeout 20 Seconds



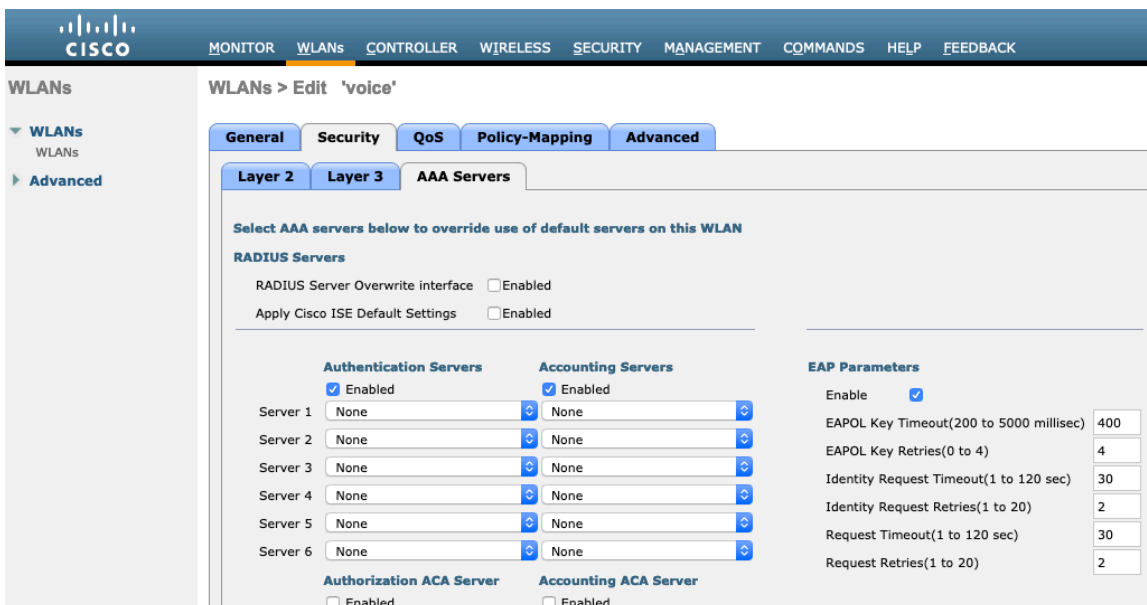
802.11r (FT), CCKM and/or PSK may also be enabled if wanting to utilize the same SSID for various type of voice clients, depending on whether 802.1x or PSK is being utilized.

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.

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

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

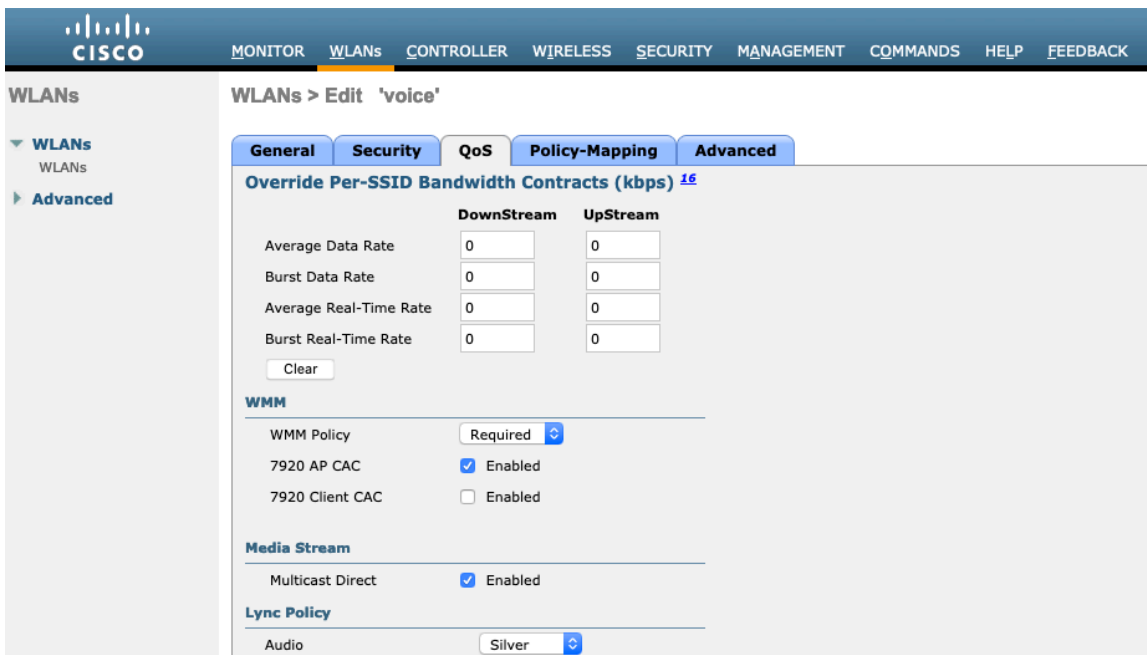
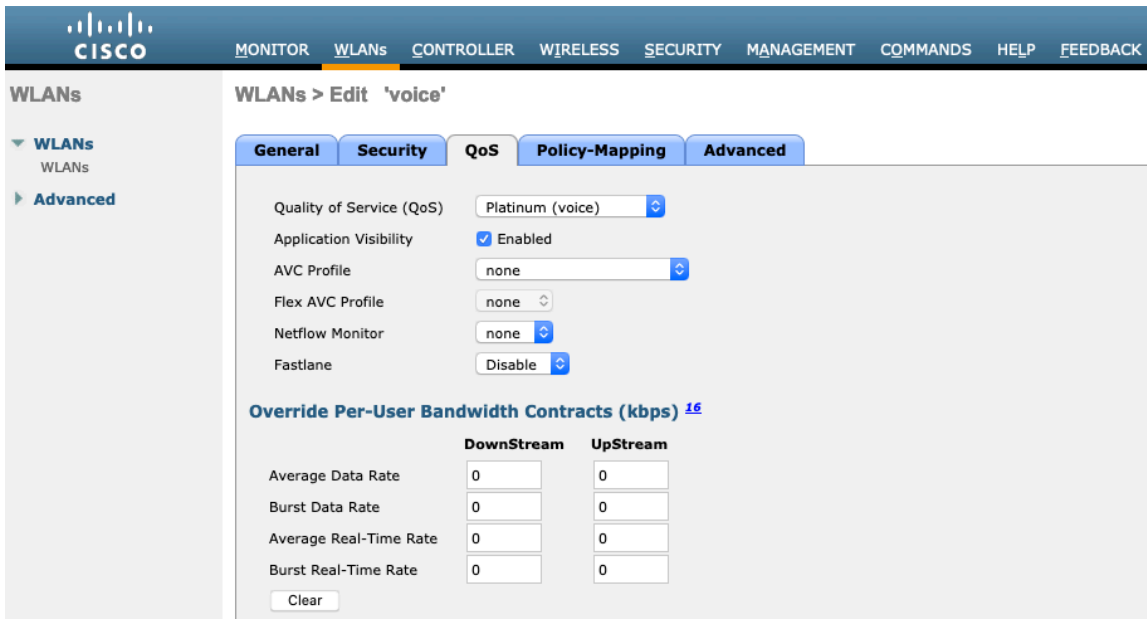


The WMM policy should be set to **Required** only if the Cisco RoomOS Series or other WMM enabled phones will be using this SSID.

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 RoomOS Series, then ensure the WMM policy is set to **Allowed**.

Enabling WMM will enable the 802.11e version of QoS.



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

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

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

Configure **Client Exclusion** as necessary.

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

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

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

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

DHCP Address Assignment Required should be disabled.

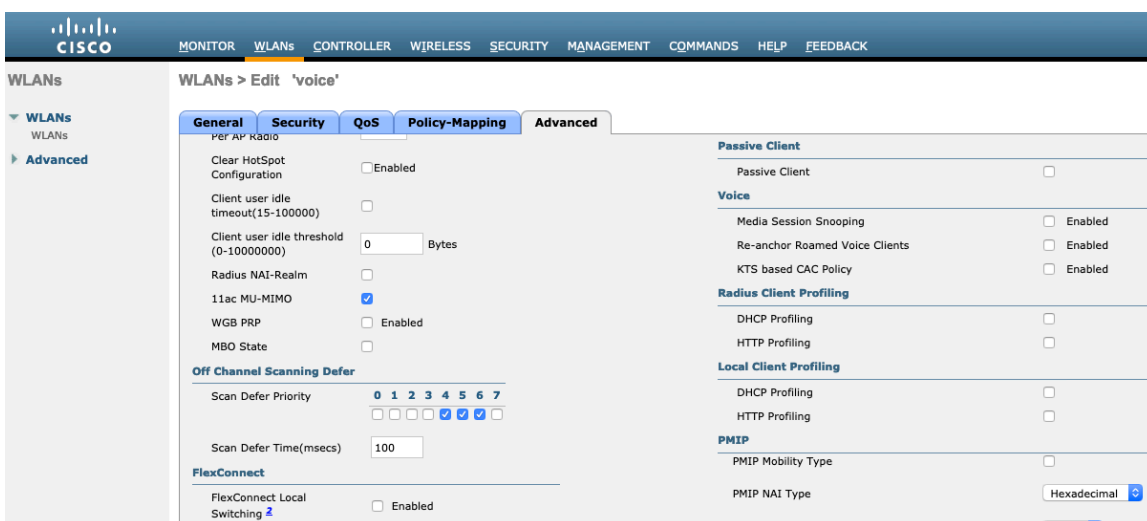
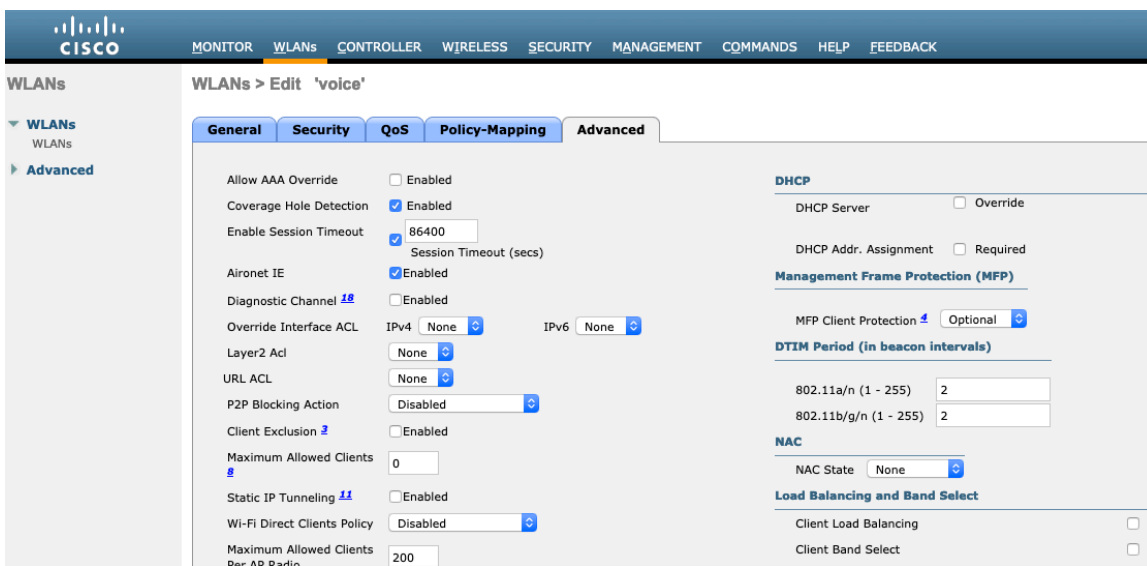
Management Frame Protection can be set to **Optional**, **Required**, or **Disabled**.

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.



WLANs > Edit 'voice'

General | Security | QoS | Policy-Mapping | **Advanced**

- FlexConnect Local Auth [?](#) Enabled
- Learn Client IP Address [?](#) Enabled
- Vlan based Central Switching [?](#) Enabled
- Central DHCP Processing Enabled
- Override DNS Enabled
- NAT-PAT Enabled
- Central Assoc Enabled

Lync

- Lync Server Disabled

11k

- Neighbor List Enabled
- Neighbor List Dual Band Enabled
- Assisted Roaming Prediction Optimization Enabled

802.11ax BSS Configuration

- Down Link MU-MIMO Enabled

PMIP Profile

PMIP Realm

Universal AP Admin Support

- Universal AP Admin

11v BSS Transition Support

- BSS Transition
- Disassociation Imminent
- Disassociation Timer(0 to 3000 TBTT)
- Optimized Roaming Disassociation Timer(0 to 40 TBTT)
- BSS Max Idle Service
- Directed Multicast Service

Tunneling

- Tunnel Profile
- EOGRE Vlan Override

mDNS

- mDNS Snooping Enabled

WLANs > Edit 'voice'

General | **Security** | QoS | Policy-Mapping | **Advanced**

802.11ax BSS Configuration

- Down Link MU-MIMO Enabled
- Up Link MU-MIMO Enabled
- Down Link OFDMA Enabled
- Up Link OFDMA Enabled

mDNS

- mDNS Snooping Enabled

TrustSec

- Security Group Tag

Umbrella

- Umbrella Mode
- Umbrella Profile
- Umbrella DHCP Override

Fabric Configuration

- Fabric Enabled

Mobility

- Selective Reanchor Enabled

U3 Interface

- U3 Interface Enabled
- U3 Reporting Interval

AP Groups

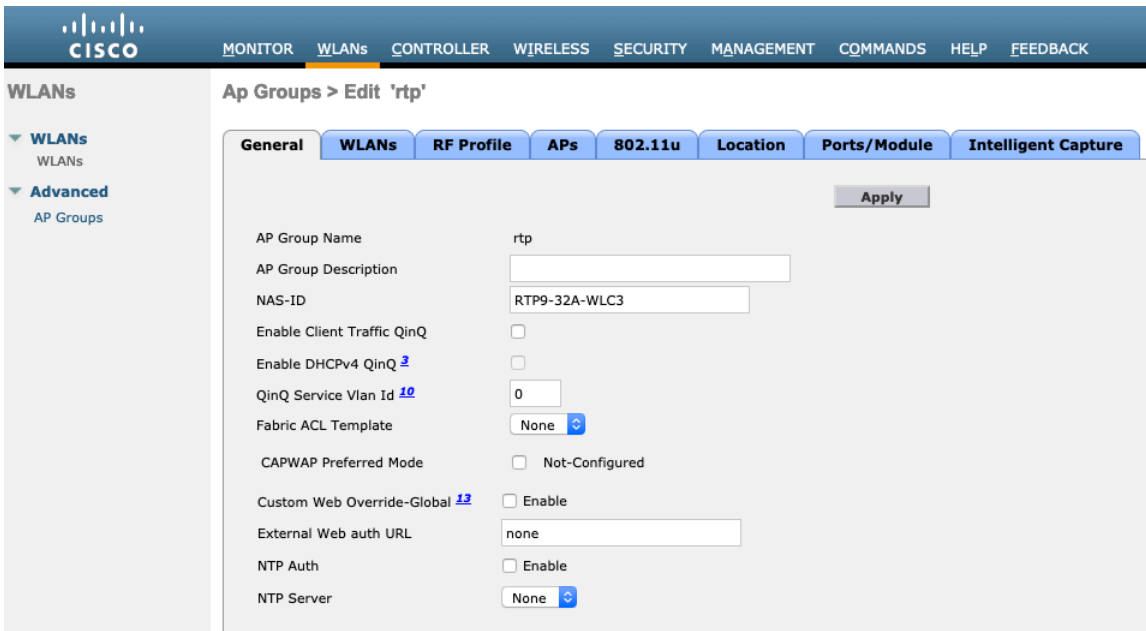
AP Groups can be created to specify which WLANs / SSIDs are to be enabled and which interface they should be mapped to as well as what RF Profile parameters should be used for the access points assigned to the AP Group.

WLANs > AP Groups

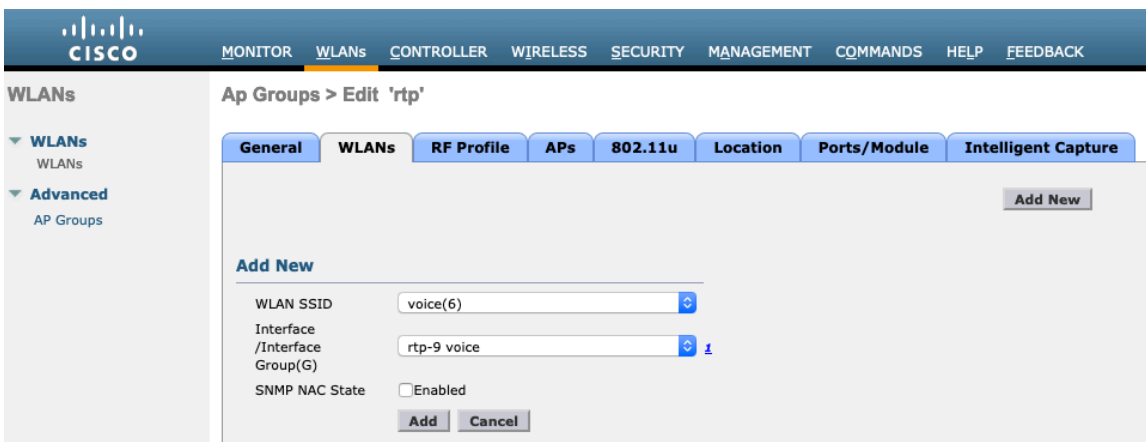
Add New AP Group

AP Group Name

Description

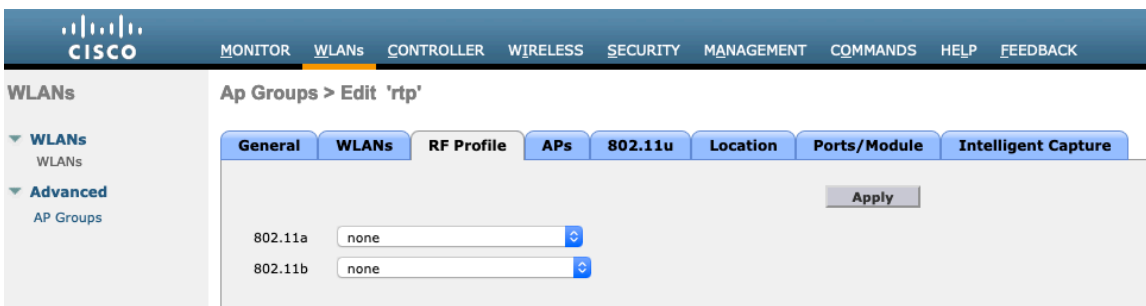


On the **WLANs** tab, select the desired SSIDs and interfaces to map to then select **Add**.



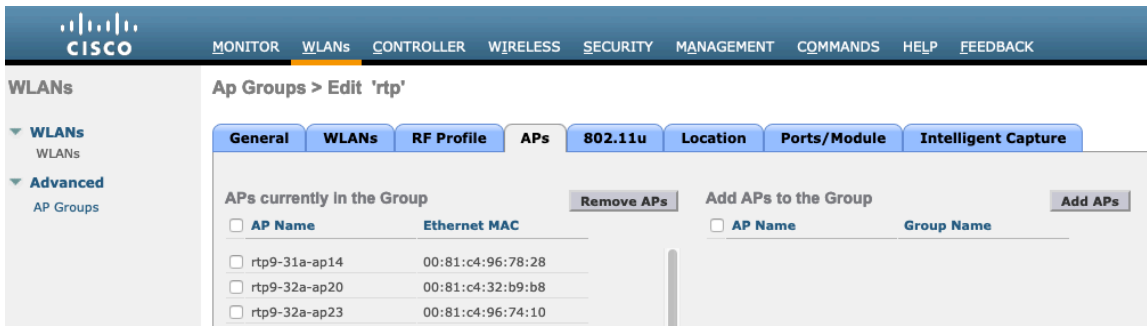
On the **RF Profile** tab, select the desired 802.11a or 802.11b RF Profile, then select **Apply**.

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.

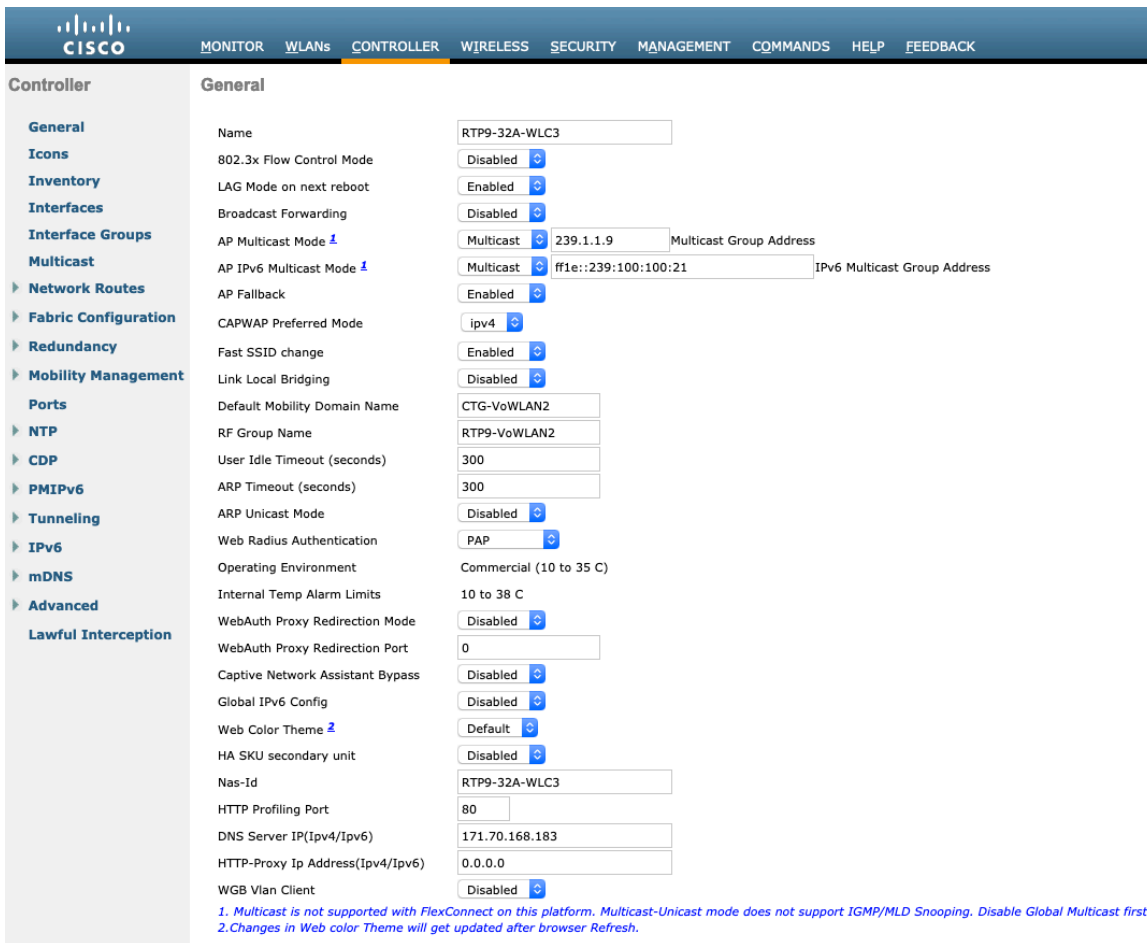


Controller Settings

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.

The screenshot shows the Cisco RoomOS Controller configuration page for Multicast settings. The navigation bar includes MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar lists various configuration categories, with Multicast selected. The main content area shows the following settings:

Setting	Value
Enable Global Multicast Mode	<input checked="" type="checkbox"/>
Enable IGMP Snooping	<input checked="" type="checkbox"/>
IGMP Timeout (30-7200 seconds)	60
IGMP Query Interval (15-2400 seconds)	20
Enable MLD Snooping	<input type="checkbox"/>
MLD Timeout (30-7200 seconds)	60
MLD Query Interval (15-2400 seconds)	20

Foot Notes:
[Changing Global Multicast configuration parameters removes configured Multicast VLAN from WLAN.](#)

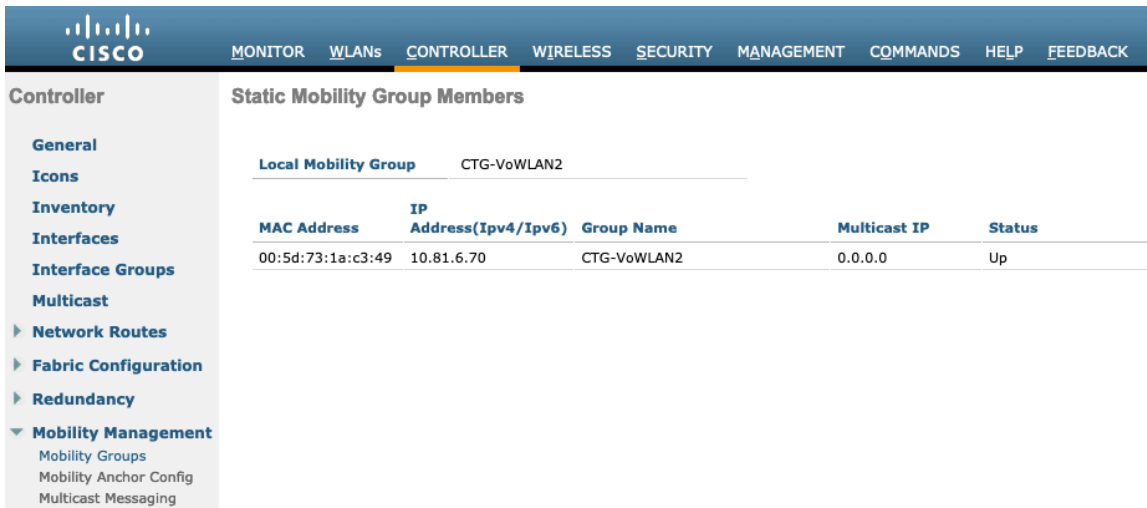
If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling** should be **Enabled**.

In the recent versions, Symmetric Mobility Tunneling is enabled by default and non-configurable.

The screenshot shows the Cisco RoomOS Controller configuration page for Mobility Anchor Config settings. The navigation bar includes MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar lists various configuration categories, with Mobility Management selected and Mobility Anchor Config chosen. The main content area shows the following settings:

Setting	Value
Keep Alive Count	3
Keep Alive Interval (1-30 seconds)	10
Symmetric Mobility Tunneling mode	Enabled
DSCP Value	0

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.



The screenshot shows the Cisco Controller web interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER (highlighted), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows a navigation menu with categories like General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, and Mobility Management. The main content area is titled 'Static Mobility Group Members' and shows a table for the 'Local Mobility Group' 'CTG-VoWLAN2'.

Local Mobility Group				
CTG-VoWLAN2				
MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
00:5d:73:1a:c3:49	10.81.6.70	CTG-VoWLAN2	0.0.0.0	Up

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.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
- Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
 - Network
 - RRM
 - RF Grouping
 - TPC
 - DCA
 - Coverage
 - General
 - Client Roaming
 - Media
 - EDCA Parameters
 - DFS (802.11h)
 - High Throughput (802.11n/ac/ax)
 - CleanAir
- 802.11b/g/n/ax

802.11a(5 GHz) > Media

Voice Video **Media**

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method ⁴ Load Based

Max RF Bandwidth (5-85)(%) 75

Reserved Roaming Bandwidth (0-25)(%) 6

Expedited bandwidth

SIP CAC Support ³ Enabled

Per-Call SIP Bandwidth ²

SIP Codec G.711

SIP Bandwidth (kbps) 64

SIP Voice Sample Interval (msecs) 20

Traffic Stream Metrics

Metrics Collection

Foot Notes

¹ 11a rates(Kbps): 6000,9000,12000,18000,24000,36000,48000,54000
¹¹ⁿ rates(Kbps): 65000,72200,130000,144400,135000,150000,270000,300000
² SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
³ SIP CAC will be supported only if SIP snooping is enabled.
⁴ Static CAC method is radio based and load-based CAC method is channel based.

Admission Control Mandatory for Video should be disabled.

802.11a(5 GHz) > Media

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method [4](#) Static

Max RF Bandwidth (5-85)(%)

Reserved Roaming Bandwidth (0-25)(%)

SIP CAC Support [3](#) Enabled

Foot Notes

1 11a rates(Kbps): 6000,9000,12000,18000,24000,36000,48000,54000
 11n rates(Kbps): 65000,72200,130000,144400,135000,150000,270000,300000
 2 SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
 3 SIP CAC will be supported only if SIP snooping is enabled.
 4 Static CAC method is radio based and load-based CAC method is channel based.

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.

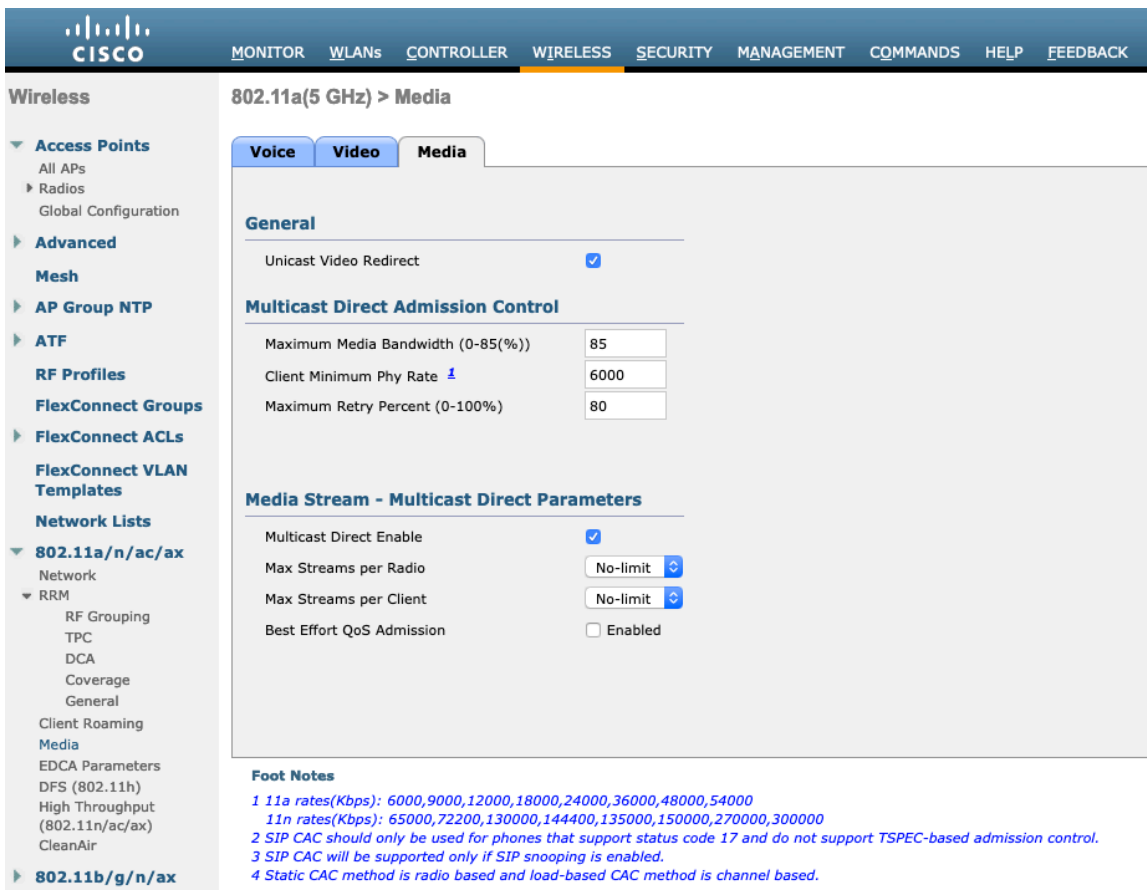
```
(Cisco Controller) >show wlan <WLAN id>
```

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

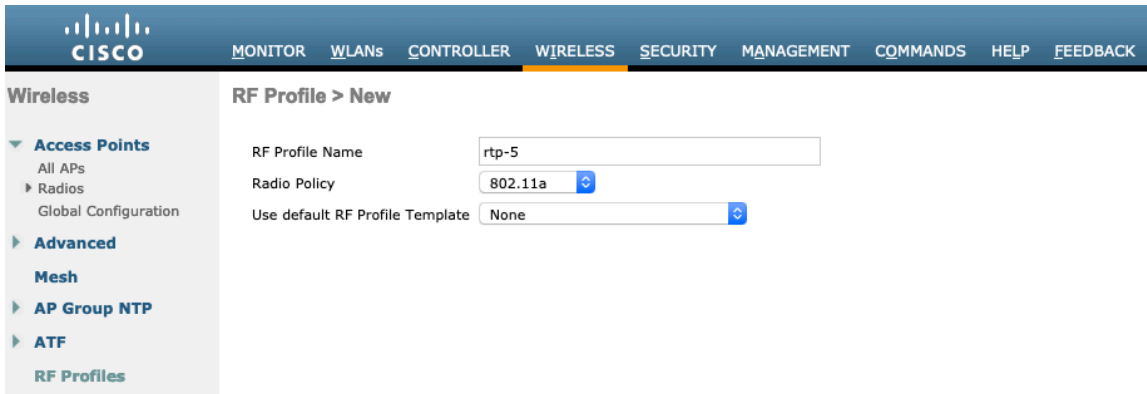
In the Media settings, **Unicast Video Redirect** and **Multicast Direct Enable** should be enabled.



RF Profiles

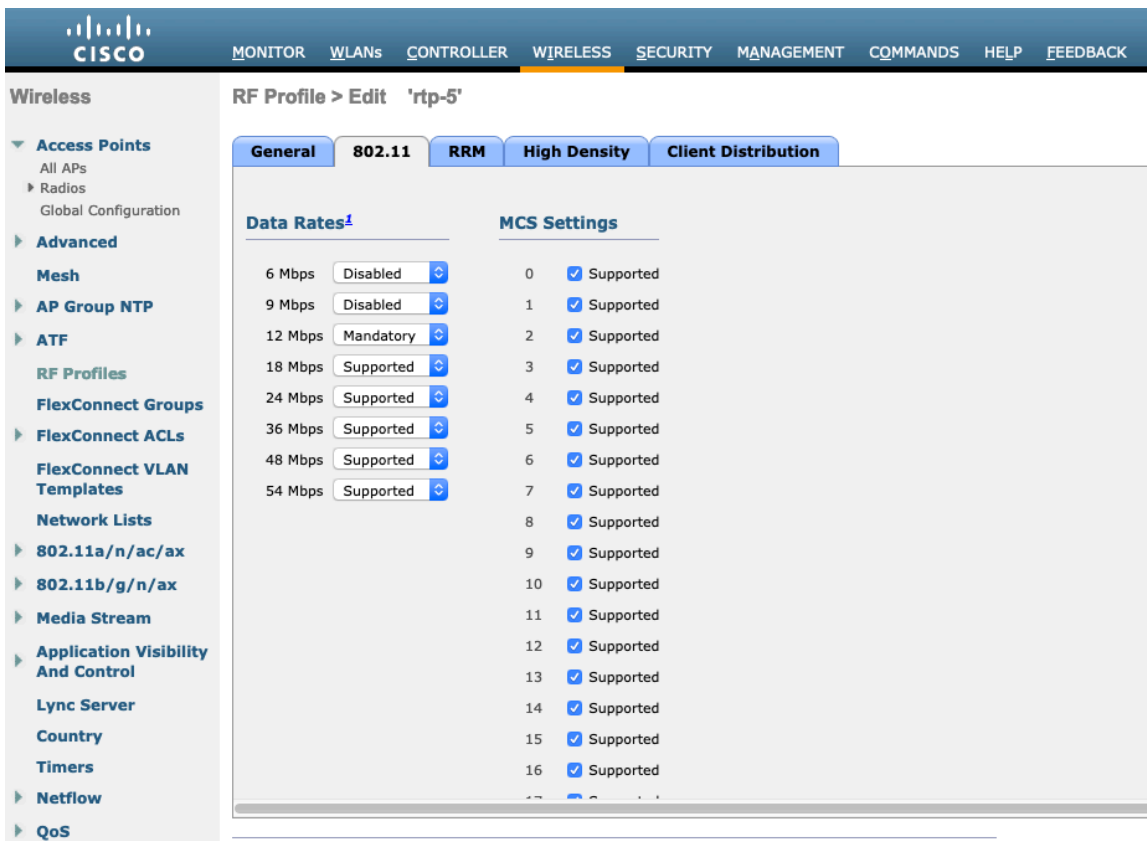
RF Profiles can be created to specify which frequency bands, data rates, RRM settings, etc. a group of access points should use. It is recommended to have the SSID used by the Cisco RoomOS Series to be applied to 5 GHz radios only. RF Profiles are applied to an AP group once created.

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.

RF Profile > Edit 'rtp-5'

General 802.11 RRM High Density Client Distribution

TPC

Maximum Power Level Assignment (-10 to 30 dBm) 30
 Minimum Power Level Assignment (-10 to 30 dBm) -10
 Power Threshold v1(-80 to -50 dBm) -70
 Power Threshold v2(-80 to -50 dBm) -67

Coverage Hole Detection

Data RSSI(-90 to -60 dBm) -80
 Voice RSSI(-90 to -60 dBm) -80
 Coverage Exception(0 to 100 %) 25
 Coverage Level(1 to 200 Clients) 3

DCA

Avoid Foreign AP Interference Enabled
 Channel Width 20 MHz 40 MHz 80 MHz 160 MHz 80+80 MHz Best

Profile Threshold For Traps

Interference (0 to 100%) 10
 Clients (1 to 200) 12
 Noise (-127 to 0 dBm) -70
 Utilization (0 to 100 %) 80

Client Network Preference

Connectivity Throughput Automatic

Client Aware

Enable Disable

High-Speed Roam

HSR mode Enabled

RF Profile > Edit 'rtp-5'

General 802.11 RRM High Density Client Distribution

Client Aware

Enable Disable

High-Speed Roam

HSR mode Enabled
 Neighbor Timeout Factor 5

DCA Channel List

DCA Channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Select	Channel
<input checked="" type="checkbox"/>	36
<input checked="" type="checkbox"/>	40
<input checked="" type="checkbox"/>	44
<input checked="" type="checkbox"/>	48
<input checked="" type="checkbox"/>	52
<input type="checkbox"/>	56
<input type="checkbox"/>	60
<input type="checkbox"/>	64
<input type="checkbox"/>	149
<input type="checkbox"/>	153
<input type="checkbox"/>	157
<input type="checkbox"/>	161

Extended UNII-2 channels Enabled

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**.

RF Profile > Edit 'rtp-5'

General 802.11 RRM High Density Client Distribution

High Density Parameters

Maximum Clients(1 to 200) 200

Multicast Parameters

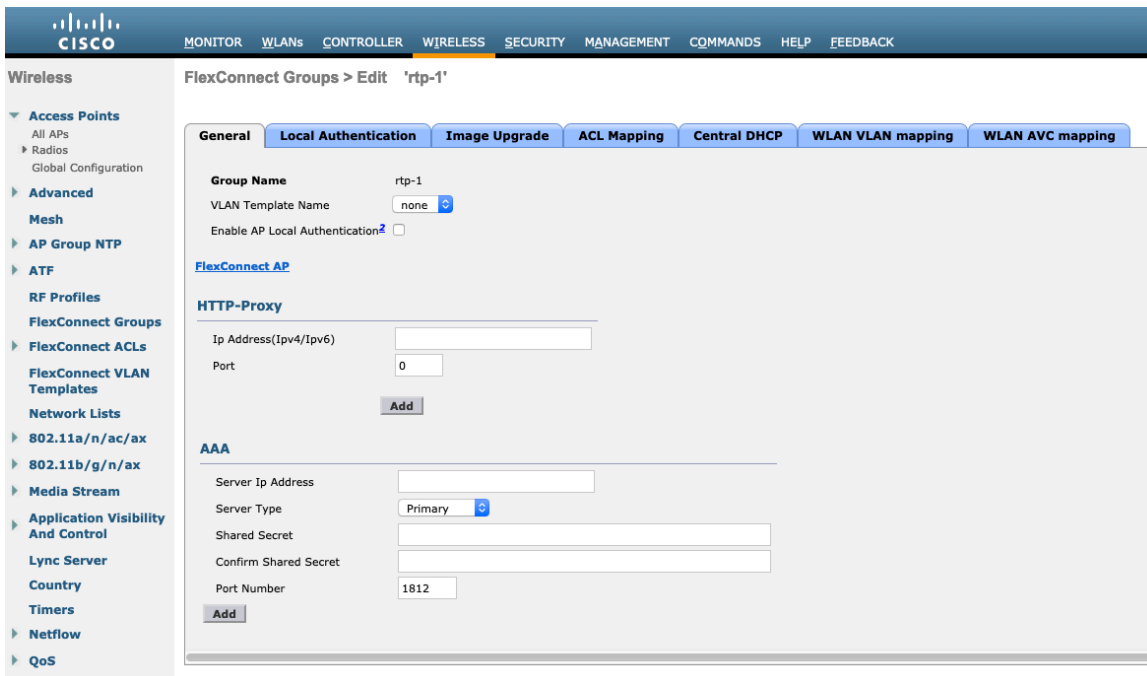
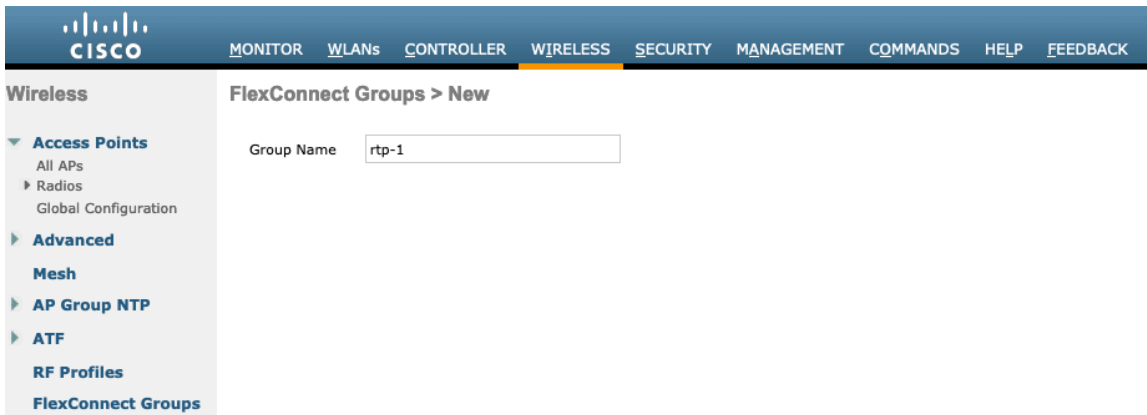
Multicast Data Rates² auto

Rx Sop Threshold Parameters⁵

Rx Sop Threshold⁶ Default 0 Custom

FlexConnect Groups

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



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



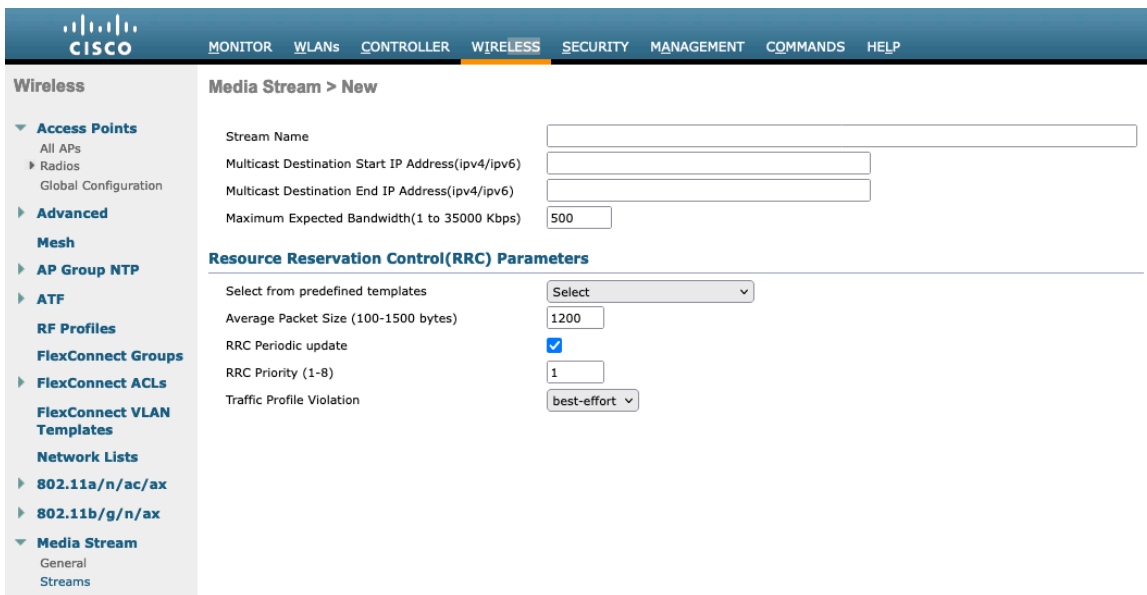
The screenshot shows the Cisco RoomOS configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, the 'Wireless' menu is expanded to show 'FlexConnect Groups'. The main content area is titled 'FlexConnect Group AP List' and shows a table with one entry: 'Group Name' is 'rtp-1'. Below this is the 'FlexConnect APs' section, which includes an 'Add AP' form. The form has a checkbox for 'Select APs from current controller' (unchecked), an input field for 'Ethernet MAC', and 'Add' and 'Cancel' buttons.

Multicast Direct

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

The screenshot shows the Cisco RoomOS configuration interface for 'Media Stream > General'. The top navigation bar is the same as in the previous screenshot. The left sidebar shows the 'Media Stream' menu expanded to 'General'. The main content area shows the 'Multicast Direct feature' is checked and set to 'Enabled'. Below this is the 'Session Message Config' section, which includes: 'Session announcement State' (unchecked), 'Session announcement URL' (input field), 'Session announcement Email' (input field), 'Session announcement Phone' (input field), and 'Session announcement Note' (text area).

Then configure the media streams as necessary.



Media Stream > New

Stream Name

Multicast Destination Start IP Address(ipv4/ipv6)

Multicast Destination End IP Address(ipv4/ipv6)

Maximum Expected Bandwidth(1 to 35000 Kbps)

Resource Reservation Control(RRC) Parameters

Select from predefined templates

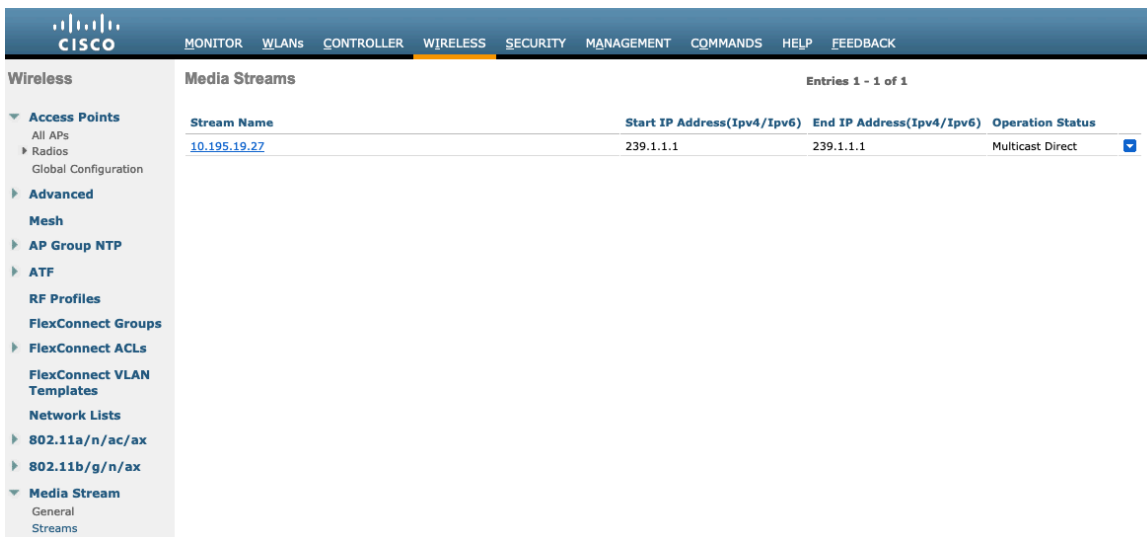
Average Packet Size (100-1500 bytes)

RRC Periodic update

RRC Priority (1-8)

Traffic Profile Violation

Once saved, then the media stream will be displayed.



Media Streams Entries 1 - 1 of 1

Stream Name	Start IP Address(Ipv4/Ipv6)	End IP Address(Ipv4/Ipv6)	Operation Status
10.195.19.27	239.1.1.1	239.1.1.1	Multicast Direct <input checked="" type="checkbox"/>

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

The screenshot shows the Cisco RoomOS configuration page for a WLAN named 'voice'. The 'QoS' tab is selected, showing bandwidth contract override settings. The 'WMM' section has 'WMM Policy' set to 'Required', '7920 AP CAC' checked, and '7920 Client CAC' unchecked. 'Media Stream' has 'Multicast Direct' checked. 'Lync Policy' has 'Audio' set to 'Silver'.

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

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

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLAN QoS Parameters

Maximum Priority	<input type="text" value="voice"/>
Unicast Default Priority	<input type="text" value="besteffort"/>
Multicast Default Priority	<input type="text" value="besteffort"/>

Wired QoS Protocol

Protocol Type

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

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLAN QoS Parameters

Maximum Priority	<input type="text" value="video"/>
Unicast Default Priority	<input type="text" value="video"/>
Multicast Default Priority	<input type="text" value="video"/>

Wired QoS Protocol

Protocol Type	<input type="text" value="802.1p"/>
802.1p Tag	<input type="text" value="4"/>



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	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority	background
Unicast Default Priority	background
Multicast Default Priority	background

Wired QoS Protocol

Protocol Type	802.1p
802.1p Tag	1

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 silver

Description For Best Effort

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority ▾

Unicast Default Priority ▾

Multicast Default Priority ▾

Wired QoS Protocol

Protocol Type ▾

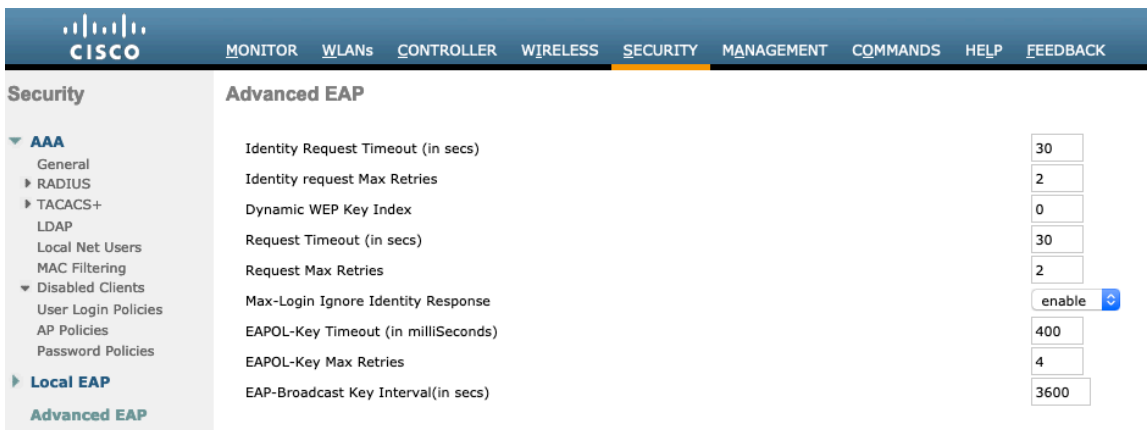
802.1p Tag

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 bcst-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
```

Rogue Policies

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

The screenshot shows the Cisco Catalyst IOS XE configuration interface for Security > Rogue Policies. The interface is divided into two main sections: 'Rogue Policies' and 'Auto Contain'.

Rogue Policies Section:

- Rogue Detection Security Level:** Radio buttons for Low, High, Critical, and Custom (selected).
- Rogue Location Discovery Protocol:** A dropdown menu set to 'Disable'.
- Expiration Timeout for Rogue AP and Rogue Client entries:** A text input field set to '1200' with the unit 'Seconds'.
- Validate rogue clients against AAA:** A checkbox labeled 'Enabled'.
- Validate rogue AP against AAA:** A checkbox labeled 'Enabled'.
- Polling Interval:** A text input field set to '0' with the unit 'Seconds'.
- Validate rogue clients against MSE:** A checkbox labeled 'Enabled'.
- Detect and report Ad-Hoc Networks:** A checked checkbox labeled 'Enabled'.
- Rogue Detection Report Interval (10 to 300 Sec):** A text input field set to '10'.
- Rogue Detection Minimum RSSI (-70 to -128):** A text input field set to '-90'.
- Rogue Detection Transient Interval (0, 120 to 1800 Sec):** A text input field set to '0'.
- Rogue Client Threshold (0 to disable, 1 to 256):** A text input field set to '0'.
- Rogue containment automatic rate selection:** A checkbox labeled 'Enabled'.

Auto Contain Section:

- Auto Containment Level:** A dropdown menu set to '1'.
- Auto Containment only for Monitor mode APs:** A checkbox labeled 'Enabled'.
- Auto Containment on FlexConnect Standalone:** A checkbox labeled 'Enabled'.
- Rogue on Wire:** A checkbox labeled 'Enabled'.
- Using our SSID:** A checkbox labeled 'Enabled'.
- Valid client on Rogue AP:** A checkbox labeled 'Enabled'.
- AdHoc Rogue AP:** A checkbox labeled 'Enabled'.

Left Navigation Menu:

- Security
 - AAA
 - General
 - RADIUS
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
 - Local EAP
 - Advanced EAP
 - Priority Order
 - Certificate
 - Access Control Lists
 - Wireless Protection Policies
 - Rogue Policies
 - General
 - Rogue Rules
 - Friendly Rogue
 - Standard Signatures
 - Custom Signatures
 - Signature Events
 - Summary
 - Client Exclusion Policies
 - AP Authentication
 - Management Frame Protection
 - Web Auth
 - TrustSec
 - Local Policies
 - Umbrella
 - Advanced

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)** and **CCKM** are not configured as mandatory
- 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**
- Disable **P2P (Peer to Peer) Blocking Action**
- Ensure **Client Exclusion Timeout** is configured correctly
- Disable **DHCP Required**
- Set **Protected Management Frame (PMF)** to **Optional, Required, 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 **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**

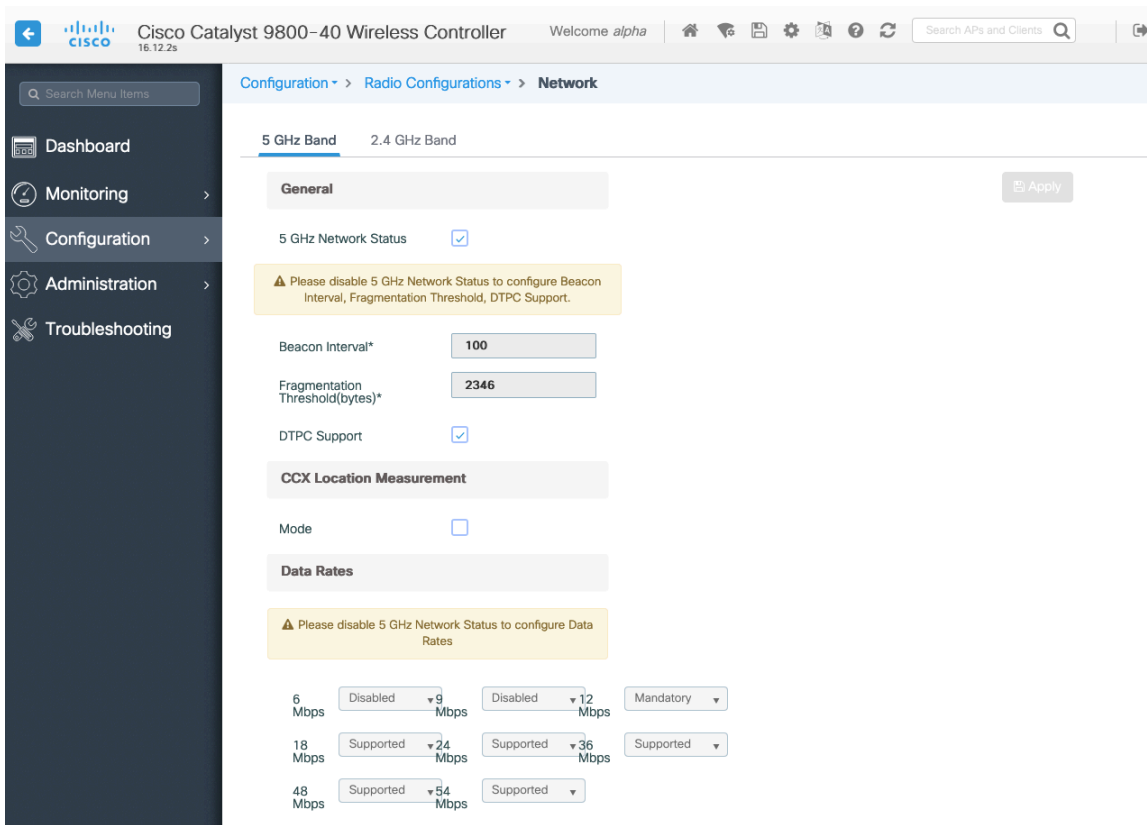
802.11 Network Settings

It is recommended to have the Cisco RoomOS Series 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**.

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.



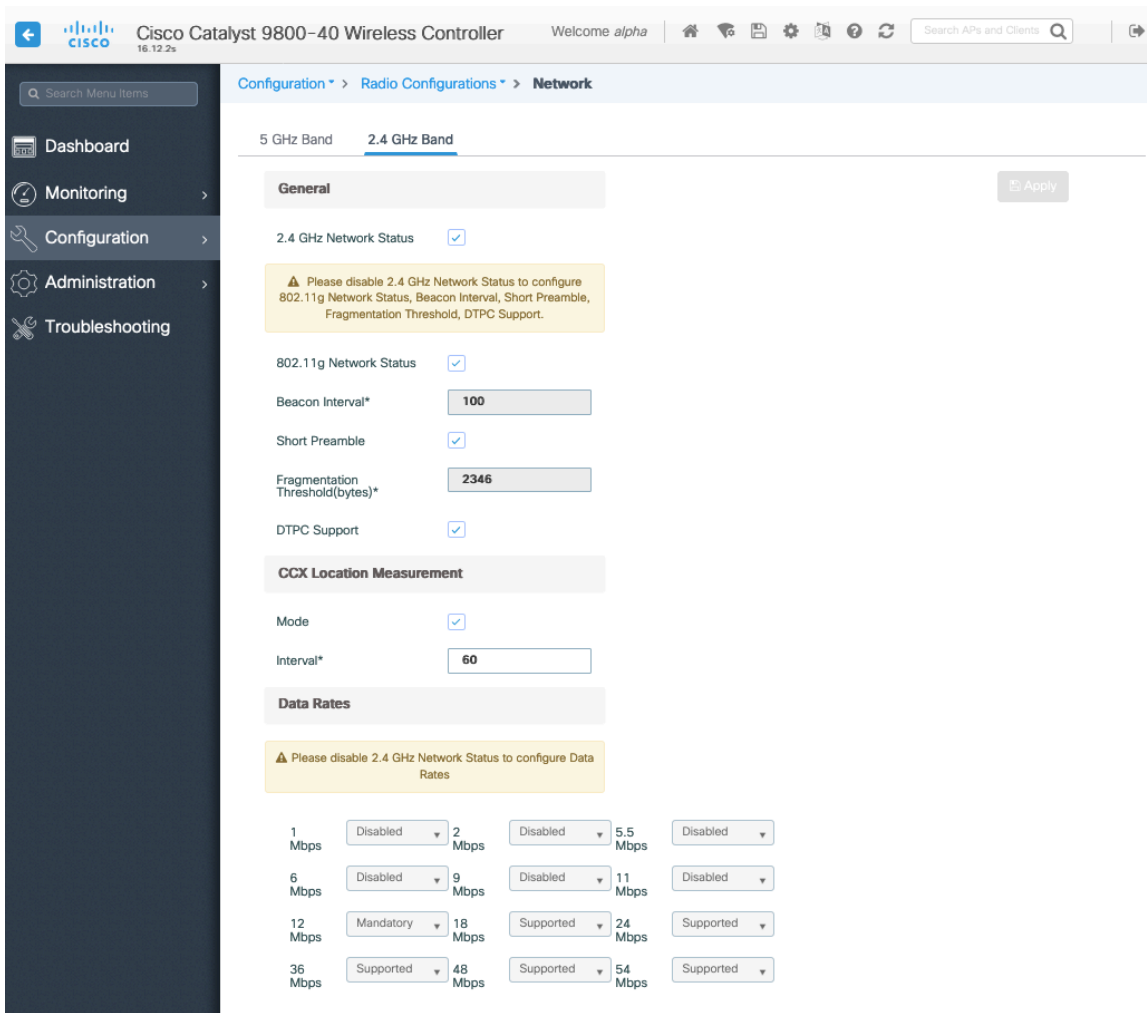
If wanting to use 2.4 GHz, ensure the 2.4 GHz network status and 802.11g network status are **Enabled**.

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.

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/ax)

The 802.11n and 802.11ax 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 **WPA3 (AES)** or **WPA2(AES)** is configured in order to utilize 802.11n/ac/ax data rates.

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

Cisco Catalyst 9800-40 Wireless Controller Welcome alpha

Configuration > Radio Configurations > High Throughput

5 GHz Band 2.4 GHz Band

Apply

11n

Enable 11n Select All

MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)
<input checked="" type="checkbox"/> 0/(7Mbps)	<input checked="" type="checkbox"/> 1/(14Mbps)	<input checked="" type="checkbox"/> 2/(21Mbps)	<input checked="" type="checkbox"/> 3/(29Mbps)
<input checked="" type="checkbox"/> 4/(43Mbps)	<input checked="" type="checkbox"/> 5/(58Mbps)	<input checked="" type="checkbox"/> 6/(65Mbps)	<input checked="" type="checkbox"/> 7/(72Mbps)
<input checked="" type="checkbox"/> 8/(14Mbps)	<input checked="" type="checkbox"/> 9/(29Mbps)	<input checked="" type="checkbox"/> 10/(43Mbps)	<input checked="" type="checkbox"/> 11/(58Mbps)
<input checked="" type="checkbox"/> 12/(87Mbps)	<input checked="" type="checkbox"/> 13/(116Mbps)	<input checked="" type="checkbox"/> 14/(130Mbps)	<input checked="" type="checkbox"/> 15/(144Mbps)
<input checked="" type="checkbox"/> 16/(22Mbps)	<input checked="" type="checkbox"/> 17/(43Mbps)	<input checked="" type="checkbox"/> 18/(65Mbps)	<input checked="" type="checkbox"/> 19/(87Mbps)
<input checked="" type="checkbox"/> 20/(130Mbps)	<input checked="" type="checkbox"/> 21/(173Mbps)	<input checked="" type="checkbox"/> 22/(195Mbps)	<input checked="" type="checkbox"/> 23/(217Mbps)
<input checked="" type="checkbox"/> 24/(29Mbps)	<input checked="" type="checkbox"/> 25/(58Mbps)	<input checked="" type="checkbox"/> 26/(87Mbps)	<input checked="" type="checkbox"/> 27/(116Mbps)
<input checked="" type="checkbox"/> 28/(173Mbps)	<input checked="" type="checkbox"/> 29/(231Mbps)	<input checked="" type="checkbox"/> 30/(260Mbps)	<input checked="" type="checkbox"/> 31/(289Mbps)

11ac

⚠ The Data rates are for 20MHz channels and Short Guard Interval

Enable 11ac Select All

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/8/(86.7Mbps)	<input checked="" type="checkbox"/> 1/9/(n/a)	<input checked="" type="checkbox"/> 2/8/(173.3Mbps)	<input checked="" type="checkbox"/> 2/9/(n/a)
<input checked="" type="checkbox"/> 3/8/(260.0Mbps)	<input checked="" type="checkbox"/> 3/9/(288.9Mbps)	<input checked="" type="checkbox"/> 4/8/(346.7Mbps)	<input checked="" type="checkbox"/> 4/9/(n/a)

11ax

Enable 11ax Select All

Multiple BSSIDs

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/7	<input checked="" type="checkbox"/> 1/9	<input checked="" type="checkbox"/> 1/11	<input checked="" type="checkbox"/> 2/7
<input checked="" type="checkbox"/> 2/9	<input checked="" type="checkbox"/> 2/11	<input checked="" type="checkbox"/> 3/7	<input checked="" type="checkbox"/> 3/9
<input checked="" type="checkbox"/> 3/11	<input checked="" type="checkbox"/> 4/7	<input checked="" type="checkbox"/> 4/9	<input checked="" type="checkbox"/> 4/11
<input checked="" type="checkbox"/> 5/7	<input checked="" type="checkbox"/> 5/9	<input checked="" type="checkbox"/> 5/11	<input checked="" type="checkbox"/> 6/7
<input checked="" type="checkbox"/> 6/9	<input checked="" type="checkbox"/> 6/11	<input checked="" type="checkbox"/> 7/7	<input checked="" type="checkbox"/> 7/9
<input checked="" type="checkbox"/> 7/11	<input checked="" type="checkbox"/> 8/7	<input checked="" type="checkbox"/> 8/9	<input checked="" type="checkbox"/> 8/11

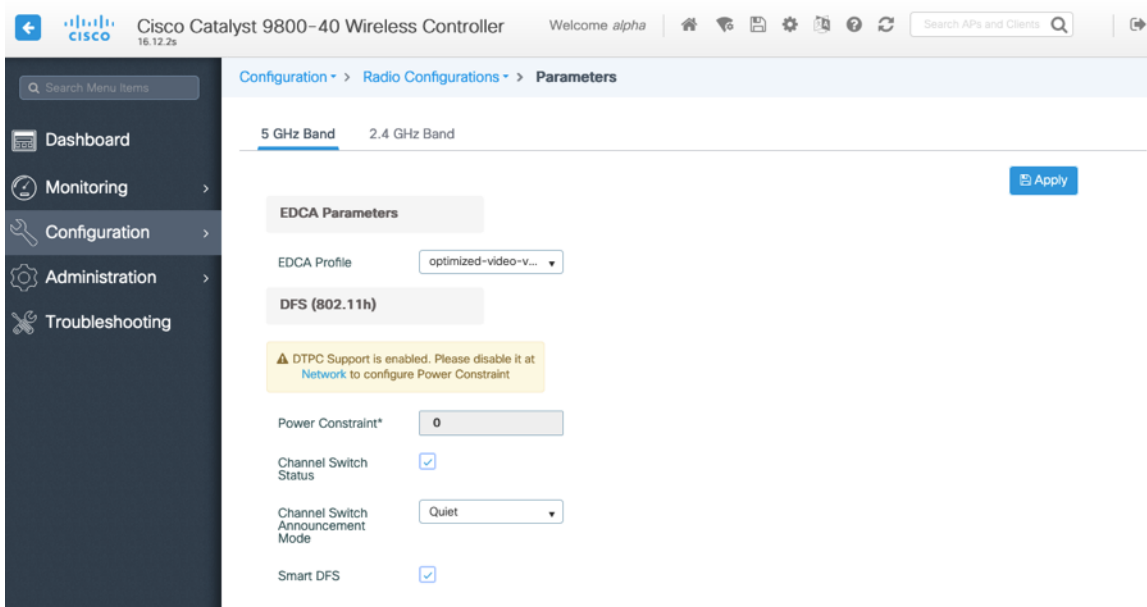
Parameters

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.

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

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

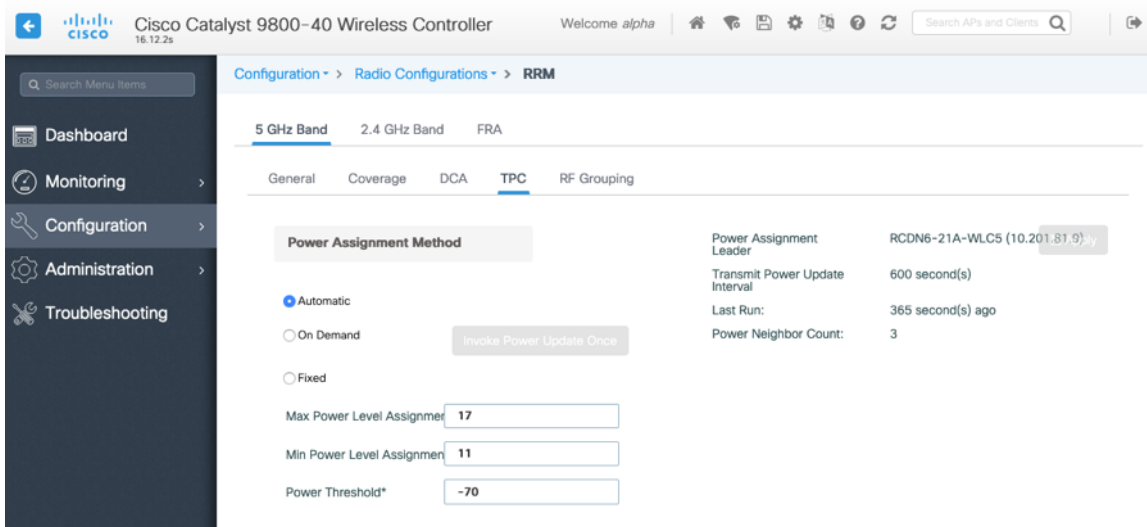


RRM

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 or 802.11ax Access Points.

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

Cisco Catalyst 9800-40 Wireless Controller | Welcome *alpha* | Search APs and Clients

Configuration > Radio Configurations > RRM

5 GHz Band | 2.4 GHz Band | FRA

General | Coverage | **DCA** | TPC | RF Grouping

Dynamic Channel Assignment Algorithm [Apply]

Channel Assignment Mode: Automatic
 Freeze [Invoke Channel Update Once]
 Off

Interval: 10 minutes
 Anchortime: 0

Avoid Foreign AP Interference:
 Avoid Cisco AP load:
 Avoid Non 5 GHz Noise:
 Avoid Persistent Non-wifi Interference:

Channel Assignment Leader: RCDN6-21A-WLC5 (10.201.81.9)
 Last Auto Channel Assignment: 475 second(s) ago
 DCA Channel Sensitivity: medium
 Channel Width: 20 MHz 40 MHz 80 MHz 160 MHz Best

Auto-RF Channel List

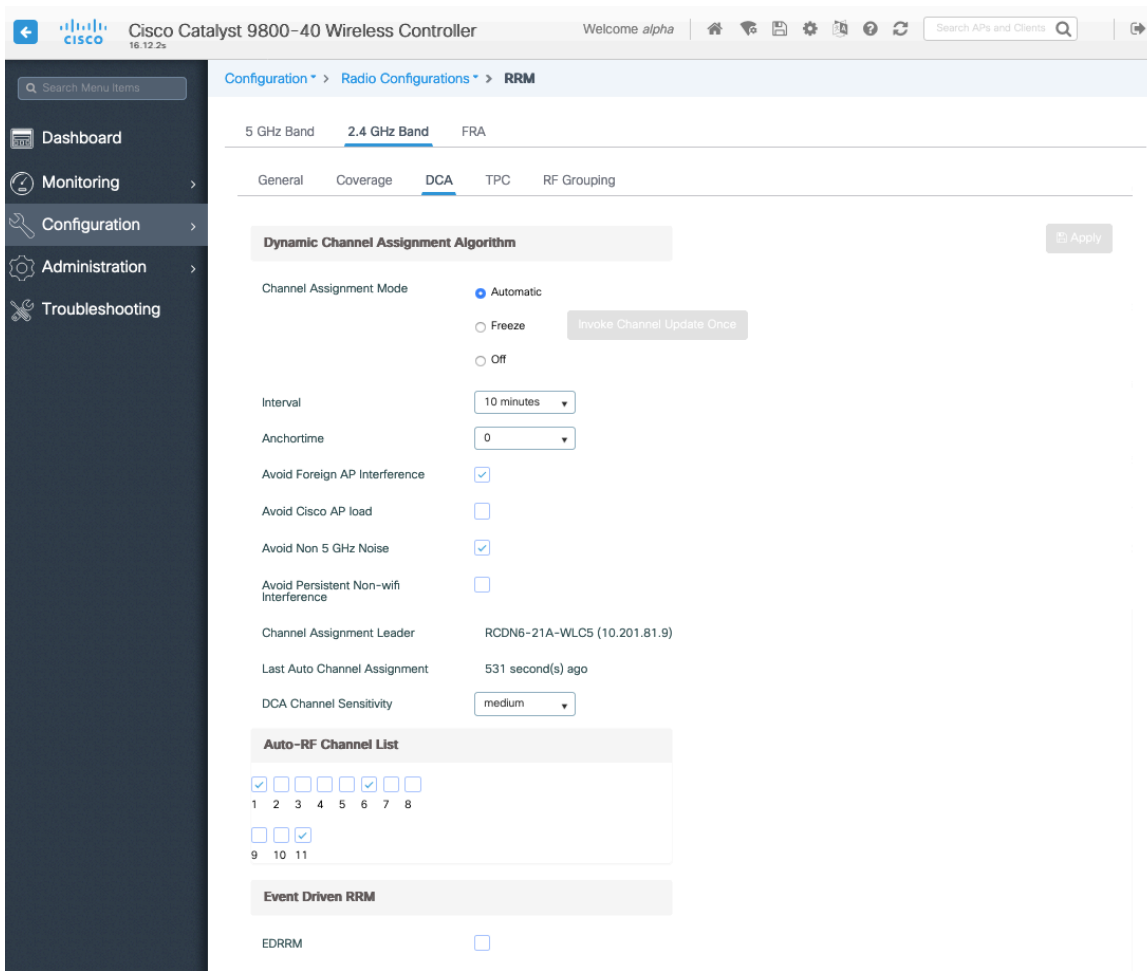
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136

140 144 149 153 157 161 165

Event Driven RRM

EDRRM:

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 or 802.11ax Access Points.

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

The screenshot shows the configuration page for a 5 GHz radio on a Cisco Catalyst 9800-40 Wireless Controller. The page is titled "Edit Radios 5 GHz Band" and has two tabs: "Configure" (active) and "Detail".

General

- AP Name: rcdn6-22a-ap1
- Admin Status: **ENABLED** (green indicator)
- CleanAir Admin Status: **ENABLED** (green indicator)

RF Channel Assignment

- Current Channel: 149
- Channel width: 40 MHz
- Assignment Method: Global

Antenna Parameters

- Antenna Type: Internal
- Antenna Mode: Omni
- Antenna A:
- Antenna B:
- Antenna C:
- Antenna D:
- Antenna Gain: 10

Tx Power Level Assignment

- Current Tx Power Level: 2
- Assignment Method: Global

Buttons at the bottom: Cancel, Update & Apply to Device.

CleanAir

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

The screenshot shows the configuration page for CleanAir on a Cisco Catalyst 9800-40 Wireless Controller. The page is titled "CleanAir" and has two tabs: "5 GHz Band" (active) and "2.4 GHz Band".

General

- Enable CleanAir:
- Enable SI:
- Report Interferers:
- Persistent Device Propagation:

Interference Types to detect

- TDD Transmitter
- Jammer
- Continuous Transmitter
- DECT-like Phone
- Video Camera

Buttons at the bottom: Apply.

WLAN Settings

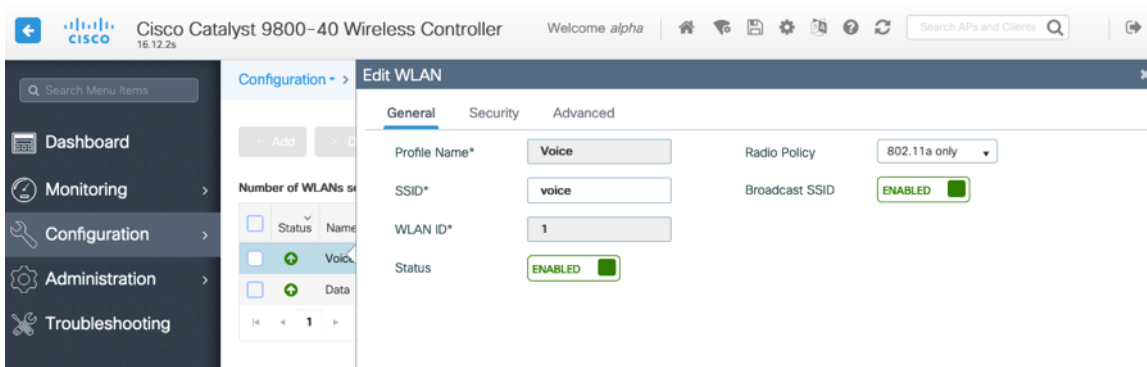
It is recommended to have a separate SSID for the Cisco RoomOS Series.

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 RoomOS Series can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

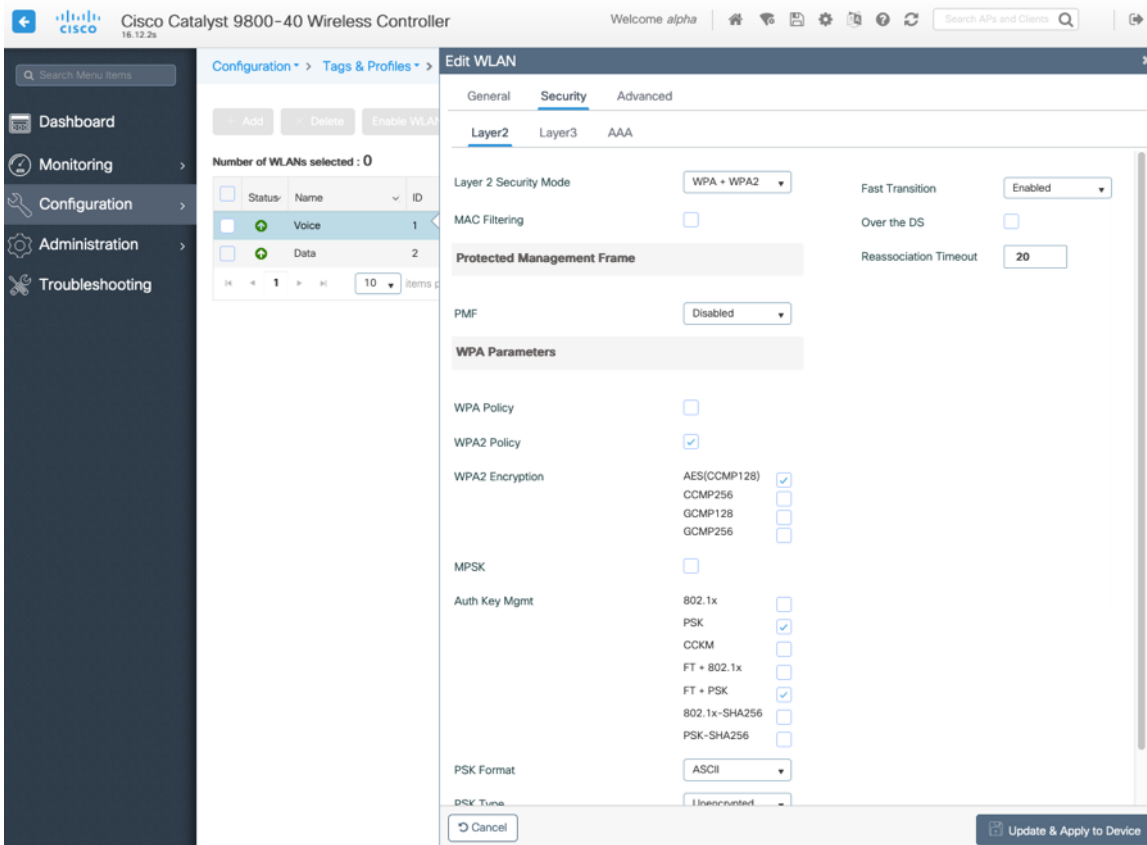
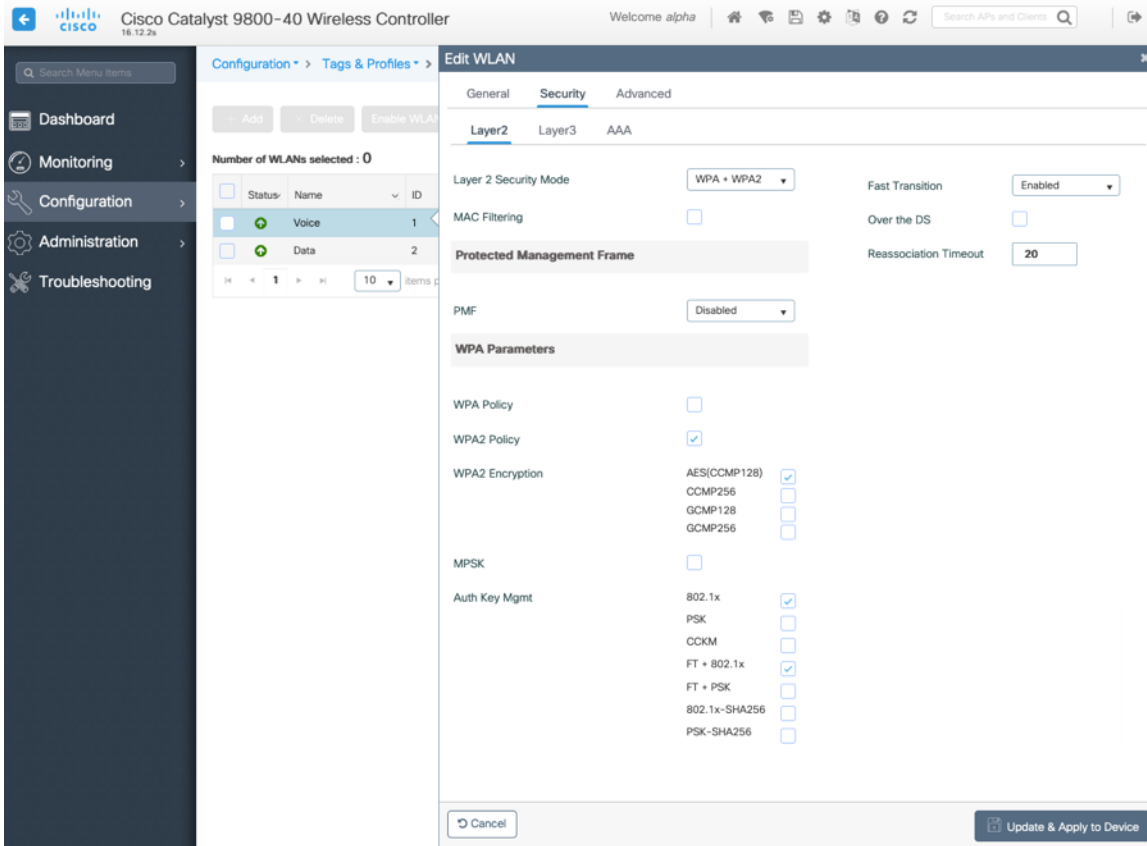
It is recommended to have the Cisco RoomOS Series operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

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.



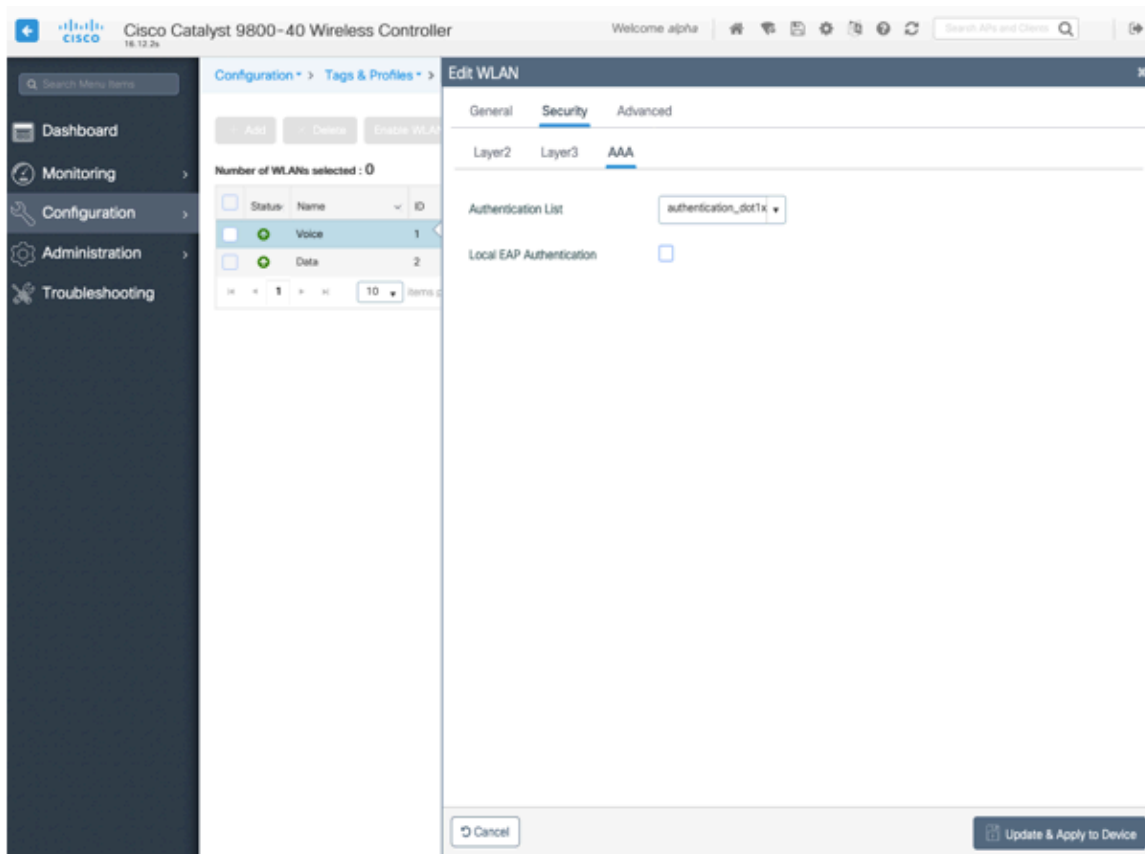
Protected Management Frame can be set to **Optional**, **Required**, or **Disabled**.

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



802.11r (FT), CCKM and/or PSK may also be enabled if wanting to utilize the same SSID for various type of voice clients, depending on whether 802.1x or PSK is being utilized.

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 RoomOS Series 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 RoomOS Series, 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 enable defer priority for queues 4-6.

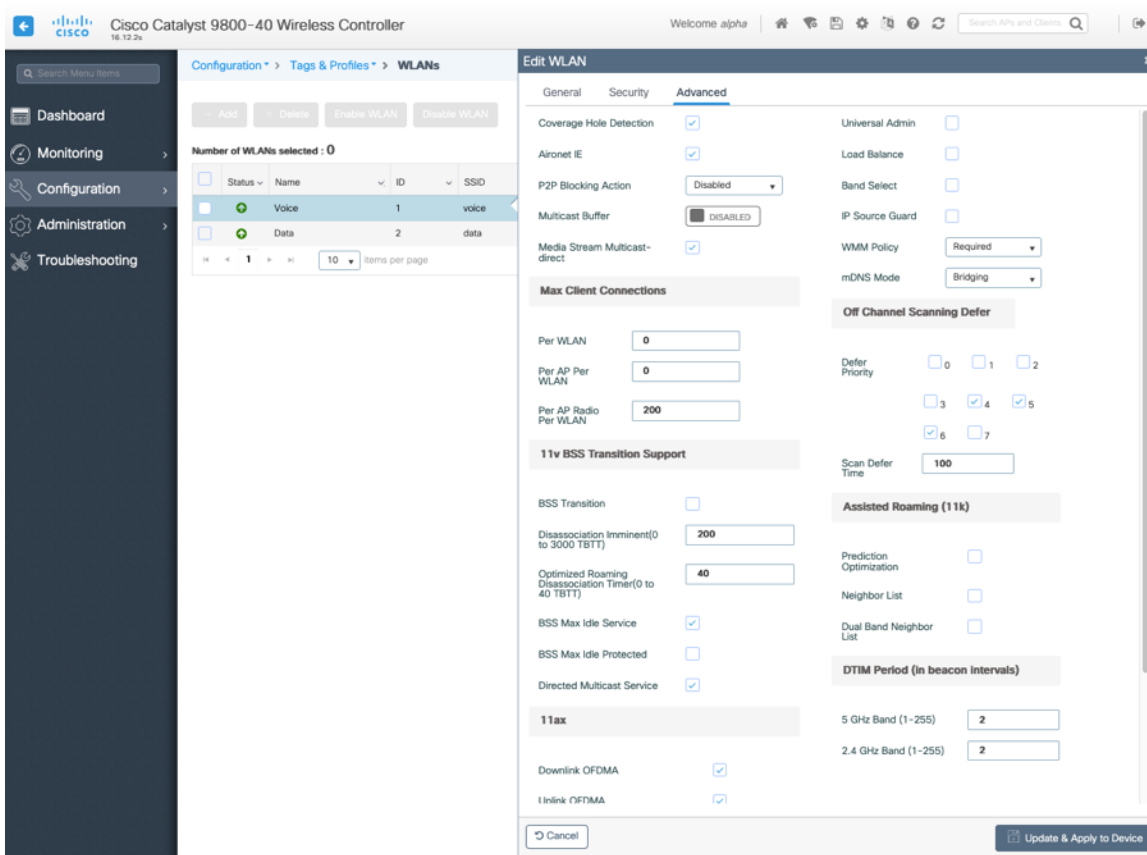
If using best effort applications frequently or if DSCP values for priority applications (e.g. voice and call control) are not preserved to the access point, then is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well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

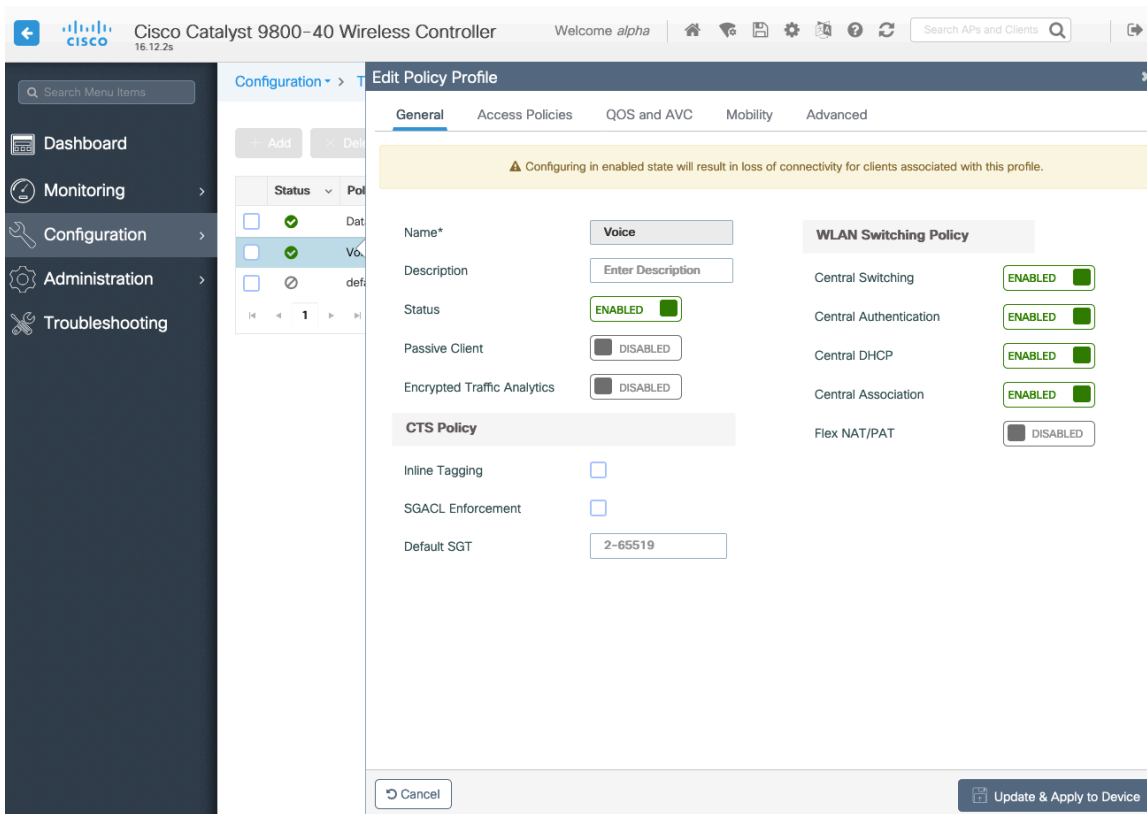
802.11k and 802.11v are not supported, therefore should be disabled.



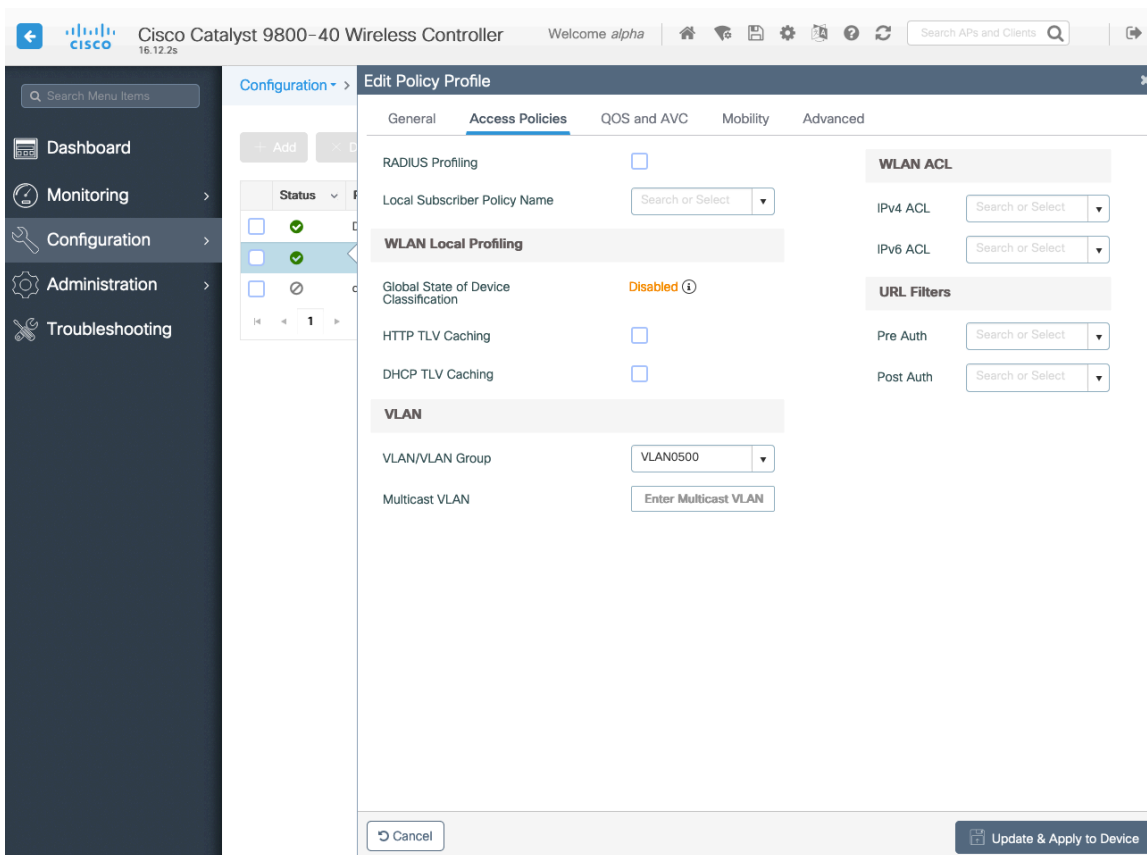
Policy Profiles

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.

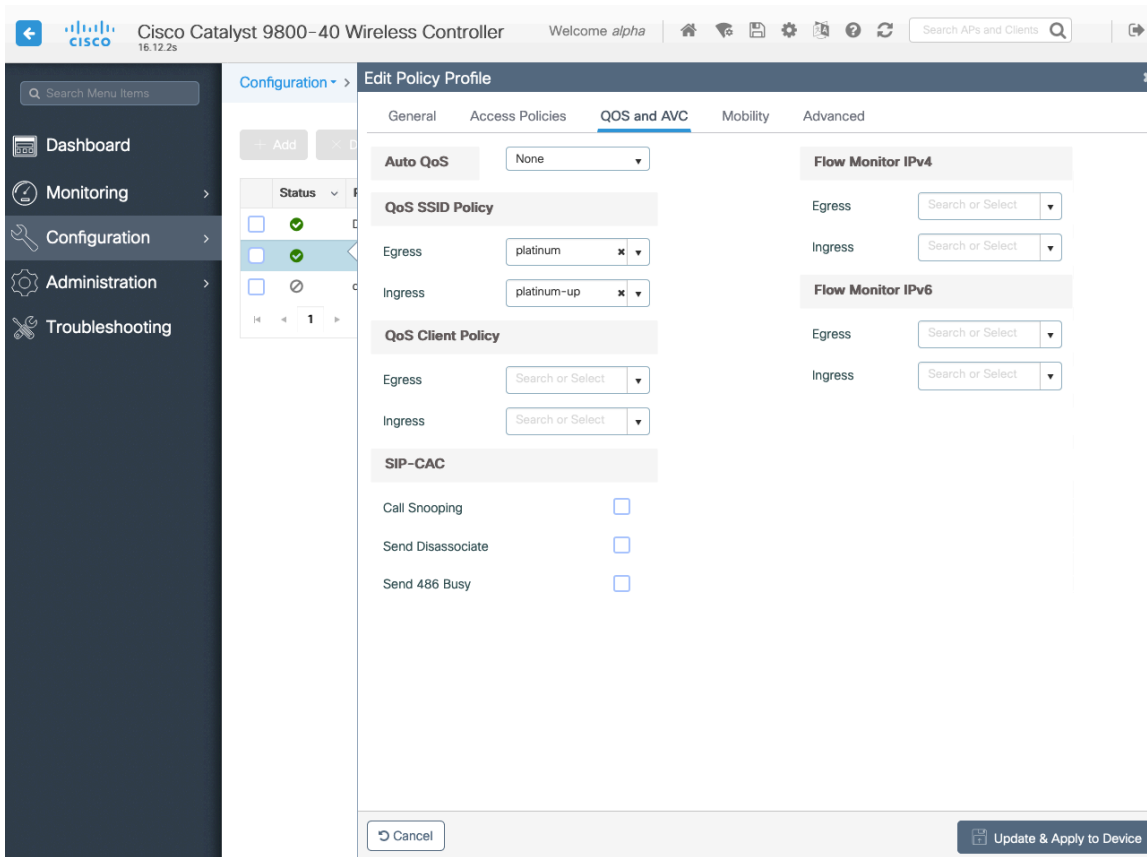
Ensure the **Status** of the policy profile is **Enabled**.



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



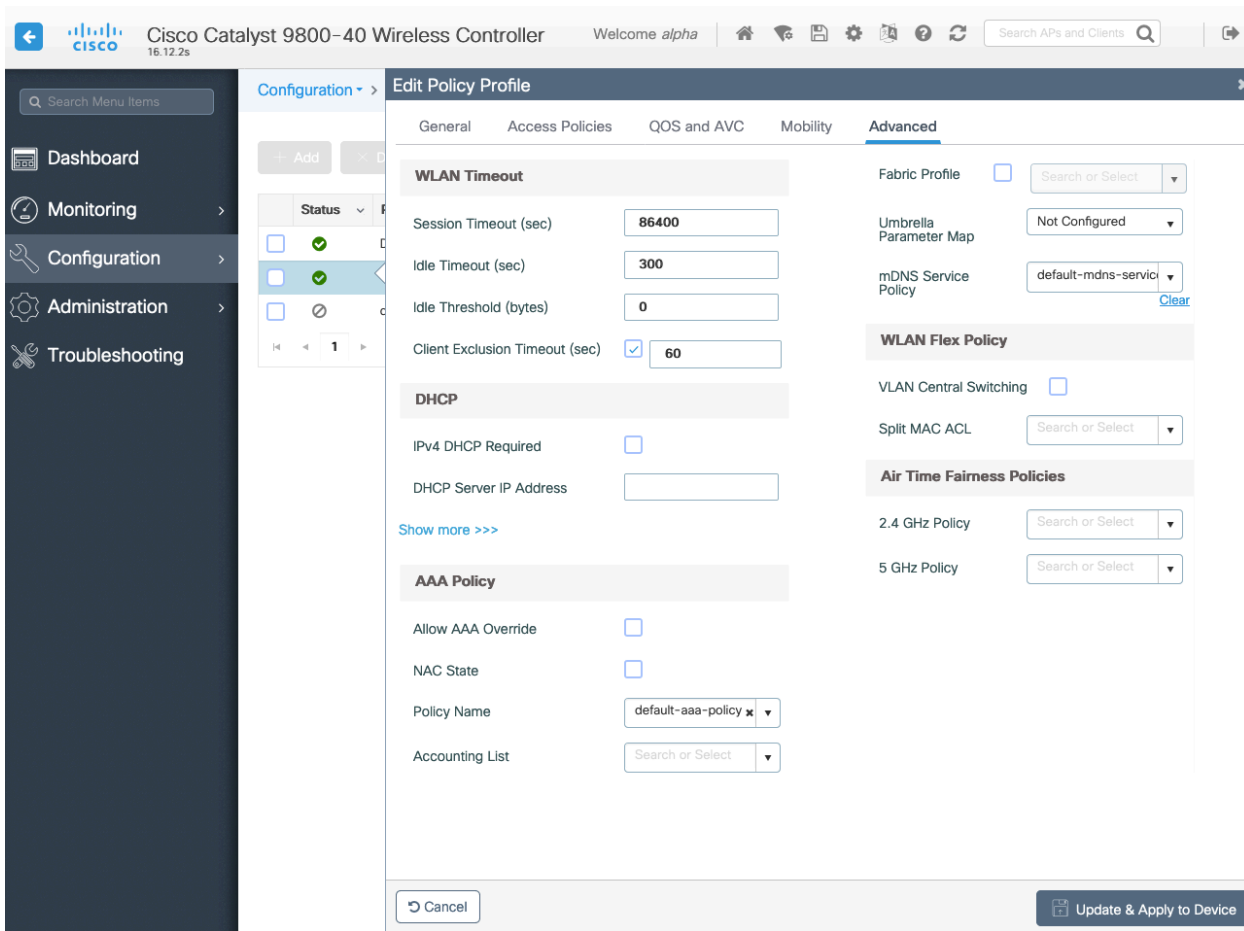
Ensure the QoS SSID Policy is set to **Platinum** for egress and **Platinum-up** for ingress.



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

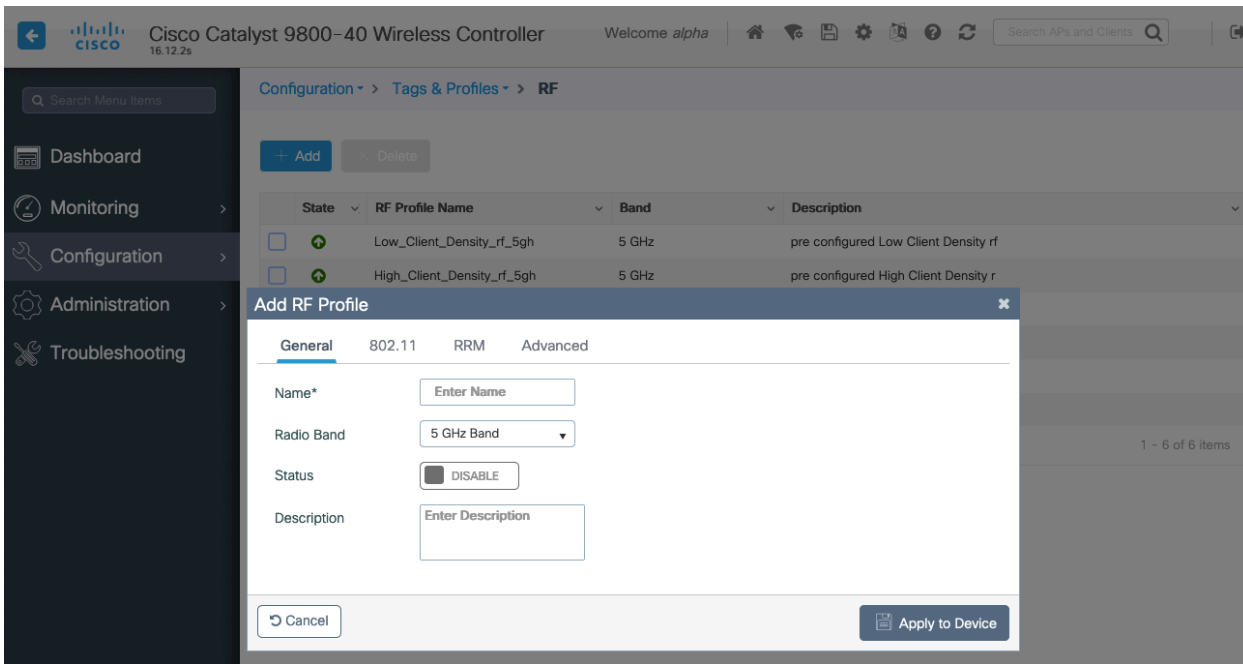
RF Profiles can be created to specify which frequency bands, data rates, RRM settings, and advanced settings a group of access points should use.

It is recommended to have the SSID used by the Cisco RoomOS Series 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.

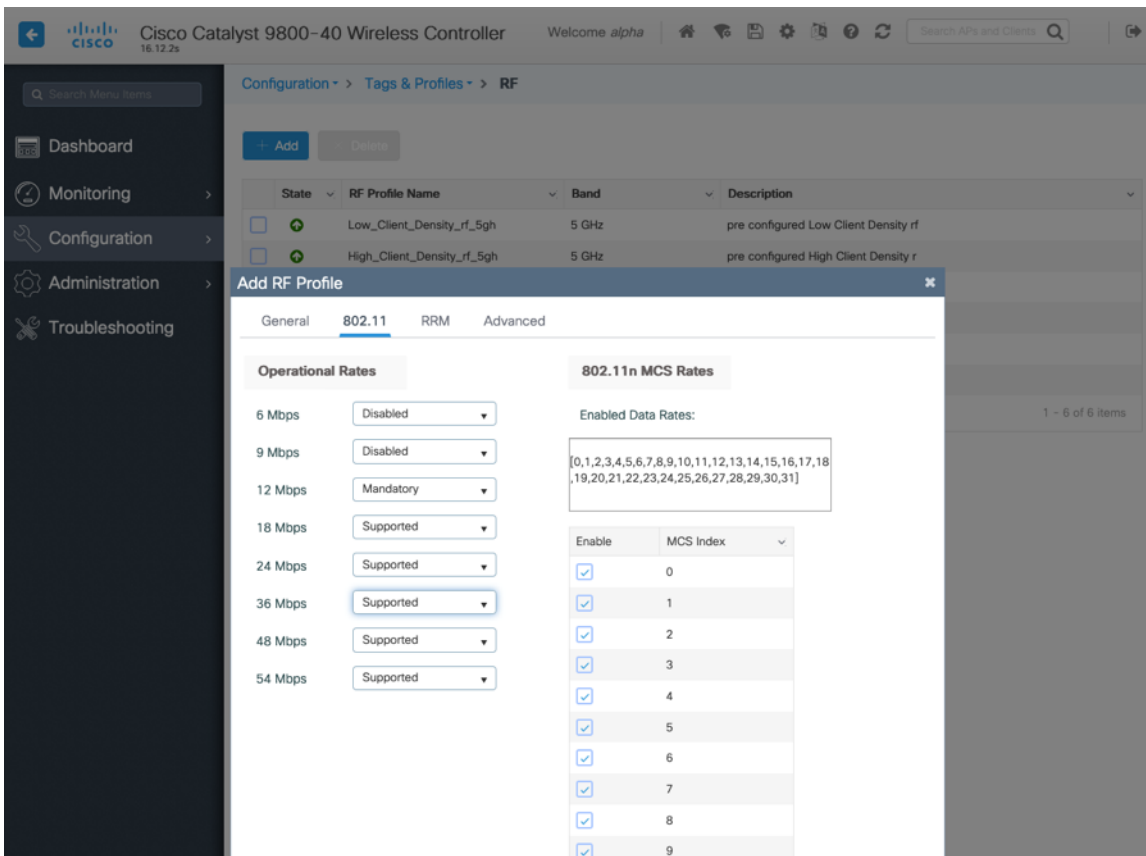
When creating an RF Profile, the **Name** and **Radio Band** must be defined.

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



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

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



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

Cisco Catalyst 9800-40 Wireless Controller | Welcome alpha

Configuration > Tags & Profiles > RF

State	RF Profile Name	Band	Description
<input type="checkbox"/>	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf
<input type="checkbox"/>	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r

Add RF Profile

General 802.11 **RRM** Advanced

General Coverage **TPC** DCA

Coverage Hole Detection

Minimum Client Level (clients)*

Data RSSI Threshold (dBm)*

Voice RSSI Threshold (dBm)*

Exception Level(%)*

Cisco Catalyst 9800-40 Wireless Controller | Welcome alpha

Configuration > Tags & Profiles > RF

State	RF Profile Name	Band	Description
<input type="checkbox"/>	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf
<input type="checkbox"/>	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r

Add RF Profile

General 802.11 **RRM** Advanced

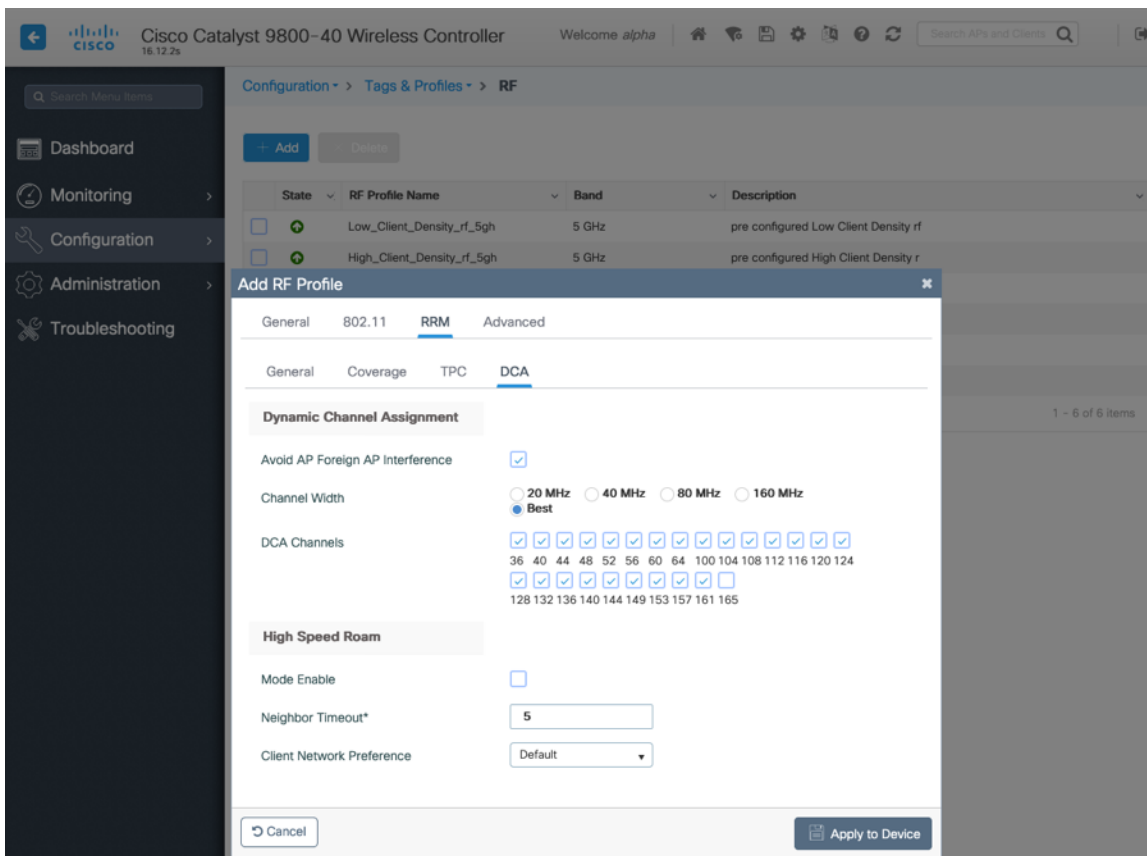
General Coverage **TPC** DCA

Transmit Power Control

Maximum Power Level(dBm)*

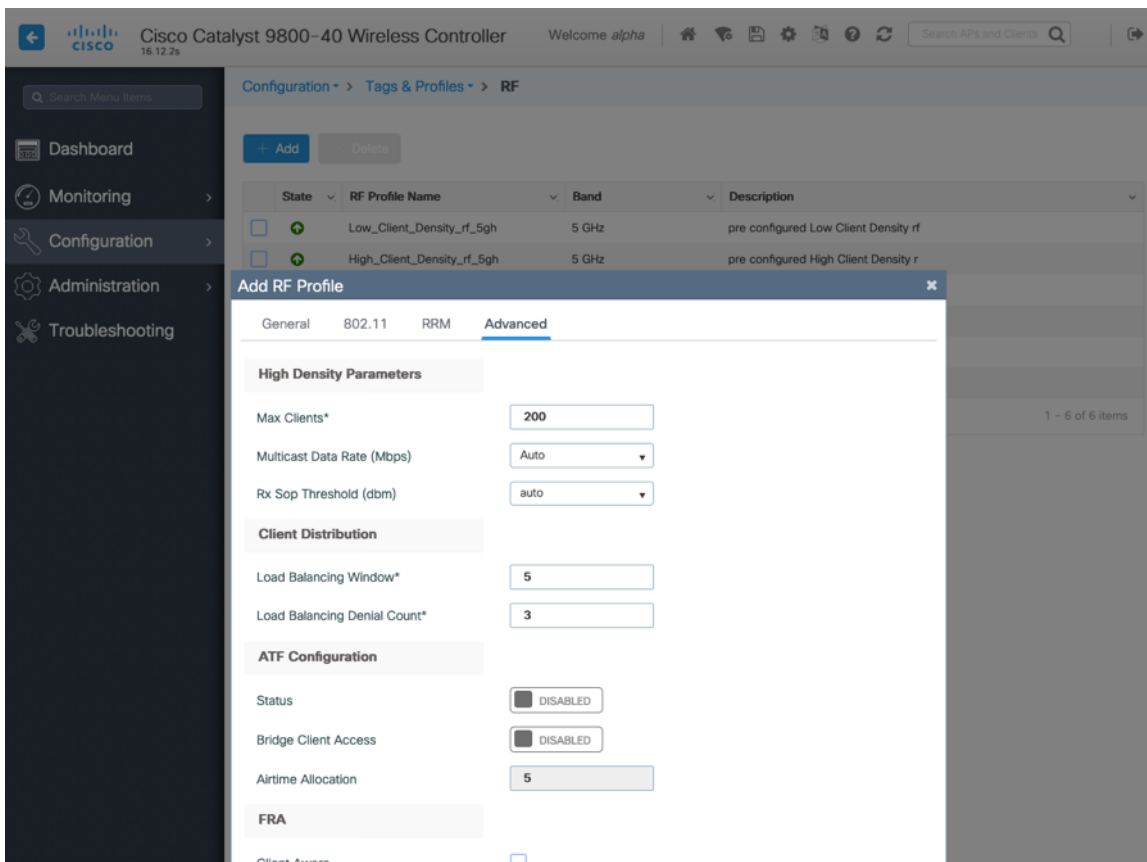
Minimum Power Level(dBm)*

Power Threshold V1(dBm)*



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

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



Flex Profiles

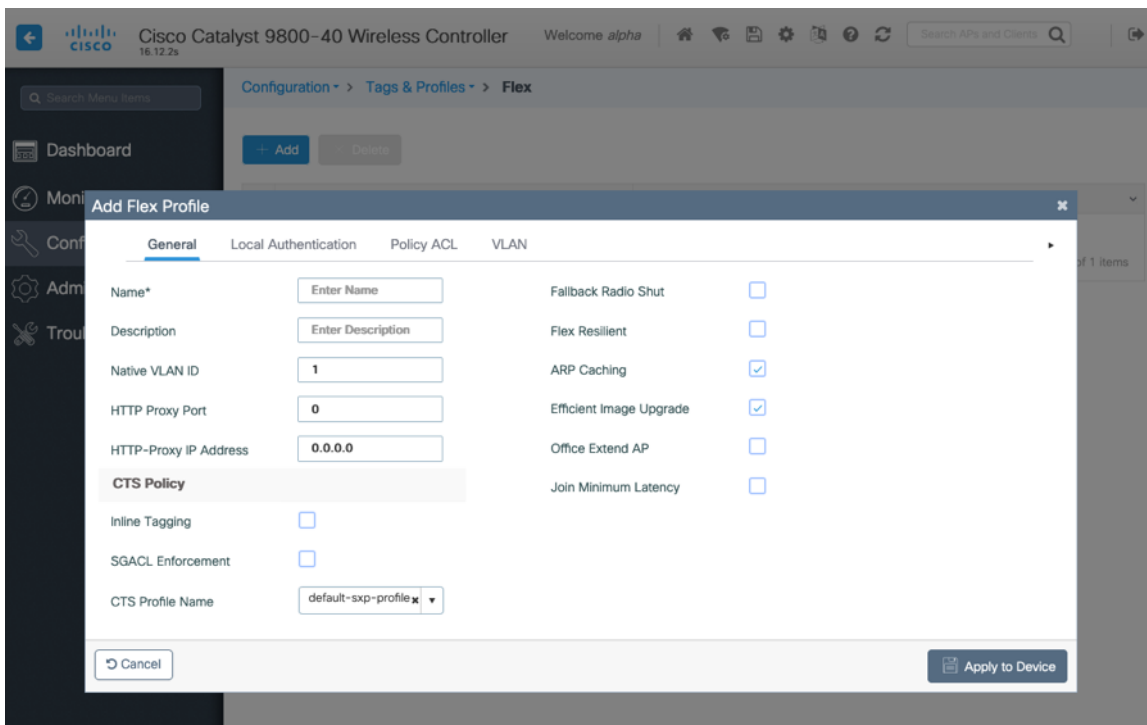
Flex Profiles are used to define the settings the access point should use when in Flexconnect mode.

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

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.



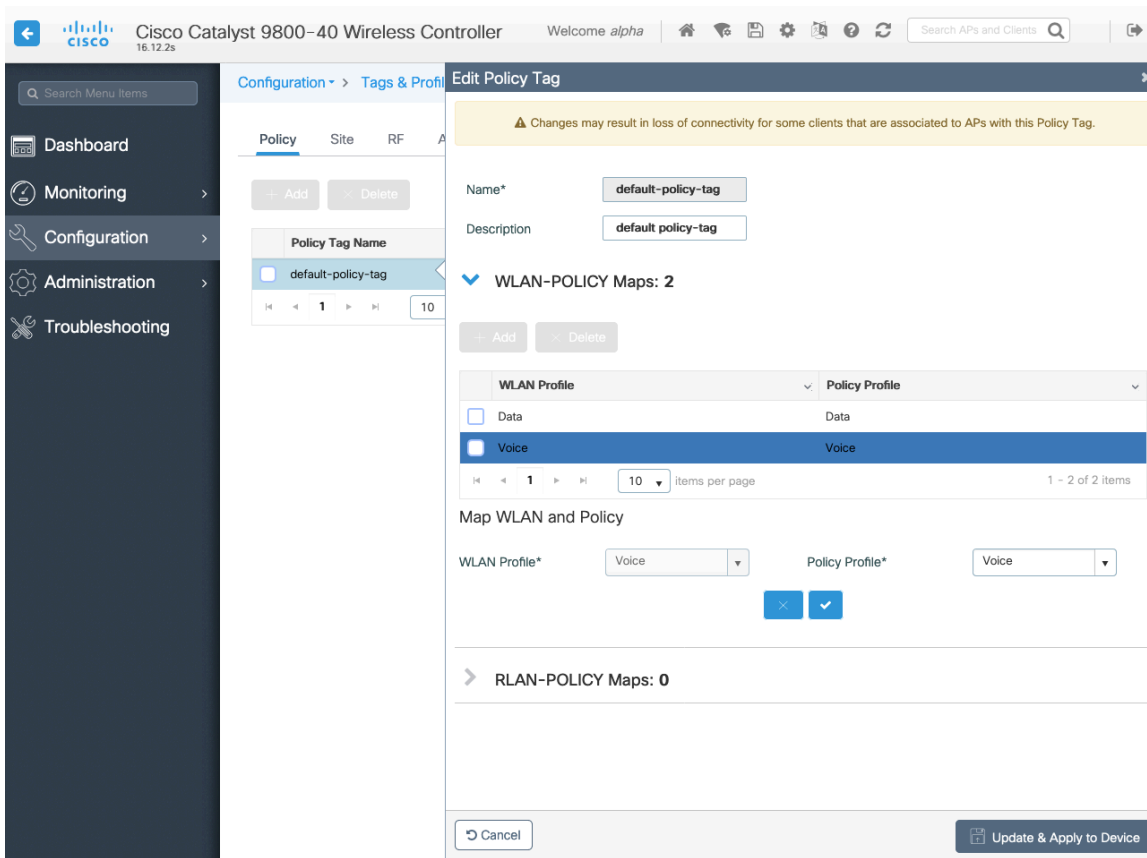
Tags

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.



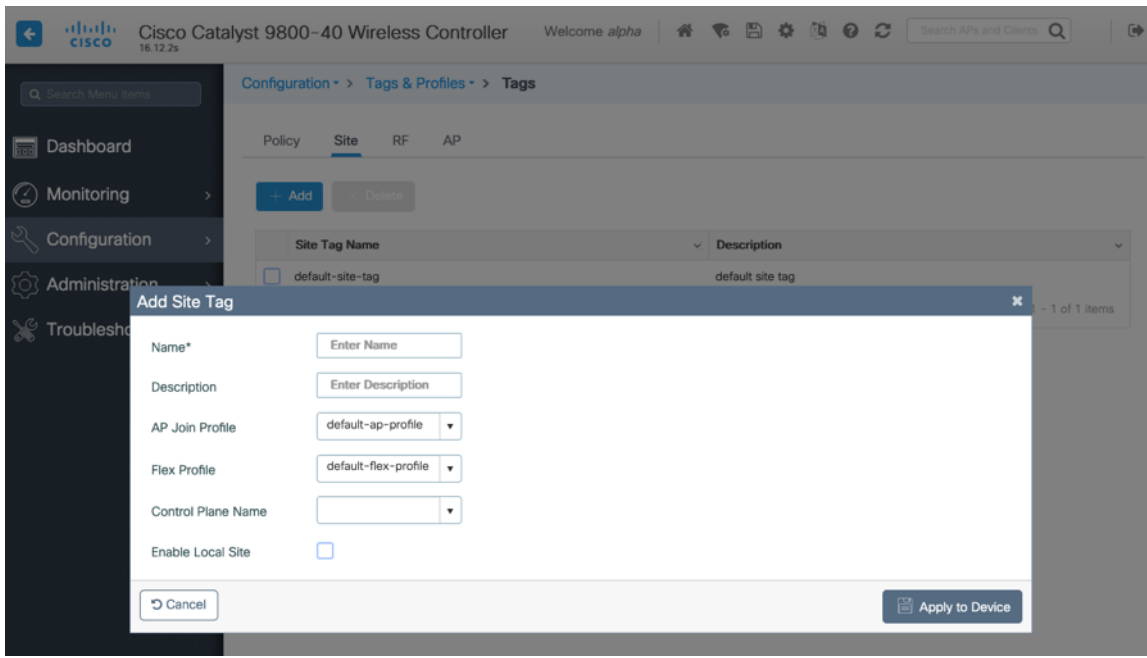
Site Tag

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**.

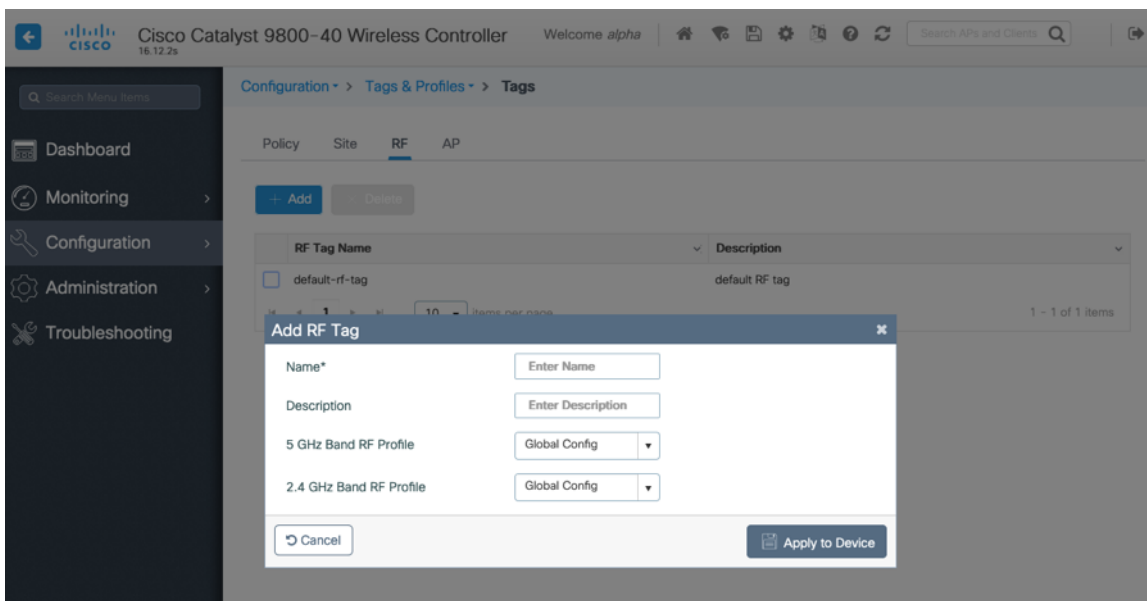


RF Tag

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

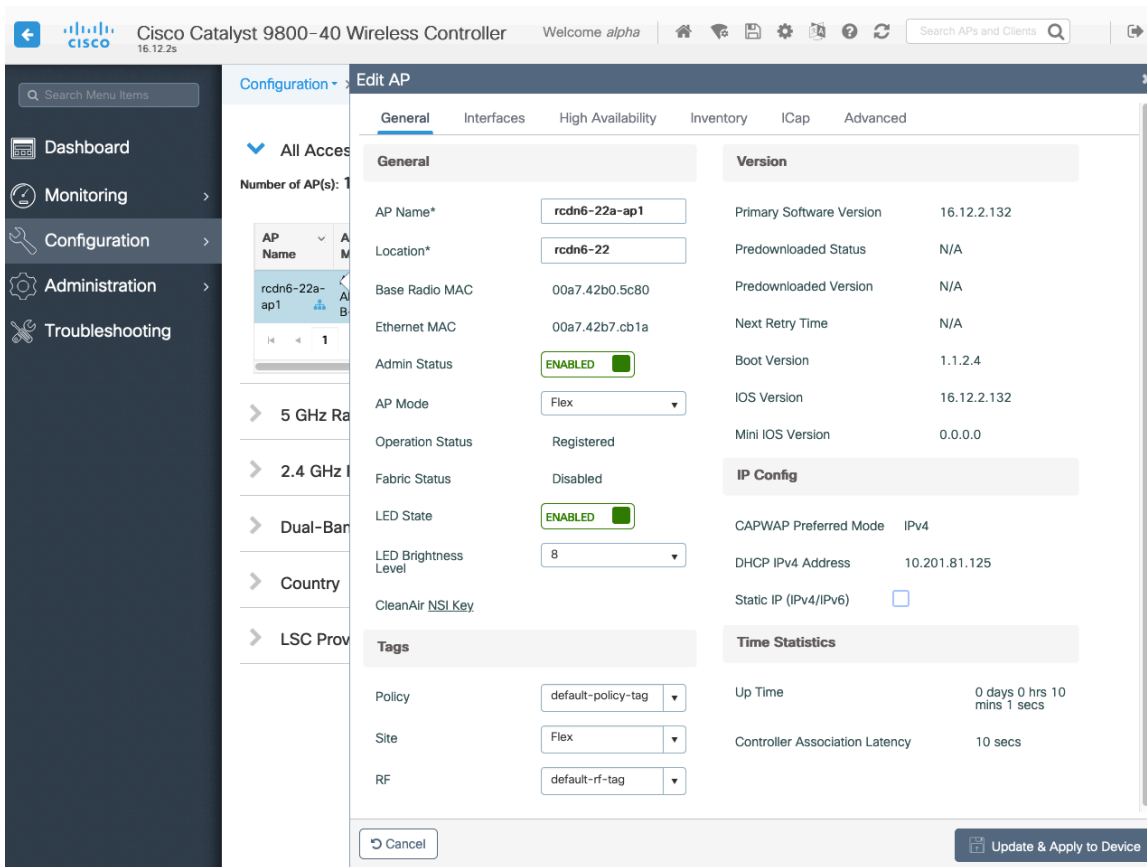
RF Tags are then applied to an access point to specify which RF Profile parameters should be used.

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.

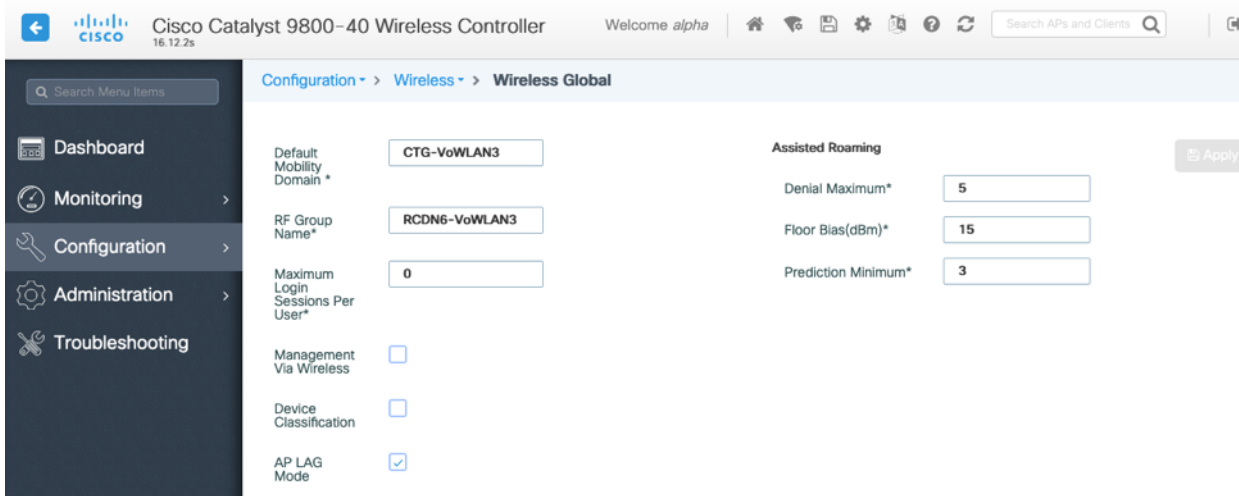
If a Site Tag is applied including a configured Flex Profile, then the **AP Mode** will be changed to **Flex** automatically.



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**.

The screenshot shows the 'Global Configuration' tab for Mobility. The following fields are visible:

- Mobility Group Name*: CTG-VoWLAN3
- Multicast IPv4 Address: 0.0.0.0
- Multicast IPv6 Address: ::
- Keep Alive Interval (sec)*: 10
- Mobility Keep Alive Count*: 3
- Mobility DSCP Value*: 48
- Mobility MAC Address*: 706d.153d.b50b

An 'Apply' button is located to the right of the 'Mobility Group Name' field.

The screenshot shows the 'Peer Configuration' tab for Mobility. It displays a table of Mobility Peer Configuration entries:

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Status	PMTU
706d.153d.b50b	10.201.81.9	N/A	CTG-VoWLAN3	0.0.0.0	N/A	N/A
6c31.0e7b.b8eb	10.201.81.10	10.201.81.10	CTG-VoWLAN3	0.0.0.0	Up	1385

Below the table, there is a '10' items per page selector and a '1 - 2 of 2 items' indicator. There are also 'Add' and 'Delete' buttons above the table.

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

The screenshot shows the 'Wireless' interface configuration page. It displays a table of wireless interfaces:

Interface Name	Interface Type	Trustpoint Name	VLAN ID	IP Address	IP Netmask	MAC Address
Vlan310	Management		310	10.201.81.9	255.255.255.240	70:6d:15:3d:b5:0b

Below the table, there is a '10' items per page selector and a '1 - 1 of 1 items' indicator. There are also 'Add' and 'Delete' buttons above the table.

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**.

The screenshot shows the configuration page for a Cisco Catalyst 9800-40 Wireless Controller, specifically the **Media Parameters** section for the **5 GHz Band**. The page is divided into two main columns: **Media** and **Voice**.

Media Section:

- General:** Unicast Video Redirect is checked.
- Multicast Direct Admission Control:** Media Stream Admission Control (ACM) is unchecked. Maximum Media Stream RF bandwidth (%) is 5. Maximum Media Bandwidth (%) is 85. Client Minimum Phy Rate (kbps) is 6000. Maximum Retry Percent (%) is 80.
- Media Stream - Multicast Direct Parameters:** Multicast Direct Enable is checked. Max streams per Radio is No Limit. Max streams per Client is No Limit. Best Effort QOS Admission is unchecked.

Voice Section:

- Call Admission Control (CAC):** Admission Control (ACM) is checked. Load Based CAC is checked. Max RF Bandwidth (%) is 75. Reserved Roaming Bandwidth (%) is 6. Expedited Bandwidth is checked.
- SIP CAC and Bandwidth:** SIP CAC Support is unchecked.
- Traffic Stream Metrics:** Metrics Collection is checked. Stream Size* is 84000. Max Streams* is 2. Inactivity Timeout is unchecked.

An **Apply** button is located at the top right of the configuration area.

Multicast

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

The screenshot shows the configuration page for Multicast on a Cisco Catalyst 9800-40 Wireless Controller. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled "Configuration > Services > Multicast".

Global Wireless Multicast Mode is **ENABLED**. Other settings include:

- Wireless mDNS Bridging: **DISABLED**
- Wireless Non-IP Multicast: **DISABLED**
- Wireless Broadcast: **DISABLED**
- AP Capwap Multicast: Unicast
- MLD Snooping: **DISABLED**
- IGMP Snooping Querier: **DISABLED**
- IGMP Snooping: **ENABLED**
- Last Member Querier Interval (milliseconds): 1000

The IGMP Snooping section is expanded, showing two tables:

Disabled		
Status	VLAN ID	Name
No Vlan available		

Enabled		
Status	VLAN ID	Name
+	1	default
+	310	VLAN0310
+	400	VLAN0400
+	500	VLAN0500

Buttons for "Apply", "Enable All", and "Disable All" are visible. A link for "Wireless Broadcast and Wireless Non-IP Multicast" is at the bottom.

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

The screenshot shows the configuration page for Media Stream on a Cisco Catalyst 9800-40 Wireless Controller. The left sidebar is the same as in the previous image. The main content area is titled "Configuration > Wireless > Media Stream".

The "General" tab is selected, showing:

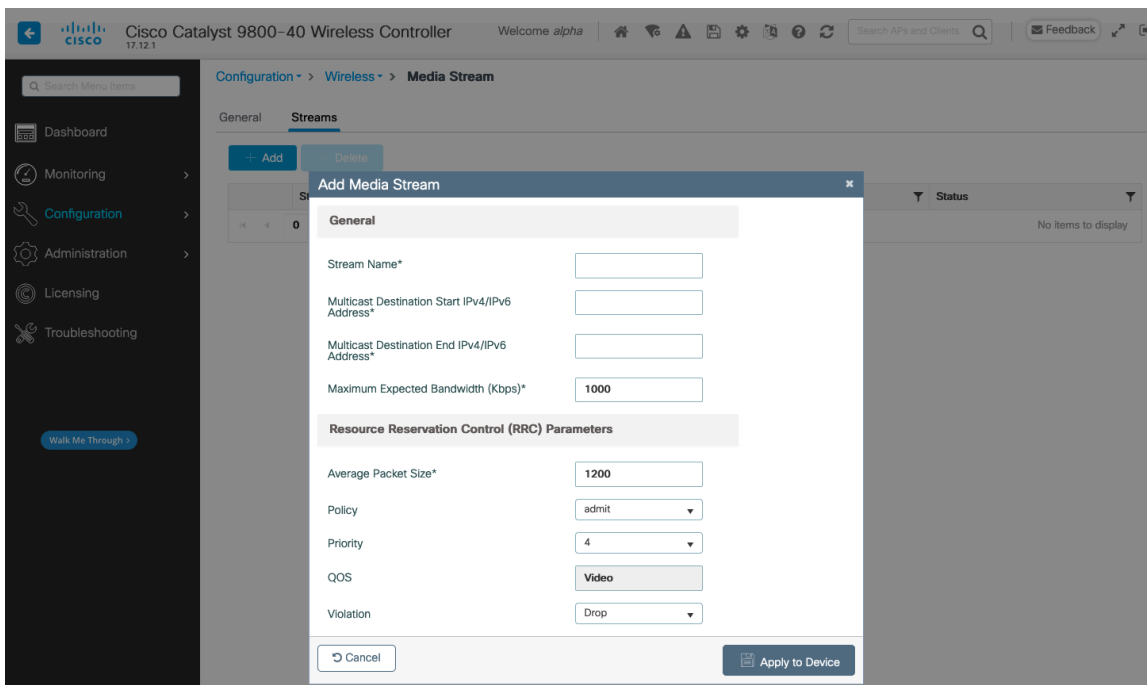
- Multicast Direct Enable:

The "Streams" tab is also visible. Below the "Session Message Config" section, there are input fields for:

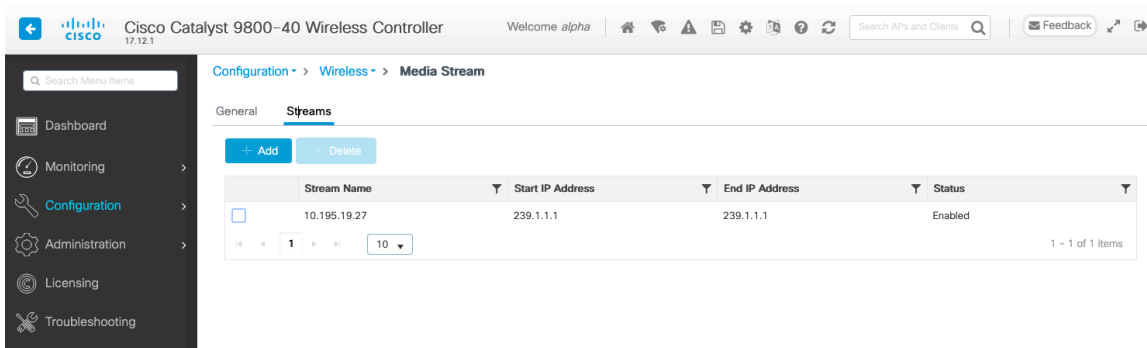
- Session Announcement State:
- Session Announcement URL:
- Session Announcement Email:
- Session Announcement Phone:
- Session Announcement Note:

An "Apply" button is located at the top right of the configuration area.

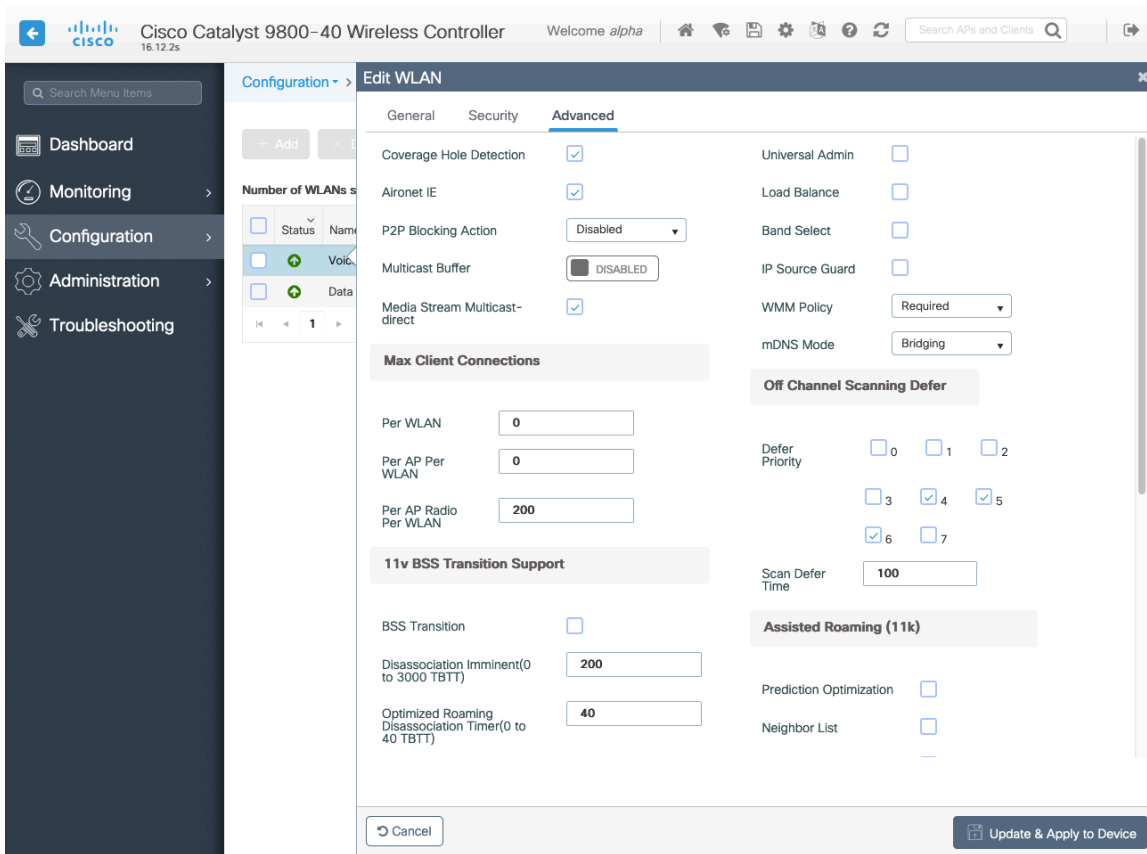
Then configure the media streams as necessary.



Once saved, then the media stream will be displayed.



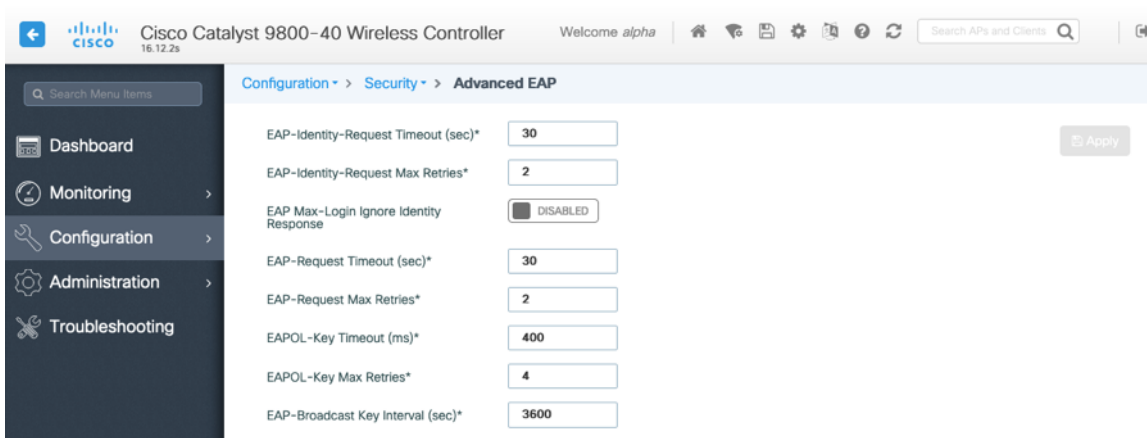
And enable **Multicast Direct** in the WLAN configuration.



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**.

The screenshot shows the configuration page for the Cisco Catalyst 9800-40 Wireless Controller. The breadcrumb navigation is Configuration > Wireless > Advanced. The 'High Density' tab is selected. Under the 'Rx Sop Threshold' section, there are two dropdown menus: 'Rx Sop Threshold 5 GHz (dbm)' and 'Rx Sop Threshold 2.4 GHz (dbm)', both set to 'auto'. Below this is the 'Multicast Data Rate' section with two dropdown menus: 'Multicast Data Rate 5 GHz (Mbps)' and 'Multicast Data Rate 2.4 GHz (Mbps)', both set to 'Auto'. An 'Apply' button is visible in the top right corner of the configuration area.

Rogue Policies

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

The screenshot shows the configuration page for the Cisco Catalyst 9800-40 Wireless Controller, specifically the 'Wireless Protection Policies' section. The breadcrumb navigation is Configuration > Security > Wireless Protection Policies. The 'RLDP' tab is selected. Under the 'Rogue Location Discovery Protocol' section, there is a dropdown menu set to 'Disable'. Below this is a 'Retry Count' field set to '1' and a 'Schedule RLDP' checkbox which is unchecked. A table for scheduling RLDP is shown with columns for 'Day', 'Start Time', and 'End Time'. The days listed are Monday through Sunday, each with a checkbox and time selection fields.

Day	Start Time	End Time
<input type="checkbox"/> Monday		
<input type="checkbox"/> Tuesday		
<input type="checkbox"/> Wednesday		
<input type="checkbox"/> Thursday		
<input type="checkbox"/> Friday		
<input type="checkbox"/> Saturday		
<input type="checkbox"/> Sunday		

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
rsa-keypair 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

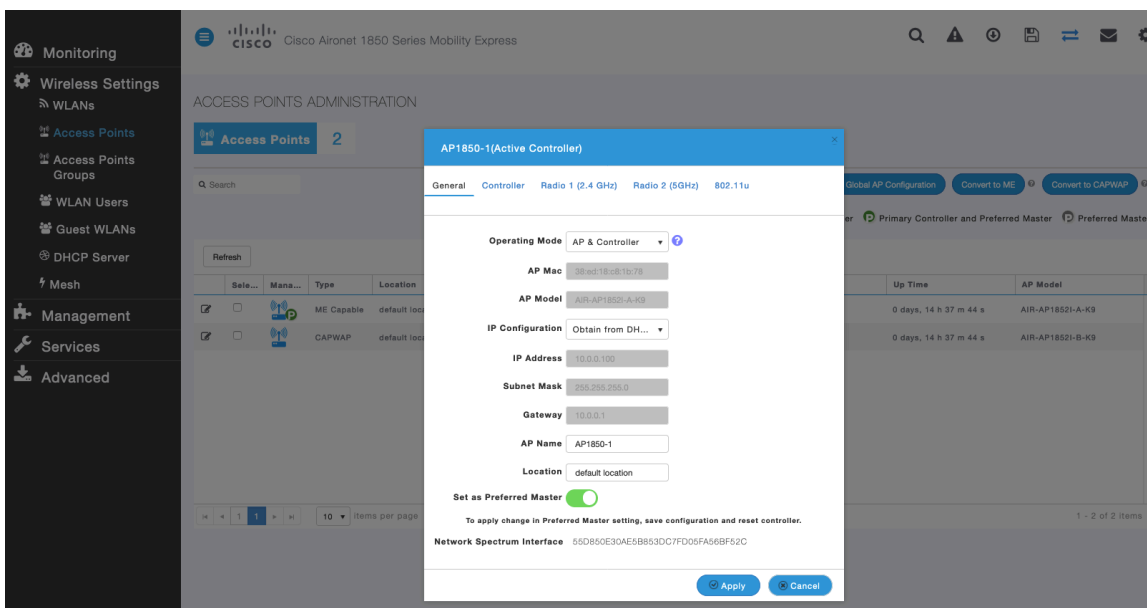
When configuring Cisco Mobility Express and Lightweight Access Points, use the following guidelines:

- Ensure **802.11r (FT)** and **CCKM** are not configured as mandatory
- Set **Quality of Service (QoS)** to **Platinum**
- Ensure **802.11k** is **Disabled**

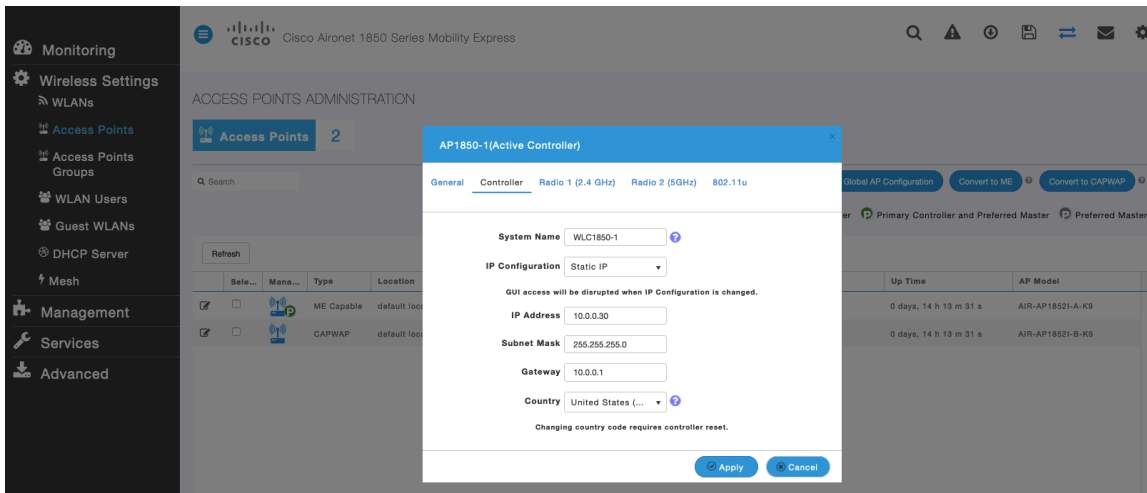
- Ensure **802.11v** is **Disabled**
- Disable **P2P (Peer to Peer) Blocking Action**
- Set **Client Band Select** to **Disabled**
- Set **Client Load Balancing** to **Disabled**
- Configure the **Data Rates** as necessary
- Configure **RF Optimization** as necessary
- Set **Traffic Type** to **Voice 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 RoomOS Series 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 or 802.11ax 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.

Advanced RF Parameters

- 2.4 GHz Band
- 5.0 GHz Band
- Automatic Flexible Radio Assignment
- 2.4 GHz Optimized Roaming
- 5 GHz Optimized Roaming
- Event Driven RRM
- CleanAir detection
- 5.0 GHz Channel Width: 40 MHz
- 2.4 GHz Data Rates: Lower Density to Higher Density slider (802.11b devices not supported)
- 5.0 GHz Data Rates: Lower Density to Higher Density slider (Some legacy devices not supported)
- Select DCA Channels:
 - 2.4 GHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
 - 5.0 GHz: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165

At least one Channel Number should be selected

Apply

RF Optimization

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

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

RF OPTIMIZATION

RF Optimization: Enabled

Client Density: Low, Typical, High

Traffic Type: Voice and Data

Apply

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 or 802.11ax 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.

The screenshot shows the 'ACCESS POINTS ADMINISTRATION' page in the Cisco Aironet 1850 Series Mobility Express interface. The left sidebar contains navigation options: Monitoring, Wireless Settings (WLANs, Access Points, Access Points Groups, WLAN Users, Guest WLANs, DHCP Server, Mesh), Management, Services, and Advanced. The main content area has a search bar and buttons for 'Global AP Configuration', 'Convert to ME', and 'Convert to CAPWAP'. Below these are radio buttons for 'Primary Controller', 'Primary Controller and Preferred Master', and 'Preferred Master'. A table lists two access points:

Select	Man...	Type	Location	Name	IP Address	AP Mac	Up Time	AP Model
<input checked="" type="checkbox"/>		ME Capable	default location	AP1850-1	10.0.0.100	38:ed:18:c8:1b:78	0 days, 14 h 37 m 44 s	AIR-AP1852I-A-K9
<input checked="" type="checkbox"/>		CAPWAP	default location	AP1850-2	10.0.0.101	38:ed:18:ca:28:40	0 days, 14 h 37 m 44 s	AIR-AP1852I-B-K9

This screenshot shows the configuration dialog for 'AP1850-1(Active Controller)' with the 'Radio 1 (2.4 GHz)' tab selected. The configuration options are:

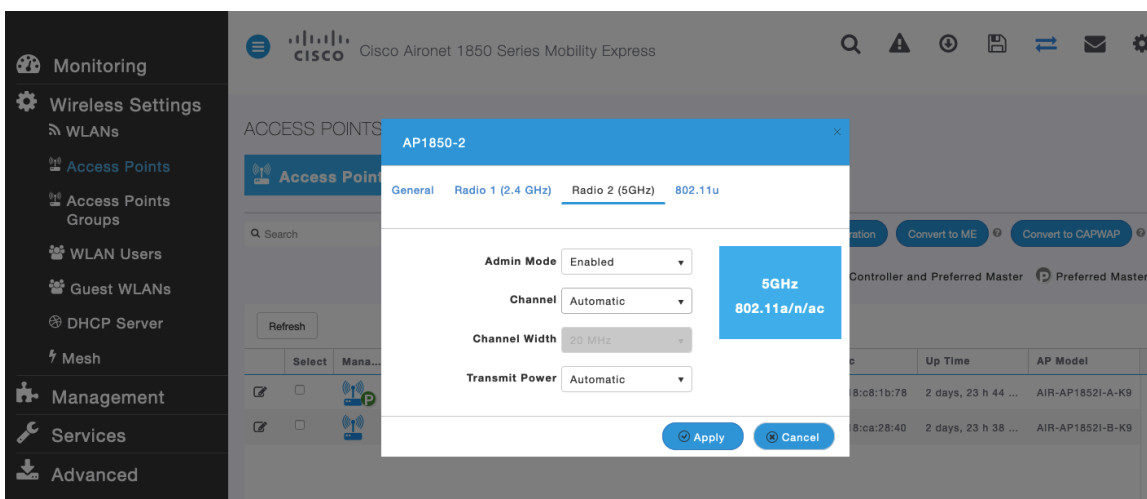
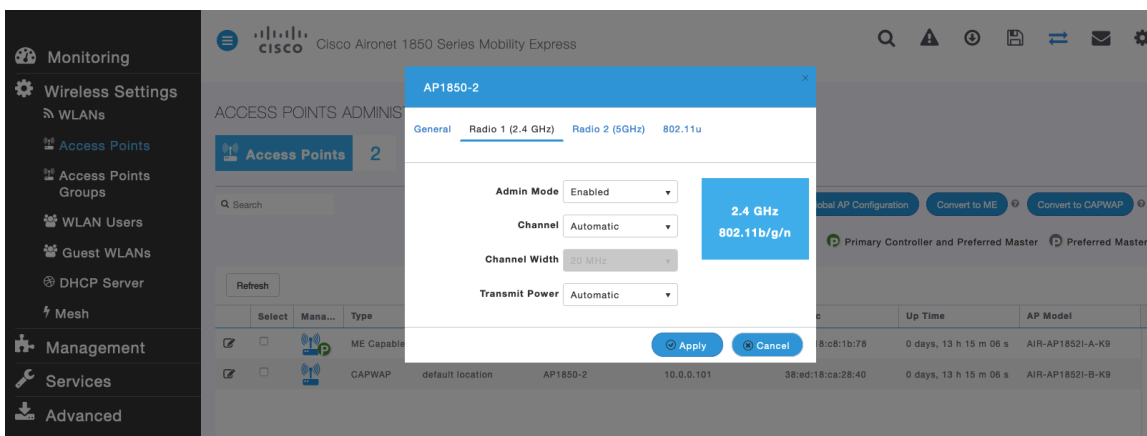
- Admin Mode: Enabled
- Channel: Automatic
- Channel Width: 20 MHz
- Transmit Power: Automatic

A blue callout box displays '2.4 GHz' and '802.11b/g/n'. The dialog includes 'Apply' and 'Cancel' buttons.

This screenshot shows the configuration dialog for 'AP1850-1(Active Controller)' with the 'Radio 2 (5GHz)' tab selected. The configuration options are:

- Admin Mode: Enabled
- Channel: Automatic
- Channel Width: 40 MHz
- Transmit Power: Automatic

A blue callout box displays '5GHz' and '802.11a/n/ac'. The dialog includes 'Apply' and 'Cancel' buttons.



WLAN Settings

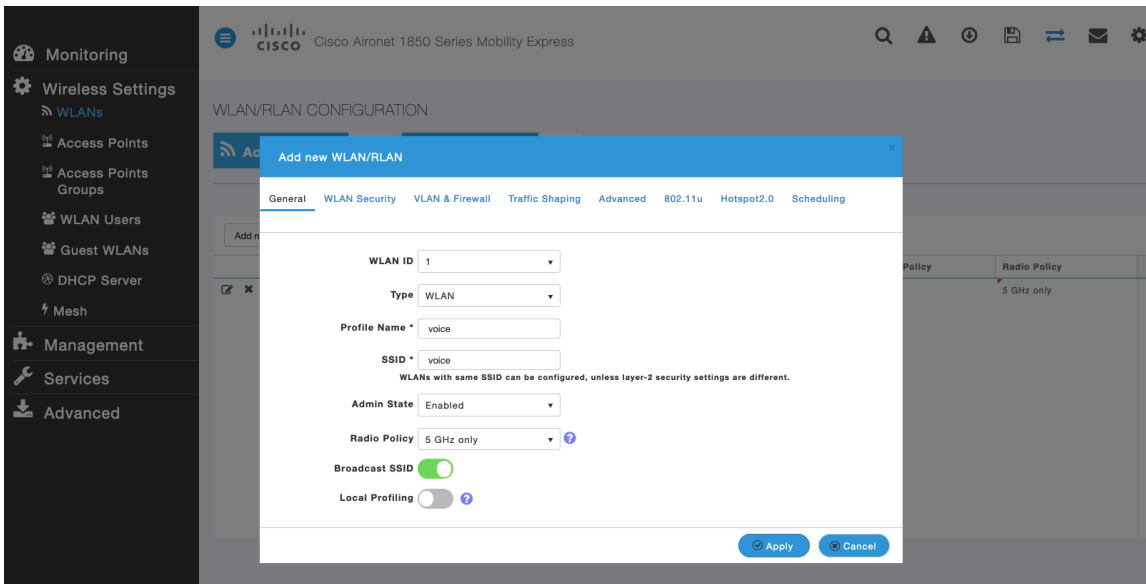
It is recommended to have a separate SSID for the Cisco RoomOS Series.

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

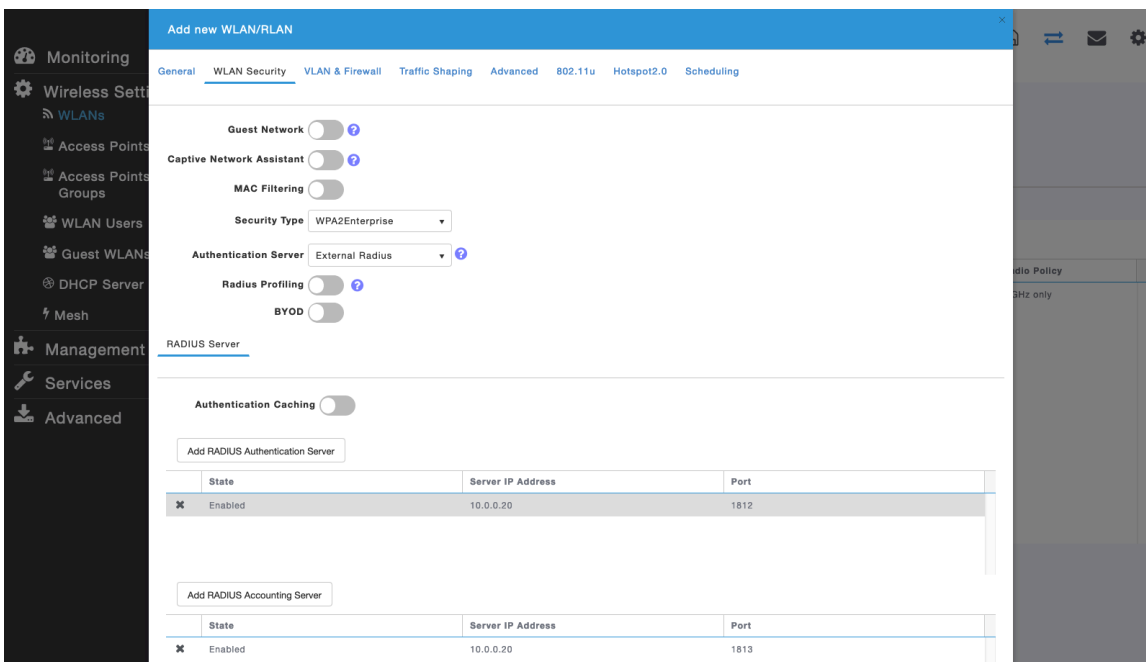
The SSID to be used by the Cisco RoomOS Series can be configured to only apply to a certain 802.11 radio type (e.g. 5 GHz only).

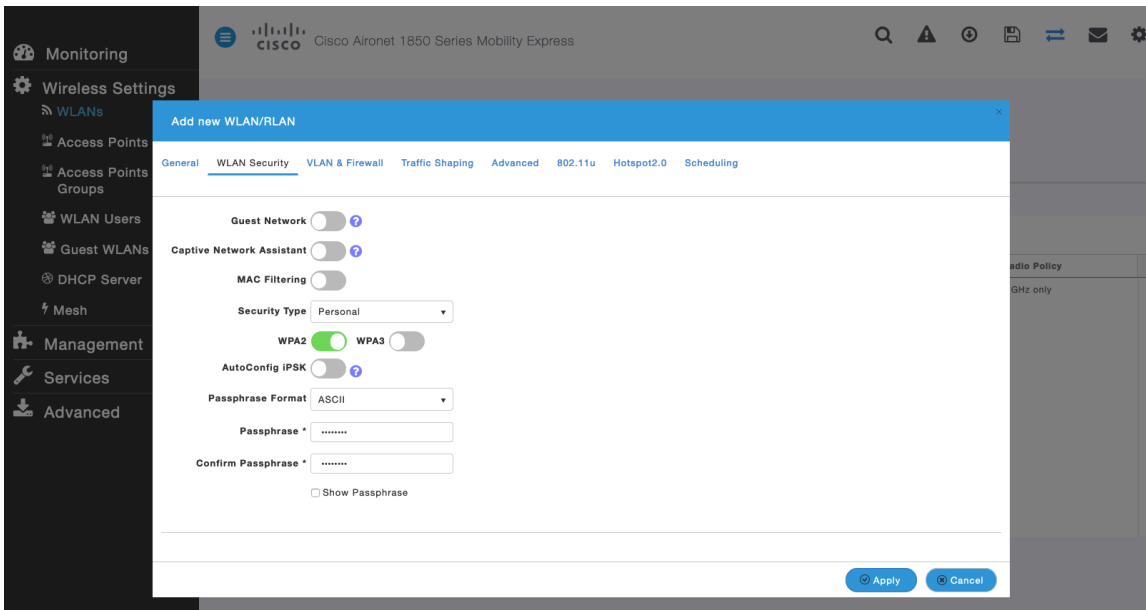
It is recommended to have the Cisco RoomOS Series operate on the 5 GHz band only due to have many channels available and not as many interferers as the 2.4 GHz band has.

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.

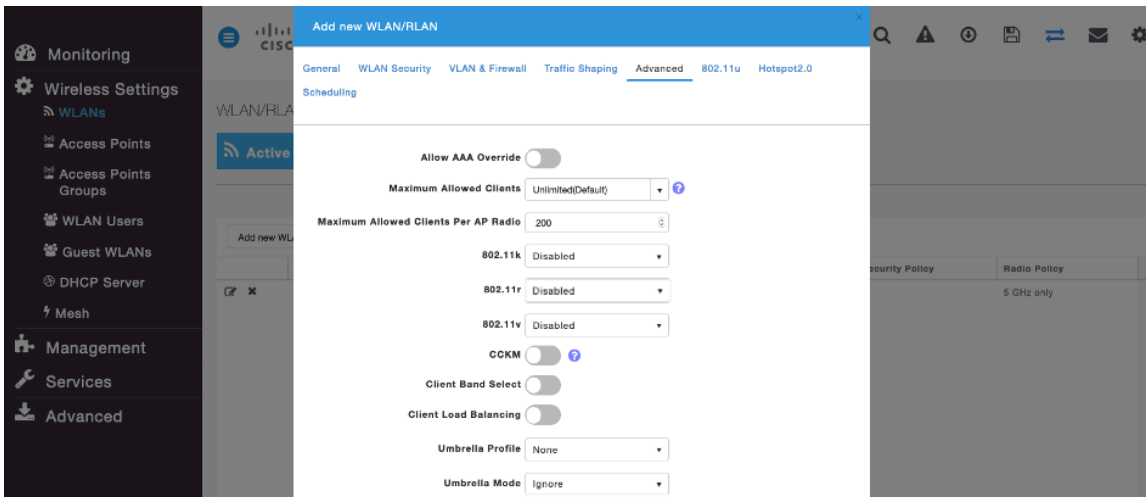


Set Security Type to either **WPA2Enterprise** or **Personal** depending on whether 802.1x or PSK is to be utilized.

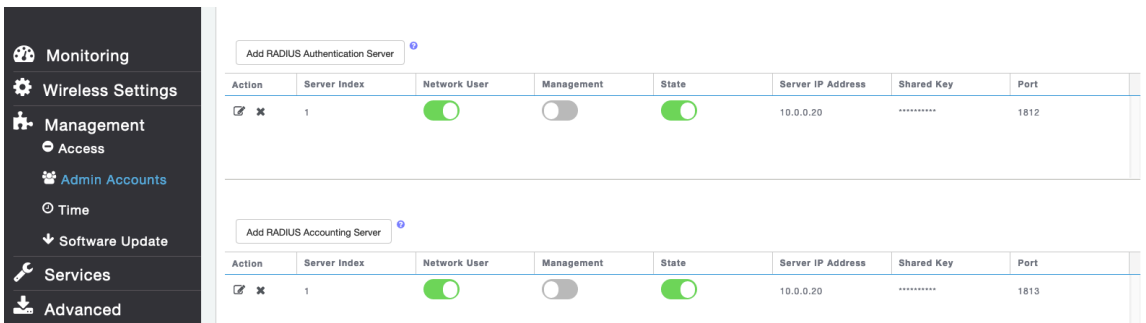
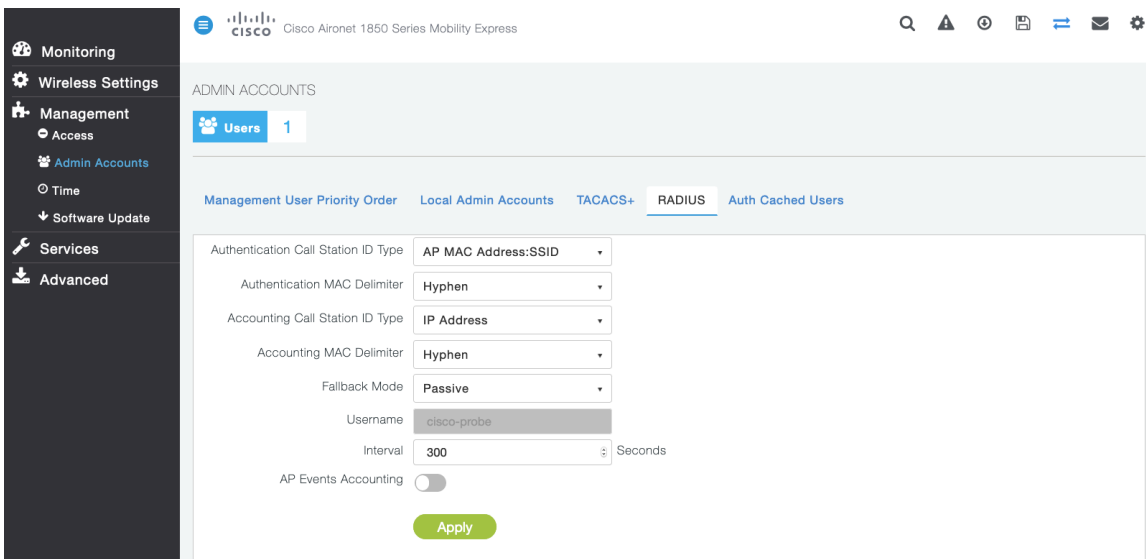
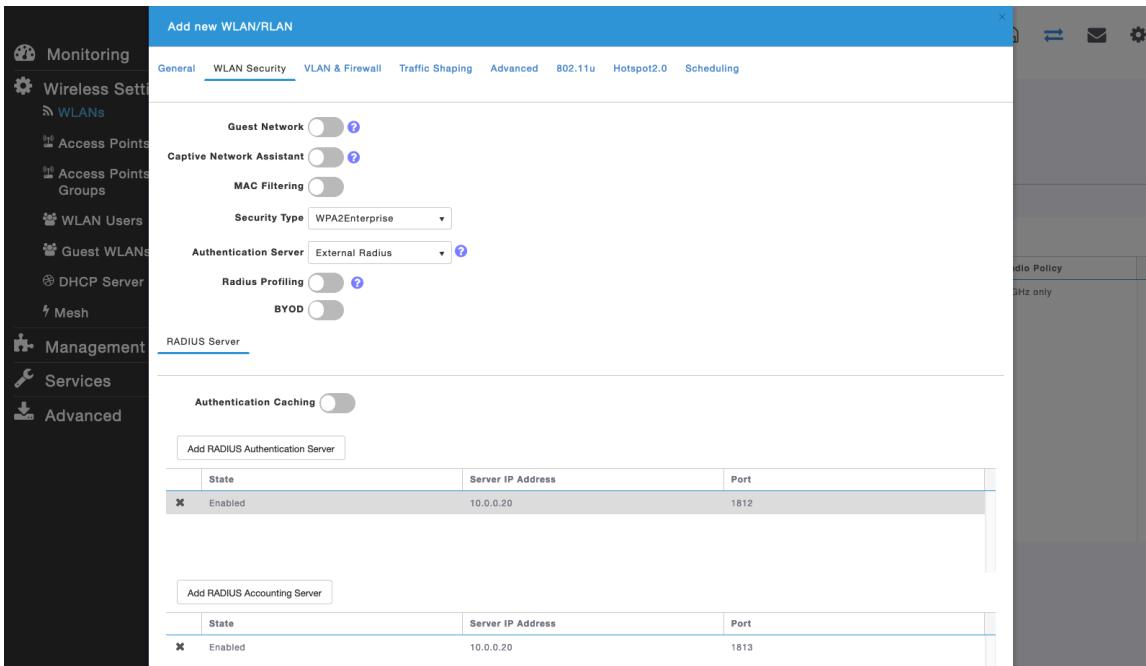




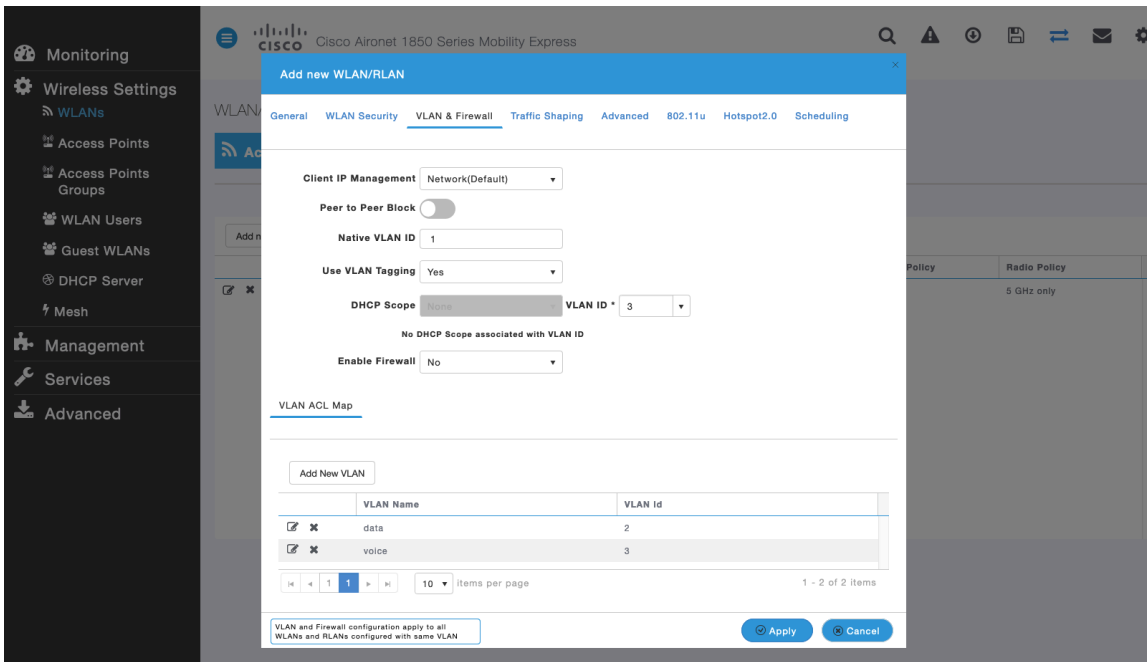
Ensure **Client Band Select** and **Client Load Balancing** are disabled.
 802.11k, 802.11r, and 802.11v are not supported, therefore should be disabled.



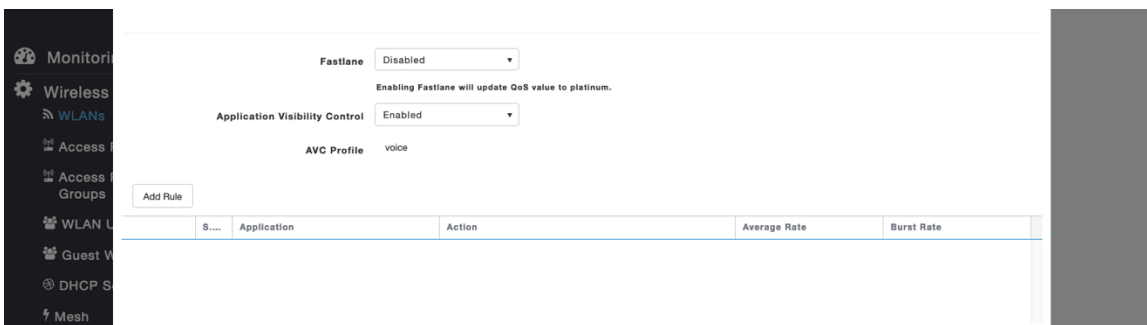
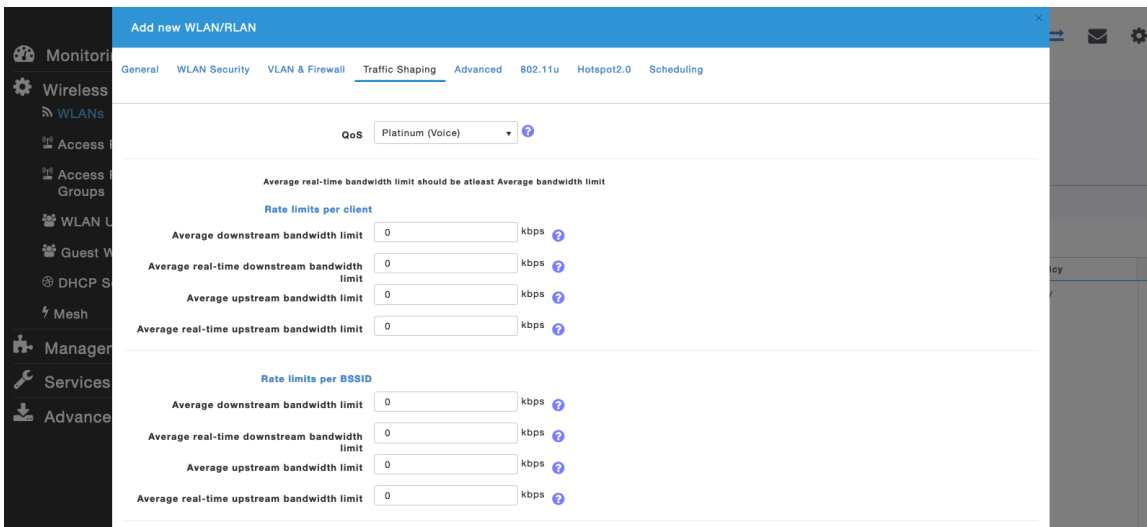
RADIUS Authentication Servers and **Account Servers** can be configured at a per WLAN level to override the global list.



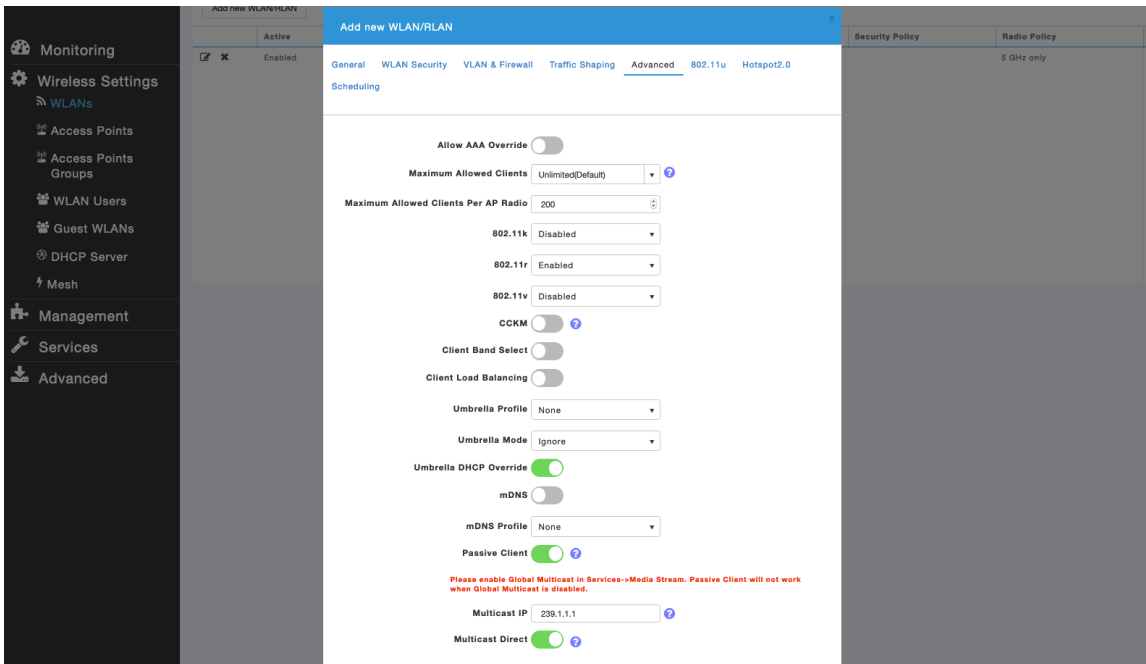
Configure the **Native VLAN ID** and **VLAN ID** for the WLAN as necessary.
 Ensure **Peer to Peer Block** is disabled.



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

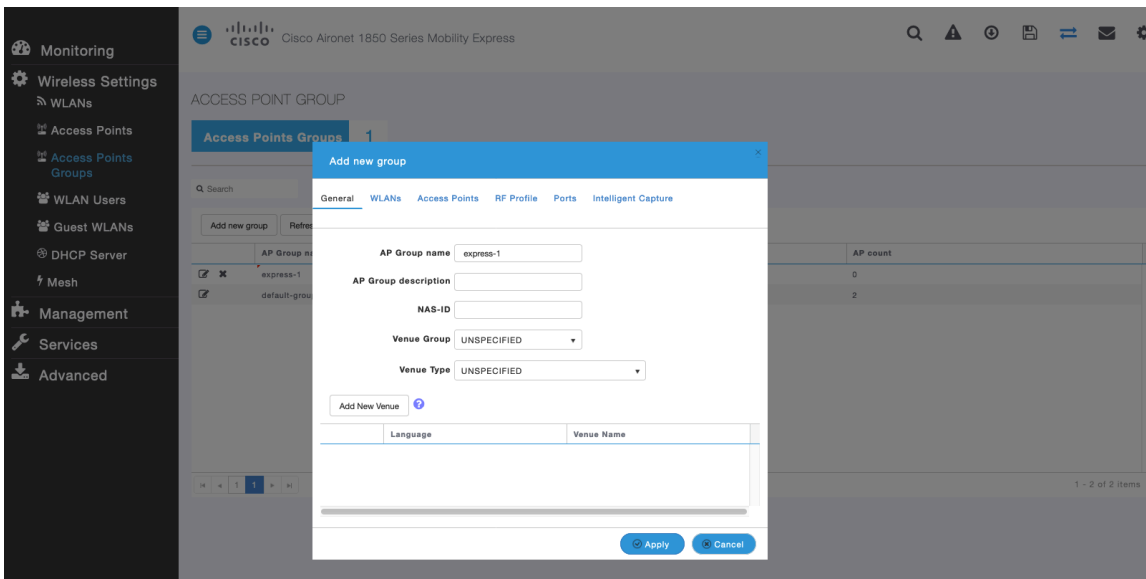


The **Maximum Allowed Clients** and **Maximum Allowed Clients Per AP Radio** can be configured as necessary.

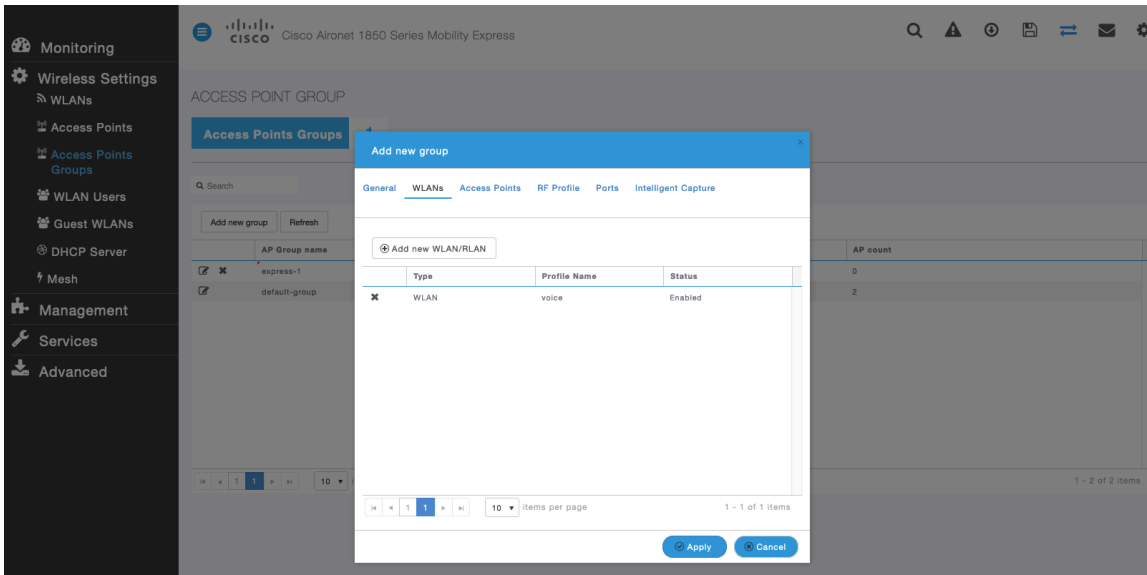
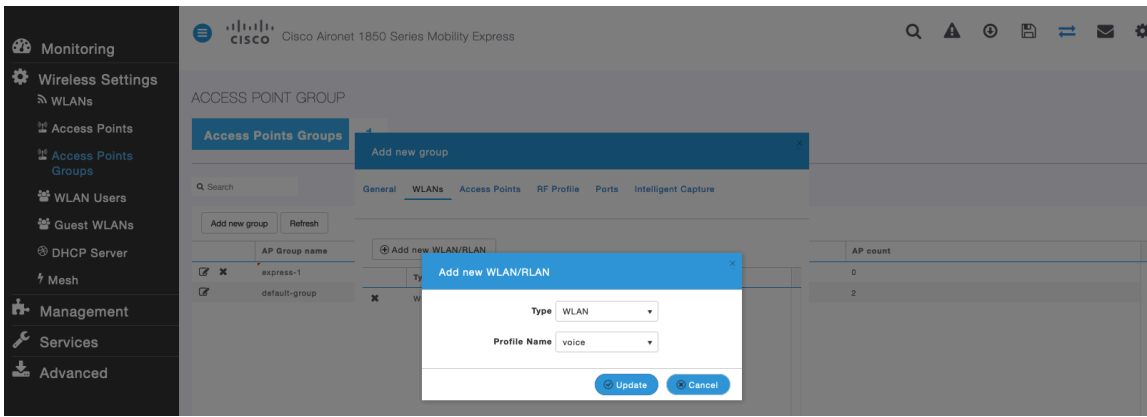


AP Groups

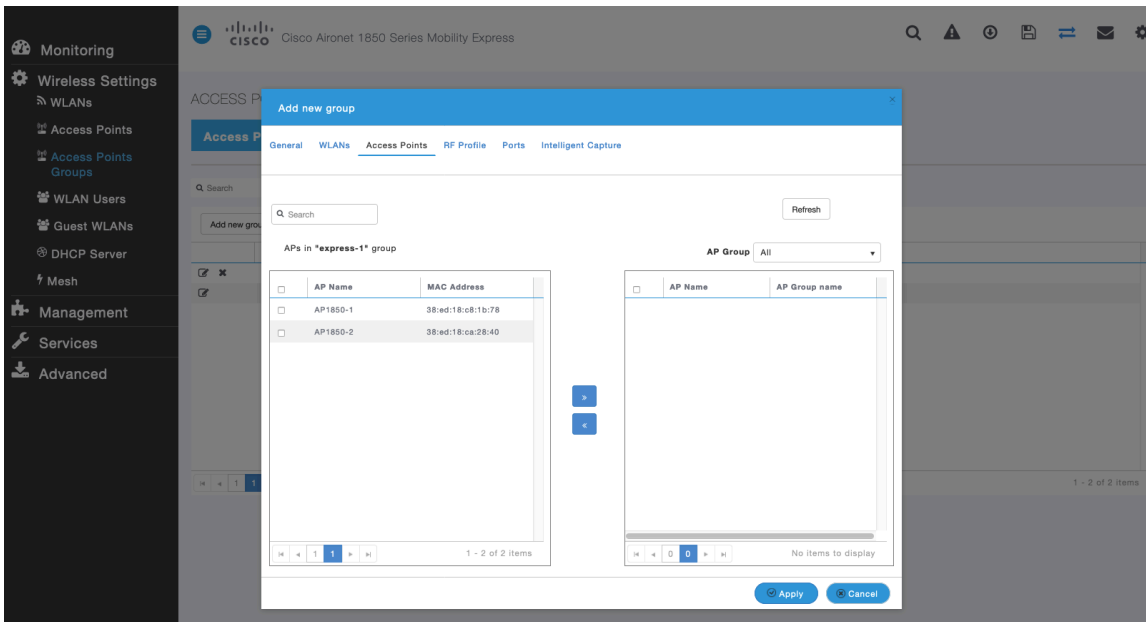
AP Groups can be created to specify which WLANs are to be enabled and which interface they should be mapped to as well as what RF Profile parameters should be used for the access points assigned to the AP Group.



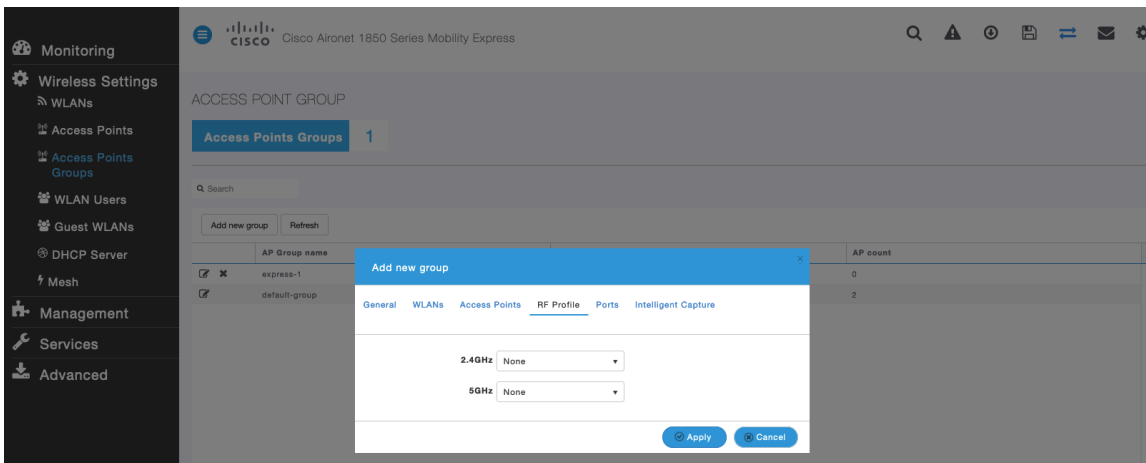
On the **WLANs** tab, select the desired WLANs and interfaces to map to then select **Add**.



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 RoomOS Series to be applied to 5 GHz radios only.

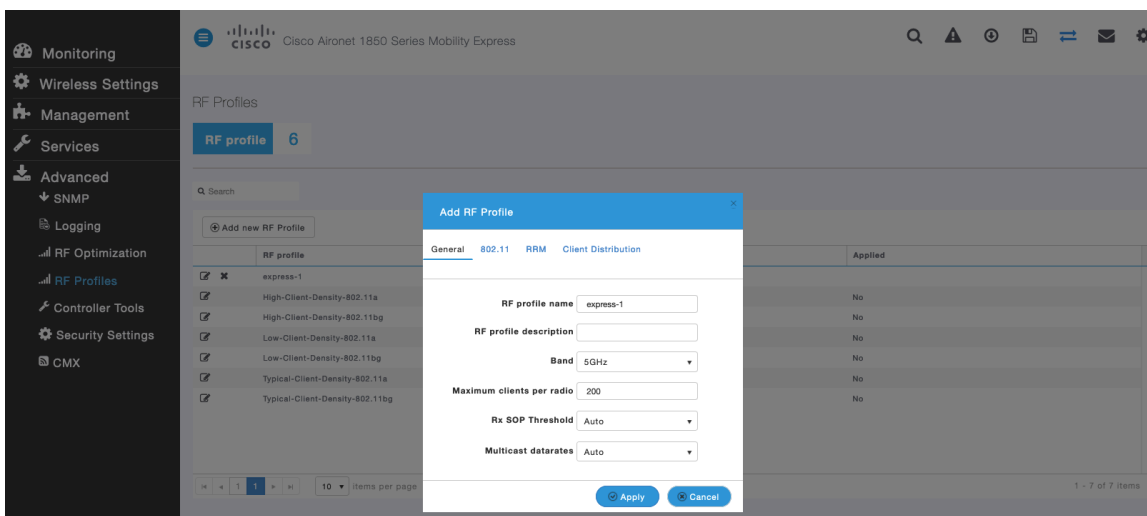
RF Profiles are applied to an AP group once created.

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

Select **5GHZ** or **2.4GHZ** for the **Radio Policy**.

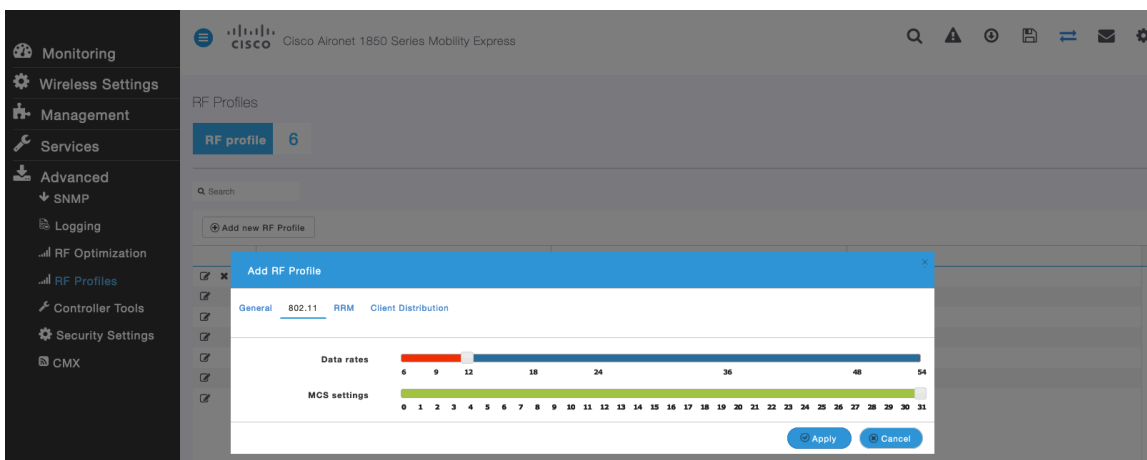
Maximum clients per radio, **Multicast data rates**, and **Rx Sop Threshold** can be configured as necessary.

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

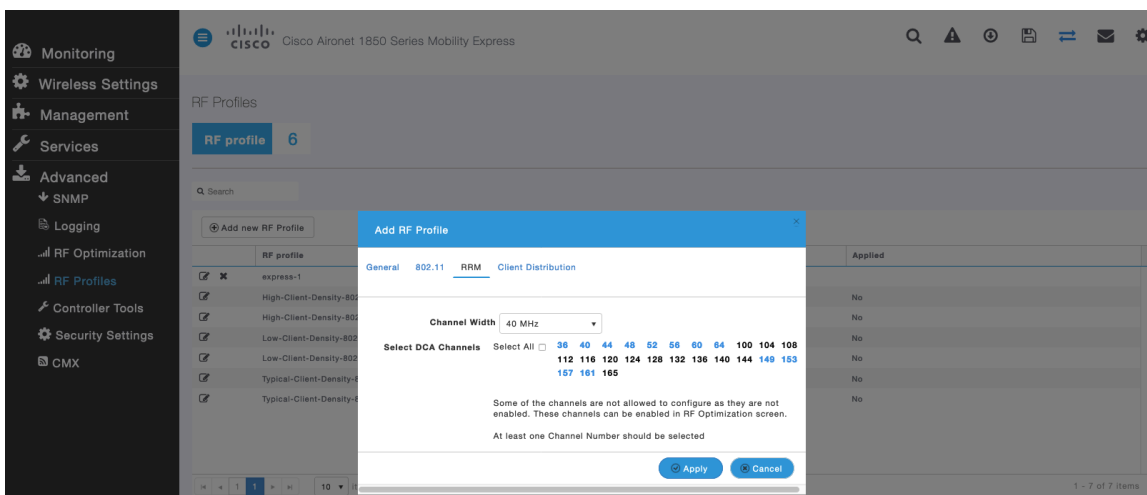


On the **802.11** tab, configure the data rates as necessary.

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

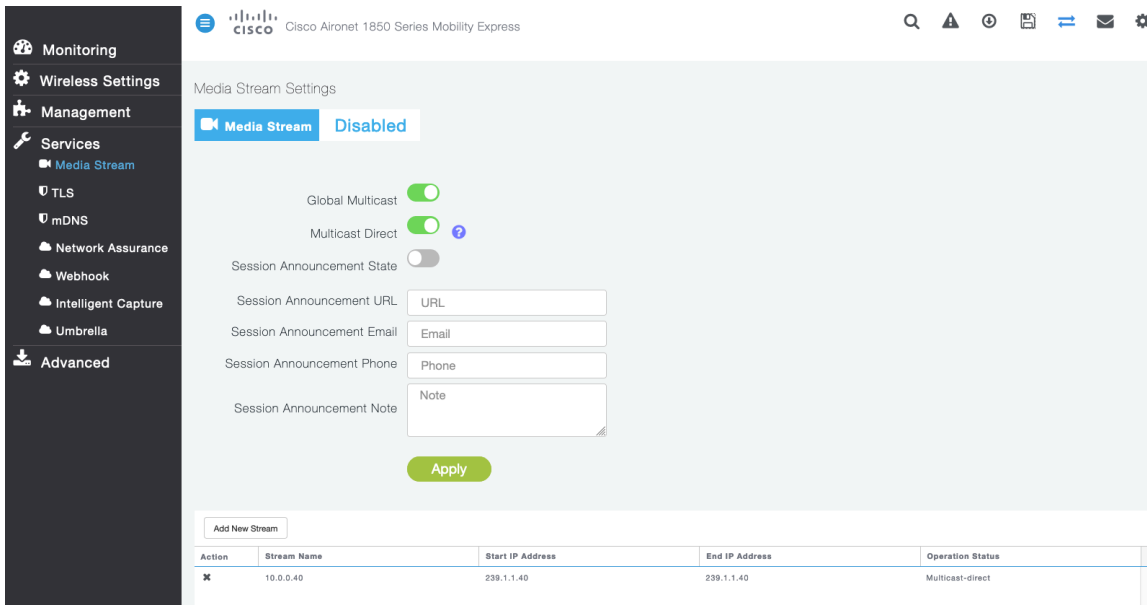


On the **RRM** tab, the **Channel Width** settings and **DCA Channels** can be configured.

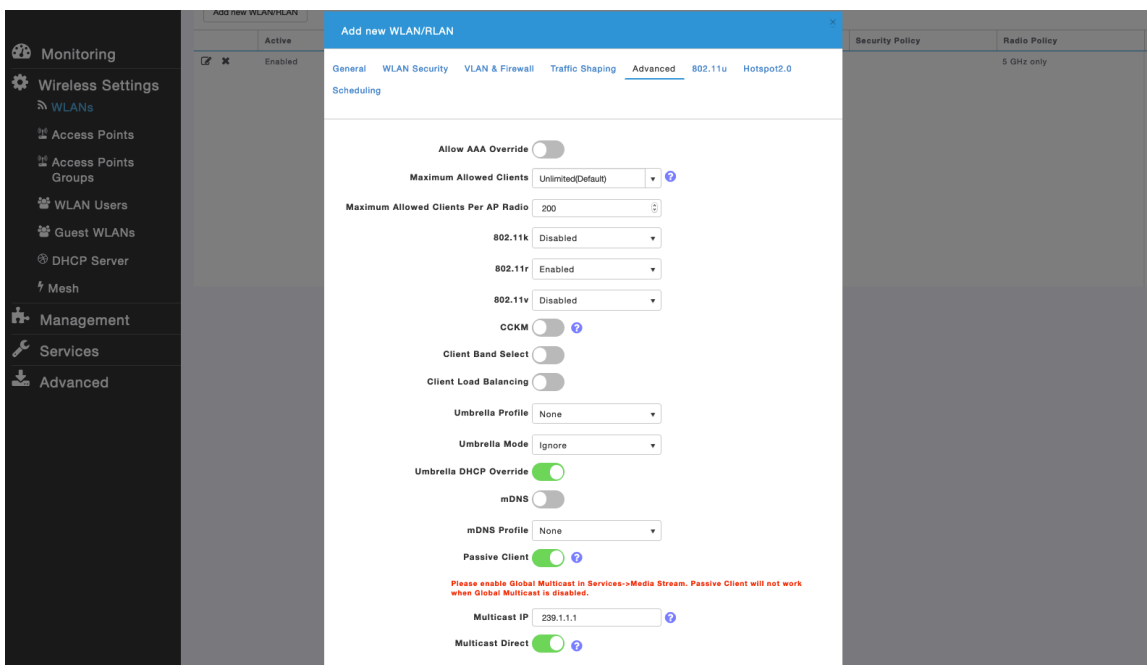


Multicast Direct

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)** and **CCKM** are not configured as mandatory
- Ensure **802.11k** is **Disabled**
- Ensure **802.11v** is **Disabled**
- Configure the **Data Rates** as necessary
- 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 RoomOS Series 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 802.11 a/n/ac network status is **Enabled**.

The screenshot shows the Cisco RoomOS configuration page for Hostname ap-1. The page includes a navigation menu with options like HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY, SERVICES, MANAGEMENT, SOFTWARE, and EVENT LOG. The main content area displays the following information:

Hostname: ap-1
ap-1 uptime is 1 day, 4 hours, 51 minutes

Network Interfaces: Summary

System Settings			
IP Address (Static)	10.9.0.9		
IP Subnet Mask	255.255.255.0		
Default Gateway	10.9.0.2		
MAC Address	18e7.281b.3f54		
Interface Status	GigabitEthernet	Radio0-802.11N2.4GHz	Radio1-802.11AC5GHz
Software Status	Enabled ↑	Disabled ↓	Enabled ↑
Hardware Status	Up ↑	Down ↓	Up ↑
Interface Resets	5	0	8

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 or 802.11ax Access Points.

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

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

RADIO1-802.11AC^{5GHz} STATUS DETAILED STATUS SETTINGS CARRIER BUSY TEST

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 56 minutes

Network Interfaces: Radio1-802.11AC^{5GHz} 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
- Spectrum [Spectrum Information](#)

Max-Client: enable disable (1-255)

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

Data Rates:

6.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
9.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
12.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
18.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
24.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
36.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
48.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
54.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a0.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a1.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a2.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a3.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a4.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a5.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a6.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a7.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a8.1-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a9.1-4Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a0.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a1.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a2.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a3.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a4.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a5.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a6.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a7.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a8.2-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a9.2-4Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
a0.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a1.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a2.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a3.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a4.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a5.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a6.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
a7.3-2Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

a8.3-2Mb/sec Require Enable Disable
a9.3-2Mb/sec Require Enable Disable

MCS Rates:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Enable	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Transmitter Power (dBm): 15 12 9 6 3 Max [Power Translation Table \(mW/dBm\)](#)

Client Power (dBm): Local 15 12 9 6 3 Max

DefaultRadio Channel: Channel 36 5180 MHz

Dynamic Frequency Selection Bands:

Band 1 - 5.150 to 5.250 GHz
Band 2 - 5.250 to 5.350 GHz
Band 3 - 5.470 to 5.725 GHz
Band 4 - 5.725 to 5.825 GHz

Channel Width: 20 MHz

World Mode Multi-Domain Operation: Disable Legacy Dot11d

Country Code: Indoor Outdoor

Radio Preamble: Short Long

Antenna: a-antenna ab-antenna abc-antenna abcd-antenna

Internal Antenna Configuration: Enable Disable
Antenna Gain(dBi): (-128 - 128)

Gratuitous Probe Response(GPR): Enable Disable
Period(Kusec): (10-255)
Transmission Speed:

Traffic Stream Metrics: Enable Disable

Aironet Extensions: Enable Disable

Ethernet Encapsulation Transform: RFC1042 802.1H

Reliable Multicast to WGB: Disable Enable

Public Secure Packet Forwarding: [PSPF must be set per VLAN. See VLAN page](#)

Beacon Privacy Guest-Mode: Enable Disable

Beacon Period: (20-4000 Kusec) Data Beacon Rate (DTIM): (1-100)

Max. Data Retries: (1-128) RTS Max. Retries: (1-128)

Fragmentation Threshold: (256-2346) RTS Threshold: (0-2347)

Root Parent Timeout: (0-65535 sec)

Root Parent MAC 1 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 2 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 3 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 4 (optional): (HHHH.HHHH.HHHH)

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 RoomOS Series.

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 RoomOS Series can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

Enable **WPA2** key management.

The screenshot shows the Cisco RoomOS Security configuration page for the SSID Manager. The page is titled "Security: Global SSID Manager" and is for the SSID "voice". The configuration is for Hostname "ap-1" with an uptime of 1 day, 4 hours, and 33 minutes. The "Current SSID List" shows "voice" selected. The "SSID Properties" section includes fields for SSID (voice), VLAN (3), and Network ID (0-4096). The "Band-Select" section has checkboxes for "Band Select", "Universal Admin Mode", and "Interface" (Radio1-802.11AC5GHz is checked). The "Client Authentication Settings" section includes "Methods Accepted" (Open Authentication with EAP, Network EAP) and "Server Priorities" (EAP and MAC Authentication Servers). The "Client Authenticated Key Management" section has "Key Management" set to "Mandatory" and "Enable WPA" checked.

Security

Admin Access
Encryption Manager
SSID Manager
Dot11u Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 33 minutes

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
data
voice

SSID: voice

VLAN: 3 [Define VLANs](#)

Backup 1:
Backup 2:
Backup 3:

Band-Select: Band Select

Universal Admin Mode: Universal Admin Mode

Interface: Radio0-802.11N2.4GHz
 Radio1-802.11AC5GHz

Network ID: (0-4096)

Delete

Client Authentication Settings

Methods Accepted:

Open Authentication: with EAP

Web Authentication Web Pass

Shared Authentication: < NO ADDITION >

Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Client Authenticated Key Management

Key Management: Mandatory CCKM Enable WPA WPAv2 dot11r

WPA Pre-shared Key: ASCII Hexadecimal

11w Configuration:

11w Association-comeback: (1000-20000)

11w Saquery-retry: (100-500)

IDS Client MFP

Enable Client MFP on this SSID:

AP Authentication

Credentials: [Define Credentials](#)

Authentication Methods Profile: [Define Authentication Methods Profiles](#)

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

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 Capabilities of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

Association Limit (optional): (1-255)

EAP Client (optional):
 Username: Password:

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

Set DataBeacon Rate (DTIM): (1-100)

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N^{2.4GHz}:

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID:

Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

Radio1-802.11AC^{5GHz}:

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID:

Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

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.

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

- Telnet/SSH
- Hot standby
- CDP
- DNS
- Filters
- HTTP
- QOS
- Stream
- SNMP
- SNTP
- VLAN
- ARP Caching
- Band Select
- Auto Config

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 48 minutes

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

Current VLAN List: < NEW >
 VLAN 2
VLAN 3
 VLAN 10 Delete

Create VLAN [Define SSIDs](#)

VLAN ID: (1-4094)

VLAN Name (optional):

Native VLAN
 Enable Public Secure Packet Forwarding
 Radio0-802.11N^{2.4GHz}
 Radio1-802.11AC^{5GHz}
 Management VLAN (if non-native)

Apply Cancel

VLAN Information

View Information for: ⌵

	GigabitEthernet Packets	Radio0-802.11N ^{2.4GHz} Packets	Radio1-802.11AC ^{5GHz} Packets
Received	65884		65884
Transmitted	5462		5462

Refresh

Ensure AES is selected for encryption type.

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Security

Admin Access
Encryption Manager
SSID Manager
Dot11u Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 32 minutes

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 3 [Define VLANs](#)

Encryption Modes

None

WEP Encryption Optional

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

Cipher AES CCMP

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Global Properties

Broadcast Key Rotation Interval: Disable Rotation
 Enable Rotation with Interval: DISABLED (10-10000000 sec)

WPA Group Key Update: Enable Group Key Update On Membership Termination
 Enable Group Key Update On Member's Capability Change

Apply Cancel

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

The screenshot displays the Cisco RoomOS Security Manager configuration page for a server named 'ap-1'. The interface is divided into several sections:

- Backup RADIUS Server:** Includes fields for IP Version (IPV4 selected), Backup RADIUS Server Name, Backup RADIUS Server (Hostname or IP Address), and Shared Secret. Buttons for Apply, Delete, and Cancel are present.
- Corporate Servers:**
 - Current Server List:** A dropdown menu is set to 'RADIUS'. A list shows '< NEW >', '10.0.0.20' (selected), and '10.9.0.9'.
 - Server Configuration:** Fields for IP Version (IPV4 selected), Server Name (10.0.0.20), Server (10.0.0.20), and Shared Secret (masked with dots).
 - Optional Ports:** Authentication Port (optional) is 1812 and Accounting Port (optional) is 1813, both with ranges (0-65535).
- Default Server Priorities:**
 - EAP Authentication:** Priority 1 is 10.0.0.20, Priority 2 and 3 are < NONE >.
 - MAC Authentication:** Priority 1, 2, and 3 are all < NONE >.
 - Accounting:** Priority 1 is 10.0.0.20, Priority 2 and 3 are < NONE >.
 - Admin Authentication (RADIUS):** Priority 1, 2, and 3 are all < NONE >.
 - Admin Authentication (TACACS+):** Priority 1, 2, and 3 are all < NONE >.

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).

Wireless Services

WDS STATUS GENERAL SET-UP SERVER GROUPS

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 50 minutes

Wireless Services: WDS/WNM - General Set-Up

WDS - Wireless Domain Services - Global Properties

Use this AP as Wireless Domain Services

Wireless Domain Services Priority: (1-255)

Use Local MAC List for Client Authentication

WNM - Wireless Network Manager - Global Configuration

Configure Wireless Network Manager

Wireless Network Manager Address: (IP Address or Hostname)

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.

Services

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 48 minutes

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

Current VLAN List Create VLAN [Define SSIDs](#)

< NEW >
VLAN 2
VLAN 3
VLAN 10

VLAN ID: (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N2.4GHz

Radio1-802.11AC5GHz

Management VLAN (If non-native)

VLAN Information

View Information for: VLAN 2

	GigabitEthernet Packets	Radio0-802.11N2.4GHz Packets	Radio1-802.11AC5GHz Packets
Received	65884		65884
Transmitted	5462		5462

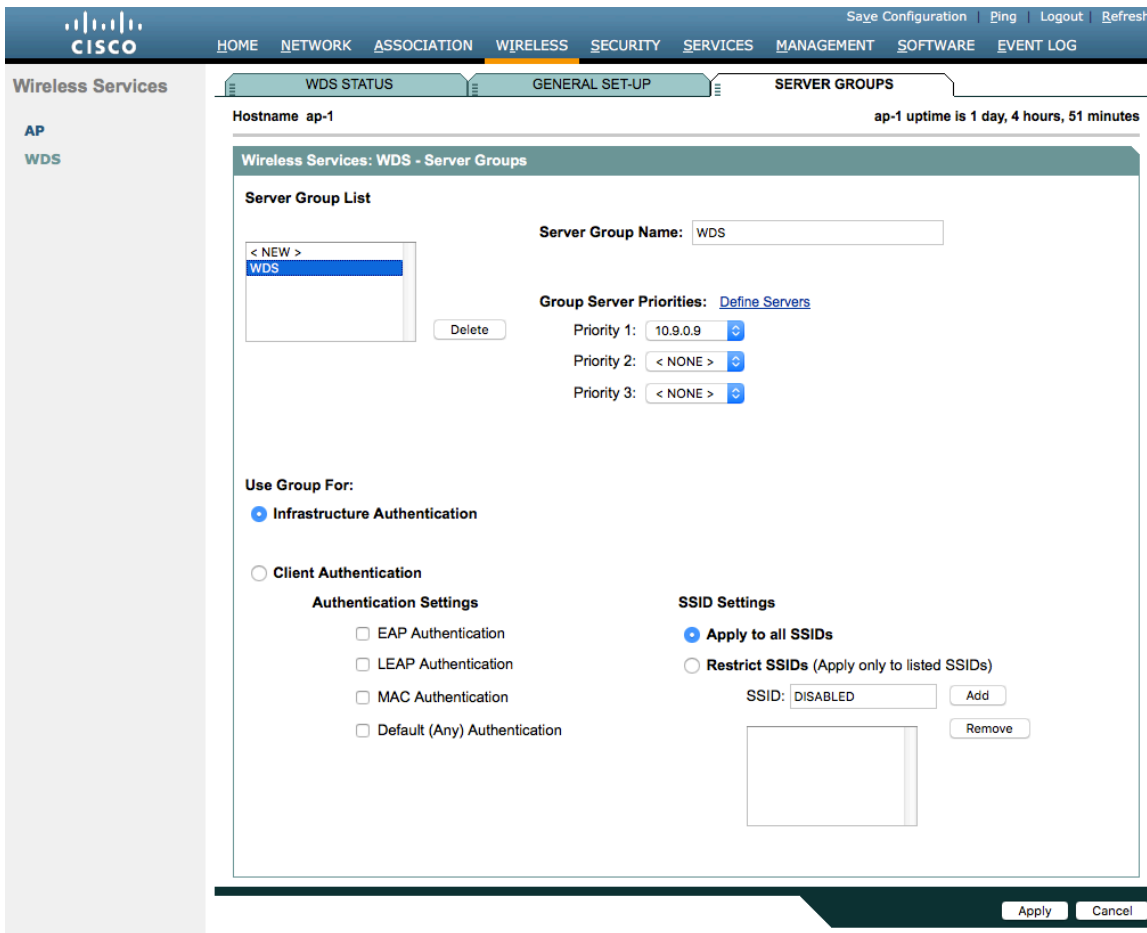
Server groups for Wireless Domain Services must be defined.

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

Cisco RoomOS Series Wireless LAN Deployment Guide

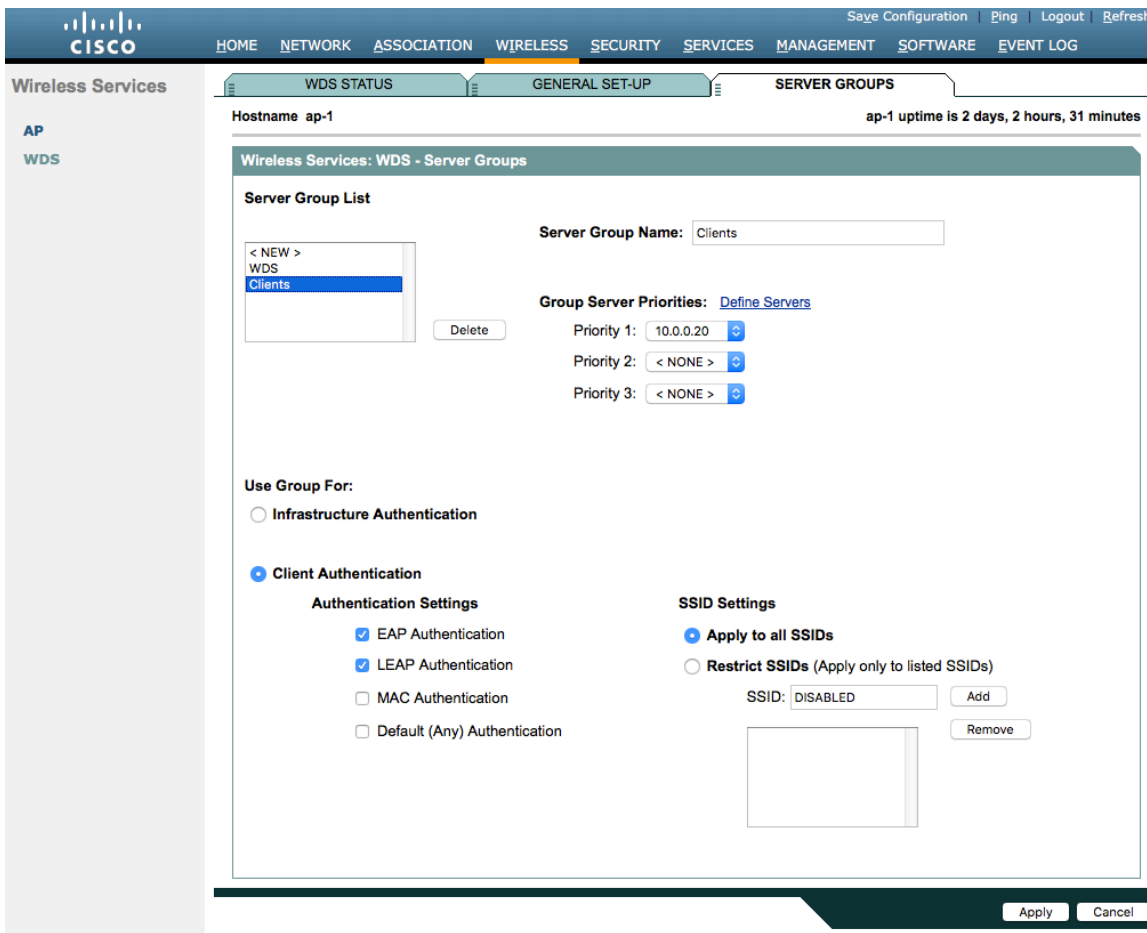
Is recommended to use local RADIUS for infrastructure authentication.

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.

The screenshot displays the Cisco RoomOS configuration page for EAP-FAST Set-Up. The page is divided into three main sections:

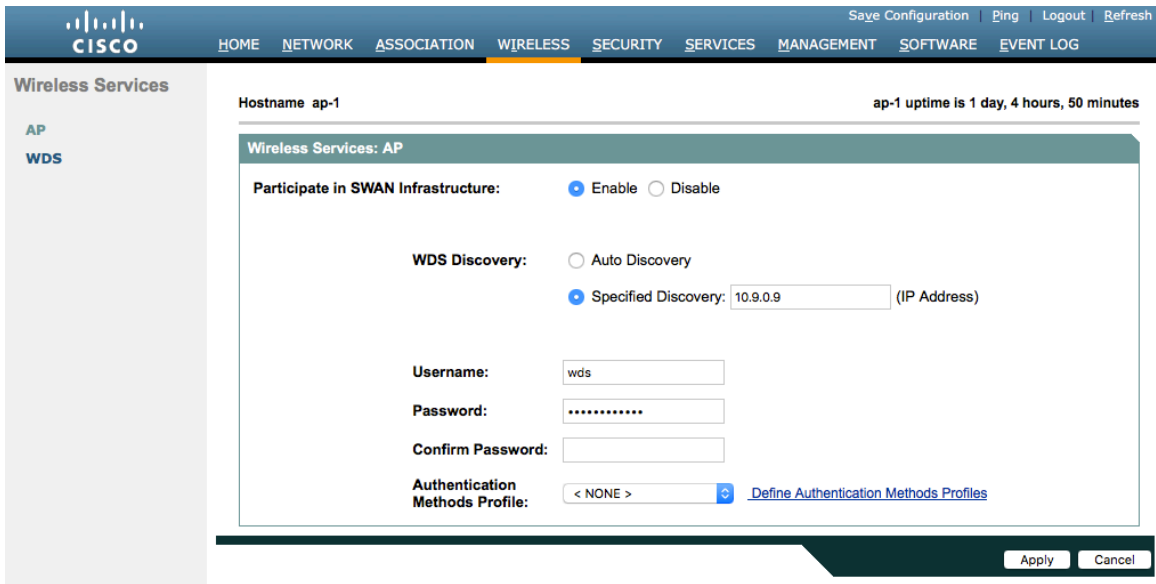
- Local Radius Server Authentication Settings:** This section includes checkboxes for enabling authentication protocols: EAP FAST, LEAP, and MAC. All three are currently checked. There are 'Apply' and 'Cancel' buttons at the bottom right of this section.
- Network Access Servers (AAA Clients):** This section shows a table of current network access servers. One server is listed with the IP address 10.9.0.9. To the right of the table, there are input fields for 'Network Access Server' (IP Address) and 'Shared Secret'. There are 'Apply' and 'Cancel' buttons at the bottom right.
- Individual Users:** This section shows a table of current users. One user is listed with the username 'wds'. To the right of the table, there are input fields for 'Username', 'Password', 'Confirm Password', and 'Group Name'. There are also radio buttons for 'Text' and 'NT Hash' (selected), and a checkbox for 'MAC Authentication Only'. There are 'Apply' and 'Cancel' buttons at the bottom right.

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.

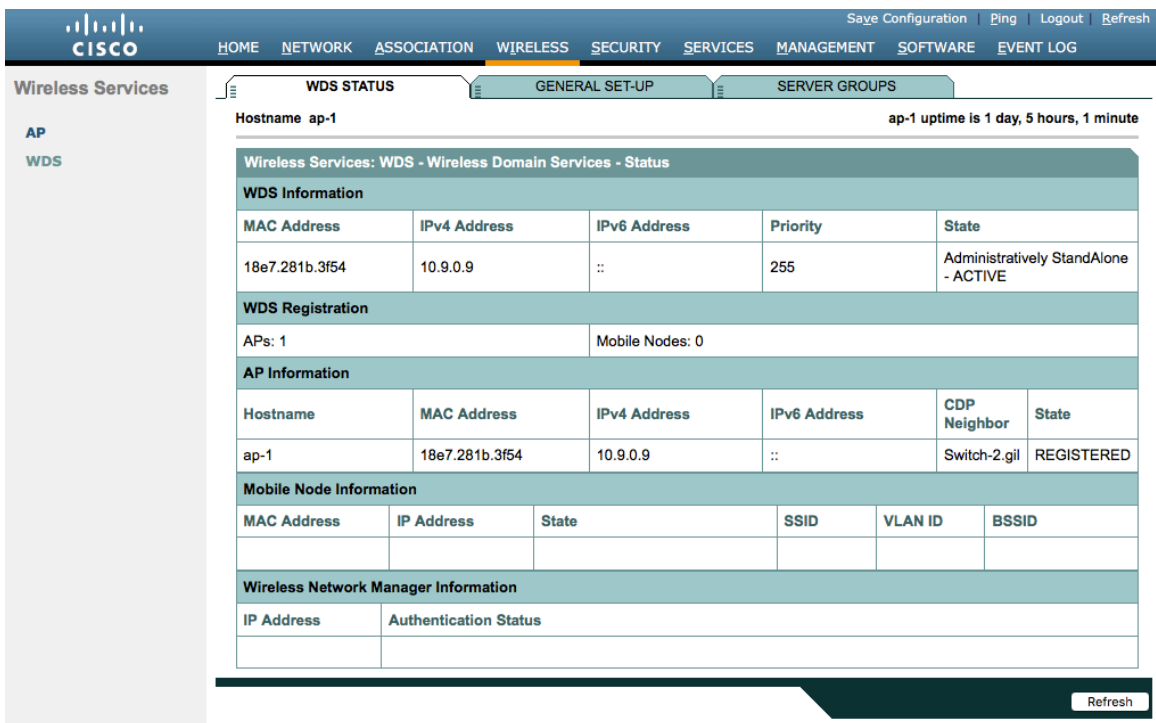
Enable **Participate in SWAN Infrastructure**.

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
admit-traffic
```

Services: QoS Policies - Access Category

Access Category Definition

Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2 ^x -1; x can be 0-10)	AP	4	4	3	2
	Client	4	4	3	2
Max Contention Window (2 ^x -1; x can be 0-10)	AP	10	6	4	3
	Client	10	10	4	3
Fixed Slot Time (0-20)	AP	7	3	1	1
	Client	7	3	2	2
Transmit Opportunity (0-65535 μS)	AP	0	0	3008	1504
	Client	0	0	3008	1504

Optimized Voice WFA Default Apply Cancel

Admission Control for Video and Voice

Video(CoS 4-5)
 Admission Control

Voice(CoS 6-7)
 Admission Control
 Max Channel Capacity (%): 75
 Roam Channel Capacity (%): 6
 Apply Cancel

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.

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QoS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Auto Config

QoS POLICIES

RADIO0-802.11N2.4GHZ ACCESS CATEGORIES RADIO1-802.11AC5GHZ ACCESS CATEGORIES ADVANCED

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 44 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: Voice

Policy Name: Voice

Classifications:

- DSCP - COS Controlled Load (4)
- DSCP - COS Video < 100ms Latency (5)
- DSCP - COS Voice < 10ms Latency (6)

 Delete Classification

Match Classifications:

- IP Precedence: Routine (0)
- IP DSCP: Best Effort (0-63) (0-63)
- IP Protocol 119
- Filter: No Filters defined. [Define Filters.](#)
- Default Classification for Packets on the VLAN: Best Effort (0)

Apply Class of Service

- Best Effort (0) Add
- Best Effort (0) Add
- Best Effort (0) Add
- Best Effort (0) Add

Rate Limiting:

- Bits per Sec.: (8000-2000000000)
- Burst Rate (Bytes): (1000-512000000)
- Conform Action: Transmit
- Exceed Action: Drop

Apply Delete Cancel

Apply Policies to Interface/ VLANs

VLAN 2	Radio0-802.11N2.4GHz	Radio1-802.11AC5GHz	GigabitEthernet0
Incoming		Data	Data
Outgoing		Data	Data
VLAN 3	Radio0-802.11N2.4GHz	Radio1-802.11AC5GHz	GigabitEthernet0
Incoming		Voice	Voice
Outgoing		< NONE >	< NONE >
VLAN 10	Radio0-802.11N2.4GHz	Radio1-802.11AC5GHz	GigabitEthernet0
Incoming		< NONE >	< NONE >
Outgoing		< NONE >	< NONE >

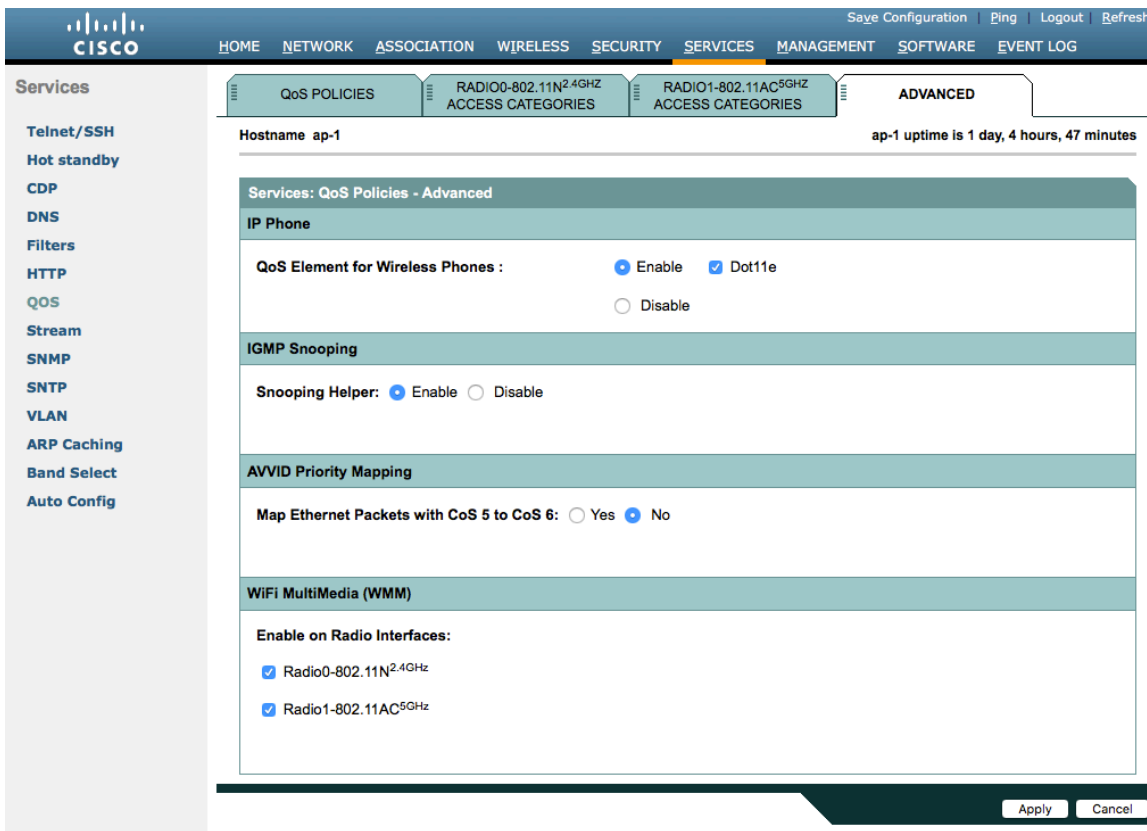
Apply Cancel

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.

The screenshot shows the Cisco RoomOS configuration interface for the 'Stream' service. The top navigation bar includes 'HOME', 'NETWORK', 'ASSOCIATION', 'WIRELESS', 'SECURITY', 'SERVICES', 'MANAGEMENT', 'SOFTWARE', and 'EVENT LOG'. The left sidebar lists various services: Telnet/SSH, Hot standby, CDP, DNS, Filters, HTTP, QOS, Stream (selected), SNMP, SNTP, VLAN, ARP Caching, Band Select, and Auto Config. The main content area is titled 'Services: Stream' and contains two sections: 'Packet Handling per User Priority' and 'Low Latency Packet Rates'. The 'Packet Handling' section is a table with columns for 'User Priority', 'Packet Handling', and 'Max Retries for Packet Discard'. The 'Low Latency Packet Rates' section lists various rates from 6.0Mb/sec to 54.0Mb/sec, each with radio buttons for 'Nominal', 'Non-Nominal', and 'Disable' (which is selected for all).

User Priority	Packet Handling	Max Retries for Packet Discard
CoS 0 (Best Effort)	Reliable	NO DISCARD (0-128)
CoS 1 (Background)	Reliable	NO DISCARD (0-128)
CoS 2 (Spare)	Reliable	NO DISCARD (0-128)
CoS 3 (Excellent)	Reliable	NO DISCARD (0-128)
CoS 4 (Controlled Load)	Reliable	NO DISCARD (0-128)
CoS 5 (Video)	Reliable	NO DISCARD (0-128)
CoS 6 (Voice)	Reliable	NO DISCARD (0-128)
CoS 7 (Network Control)	Reliable	NO DISCARD (0-128)

Low Latency Packet Rates:

- 6.0Mb/sec : Nominal Non-Nominal Disable
- 9.0Mb/sec : Nominal Non-Nominal Disable
- 12.0Mb/sec : Nominal Non-Nominal Disable
- 18.0Mb/sec : Nominal Non-Nominal Disable
- 24.0Mb/sec : Nominal Non-Nominal Disable
- 36.0Mb/sec : Nominal Non-Nominal Disable
- 48.0Mb/sec : Nominal Non-Nominal Disable
- 54.0Mb/sec : Nominal Non-Nominal Disable

Buttons: Apply, Cancel

Power Management

Proxy ARP will help answer any ARP requests on behalf of the device.

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.

The screenshot shows the Cisco RoomOS configuration interface for the 'ARP Caching' service. The top navigation bar and left sidebar are identical to the previous screenshot. The main content area is titled 'Services: ARP Caching' and contains two settings: 'Client ARP Caching' (set to 'Enable') and 'Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known' (checked).

Client ARP Caching: Enable Disable

Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known

Buttons: Apply, Cancel

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
!
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
rsa keypair 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 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 BV11
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 BV11
!
radius-server local
nas 10.9.0.9 key 7 <REMOVED>
user wds nhash 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 BV11
!
line con 0
access-class 111 in
line vty 0 4
access-class 111 in
transport input all
!
ntp server 10.0.0.2
ntp broadcast client
end

```

Cisco Meraki Access Points

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

- 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**.

Search Dashboard

Create network

Setup network

Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization. ⓘ


Network name:

Network type: ⓘ

Network configuration:

- Default Meraki configuration
- Bind to template No templates to bind to ⓘ
- Clone from existing network

Select devices from inventory



You have no unused devices

Add new devices or go to the inventory page to select devices that are already in networks

[Add devices](#) [Go to inventory](#)

[Create network](#)

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**.

Claim by serial and/or order number

Enter one or more serial/order numbers (one per row). [Where can I find these numbers?](#)

Close

Claim

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

Inventory

View used and unused devices in your organization. You can [claim](#) new devices to add the list below.

Add to ... Unclaim Unused Used Both Search inventory

Existing network

Meraki WLAN

New network

Add to existing

Model ^	Claimed on
9K7	MR53
	4/29/2020 2:59 PM

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

Add access points

Add access points from your organization's inventory. When you claim an order by order number, the devices in the order will be added to your inventory. When you claim a device by its serial number, that device will be added to your inventory. Once in your inventory, you can add devices to your network(s).

Search inventory

MAC address	Serial number	Model ^	Claimed on
<input checked="" type="checkbox"/> 88:15:44:60:18:8c	Q2MD-MWQS-J9K7	MR53	4/29/2020 2:59 PM

Add access points

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 RoomOS Series; 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.

The screenshot shows the Cisco Meraki configuration dashboard. On the left is a navigation sidebar with the Meraki logo and menu items: NETWORK, Meraki WLAN (selected), Network-wide, Wireless (highlighted), and Organization. The main content area is titled 'Configuration overview' and shows 'SSIDs' with 'Showing 4 of 15 SSIDs. [Show all my SSIDs.](#)'

meraki-voice	
Enabled	enabled
Name	rename
Access control	edit settings
Encryption	802.1X with Meraki RADIUS
Sign-on method	None
Bandwidth limit	unlimited
Client IP assignment	Local LAN
Clients blocked from using LAN	no
Wired clients are part of Wi-Fi network	no
VLAN tag	3
VPN	Disabled
Splash page	
Splash page enabled	no
Splash theme	n/a

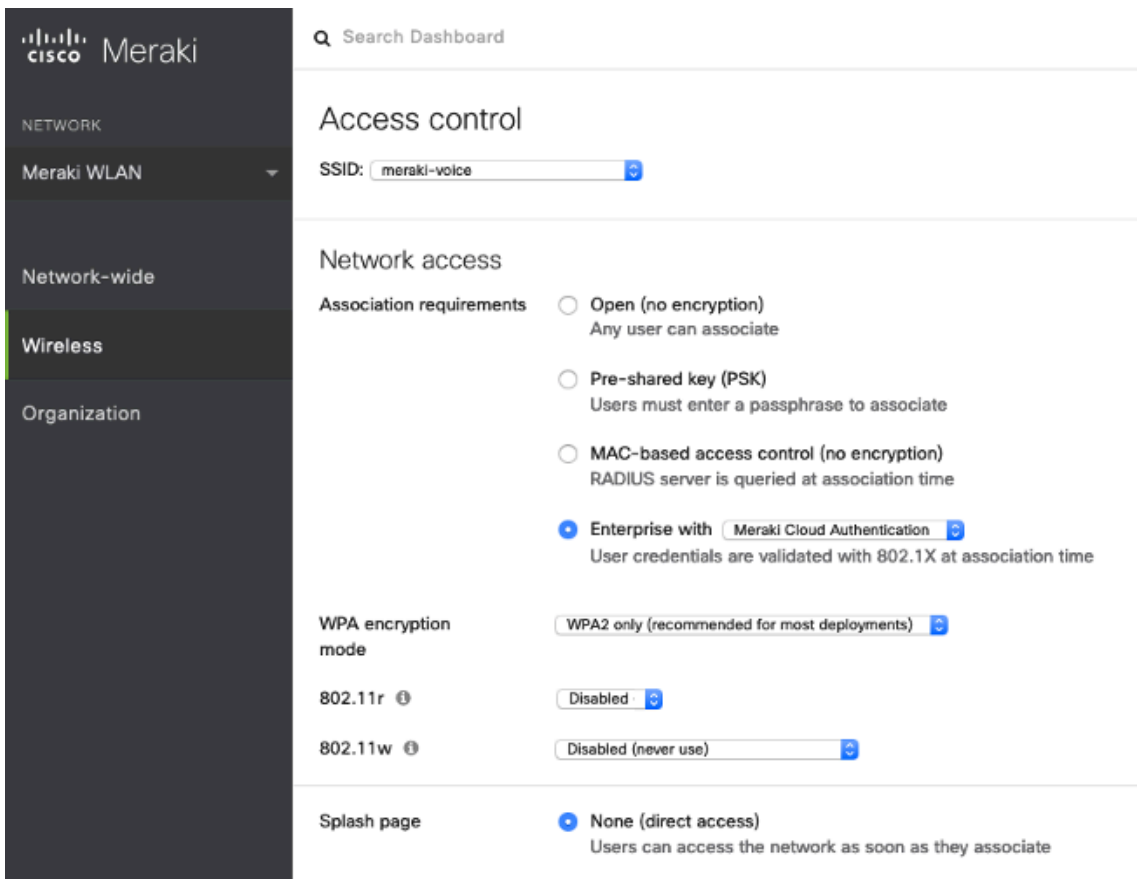
On the **Wireless > Configure > Access control** page, select **WPA2-Enterprise** to enable 802.1x authentication.

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.

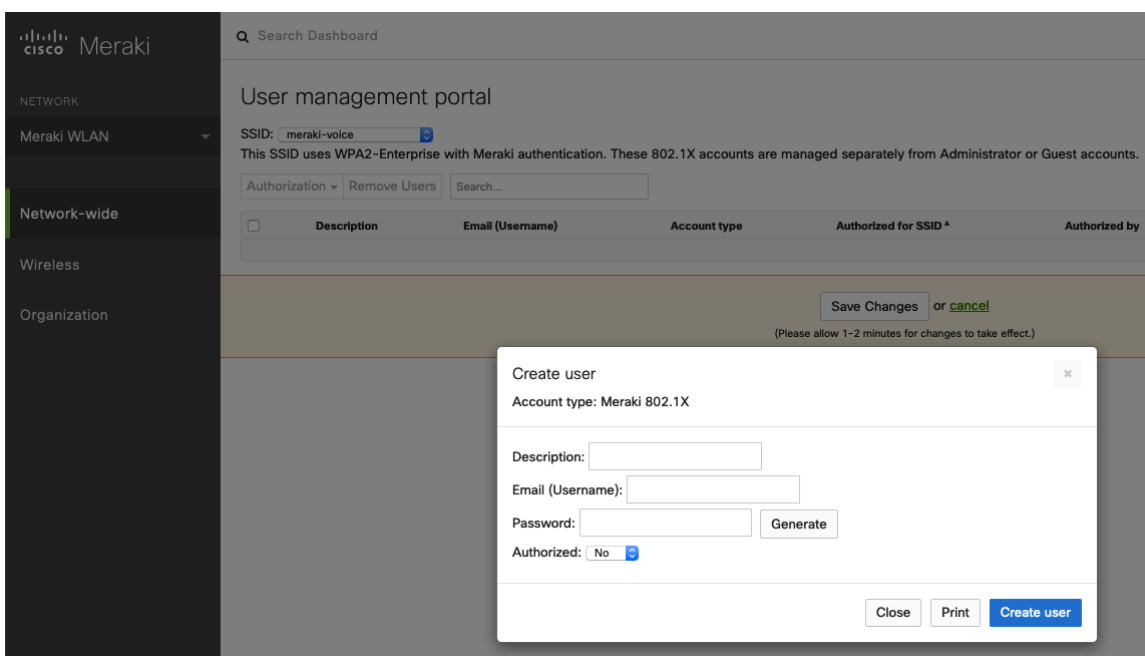
Other authentication types (e.g. Pre-Shared Key) are available as well.

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



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 RoomOS Series 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 RoomOS Series 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
```

The screenshot shows the Meraki configuration page for 'Addressing and traffic'. The left sidebar has 'Wireless' selected. The main content area has several sections:

- Client IP assignment:** Radio buttons for 'NAT mode: Use Meraki DHCP', 'Bridge mode: Make clients part of the LAN' (selected), 'Layer 3 roaming', 'Layer 3 roaming with a concentrator', and 'VPN: tunnel data to a concentrator'.
- VLAN tagging:** A dropdown menu set to 'Use VLAN tagging'.
- VLAN ID:** A table with columns 'AP tags', 'VLAN ID', and 'Actions'. The first row is 'All other APs' with '3' in the 'VLAN ID' column and an 'Add VLAN' link in the 'Actions' column.
- Content filtering:** A dropdown menu set to 'Don't filter content'.
- Bonjour forwarding:** A dropdown menu set to 'Enable Bonjour Gateway'.

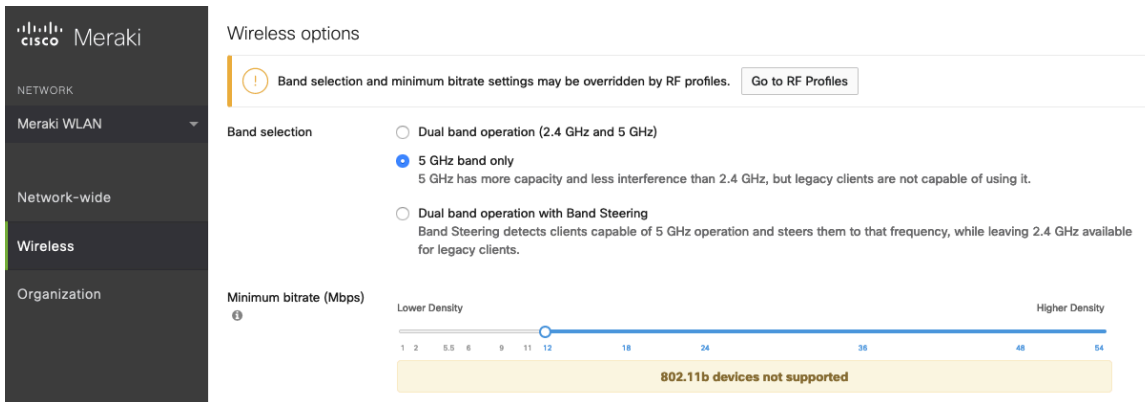
On the **Wireless > Configure > Access control** page, the frequency band for the SSID to be used by the Cisco RoomOS Series can be configured as necessary.

It is recommended to select **5 GHz band only** to have the Cisco RoomOS Series 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.

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

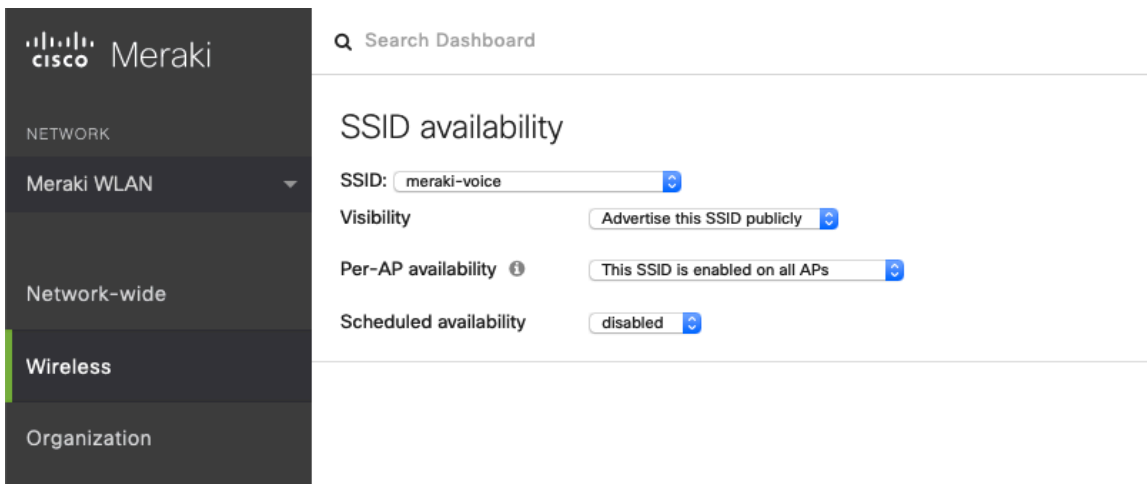
Cisco Meraki access points currently utilize a DTIM period of **1** with a beacon period of **100 ms**; which both are non-configurable.



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

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

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

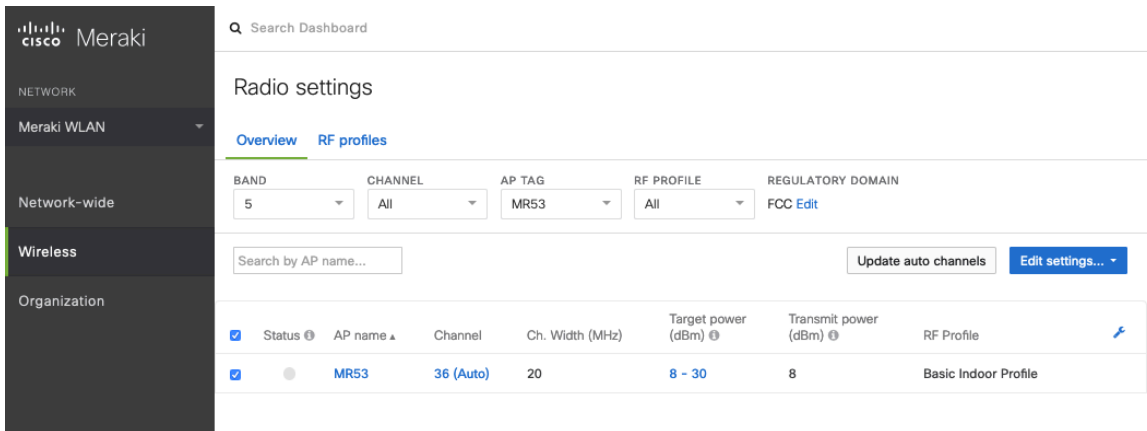


Radio Settings

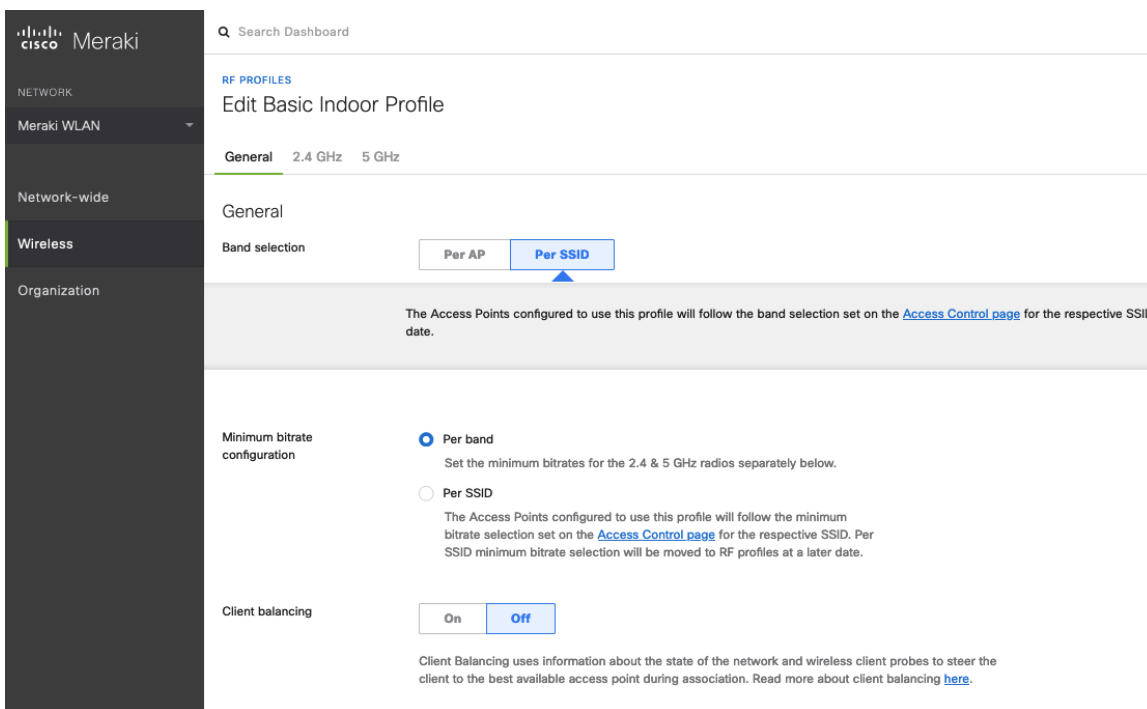
On the **Wireless > Configure > Radio settings** page, access points can be configured in bulk or by individual access point to define the automatic or manual channel and transmit power settings.

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 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.

General 2.4 GHz **5 GHz**

5 GHz radio settings

Turn off 5GHz radio See band selection above.

Channel width **Auto** **Manual**

Manual 5 GHz channel width

Disable auto channel width by manually selecting a channel width for the APs in this profile.

- 20 MHz (19 channels)
Recommended for High Density deployments and environments expected to encounter DFS events. More unique channels available, reducing chance of interference.
- 40 MHz (10 channels)
For low to medium density deployments.
- 80 MHz (5 channels)
For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.

Channel assignment method **AutoChannel** will assign radios to channels with low interference.
[Change channels used by AutoChannel...](#)

Radio transmit power range (dBm)

Transmit shorter distance Transmit farther

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

[Set RX-SOP...](#)

Minimum bitrate

Lower Density Higher Density

6 9 12 18 24 36 48 54

Change 5 GHz channels used by AutoChannel

Available channels for AutoChannel

If you deselect a channel, AutoChannel will not assign it to any AP with this profile. Click on a channel to toggle its selection.

Channel Width	UNII-1	UNII-2	UNII-2-Extended	Weather Radar	UNII-3	ISM
20 MHz	36, 40, 44, 48, 52, 56, 60, 64		100, 104, 108, 112	116, 120, 124, 128, 132, 136, 140, 144	149, 153, 157, 161	165
40 MHz	38, 46	54, 62	102, 110	118, 126	134, 142	151, 159
80 MHz	42	58	106	122	138	155

DFS channels **Deselect DFS channels**

Cancel **Done**

For low to medium density deployments.

- 80 MHz (5 channels)
For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.

Firewall and Traffic Shaping

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

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

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

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

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

The screenshot shows the Cisco Meraki dashboard interface. On the left is a dark sidebar with navigation options: NETWORK, Meraki WLAN, Network-wide, Wireless (highlighted), and Organization. The main content area is titled 'Firewall & traffic shaping' and is for the 'meraki-voice' SSID. It is divided into three sections: 'Block IPs and ports', 'Block applications and content categories', and 'Traffic shaping rules'. The 'Block IPs and ports' section shows 'Layer 2 LAN isolation' as 'Disabled (bridge mode only)' and a table of 'Layer 3 firewall rules' with two entries: 'Allow Any Local LAN Any Wireless clients accessing LAN' and 'Allow Any Any Any Default rule'. The 'Block applications and content categories' section shows 'Layer 7 firewall rules' as 'There are no rules defined for this SSID'. The 'Traffic shaping rules' section shows 'Per-client bandwidth limit' and 'Per-SSID bandwidth limit' both set to 'unlimited', and 'Shape traffic' set to 'Shape traffic on this SSID'.

Q Search Dashboard

Firewall & traffic shaping

SSID: meraki-voice

Block IPs and ports

Layer 2 LAN isolation Disabled (bridge mode only)

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
	Allow	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules There are no rules defined for this SSID.
[Add a layer 7 firewall rule](#)

Traffic shaping rules

Per-client bandwidth limit unlimited [details](#) Enable SpeedBurst

Per-SSID bandwidth limit unlimited [details](#)

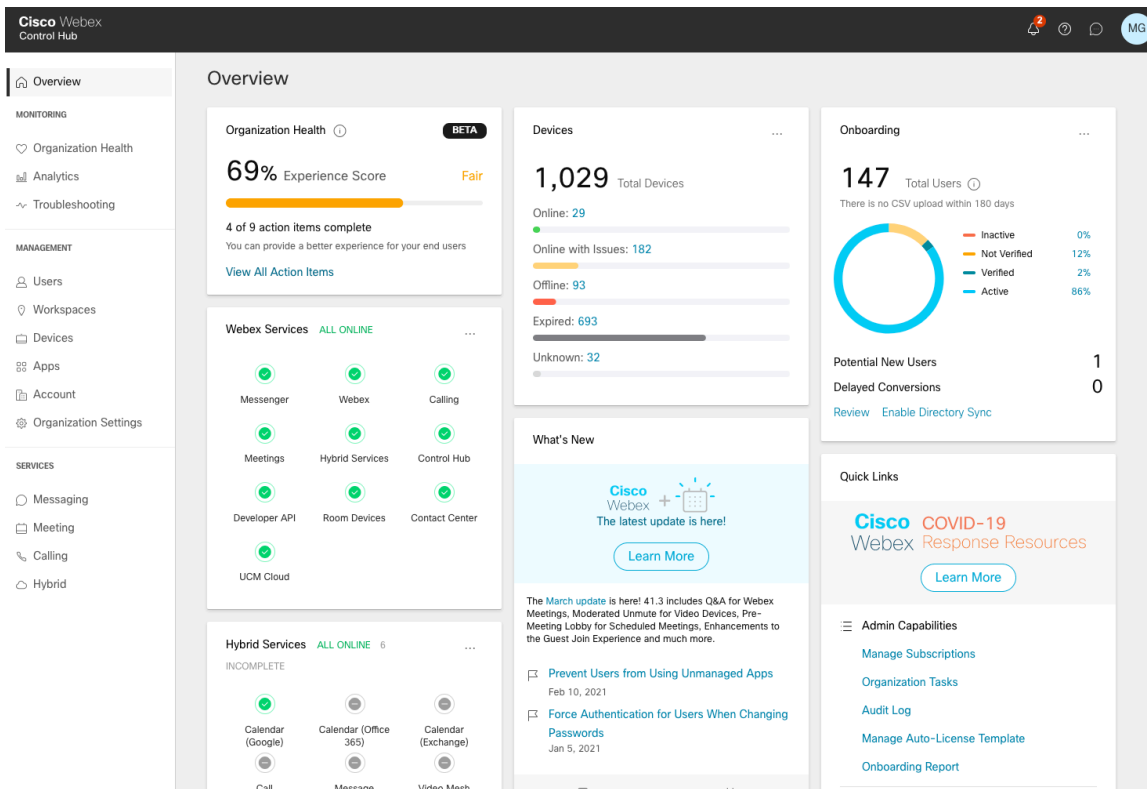
Shape traffic Shape traffic on this SSID

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

Configuring Cisco Call Control

Webex

Webex enables cloud registration, therefore a VPN connection is not required as long as the Cisco RoomOS Series has direct internet connectivity.



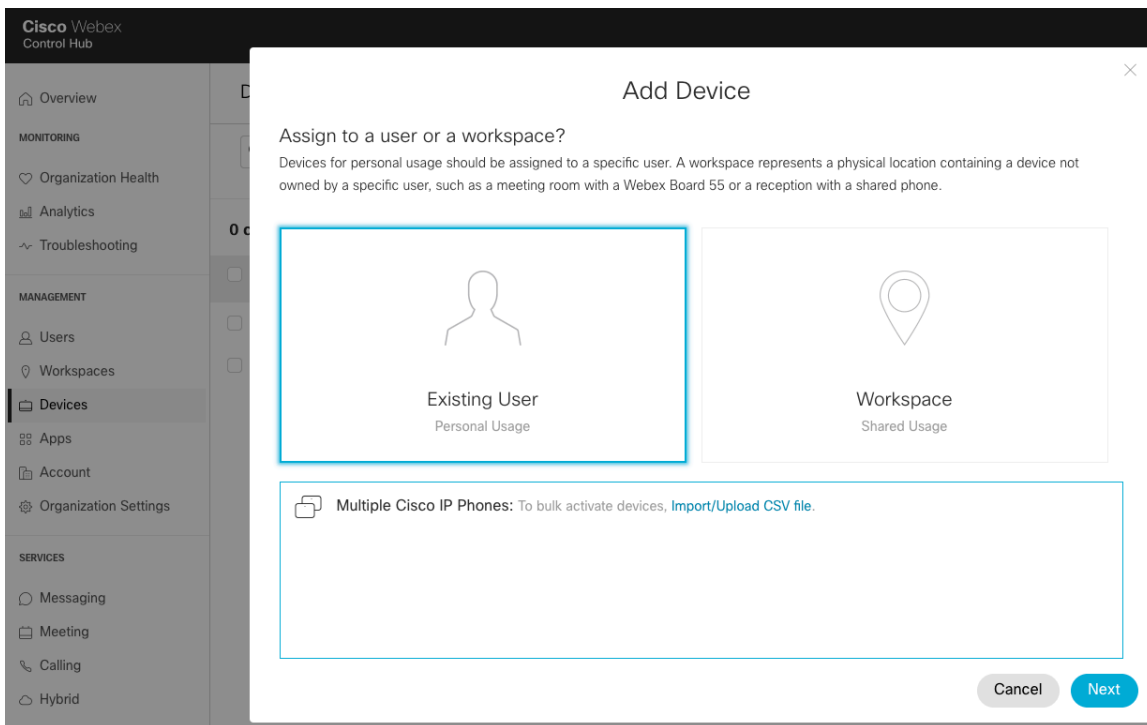
A Cisco RoomOS Series can be added to Webex and assigned to a user for personal usage or as a workspace for shared usage.

Personal Usage

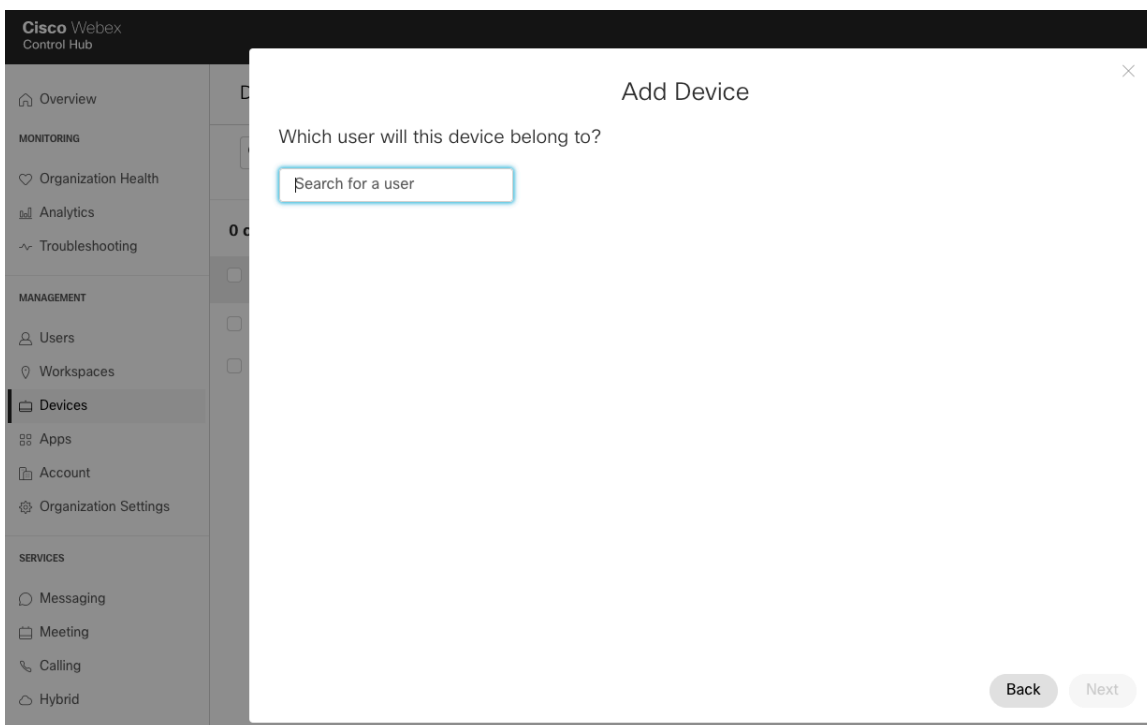
A Cisco RoomOS Series can be configured for a user for personal usage via **Devices**.

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

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



Search for the user to assign the Cisco RoomOS Series to, then click **Next**.



The **Activation Code** to enter into the Cisco RoomOS Series will then be displayed.

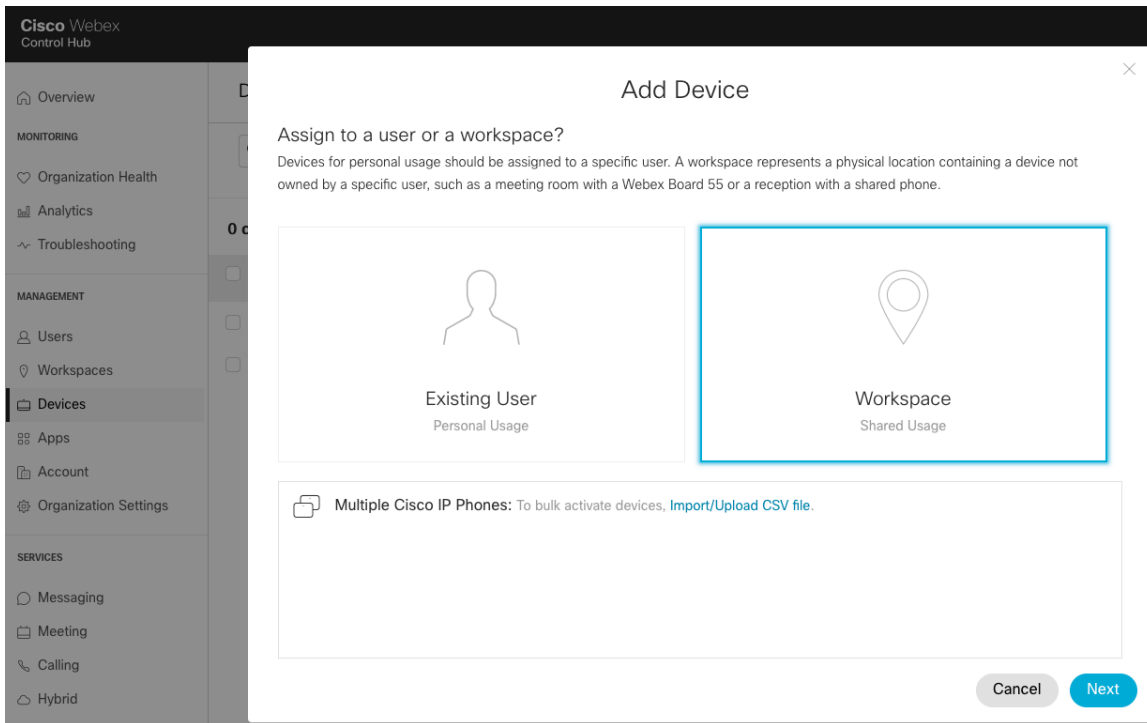
Select the user via **Users** to configure or modify services.

Shared Usage

A Cisco RoomOS Series can be configured as a workspace either via **Devices** or **Workspaces**.

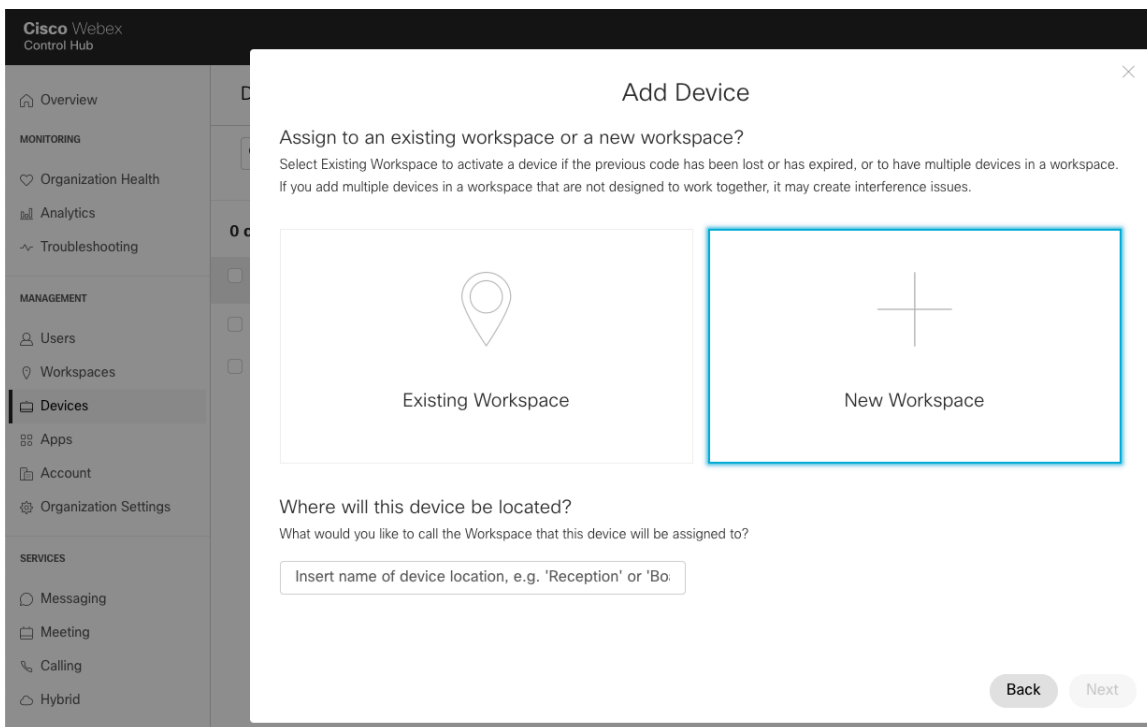
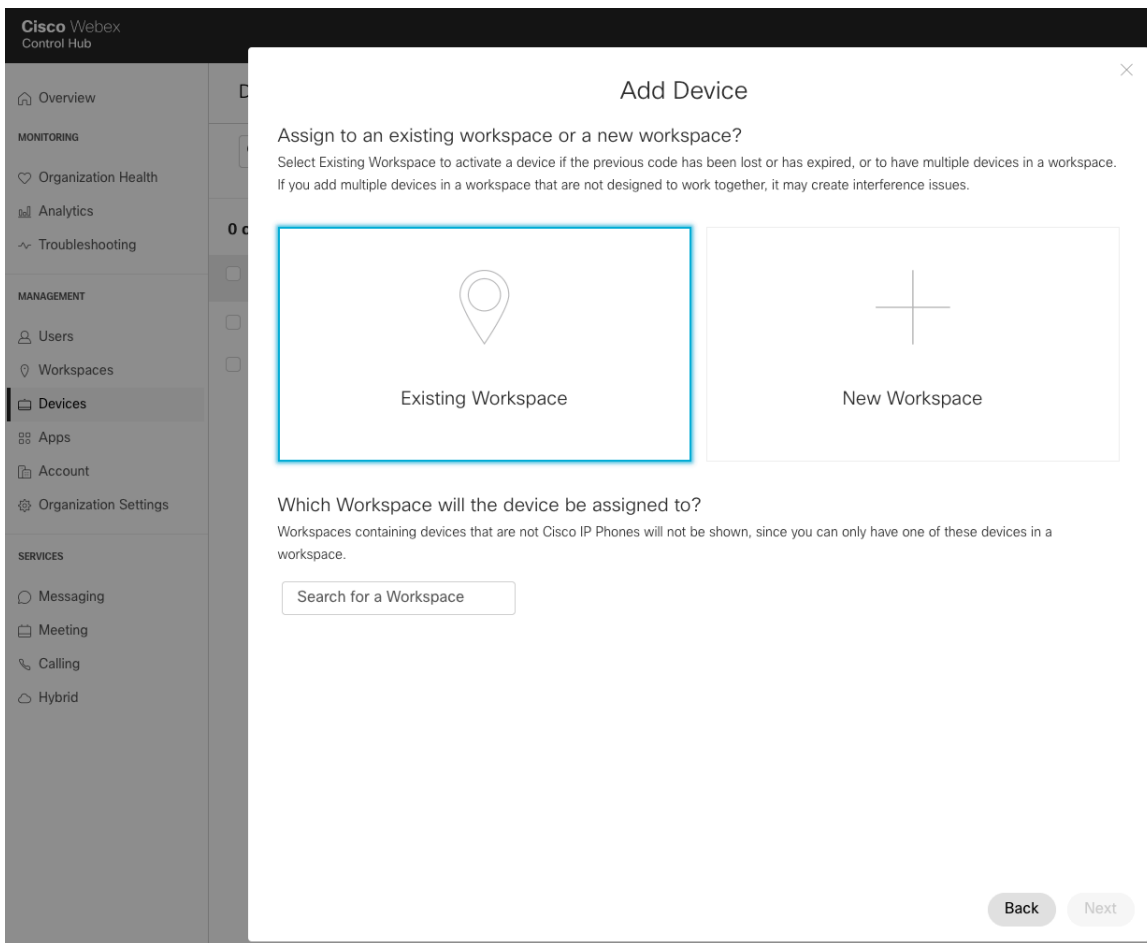
To add a workspace via **Devices**, navigate to **Devices**, then select **Add Device**.

On the next screen, select **Workspace**, then click **Next**.

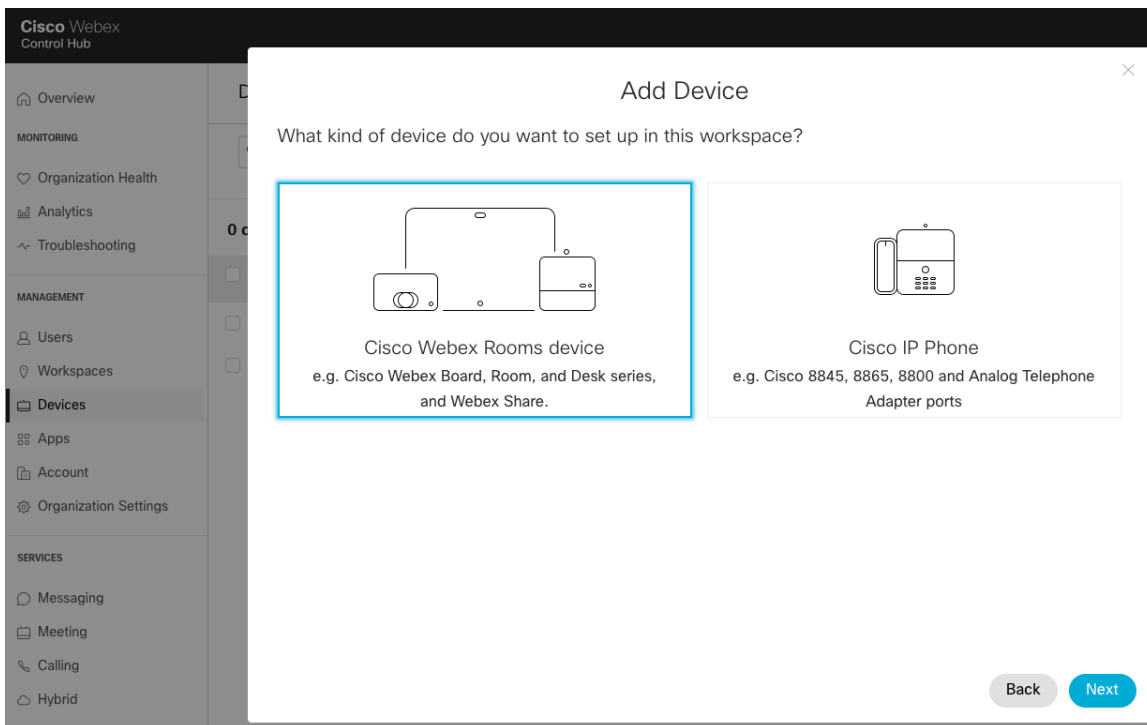


Select either **Existing Workspace** or **New Workspace**.

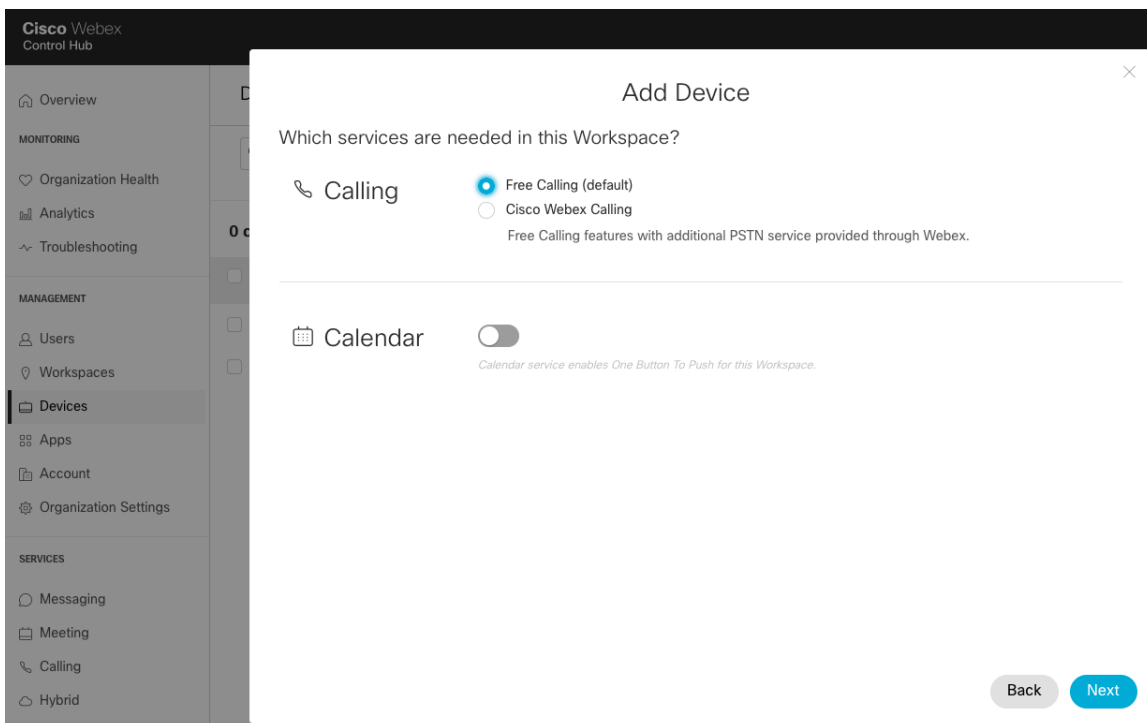
Depending on which option is selected, either search for or enter the workspace name, then click **Next**.



If **New Workspace** was selected prior, select **Webex Rooms** device, then click **Next**.



Additionally, if **New Workspace** was selected, configure the desired services, then click **Next**.



The **Activation Code** to enter into the Cisco RoomOS Series will then be displayed.

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

For information on network requirements for Webex, refer to the **Network Requirements for Webex Services** document at this URL:

<https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Services>

For more information, see the **Cisco RoomOS Series Administrator Guide**.

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html>

Cisco Unified Communications Manager

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

Device Enablement

To enable the Cisco RoomOS Series device types 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 RoomOS Series to the Cisco Unified Communications Manager it must be provisioned using the Ethernet MAC address as the Wireless LAN MAC is used for Wi-Fi connectivity only.

The Ethernet MAC address can be found by navigating to **About** or **Settings** > **About this device** on the Cisco RoomOS Series.

Device Information	
<input checked="" type="checkbox"/> Device is trusted	
MAC Address*	<input type="text"/>
Description	<input type="text"/>
Device Pool*	-- Not Selected -- View Details
Common Device Configuration	< None > View Details
Phone Button Template*	-- Not Selected --
Common Phone Profile*	Standard Common Phone Profile

Device Pools

When creating a new Cisco RoomOS Series, 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.

Device Pool Settings	
Device Pool Name*	<input type="text" value="Default"/>
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >

Roaming Sensitive Settings	
Date/Time Group*	CMLocal
Region*	Default
Media Resource Group List	< None >
Location	< None >
Network Locale	< None >
SRST Reference*	Disable
Connection Monitor Duration***	<input type="text"/>
Single Button Barge*	Default
Join Across Lines*	Default
Physical Location	< None >
Device Mobility Group	< None >
Wireless LAN Profile Group	< None > View Details

Phone Button Templates

When creating a new Cisco RoomOS Series, a **Phone Button Template** must be configured.

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

Phone Button Template Information

Button Template Name *

Button Information

Button	Feature
1	Line ** <input type="text" value="Line"/>

Security Profiles

When creating a new Cisco RoomOS Series, a **Device Security Profile** must be configured.

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

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

The Cisco RoomOS Series has a Manufacturing Installed Certificate (MIC), which can be utilized with a security profile as well.

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

BLF Presence Group*

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

Digest User

Media Termination Point Required

Unattended Port

Require DTMF Reception

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

Phone Security Profile Information	
Product Type:	Cisco Webex Desk Pro
Device Protocol:	SIP
Name *	Cisco Webex Desk Pro - Standard SIP Non-Secure Pr
Description	Cisco Webex Desk Pro - Standard SIP Non-Secure Pr
Nonce Validity Time *	600
Device Security Mode	Non Secure
Transport Type *	TCP+UDP
<input type="checkbox"/> Enable Digest Authentication <input type="checkbox"/> TFTP Encrypted Config <input type="checkbox"/> Exclude Digest Credentials in Configuration File	
Phone Security Profile CAPF Information	
Authentication Mode *	By Null String
Key Order *	RSA Only
RSA Key Size (Bits) *	2048
EC Key Size (Bits)	< None >
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.	
Parameters used in Phone	
SIP Phone Port *	5060

SIP Profiles

When creating a new Cisco RoomOS Series, a **SIP Profile** must be configured.

It is recommended to create a custom SIP Profile for the Cisco RoomOS Series (do not use the **Standard SIP Profile** or **Standard SIP Profile for Mobile Device**).

Protocol Specific Information	
Packet Capture Mode *	None
Packet Capture Duration	0
BLF Presence Group *	Standard Presence group
MTP Preferred Originating Codec *	711ulaw
Device Security Profile *	Cisco Webex Desk Pro - Standard SIP Non-Secure
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile *	Custom Webex Desk Pro SIP Profile View Details
Digest User	< None >
<input type="checkbox"/> Media Termination Point Required <input type="checkbox"/> Unattended Port <input type="checkbox"/> Require DTMF Reception	

To create a custom SIP Profile for the Cisco RoomOS Series, use the **Standard SIP Profile** as the reference template.

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

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

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

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

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

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

Custom SIP Profile Example

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

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

<input type="checkbox"/> Enable Trace	
Parameter Name	Parameter Value
1	<input type="text"/> <input type="text"/> <input type="button" value="+"/> <input type="button" value="-"/>

Incoming Requests FROM URI Settings

Caller ID DN

Caller Name

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*

Resource Priority Namespace List

SIP Rel1XX Options*

Video Call Traffic Class*

Calling Line Identification Presentation*

Session Refresh Method*

Early Offer support for voice and video calls*

Enable ANAT

Deliver Conference Bridge Identifier

Allow Passthrough of Configured Line Device Caller Information

Reject Anonymous Incoming Calls

Reject Anonymous Outgoing Calls

Send ILS Learned Destination Route String

Connect Inbound Call before Playing Queuing Announcement

SIP OPTIONS Ping

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)*

Ping Interval for Out-of-service Trunks (seconds)*

Ping Retry Timer (milliseconds)*

Ping Retry Count*

SDP Information

Send send-receive SDP in mid-call INVITE

Allow Presentation Sharing using BFCP

Allow IX Application Media

Allow multiple codecs in answer SDP

QoS Parameters

The DSCP values to be used for SIP communications, phone configuration, and phone based services to be used by the device 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.

Parameter Name	Parameter Value	Suggested Value
Cluster ID *	StandAloneCluster	StandAloneCluster
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
Auto Registration Legacy Mode *	False	False
BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	Disabled	Disabled
Services Provisioning *	Internal	Internal
Feature Control Policy	< None >	
Wi-Fi Hotspot Profile	< None >	
IMS Inter Operator Id *	IMS Inter Operator Identification	IMS Inter Operator Identification
URI Lookup Policy *	Case Sensitive	Case Sensitive

Audio and Video Bit Rates

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

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

For typical deployments, it is recommended to utilize 600p (1100-3000 Kbps) or HD 720p (1000-1599 Kbps) for the video stream.

For enhanced video quality, set the video call bit rate to 1 Mbps to utilize HD 720p (total 1064 Kbps including G.722 audio) or 2 Mbps to utilize FHD 1080p (total 2064 Kbps including G.722 audio).

Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Keep Current Setting	<input checked="" type="radio"/> 64 kbps (G.722, G.711) <input type="radio"/> kbps	<input type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input checked="" type="radio"/> 2000 kbps	<input checked="" type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input type="radio"/> kbps

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

Audio Codec	Audio Bit Rate
AAC-LD	128-256 Kbps
Opus	6-510 Kbps

G.722 / G.711	64 Kbps
G.722.1	32 Kbps
G.729	8 Kbps

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

The value configured will determine the resolution of the transmitted video stream from the Cisco RoomOS Series.

The Cisco RoomOS Series can receive up to FHD 1080p video depending on the remote device’s capabilities, where the region settings configuration is factored in.

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

Video Type	Video Resolution	Frames per Second (fps)	Video Bit Rate Range
qnHD 180p	320 x 180	30	Up to 128 Kbps
CIF 288p	512 x 288	30	129-256 Kbps
nHD 360p	640 x 360	30	257-384 Kbps
SD 448p	768 x 448	30	385-512 Kbps
WSVGA 576p	1024 x 576	30	513-768 Kbps
HD 720p	1280 x 720	30	769-1472 Kbps
FHD 1080p	1920 x 1080	30	1473-4000 Kbps

Product Specific Configuration Options





















In Cisco Unified Communications Manager Administration, the following configuration options are available for the Cisco RoomOS Series.















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 RoomOS Series Configuration Options (versions prior to 12.5)

Product Specific Configuration Layout		Parameter Value	Override Enterprise/Common Phone Profile Settings
Room Name (from Exchange(R))		<input type="text"/>	
Web Access*		Disabled 	
SSH Access*		Disabled 	
Default Call Protocol*		SIP 	
Quality Improvement Server		<input type="text"/>	
Multipoint Mode*		Use Endpoint 	
Telnet Access*		Off 	
Microphone Unmute On Disconnect*		On 	
Call Logging Mode*		On 	
OSD Encryption Indicator*		Auto 	
Alternate phone book server type*		UDS 	
Alternate phone book server address		<input type="text"/>	
Default Volume		70	
Max Total Downstream Rate		15000	
Max Total Upstream Rate		10000	
Load Server		<input type="text"/>	
WiFi Allowed*		On 	
System Name		<input type="text"/>	
Wake-up On Motion Detection*		On 	
Custom Message		<input type="text"/>	
Settings Menu Mode*		Unlocked 	
Accessibility Call Notification*		Default 	
Configuration Control Mode*		Unified CM and Endpoint 	
Webex Devices Onboarding Token		<input type="text"/>	
Easy Webex join*		Auto 	
Far End Camera Control Settings			
Far End Camera Control*		On 	
Far End Camera Control Signaling Capability*		On 	
Facility Service Settings			
Facility Service Type*		Helpdesk 	
Facility Service Name		<input type="text"/>	
Facility Service Number		<input type="text"/>	
Facility Service Call Type*		Video 	

Standby Settings	
Standby Mode*	On 
Standby Delay	10
Serial Port Settings	
Serial Port*	On 
Serial Port Login Required*	On 
Admin username and password	
Admin Username	<input type="text"/>
Admin Password	<input type="password"/>
Proximity	
Proximity Mode*	On 
Call Control*	Disabled 
Proximity Content Share From Clients*	Disabled 
Proximity Content Share To Clients*	Disabled 
LDAP User Management	
LDAP Mode*	Off 
LDAP Server Address	<input type="text"/>
LDAP Server Port	0
LDAP Attribute	<input type="text"/>
LDAP Base DN	<input type="text"/>
LDAP Encryption*	LDAPS 
LDAP Minimum TLS Version*	TLSv1.2 
LDAP Verify Server Certificate*	Off 
LDAP Admin Filter	<input type="text"/>
LDAP Admin Group	<input type="text"/>
Customization Provisioning	
Customization File	<input type="text"/>
Customization Hash Type*	SHA512 
Customization Hash	<input type="text"/>
SMTP Provisioning	
SMTP Mode*	Off 
SMTP Server	<input type="text"/>
SMTP Port	0
SMTP Security type*	None 
SMTP Username	<input type="text"/>
SMTP Password	<input type="password"/>
SMTP From address	<input type="text"/>

<u>Field Name</u>	<u>Description</u>
Room Name (from Exchange(R))	This is the Exchange Conference Room Name. It is used for scheduling meetings where this TelePresence system participates. (Note: This setting must match the name used in Exchange exactly)
Web Access	This parameter indicates whether the device will accept connections from a web browser or other HTTP client. Disabling the web server functionality of the

	device will block access to the phone's internal web pages and certain support capabilities, but will not degrade normal operation. A device RESET is required for this parameter to take effect.
SSH Access	This parameter indicates whether the device will accept ssh connections. Disabling the ssh server functionality of the device will block certain support capabilities such as log file collection but will not degrade normal operation.
Default Call Protocol	This parameter sets the default call protocol of the device. This device only supports SIP when registering to Cisco Unified Communications Manager.
Quality Improvement Server	Specifies a hostname or IP address of a remote system to collect quality improvement reports from the device.
Multipoint Mode	This field defines how multipoint calls are established when participants are added to point to point calls. Using the Endpoint mode limits the capabilities of multipoint calls to the capabilities of the endpoint initiating the multipoint call. The capabilities will vary depending on the endpoint model as well as the presence of options such as Multisite. Using the Media Resource Group List mode will utilize the resources made available to the endpoint via the associated media resource group list. This can include audio and or video conferencing resources.
Telnet Access	This parameter indicates whether the device will accept telnet connections. Disabling the telnet server functionality of the device will block certain support capabilities such as log file collection but will not degrade normal operation.
Microphone Unmute on Disconnect	Determine if the microphones shall be unmuted automatically when all calls are disconnected. In a meeting room or other shared resource this could be done to prepare the system for the next user.
Call Logging Mode	Set the call logging mode for calls that are received or placed by the system. The call logs may then be viewed via the web interface or using the xHistory command.
OSD Encryption Indicator	Define for how long the encryption indicator (a padlock) will be shown on screen. The setting applies to both encrypted and non-encrypted calls, i.e. both to secure and non-secure conferences. The icon for encrypted calls is a locked padlock, and the icon for non-encrypted calls is a crossed out locked padlock. Auto: If the Conference Encryption Mode setting is set to BestEffort and the call is encrypted, the encryption indicator is shown during the first seconds of a call. If the Conference Encryption Mode setting is set to BestEffort and the call is non-encrypted, the crossed out encryption indicator is shown during the entire call. If the Conference Encryption Mode setting is NOT set to BestEffort, the encryption indicator is not shown at all. AlwaysOn: The encryption indicator is displayed on screen during the entire call. This applies to both encrypted and non-encrypted calls for all Conference Encryption Mode settings. AlwaysOff: The encryption indicator is never displayed on screen. This applies to both encrypted and non-encrypted calls for all Conference Encryption Mode settings.
Alternate phone book server type	By default the endpoint uses the UDS server on the UCM it's registered to, but if you wish to use an alternate phone book server, this parameter combined with an alternate phone book address will override the default setting of the endpoint. UDS will set the alternate phone book type as UDS, and TMS will set the type to TMS.
Alternate phone book server address	By default the endpoint uses the UDS server on the UCM it's registered to, but if you wish to use an alternate phone book server, this parameter combined with the

	alternate phone book type will override the default setting of the endpoint. The field requires a full URL for the phone book servers. Example for UDS server url: https://uds-host-name:8443/cucm-uds/users and TMS example: https://tms-host-name/tms/public/external/phonebook/phonebookservice.asmx
Default Volume	The value must be between 0 and 100. The values from 1 to 100 correspond to the range from -34.5dB to 15dB (0.5 dB steps). The value 0 means that audio is switched off.
Max Total Downstream Rate	This configuration specifies the maximum overall receive bitrate allowed. The bitrate will be divided fairly among all active calls at any time. Value space ranges between 64 - 10000.
Max Total Upstream Rate	This configuration specifies the maximum overall transmit bitrate allowed. The bitrate will be divided fairly among all active calls at any time. Value space ranges between 64 - 10000.
Load Server	Address of alternate server that contains firmware for the device. Please provide full path and port. e.g http://example.com/firmware
WiFi Allowed	Setting to indicate if the endpoint should be allowed to enable Wi-Fi or not.
System Name	Name of the system. Can be used as hostname for the device.
Wake-up On Motion Detection	Setting to control if the TelePresence endpoint should get out of standby mode when detecting motion in the room.
Custom Message	Setting a custom message to be displayed on the TelePresence endpoint user interface.
Settings Menu Mode	Setting to indicate whether the endpoint settings meny should be locked or not, i.e. requiring a user login with a password.
Accessibility Call Notification	Setting to indicate if the endpoint should use amplified visuals for incoming call notification as an accessibility setting for hearing impaired users.
Configuration Control Mode	Xconfiguration Settings Source.
Webex Devices Onboarding Token	A 16-digit one-time password needed to register a device in the Webex Cloud.
Easy Webex join	Enable or hide the easy Webex join feature.
Far End Camera Control Settings	
Far End Camera Control	Lets you decide if the remote side (far end) should be allowed to select your video sources and control your local camera (pan, tilt, zoom).
Far End Camera Control Signaling Capability	Set the far end control (H.224) signal capability mode.
Facility Service Settings	
Facility Service Type	With this setting you can select what kind of services they are. A facility service is not available unless both the facility name and the facility service number settings are properly set. Only FacilityService Service 1 with Type Helpdesk is available on the Touch controller. Facility services are not available when using the remote control and on-screen menu.
Facility Service Name	Set the name of each facility service. A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number

	settings are properly set. Only FacilityService Service 1 is available on the Touch controller, and its Name is used on the facility service call button. Facility services are not available when using the remote control and on-screen menu.
Facility Service Number	Set the number for each facility service. A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number settings are properly set. Only FacilityService Service 1 is available on the Touch controller. Facility services are not available when using the remote control and on-screen menu.
Facility Service Call Type	Set the call type for each facility service. A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number settings are properly set. Only FacilityService Service 1 is available on the Touch controller. Facility services are not available when using the remote control and on-screen menu.
Standby Settings	
Standby Mode	This parameter determines if the system should go into standby mode or not.
Standby Delay	Define how long (in minutes) the system shall be in idle mode before it goes into standby mode. NOTE: Requires the Standby Control to be enabled.
Serial Port Settings	
Serial Port	This parameter indicates whether the device will enable the serial port.
Serial Port Login Required	This parameter determines if login shall be required when connecting to the serial port.
Admin username and password	
Admin Username	Enter a user ID for the admin user.
Admin Password	Enter the password for the admin user.
Proximity	
Proximity Mode	Allow the proximity app to pair with the endpoint.
Call Control	Allow proximity app to do call control.
Proximity Content Share From Clients	Allow proximity app to do content sharing, sending content as a presentation from the device, to the TelePresence endpoint.
Proximity Content Share To Clients	Allow proximity app to receive presentation slides from the TelePresence endpoint.
LDAP User Management	
LDAP Mode	The video system supports the use of an LDAP (Lightweight Directory Access Protocol) server as a central place to store and validate user names and passwords. Use this setting to configure whether or not to use LDAP authentication. Our implementation is tested for the Microsoft Active Directory (AD) service.
LDAP Server Address	Set the IP address or hostname of the LDAP server.

LDAP Server Port	Set the port to connect to the LDAP server on. If set to 0, use the default for the selected protocol (see the UserManagement LDAP Encryption setting).
LDAP Attribute	The attribute used to map to the provided username. If not set, sAMAccountName is used.
LDAP Base DN	The distinguishing name of the entry at which to start a search (base). Example: "DC=company, DC=com"
LDAP Encryption	Define how to secure the communication between the video system and the LDAP server. You can override the port number by using the UserManagement LDAP Server Port setting. LDAPS: Connect to the LDAP server on port 636 over TLS (Transport Layer Security). None: Connect to LDAP server on port 389 with no encryption. STARTTLS: Connect to LDAP server on port 389, then send STARTTLS to enable TLS encryption.
LDAP Minimum TLS Version	Set the lowest version of the TLS (Transport Layer Security) protocol that is allowed. TLSv1.0: Support TLS version 1.0 or higher. TLSv1.1: Support TLS version 1.1 or higher. TLSv1.2: Support TLS version 1.2 or higher.
LDAP Verify Server Certificate	When the video system connects to an LDAP server, the server will identify itself to the video system by presenting its certificate. Use this setting to determine whether or not the video system will verify the server certificate.
LDAP Admin Filter	The LDAP filter is used to determine which users should be granted administrator privileges. If set, this setting takes precedence over the UserManagement LDAP Admin Group setting. Example: (CN=adminuser). See the LDAP specification for the syntax details.
LDAP Admin Group	Members of this AD (Active Directory) group will be given administrator access. This setting is a shorthand for saying (memberOf:1.2.840.113556.1.4.1941:=). If UserManagement LDAP Admin Filter is set, this setting is ignored. Example: CN=admin_group, OU=company groups, DC=company, DC=com
Customization Provisioning	
Customization File	The address where the customization provisioning file is stored. The field requires a full URL of the customization bundle file or just the filename, if it is hosted on the CUCM in use.
Customization Hash Type	Set the type of the hash function used.
Customization Hash	Set the hash checksum generated from the customization provisioning file, in order for the endpoint to verify the file integrity.
SMTP Provisioning	
SMTP Mode	This setting enables or disables SMTP on the endpoint.
SMTP Server	Set the SMTP server address to be used.
SMTP Port	Set the SMTP server port number.
SMTP Security Type	Set the SMTP security type to be used.
SMTP Username	Set the SMTP username to be used.
SMTP Password	Set the SMTP password to be used.

SMTP From address	Set the from address to be used when sending e-mail over SMTP from the endpoint.
-------------------	--

Cisco Desk Pro Configuration Options (versions 12.5 and later)

Product Specific Configuration Layout

Parameter Value Pull xConfig. from device

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

Audio

Bluetooth

BYOD

CallHistory

Cameras

Conference

FacilityService

HttpClient

HttpFeedback

Logging

Macros

NetworkServices

Phonebook

RoomAnalytics

RoomScheduler

General Settings

DefaultVolume #

Microphones Mute Enabled* ▼

Ultrasound MaxVolume

Input

HDMI 1

Level

Mode* ▼

MicrophoneMode* ▼

USBC 1

Level

Mode* ▼

SoundsAndAlerts

RingTone

RingVolume

KeyClickDetector

Enabled* ▼

Attenuate* ▼

SIP
Security
SerialPort
Standby
SystemUnit
UserInterface
Peripherals
Proximity
UserManagement
Video
VoiceControl
WebEngine
Webex
RoomCleanup
Bookings
Miscellaneous

Audio

General Settings	
DefaultVolume	<input type="text" value="50"/> #
Microphones Mute Enabled*	<input type="button" value="True"/> ▾
Ultrasound MaxVolume	<input type="text" value="70"/>
Input	
HDMI 1	
Level	<input type="text" value="0"/>
Mode*	<input type="button" value="On"/> ▾
MicrophoneMode*	<input type="button" value="Focused"/> ▾
USBC 1	
Level	<input type="text" value="0"/>
Mode*	<input type="button" value="On"/> ▾
SoundsAndAlerts	
RingTone	<input type="text" value="Sunrise"/>
RingVolume	<input type="text" value="50"/>
KeyClickDetector	
Enabled*	<input type="button" value="True"/> ▾
Attenuate*	<input type="button" value="True"/> ▾

Bluetooth

General Settings

Allowed *	True	▼
Enabled *	False	▼

BYOD

General Settings

HidForwarding Enabled *	False	▼
TouchForwarding Enabled *	True	▼

Call History

General Settings

Mode *	On	▼ #
--------	----	-----

Cameras

Background

Enabled *	False	▼
UserImagesAllowed *	True	▼
PowerLine Frequency *	Auto	▼
SpeakerTrack Mode *	Auto	▼

Camera

Brightness

DefaultLevel	20	
Mode *	Auto	▼

ExposureCompensation

Level	0
-------	---

Conference

DefaultCall	
Protocol*	Sip <input type="button" value="v"/> #
Rate	6000 <input type="text"/>
DoNotDisturb DefaultTimeout	60 <input type="text"/>
Encryption Mode*	BestEffort <input type="button" value="v"/>
FarEndMessage Mode*	Off <input type="button" value="v"/>
MaxReceiveCallRate	6000 <input type="text"/>
MaxTotalReceiveCallRate	15000 <input type="text"/> #
MaxTotalTransmitCallRate	15000 <input type="text"/> #
MaxTransmitCallRate	6000 <input type="text"/>
MicUnmuteOnDisconnect Mode*	On <input type="button" value="v"/> #
Multipoint Mode*	Auto <input type="button" value="v"/> #

FarEndControl	
Mode*	On <input type="button" value="v"/> #
SignalCapability*	On <input type="button" value="v"/> #

Facility Service

Service 1	
CallType*	Video <input type="button" value="v"/> #
Name	Live Support <input type="text"/> #
Number	<input type="text"/> #
Type*	Helpdesk <input type="button" value="v"/> #

Service 2	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>

Service 3	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>

Service 4	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>

Service 5	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>

HTTP Client

General Settings	
Mode*	Off
AllowInsecureHTTPS*	False
AllowHTTP*	True
UseHttpProxy*	On

HTTP Feedback

General Settings	
TlsVerify*	On
UseHttpProxy*	On

Logging

General Settings	
CloudUpload Mode*	Off
Internal Mode*	On

External	
Mode*	Off
Protocol*	SyslogTLS
TlsVerify*	On

Server	
Address	
Port	514

Macros

General Settings	
AutoStart*	On
Mode*	Off
UnresponsiveTimeout	5

Network Services

General Settings

H323 Mode*	Off
UPnP Mode*	On
Websocket*	Off
WelcomeText*	On
Wifi Allowed*	True

HTTP

Mode*	Off
-------	-----

Proxy

Mode*	Off
Url	
LoginName	
Password	
PACUrl	

HTTPS

VerifyClientCertificate*	Off
StrictTransportSecurity*	Off

Server

MinimumTLSVersion*	TLSv1.1
--------------------	---------

SNMP

CommunityName	
Mode*	Off
SystemContact	
SystemLocation	

SSH

HostKeyAlgorithm*	RSA
Mode*	Off

SMTP

Mode*	Off
Server	
Port	0
Security*	StartTls
Username	
Password	
From	

Phone Book

Server 1

ID	
Type*	CUCM
URL	
Pagination*	Enabled
TlsVerify*	On

Room Analytics

General Settings	
PeopleCountOutOfCall*	Off
PeoplePresenceDetector*	Off

AmbientNoiseEstimation	
Mode*	Off
Interval	10

Room Scheduler

General Settings	
Enabled*	False

SIP

General Settings	
MinimumTLSVersion*	TLSv1.0

Security

Audit	
Logging	
Mode*	Internal

OnError	
Action*	Ignore

Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off

Session	
InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

Serial Port

General Settings	
BaudRate*	115200
LoginRequired*	On
Mode*	On

Standby

General Settings	
BootAction*	RestoreCameraPosition ▾
Control*	On ▾ #
Delay	10 #
StandbyAction*	PrivacyPosition ▾ #
WakeupAction*	RestoreCameraPosition ▾
WakeupOnMotionDetection*	On ▾ #

Signage	
Url	<input type="text"/>
Mode*	Off ▾
InteractionMode*	NonInteractive ▾
RefreshInterval	0 #
Audio*	Off ▾

System Unit

General Settings	
Name	<input type="text"/> #

CrashReporting	
Mode*	Off ▾
URL	<input type="text"/> #

User Interface

General Settings	
Accessibility IncomingCallNotification *	Default <input type="button" value="v"/> #
Bookings Visibility Title *	Auto <input type="button" value="v"/>
ContactInfo Type *	Auto <input type="button" value="v"/>
Diagnostics Notifications *	Auto <input type="button" value="v"/>
Branding AwakeBranding Colors *	Auto <input type="button" value="v"/>
KeyTones Mode *	Off <input type="button" value="v"/>
SoundEffects Mode *	On <input type="button" value="v"/>
Proximity Notifications *	Auto <input type="button" value="v"/>
CustomMessage	<input type="text" value=""/>
Whiteboard ActivityIndicators *	On <input type="button" value="v"/>
Assistant Mode *	On <input type="button" value="v"/>
Security Mode *	Normal <input type="button" value="v"/>

Features	
HideAll *	False <input type="button" value="v"/>
Call	
Start *	Auto <input type="button" value="v"/>
MidCallControls *	Auto <input type="button" value="v"/>
End *	Auto <input type="button" value="v"/>
JoinWebex *	Auto <input type="button" value="v"/> #
Keypad *	Auto <input type="button" value="v"/>
MusicMode *	Hidden <input type="button" value="v"/>
Share	
Start *	Auto <input type="button" value="v"/>
Whiteboard	
Start *	Auto <input type="button" value="v"/>

OSD	
EncryptionIndicator *	Auto <input type="button" value="v"/> #
Output *	1 <input type="button" value="v"/>
HalfwakeMessage	<input type="text" value=""/>
Mode *	Auto <input type="button" value="v"/>

Phonebook	
Mode *	ReadWrite <input type="button" value="v"/>
DefaultSearchFilter *	All <input type="button" value="v"/>

SettingsMenu	
Mode *	Unlocked <input type="button" value="v"/> #
Visibility *	Auto <input type="button" value="v"/>

Peripherals

General Settings	
InputDevice Mode*	Off
Pairing CiscoTouchPanels RemotePairing*	On

Profile	
TouchPanels*	0
Cameras*	0
ControlSystems*	NotSet

Proximity

General Settings	
Mode*	Off

Services	
ContentShare	
ToClients*	Disabled
FromClients*	Enabled
CallControl*	Disabled

User Management

LDAP	
Mode*	Off
Encryption*	LDAPS
VerifyServerCertificate*	Off
BaseDN	
Attribute	
MinimumTLSVersion*	TLSv1.2
Server	
Address	
Port	0
Admin	
Group	
Filter	

PasswordPolicy	
ReuseLimit	12
MaxLifetime	0
Complexity	
MinimumLength	8
MinimumUppercase	0
MinimumLowercase	0
MinimumDigits	0
MinimumSpecial	0

Video

Input	
Connector 1	
InputSourceType*	camera
Name	Camera
Visibility*	Never
CameraControl	
CameraId*	1
Mode*	On
Connector 2	
InputSourceType*	PC
Name	PC (USB-C)
PresentationSelection*	Desktop
Quality*	Sharpness
RGBQuantizationRange*	Auto
Visibility*	IfSignal
PreferredResolution*	3840_2160_60
CameraControl	
CameraId*	1
Mode*	Off
CEC	
Mode*	On
Connector 3	
InputSourceType*	PC
Name	PC (HDMI)
PresentationSelection*	Desktop
Quality*	Sharpness
RGBQuantizationRange*	Auto
Visibility*	IfSignal
PreferredResolution*	3840_2160_60
CameraControl	
CameraId*	1
Mode*	Off
CEC	
Mode*	On
Monitors*	Auto
DefaultMainSource*	1

Output

Connector 1

BrightnessMode*

Resolution*

Connector 2

MonitorRole*

RGBQuantizationRange*

Resolution*

Location

HorizontalOffset

VerticalOffset

CEC

Mode*

Presentation

DefaultSource*

Priority*

Selfview

Default

FullscreenMode*

Mode*

OnMonitorRole*

PIPPosition*

OnCall

Duration

Mode*

Voice Control

General Settings

Wakeword Mode*

Web Engine

General Settings

Mode*

RemoteDebugging*

UseHttpProxy*

Webex

General Settings

CloudProximity Mode*

Room Cleanup

AutoRun	
HourOfDay	<input type="text" value="0"/>
ContentType	
Whiteboards*	<input type="text" value="Daily"/>
WebData*	<input type="text" value="Daily"/>

Bookings

General Settings	
ProtocolPriority*	<input type="text" value="Auto"/>

Miscellaneous

General Settings	
Configuration Control Mode*	<input type="text" value="Unified CM and Endpoint"/>
Room Name (from Exchange(R))	<input type="text"/>
LoadServer	<input type="text"/>
Webex Devices Onboarding Token	<input type="text"/>

Admin username and password	
Admin Username	<input type="text" value="admin"/>
Admin Password	<input type="text"/>

Customization Provisioning	
Customization File	<input type="text"/>
Customization Hash Type*	<input type="text" value="SHA512"/>
Customization Hash	<input type="text"/>

Cisco Desk Limited Edition Configuration Options (versions 12.5 and later)

Product Specific Configuration Layout

Parameter Value Pull xConfig. from device

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

- Audio
- Bluetooth
- BYOD
- CallHistory
- Cameras
- Conference
- FacilityService
- HttpClient
- HttpFeedback
- Logging
- Macros
- NetworkServices
- Phonebook
- RoomAnalytics
- RoomScheduler
- SIP
- Security
- SerialPort
- Standby
- SystemUnit

General Settings

DefaultVolume #

Ultrasound MaxVolume

USB Mode*

Input

HDMI 1

Level

Mode*

MicrophoneMode*

USBC 1

Level

Mode*

Microphones

Mute

Enabled*

NoiseRemoval

Mode*

SoundsAndAlerts

RingTone

RingVolume

KeyClickDetector

Enabled*

Attenuate*

- UserInterface
- Peripherals
- Proximity
- UserManagement
- Video
- VoiceControl
- WebEngine
- Webex
- RoomCleanup
- Bookings
- Miscellaneous

Audio

General Settings	
DefaultVolume	<input type="text" value="50"/> #
Ultrasound MaxVolume	<input type="text" value="70"/>
USB Mode*	<input type="text" value="SpeakerAndMicrophone"/>

Input	
HDMI 1	
Level	<input type="text" value="0"/>
Mode*	<input type="text" value="On"/>
MicrophoneMode*	<input type="text" value="Focused"/>
USBC 1	
Level	<input type="text" value="0"/>
Mode*	<input type="text" value="On"/>

Microphones	
Mute	
Enabled*	<input type="text" value="True"/>
NoiseRemoval	
Mode*	<input type="text" value="Manual"/>

SoundsAndAlerts	
RingTone	<input type="text" value="Sunrise"/>
RingVolume	<input type="text" value="50"/>

KeyClickDetector	
Enabled*	<input type="text" value="False"/>
Attenuate*	<input type="text" value="True"/>

Bluetooth

General Settings	
Allowed*	<input type="text" value="True"/>
Enabled*	<input type="text" value="False"/>

BYOD

General Settings	
HidForwarding Enabled*	<input type="text" value="False"/>
TouchForwarding Enabled*	<input type="text" value="True"/>

Call History

General Settings	
Mode*	<input type="text" value="On"/> #

Cameras

Background

Enabled*	False	▼
UserImagesAllowed*	True	▼
PowerLine Frequency*	Auto	▼
SpeakerTrack Mode*	Auto	▼

Camera

Brightness

DefaultLevel	20	
Mode*	Auto	▼

ExposureCompensation

Level	0
-------	---

Conference

DefaultCall

Protocol*	Sip	▼	#
Rate	6000		
DoNotDisturb DefaultTimeout	60		
Encryption Mode*	BestEffort	▼	
FarEndMessage Mode*	Off	▼	
MaxReceiveCallRate	6000		
MaxTotalReceiveCallRate	15000		#
MaxTotalTransmitCallRate	15000		#
MaxTransmitCallRate	6000		
MicUnmuteOnDisconnect Mode*	On	▼	#
Multipoint Mode*	Auto	▼	#

FarEndControl

Mode*	On	▼	#
SignalCapability*	On	▼	#

Facility Service

Service 1	
CallType*	Video <input type="button" value="v"/>
Name	Live Support <input type="button" value="x"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 2	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 3	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 4	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>
Service 5	
CallType*	Video <input type="button" value="v"/>
Name	<input type="text"/>
Number	<input type="text"/>
Type*	Helpdesk <input type="button" value="v"/>

HTTP Client

General Settings	
Mode*	Off <input type="button" value="v"/>
AllowInsecureHTTPS*	False <input type="button" value="v"/>
AllowHTTP*	True <input type="button" value="v"/>
UseHttpProxy*	On <input type="button" value="v"/>

HTTP Feedback

General Settings	
TlsVerify*	On <input type="button" value="v"/>
UseHttpProxy*	On <input type="button" value="v"/>

Logging

General Settings	
CloudUpload Mode*	Off
Internal Mode*	On

External	
Mode*	Off
Protocol*	SyslogTLS
TlsVerify*	On

Server	
Address	
Port	514

Macros

General Settings	
AutoStart*	On
Mode*	Off
UnresponsiveTimeout	5

Network Services

General Settings

H323 Mode*	Off
UPnP Mode*	On
Websocket*	Off
WelcomeText*	On
Wifi Allowed*	True

HTTP

Mode*	Off
-------	-----

Proxy

Mode*	Off
Url	
LoginName	
Password	
PACUrl	

HTTPS

VerifyClientCertificate*	Off
StrictTransportSecurity*	Off

Server

MinimumTLSVersion*	TLSv1.1
--------------------	---------

SNMP

CommunityName	
Mode*	Off
SystemContact	
SystemLocation	

SSH

HostKeyAlgorithm*	RSA
Mode*	Off

SMTP

Mode*	Off
Server	
Port	0
Security*	StartTls
Username	
Password	
From	

Phone Book

Server 1

ID	
Type*	CUCM
URL	
Pagination*	Enabled
TlsVerify*	On

Room Analytics

General Settings	
PeopleCountOutOfCall*	Off
PeoplePresenceDetector*	Off

AmbientNoiseEstimation	
Mode*	Off
Interval	10

Room Scheduler

General Settings	
Enabled*	False

SIP

General Settings	
MinimumTLSVersion*	TLSv1.0

Security

Audit	
Logging	
Mode*	Internal

OnError	
Action*	Ignore

Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off

Session	
InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

Serial Port

General Settings	
BaudRate*	115200
LoginRequired*	On
Mode*	On

Standby

General Settings	
BootAction*	RestoreCameraPosition ▾
Control*	On ▾ #
Delay	10 #
StandbyAction*	PrivacyPosition ▾ #
WakeupAction*	RestoreCameraPosition ▾
WakeupOnMotionDetection*	On ▾ #

Signage	
Url	<input type="text"/>
Mode*	Off ▾
InteractionMode*	NonInteractive ▾
RefreshInterval	0 #
Audio*	Off ▾

System Unit

General Settings	
CustomDeviceId	<input type="text"/>
Name	<input type="text"/> #

CrashReporting	
Mode*	Off ▾
URL	<input type="text"/> #

User Interface

General Settings	
Accessibility IncomingCallNotification *	Default <input type="button" value="v"/> #
Bookings Visibility Title *	Auto <input type="button" value="v"/>
ContactInfo Type *	Auto <input type="button" value="v"/>
Diagnostics Notifications *	Auto <input type="button" value="v"/>
Branding AwakeBranding Colors *	Auto <input type="button" value="v"/>
KeyTones Mode *	Off <input type="button" value="v"/>
SoundEffects Mode *	On <input type="button" value="v"/>
Proximity Notifications *	Auto <input type="button" value="v"/>
CustomMessage	<input type="text" value=""/>
Whiteboard ActivityIndicators *	On <input type="button" value="v"/>
Assistant Mode *	On <input type="button" value="v"/>
Security Mode *	Normal <input type="button" value="v"/>

Features	
HideAll *	False <input type="button" value="v"/>
Call	
Start *	Auto <input type="button" value="v"/>
MidCallControls *	Auto <input type="button" value="v"/>
End *	Auto <input type="button" value="v"/>
JoinWebex *	Auto <input type="button" value="v"/> #
Keypad *	Auto <input type="button" value="v"/>
MusicMode *	Hidden <input type="button" value="v"/>
Share	
Start *	Auto <input type="button" value="v"/>
Whiteboard	
Start *	Auto <input type="button" value="v"/>

OSD	
EncryptionIndicator *	Auto <input type="button" value="v"/> #
Output *	1 <input type="button" value="v"/>
HalfwakeMessage	<input type="text" value=""/>
Mode *	Auto <input type="button" value="v"/>

Phonebook	
Mode *	ReadWrite <input type="button" value="v"/>
DefaultSearchFilter *	All <input type="button" value="v"/>

SettingsMenu	
Mode *	Unlocked <input type="button" value="v"/> #
Visibility *	Auto <input type="button" value="v"/>

Peripherals

General Settings

InputDevice Mode*	Off	▼
Pairing CiscoTouchPanels RemotePairing*	On	▼

Profile

TouchPanels*	0	▼
Cameras*	0	▼
ControlSystems*	NotSet	▼

Proximity

General Settings

Mode*	Off	▼	#
AlternatePort Enabled*	False	▼	

Services

ContentShare

ToClients*	Disabled	▼	#
FromClients*	Enabled	▼	#
CallControl*	Disabled	▼	#

User Management

LDAP

Mode*	Off	▼	#
Encryption*	LDAPS	▼	#
VerifyServerCertificate*	Off	▼	#
BaseDN	<input type="text"/>		
Attribute	<input type="text"/>		
MinimumTLSVersion*	TLSv1.2	▼	#

Server

Address	<input type="text"/>		
Port	0	<input type="text"/>	

Admin

Group	<input type="text"/>		
Filter	<input type="text"/>		

PasswordPolicy

ReuseLimit	<input type="text" value="12"/>
MaxLifetime	<input type="text" value="0"/>

Complexity

MinimumLength	<input type="text" value="8"/>
MinimumUppercase	<input type="text" value="0"/>
MinimumLowercase	<input type="text" value="0"/>
MinimumDigits	<input type="text" value="0"/>
MinimumSpecial	<input type="text" value="0"/>

Video

Input	
Connector 1	
InputSourceType*	camera
Name	Camera
Visibility*	Never
CameraControl	
CameraId*	1
Mode*	On
Connector 2	
InputSourceType*	PC
Name	PC (USB-C)
PresentationSelection*	Desktop
Quality*	Sharpness
RGBQuantizationRange*	Auto
Visibility*	IfSignal
PreferredResolution*	1920_1080_60
CameraControl	
CameraId*	1
Mode*	Off
CEC	
Mode*	On
Connector 3	
InputSourceType*	PC
Name	PC (HDMI)
PresentationSelection*	Desktop
Quality*	Sharpness
RGBQuantizationRange*	Auto
Visibility*	IfSignal
PreferredResolution*	1920_1080_60
CameraControl	
CameraId*	1
Mode*	Off
CEC	
Mode*	On
Monitors*	Auto
DefaultMainSource*	1

Output

Connector 1

BrightnessMode* ▾

Resolution* ▾

Connector 2

MonitorRole* ▾

RGBQuantizationRange* ▾

Resolution* ▾

Location

HorizontalOffset

VerticalOffset

CEC

Mode* ▾

Presentation

DefaultSource* ▾

Priority* ▾

Selfview

Default

FullscreenMode* ▾

Mode* ▾

OnMonitorRole* ▾

PIPPosition* ▾

OnCall

Duration

Mode* ▾

Voice Control

General Settings

Wakeword Mode* ▾

Web Engine

General Settings

Mode* ▾

RemoteDebugging* ▾

UseHttpProxy* ▾

MinimumTLSVersion* ▾

Webex

General Settings

Meetings JoinProtocol*	SIP	▼
CloudUpgrades Mode*	Off	▼

CloudProximity

Mode*	Off	▼
GuestShare*	Auto	▼

Room Cleanup**AutoRun**

HourOfDay	0
-----------	---

ContentType

Whiteboards*	Daily	▼
WebData*	Daily	▼

Bookings**General Settings**

ProtocolPriority*	Auto	▼
-------------------	------	---

Miscellaneous**General Settings**

Configuration Control Mode*	Unified CM and Endpoint	▼	#
Room Name (from Exchange(R))			#
LoadServer			#
Webex Devices Onboarding Token			#

Admin username and password

Admin Username	admin	#
Admin Password		#

Customization Provisioning

Customization File		#	
Customization Hash Type*	SHA512	▼	#
Customization Hash		#	

Cisco Desk Configuration Options (versions 12.5 and later)

Product Specific Configuration Layout

Parameter Value Pull xConfig. from device

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

Audio	<p>General Settings</p> <p>DefaultVolume <input style="width: 150px;" type="text" value="50"/> #</p> <p>Input MicrophoneMode* <input style="width: 150px;" type="text" value="Focused"/> ▼</p> <p>Ultrasound MaxVolume <input style="width: 150px;" type="text" value="70"/></p> <p>USB Mode* <input style="width: 150px;" type="text" value="SpeakerAndMicrophone"/> ▼</p>
Bluetooth	<p>Microphones</p> <p>Mute</p> <p>Enabled* <input style="width: 150px;" type="text" value="True"/> ▼</p>
CallHistory	<p>NoiseRemoval</p> <p>Mode* <input style="width: 150px;" type="text" value="Manual"/> ▼</p>
Cameras	<p>SoundsAndAlerts</p> <p>RingTone <input style="width: 150px;" type="text" value="Sunrise"/></p> <p>RingVolume <input style="width: 150px;" type="text" value="50"/></p>
Conference	
FacilityService	
HttpClient	
HttpFeedback	
Logging	
Macros	
NetworkServices	
Phonebook	
RoomAnalytics	
RoomScheduler	
SIP	
Security	
SerialPort	
Standby	
SystemUnit	
UserInterface	
Peripherals	
Proximity	
UserManagement	
Video	
VoiceControl	
WebEngine	
Webex	
RoomCleanup	
Bookings	
Miscellaneous	

Audio

General Settings	
DefaultVolume	<input type="text" value="50"/> #
Input MicrophoneMode*	<input type="text" value="Focused"/> ▾
Ultrasound MaxVolume	<input type="text" value="70"/>
USB Mode*	<input type="text" value="SpeakerAndMicrophone"/> ▾

Microphones	
Mute	
Enabled*	<input type="text" value="True"/> ▾

NoiseRemoval	
Mode*	<input type="text" value="Manual"/> ▾

SoundsAndAlerts	
RingTone	<input type="text" value="Sunrise"/>
RingVolume	<input type="text" value="50"/>

Bluetooth

General Settings	
Allowed*	<input type="text" value="True"/> ▾
Enabled*	<input type="text" value="False"/> ▾

Call History

General Settings	
Mode*	<input type="text" value="On"/> # ▾

Cameras

Background	
Enabled*	<input type="text" value="True"/> ▾
UserImagesAllowed*	<input type="text" value="True"/> ▾
PowerLine Frequency*	<input type="text" value="Auto"/> ▾
SpeakerTrack Mode*	<input type="text" value="Auto"/> ▾

Camera	
Brightness	
DefaultLevel	<input type="text" value="20"/>
Mode*	<input type="text" value="Auto"/> ▾

ExposureCompensation	
Level	<input type="text" value="0"/>

Conference

DefaultCall

Protocol *	Sip	#
Rate	6000	
DoNotDisturb DefaultTimeout	60	
Encryption Mode *	BestEffort	
FarEndMessage Mode *	Off	
MaxReceiveCallRate	6000	
MaxTotalReceiveCallRate	6000	#
MaxTotalTransmitCallRate	6000	#
MaxTransmitCallRate	6000	
MicUnmuteOnDisconnect Mode *	On	#
Multipoint Mode *	Auto	#

FarEndControl

Mode *	On	#
SignalCapability *	On	#

Facility Service

Service 1

CallType *	Video	#
Name	Live Support	#
Number		#
Type *	Helpdesk	#

Service 2

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

Service 3

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

Service 4

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

Service 5

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

HTTP Client

General Settings	
Mode*	Off
AllowInsecureHTTPS*	False
AllowHTTP*	True
UseHttpProxy*	On

HTTP Feedback

General Settings	
TlsVerify*	On
UseHttpProxy*	On

Logging

General Settings	
CloudUpload Mode*	Off
Internal Mode*	On

External	
Mode*	Off
Protocol*	SyslogTLS
TlsVerify*	On

Server	
Address	
Port	514

Macros

General Settings	
AutoStart*	On
Mode*	Off
UnresponsiveTimeout	5

Network Services

General Settings

H323 Mode*	Off	▼
UPnP Mode*	On	▼
Websocket*	FollowHTTPService	▼
WelcomeText*	On	▼
Wifi Allowed*	True	▼

HTTP

Mode*	Off	▼	#
-------	-----	---	---

Proxy

Mode*	Off	▼
Url	<input type="text"/>	
LoginName	<input type="text"/>	
PACUrl	<input type="text"/>	

HTTPS

VerifyClientCertificate*	Off	▼
StrictTransportSecurity*	Off	▼

Server

MinimumTLSVersion*	TLSv1.1	▼
--------------------	---------	---

SNMP

CommunityName	<input type="text"/>	
Mode*	Off	▼
SystemContact	<input type="text"/>	
SystemLocation	<input type="text"/>	

SSH

HostKeyAlgorithm*	RSA	▼	
Mode*	Off	▼	#

SMTP

Mode*	Off	▼	#
Server	<input type="text"/>	#	
Port	0	#	
Security*	StartTls	▼	#
Username	<input type="text"/>	#	
From	<input type="text"/>	#	

Phone Book

Server 1

ID	<input type="text"/>		
Type*	CUCM	▼	#
URL	<input type="text"/>	#	
Pagination*	Enabled	▼	
TlsVerify*	On	▼	

Room Analytics

General Settings

PeopleCountOutOfCall*

PeoplePresenceDetector*

AmbientNoiseEstimation

Mode*

Interval

ReverberationTime

Mode*

Interval

Room Scheduler

General Settings

Enabled*

SIP

General Settings

MinimumTLSVersion*

Security

Audit

Logging

Mode*

OnError

Action*

Server

Address

Port

PortAssignment*

Fips Mode*

Session

InactivityTimeout

ShowLastLogon*

MaxTotalSessions

MaxSessionsPerUser

MaxFailedLogins

FailedLoginsLockoutTime

Serial Port

General Settings

BaudRate*	115200	▼
LoginRequired*	On	▼ #
Mode*	On	▼ #

Standby

General Settings

BootAction*	DefaultCameraPosition	▼
Control*	On	▼ #
Delay	10	#
StandbyAction*	PrivacyPosition	▼ #
WakeupAction*	RestoreCameraPosition	▼
WakeupOnMotionDetection*	Off	▼ #

Signage

Url	<input type="text"/>	
Mode*	Off	▼
RefreshInterval	0	<input type="text"/>
Audio*	Off	▼

System Unit

General Settings

CustomDeviceId	<input type="text"/>
Name	<input type="text"/> #

CrashReporting

Mode*	Off	▼
URL	<input type="text"/> #	

User Interface

General Settings

Accessibility IncomingCallNotification*	Default	⌵	#
Bookings Visibility Title*	Auto	⌵	
ContactInfo Type*	Auto	⌵	
Diagnostics Notifications*	Auto	⌵	
Branding AwakeBranding Colors*	Auto	⌵	
KeyTones Mode*	On	⌵	
SoundEffects Mode*	On	⌵	
Proximity Notifications*	Auto	⌵	
CustomMessage			#
Whiteboard ActivityIndicators*	On	⌵	
Assistant Mode*	On	⌵	
Security Mode*	Normal	⌵	

Features

HideAll*	False	⌵
----------	-------	---

Call

Start*	Auto	⌵	
MidCallControls*	Auto	⌵	
End*	Auto	⌵	
VideoMute*	Auto	⌵	
JoinWebex*	Auto	⌵	#
Keypad*	Auto	⌵	
MusicMode*	Hidden	⌵	

Share

Start*	Auto	⌵
--------	------	---

Whiteboard

Start*	Auto	⌵
--------	------	---

OSD

EncryptionIndicator*	Auto	⌵	#
Output*	1	⌵	
HalfwakeMessage			
Mode*	Auto	⌵	

Phonebook

Mode*	ReadWrite	⌵
DefaultSearchFilter*	All	⌵

SettingsMenu

Mode*	Unlocked	⌵	#
Visibility*	Auto	⌵	

Peripherals

General Settings

InputDevice Mode*	Off	⌵
Pairing CiscoTouchPanels RemotePairing*	On	⌵

Profile

TouchPanels*	0	⌵
Cameras*	Minimum1	⌵
ControlSystems*	NotSet	⌵

Proximity

General Settings	
Mode*	Off <input type="button" value="v"/> #
AlternatePort Enabled*	False <input type="button" value="v"/> #

Services	
ContentShare	
ToClients*	Disabled <input type="button" value="v"/> #
FromClients*	Enabled <input type="button" value="v"/> #
CallControl*	Disabled <input type="button" value="v"/> #

User Management

LDAP	
Mode*	Off <input type="button" value="v"/> #
Encryption*	LDAPS <input type="button" value="v"/> #
VerifyServerCertificate*	Off <input type="button" value="v"/> #
BaseDN	<input type="text"/> #
Attribute	<input type="text"/> #
MinimumTLSVersion*	TLSv1.2 <input type="button" value="v"/> #
Server	
Address	<input type="text"/> #
Port	0 <input type="text"/> #
Admin	
Group	<input type="text"/> #
Filter	<input type="text"/> #

PasswordPolicy	
ReuseLimit	<input type="text" value="12"/>
MaxLifetime	<input type="text" value="0"/>
Complexity	
MinimumLength	<input type="text" value="8"/>
MinimumUppercase	<input type="text" value="0"/>
MinimumLowercase	<input type="text" value="0"/>
MinimumDigits	<input type="text" value="0"/>
MinimumSpecial	<input type="text" value="0"/>

Video

Input	
Connector 1	
InputSourceType*	camera
Name	Camera
Visibility*	Never
CameraControl	
CameraId*	1
Mode*	On
Connector 2	
InputSourceType*	PC
Name	PC (USB-C)
PresentationSelection*	Desktop
Quality*	Sharpness
RGBQuantizationRange*	Auto
Visibility*	IfSignal
PreferredResolution*	1920_1080_60
CameraControl	
CameraId*	1
Mode*	Off
CEC	
Mode*	On
Connector 3	
InputSourceType*	PC
Name	PC (HDMI)
PresentationSelection*	Desktop
Quality*	Sharpness
RGBQuantizationRange*	Auto
Visibility*	IfSignal
PreferredResolution*	1920_1080_60
CameraControl	
CameraId*	1
Mode*	Off
CEC	
Mode*	On
Monitors*	Auto
Output Connector 1 Resolution*	1920_1080_60
DefaultMainSource*	1

Presentation

DefaultSource* ▼

Priority* ▼

Selfview

Default

FullscreenMode* ▼

Mode* ▼

OnMonitorRole* ▼

PIPPosition* ▼

OnCall

Duration

Mode* ▼

Voice Control

General Settings

Wakeword Mode* ▼

Web Engine

General Settings

Mode* ▼

RemoteDebugging* ▼

UseHttpProxy* ▼

MinimumTLSVersion* ▼

Webex

General Settings

Meetings JoinProtocol* ▼

CloudUpgrades Mode* ▼

CloudProximity

Mode* ▼

GuestShare* ▼

Room Cleanup

AutoRun

HourOfDay

ContentType

Whiteboards* ▼

WebData* ▼

Bookings

General Settings

ProtocolPriority* ▾

Miscellaneous

General Settings

Configuration Control Mode* ▾ #

Room Name (from Exchange(R)) #

LoadServer #

Webex Devices Onboarding Token #

Admin username and password

Admin Username #

Admin Password #

Customization Provisioning


Customization File #


Customization Hash Type* ▾ #

Customization Hash #

Cisco Desk Mini Configuration Options (versions 12.5 and later)

Product Specific Configuration Layout

 **Parameter Value** Pull xConfig. from device

 **Note:** Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

<ul style="list-style-type: none"> Audio Bluetooth CallHistory Cameras Conference FacilityService HttpClient HttpFeedback Logging Macros NetworkServices 	<p>General Settings</p> <p>DefaultVolume <input type="text" value="50"/> #</p> <p>Input MicrophoneMode* <input type="text" value="Focused"/> ▾</p> <p>Ultrasound MaxVolume <input type="text" value="70"/></p> <p>USB Mode* <input type="text" value="SpeakerAndMicrophone"/> ▾</p> <p>Microphones</p> <p>Mute</p> <p>Enabled* <input type="text" value="True"/> ▾</p> <p>NoiseRemoval</p> <p>Mode* <input type="text" value="Manual"/> ▾</p> <p>SoundsAndAlerts</p> <p>RingTone <input type="text" value="Sunrise"/></p> <p>RingVolume <input type="text" value="50"/></p>
---	--

Phonebook
RoomAnalytics
RoomScheduler
SIP
Security
SerialPort
Standby
SystemUnit
UserInterface
Peripherals
Proximity
UserManagement
Video
VoiceControl
WebEngine
Webex
RoomCleanup
Bookings
Miscellaneous

Audio

General Settings	
DefaultVolume	<input type="text" value="50"/> #
Input MicrophoneMode *	<input type="text" value="Focused"/> ▾
Ultrasound MaxVolume	<input type="text" value="70"/>
USB Mode *	<input type="text" value="SpeakerAndMicrophone"/> ▾
Microphones	
Mute	
Enabled *	<input type="text" value="True"/> ▾
NoiseRemoval	
Mode *	<input type="text" value="Manual"/> ▾
SoundsAndAlerts	
RingTone	<input type="text" value="Sunrise"/>
RingVolume	<input type="text" value="50"/>

Bluetooth

General Settings

Allowed*	True	▼
Enabled*	False	▼

Call History

General Settings

Mode*	On	▼	#
-------	----	---	---

Cameras

Background

Enabled*	True	▼
UserImagesAllowed*	True	▼
PowerLine Frequency*	Auto	▼

Camera

Brightness

DefaultLevel	20	
Mode*	Auto	▼

ExposureCompensation

Level	0
-------	---

SpeakerTrack

Mode*	Auto	▼
TrackingMode*	Auto	▼
Closeup*	Auto	▼

Whiteboard

Mode*	Off	▼
-------	-----	---

ConnectorDetection

Mode*	Auto	▼
CameraRight	2	
CameraLeft	1	

Conference

DefaultCall

Protocol *	Sip	#
Rate	6000	
DoNotDisturb DefaultTimeout	60	
Encryption Mode *	BestEffort	
FarEndMessage Mode *	Off	
MaxReceiveCallRate	6000	
MaxTotalReceiveCallRate	6000	#
MaxTotalTransmitCallRate	6000	#
MaxTransmitCallRate	6000	
MicUnmuteOnDisconnect Mode *	On	#
Multipoint Mode *	Auto	#

FarEndControl

Mode *	On	#
SignalCapability *	On	#

Facility Service

Service 1

CallType *	Video	#
Name	Live Support	#
Number		#
Type *	Helpdesk	#

Service 2

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

Service 3

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

Service 4

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

Service 5

CallType *	Video	
Name		
Number		
Type *	Helpdesk	

HTTP Client

General Settings	
Mode*	Off
AllowInsecureHTTPS*	False
AllowHTTP*	True
UseHttpProxy*	On

HTTP Feedback

General Settings	
TlsVerify*	On
UseHttpProxy*	On

Logging

General Settings	
CloudUpload Mode*	Off
Internal Mode*	On

External	
Mode*	Off
Protocol*	SyslogTLS
TlsVerify*	On

Server	
Address	
Port	514

Macros

General Settings	
AutoStart*	On
Mode*	Off
UnresponsiveTimeout	5

Network Services

General Settings

H323 Mode*	Off	▼
UPnP Mode*	On	▼
Websocket*	FollowHTTPService	▼
WelcomeText*	On	▼
Wifi Allowed*	True	▼

HTTP

Mode*	Off	▼	#
-------	-----	---	---

Proxy

Mode*	Off	▼
Url	<input type="text"/>	
LoginName	<input type="text"/>	
PACUrl	<input type="text"/>	

HTTPS

VerifyClientCertificate*	Off	▼
StrictTransportSecurity*	Off	▼

Server

MinimumTLSVersion*	TLSv1.1	▼
--------------------	---------	---

SNMP

CommunityName	<input type="text"/>	
Mode*	Off	▼
SystemContact	<input type="text"/>	
SystemLocation	<input type="text"/>	

SSH

HostKeyAlgorithm*	RSA	▼	
Mode*	Off	▼	#

SMTP

Mode*	Off	▼	#
Server	<input type="text"/>	#	
Port	0	#	
Security*	StartTls	▼	#
Username	<input type="text"/>	#	
From	<input type="text"/>	#	

Phone Book

Server 1

ID	<input type="text"/>		
Type*	CUCM	▼	#
URL	<input type="text"/>	#	
Pagination*	Enabled	▼	
TlsVerify*	On	▼	

Room Analytics

General Settings	
PeopleCountOutOfCall*	Off
PeoplePresenceDetector*	Off

AmbientNoiseEstimation	
Mode*	Off
Interval	10

ReverberationTime	
Mode*	Off
Interval	1800

Room Scheduler

General Settings	
Enabled*	False

SIP

General Settings	
MinimumTLSVersion*	TLSv1.0

Security

Audit	
Logging	
Mode*	Internal
OnError	
Action*	Ignore
Server	
Address	
Port	514
PortAssignment*	Auto
Fips Mode*	Off
Session	
InactivityTimeout	0
ShowLastLogon*	Off
MaxTotalSessions	20
MaxSessionsPerUser	20
MaxFailedLogins	0
FailedLoginsLockoutTime	60

Serial Port

General Settings

BaudRate*	115200	▼
LoginRequired*	On	▼ #
Mode*	On	▼ #

Standby

General Settings

BootAction*	DefaultCameraPosition	▼
Control*	On	▼ #
Delay	10	#
StandbyAction*	PrivacyPosition	▼ #
WakeupAction*	RestoreCameraPosition	▼
WakeupOnMotionDetection*	Off	▼ #

Signage

Url	<input type="text"/>	
Mode*	Off	▼
RefreshInterval	0	<input type="text"/>
Audio*	Off	▼

System Unit

General Settings

CustomDeviceId	<input type="text"/>
Name	<input type="text"/> #

CrashReporting

Mode*	Off	▼
URL	<input type="text"/> #	

User Interface

General Settings

Accessibility IncomingCallNotification*	Default	ⓘ
Bookings Visibility Title*	Auto	▼
ContactInfo Type*	Auto	▼
Diagnostics Notifications*	Auto	▼
Branding AwakeBranding Colors*	Auto	▼
KeyTones Mode*	On	▼
SoundEffects Mode*	On	▼
Proximity Notifications*	Auto	▼
CustomMessage	<input type="text"/>	ⓘ
Whiteboard ActivityIndicators*	On	▼
Assistant Mode*	On	▼
Security Mode*	Normal	▼

Features

HideAll*	False	▼
Call		
Start*	Auto	▼
MidCallControls*	Auto	▼
End*	Auto	▼
VideoMute*	Auto	▼
JoinWebex*	Auto	▼ ⓘ
Keypad*	Auto	▼
MusicMode*	Hidden	▼
Share		
Start*	Auto	▼
Whiteboard		
Start*	Auto	▼

OSD

EncryptionIndicator*	Auto	▼ ⓘ
Output*	1	▼
HalfwakeMessage	<input type="text"/>	
Mode*	Auto	▼

Phonebook

Mode*	ReadWrite	▼
DefaultSearchFilter*	All	▼

SettingsMenu

Mode*	Unlocked	▼ ⓘ
Visibility*	Auto	▼

Peripherals

General Settings

InputDevice Mode*	Off	▼
Pairing CiscoTouchPanels RemotePairing*	On	▼

Profile

TouchPanels*	0	▼
Cameras*	Minimum1	▼
ControlSystems*	NotSet	▼

Proximity

General Settings	
Mode*	Off <input type="button" value="v"/> #
AlternatePort Enabled*	False <input type="button" value="v"/> #

Services	
ContentShare	
ToClients*	Disabled <input type="button" value="v"/> #
FromClients*	Enabled <input type="button" value="v"/> #
CallControl*	Disabled <input type="button" value="v"/> #

User Management

LDAP	
Mode*	Off <input type="button" value="v"/> #
Encryption*	LDAPS <input type="button" value="v"/> #
VerifyServerCertificate*	Off <input type="button" value="v"/> #
BaseDN	<input type="text"/> #
Attribute	<input type="text"/> #
MinimumTLSVersion*	TLSv1.2 <input type="button" value="v"/> #
Server	
Address	<input type="text"/> #
Port	0 <input type="text"/> #
Admin	
Group	<input type="text"/> #
Filter	<input type="text"/> #

PasswordPolicy	
ReuseLimit	<input type="text" value="12"/>
MaxLifetime	<input type="text" value="0"/>
Complexity	
MinimumLength	<input type="text" value="8"/>
MinimumUppercase	<input type="text" value="0"/>
MinimumLowercase	<input type="text" value="0"/>
MinimumDigits	<input type="text" value="0"/>
MinimumSpecial	<input type="text" value="0"/>

Video

Input

Connector 1

InputSourceType* camera

Name Camera

Visibility* Never

CameraControl

CameraId* 1

Mode* On

Connector 2

InputSourceType* PC

Name PC (USB-C)

PresentationSelection* Desktop

Quality* Sharpness

RGBQuantizationRange* Auto

Visibility* IfSignal

PreferredResolution* 1920_1080_60

CameraControl

CameraId* 1

Mode* Off

CEC

Mode* On

Monitors* Auto

Output Connector 1 Resolution* 1920_1080_60

DefaultMainSource* 1

Presentation

DefaultSource* 2

Priority* Equal

Selfview

Default

FullscreenMode* Current

Mode* Current

OnMonitorRole* Current

PIPPosition* Current

OnCall

Duration 10

Mode* Off

Voice Control

General Settings

Wakeword Mode* On

Web Engine

General Settings

Mode*	Off	▼
RemoteDebugging*	Off	▼
UseHttpProxy*	On	▼
MinimumTLSVersion*	TLSv1.1	▼

Webex**General Settings**

Meetings JoinProtocol*	SIP	▼
CloudUpgrades Mode*	Off	▼

CloudProximity

Mode*	Off	▼
GuestShare*	Auto	▼

Room Cleanup**AutoRun**

HourOfDay	0
-----------	---

ContentType

Whiteboards*	Daily	▼
WebData*	Daily	▼

Bookings**General Settings**

ProtocolPriority*	Auto	▼
-------------------	------	---

Miscellaneous**General Settings**

Configuration Control Mode*	Unified CM and Endpoint	▼	#
Room Name (from Exchange(R))			#
LoadServer			#
Webex Devices Onboarding Token			#

Admin username and password

Admin Username	admin	#
Admin Password		#

Customization Provisioning

Customization File		#	
Customization Hash Type*	SHA512	▼	#
Customization Hash		#	

Note: If wanting to enable the admin username and password or SMTP password enabled, then should utilize a secure profile with TFTP encryption enabled.

For information about TCP and UDP ports used by the Cisco RoomOS Series and the Cisco Unified Communications Manager, refer to the **Cisco Unified Communications Manager TCP and UDP Port Usage** document at this URL:

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

For more information, see the **Cisco RoomOS Series Administrator Guide**.

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html>

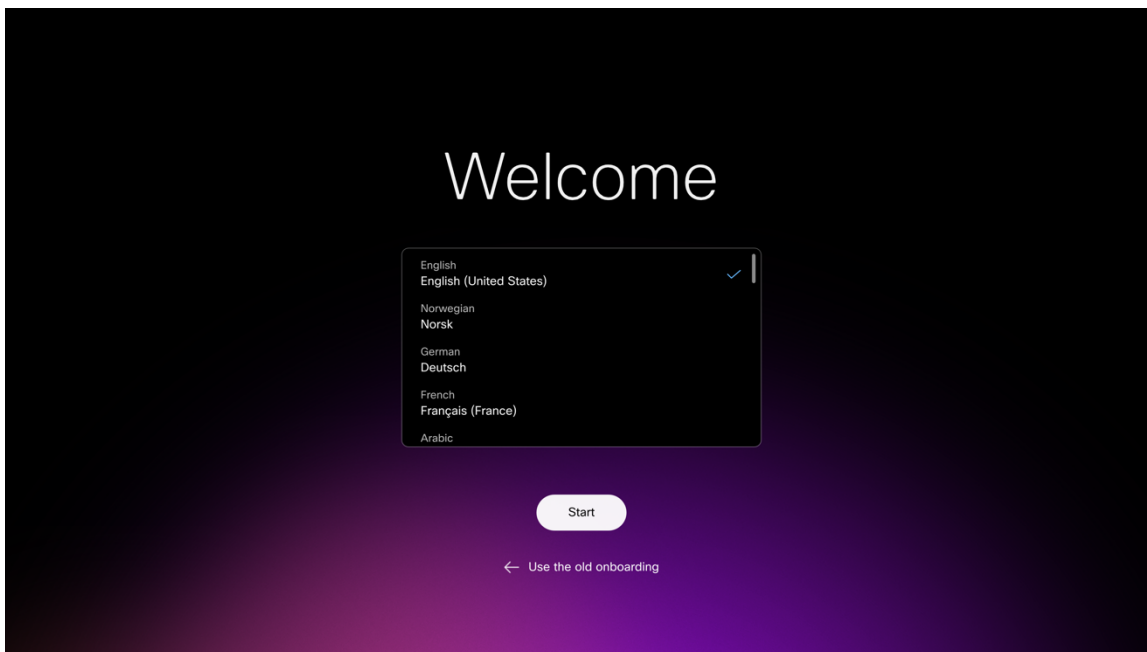
Configuring the Cisco RoomOS Series

To configure the Cisco RoomOS Series, use the local user interface.

Wi-Fi Profile Configuration

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

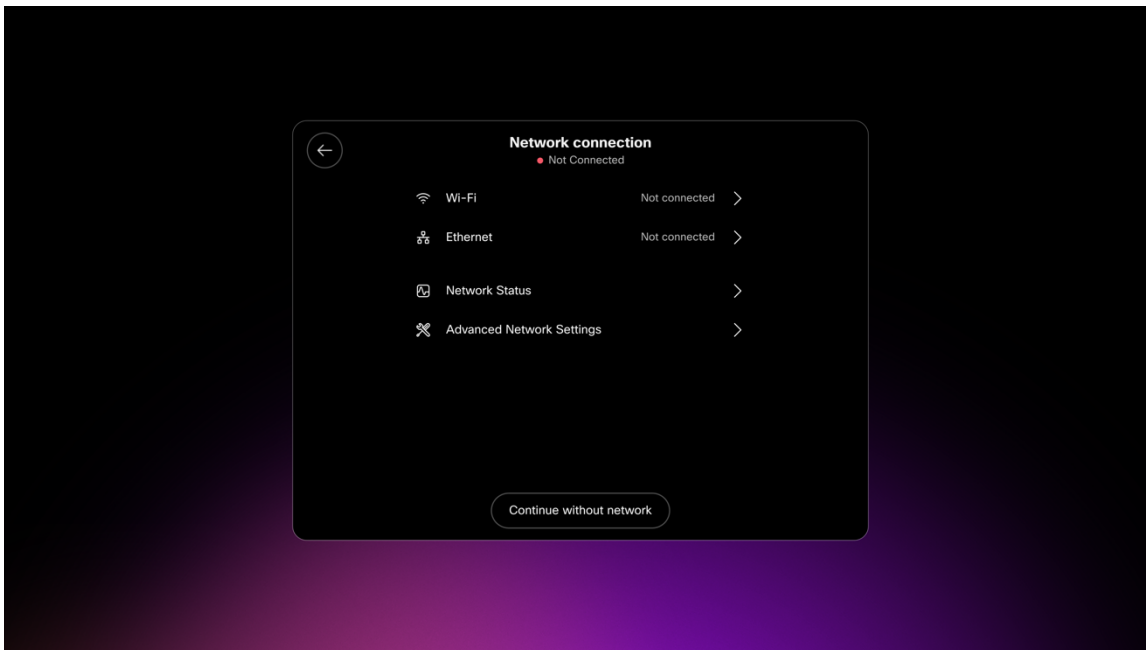
- For an out of box (factory reset) Cisco RoomOS Series, configure the Wi-Fi network via the startup wizard.



- Configuration options will be determined by whether a broadcasted Wi-Fi network is being configured or a Wi-Fi network is being manually configured.
- Below lists the available security modes supported and the key management and encryption types that can be used for each mode.
The key management and encryption type (cipher) will be auto-configured based on the access point's current configuration, where precedence is giving to the strongest key management type enabled (e.g. WPA3) then the strongest cipher enabled (e.g. AES).

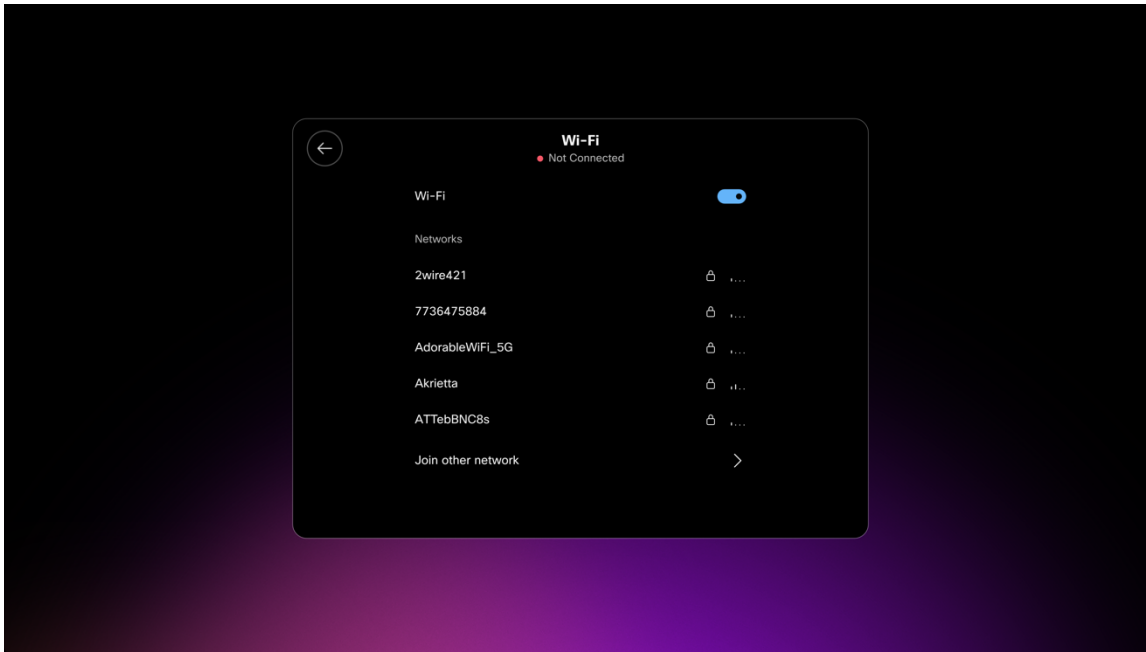
Security	802.1x Type	Key Management	Encryption
None	N/A	None	None
Personal	N/A	WPA3-SAE WPA2-PSK-SHA256 WPA2-PSK	AES TKIP
Enterprise	FAST PEAP TLS TTLS	WPA3-802.1X-SHA256 WPA2-802.1X-SHA256 WPA2-802.1X	AES TKIP

- Select **Wi-Fi** to configure a Wi-Fi network.

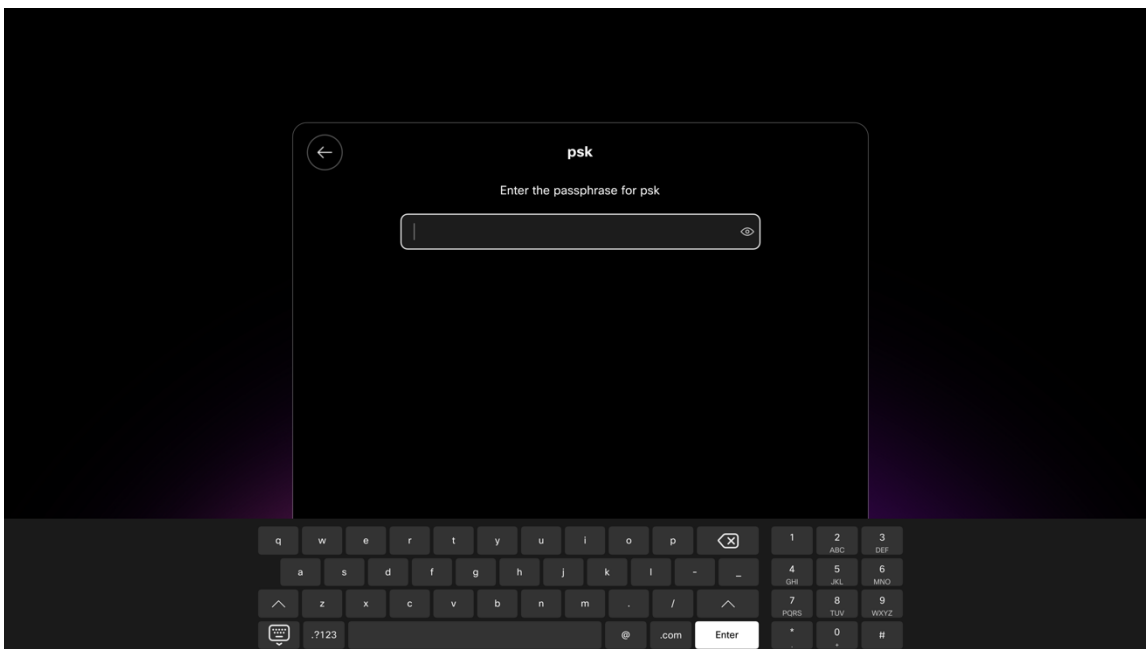


Configuring a Broadcasted Wi-Fi Network

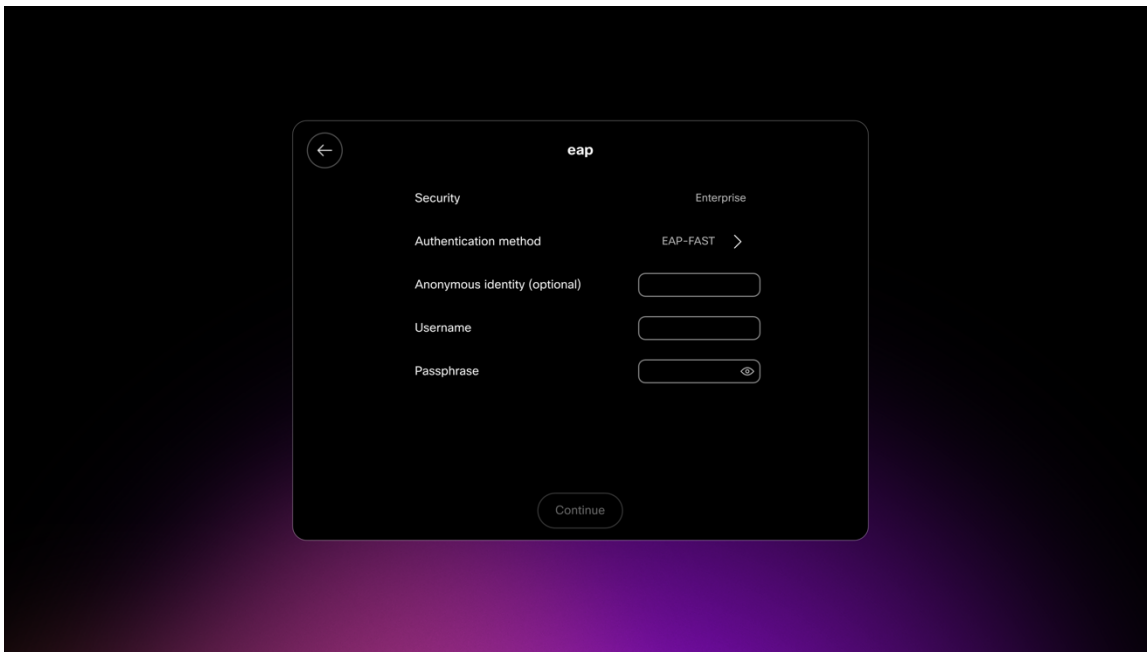
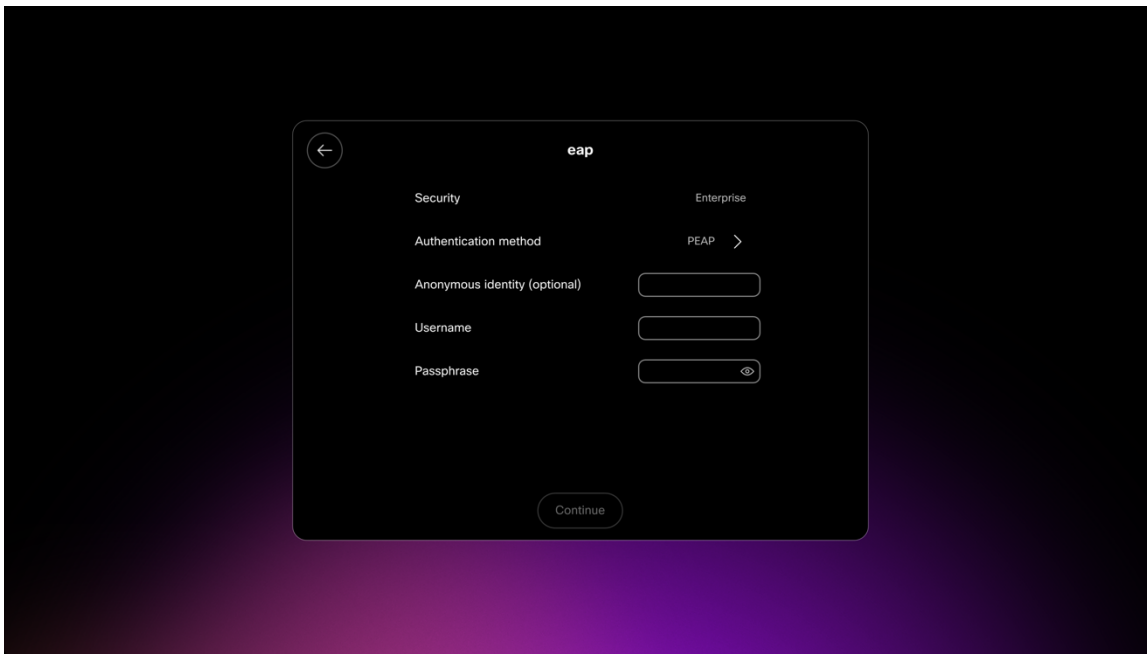
- If the Wi-Fi network is broadcasted, select the desired Wi-Fi network from the list, then enter the required credentials depending on the Wi-Fi network's security settings.

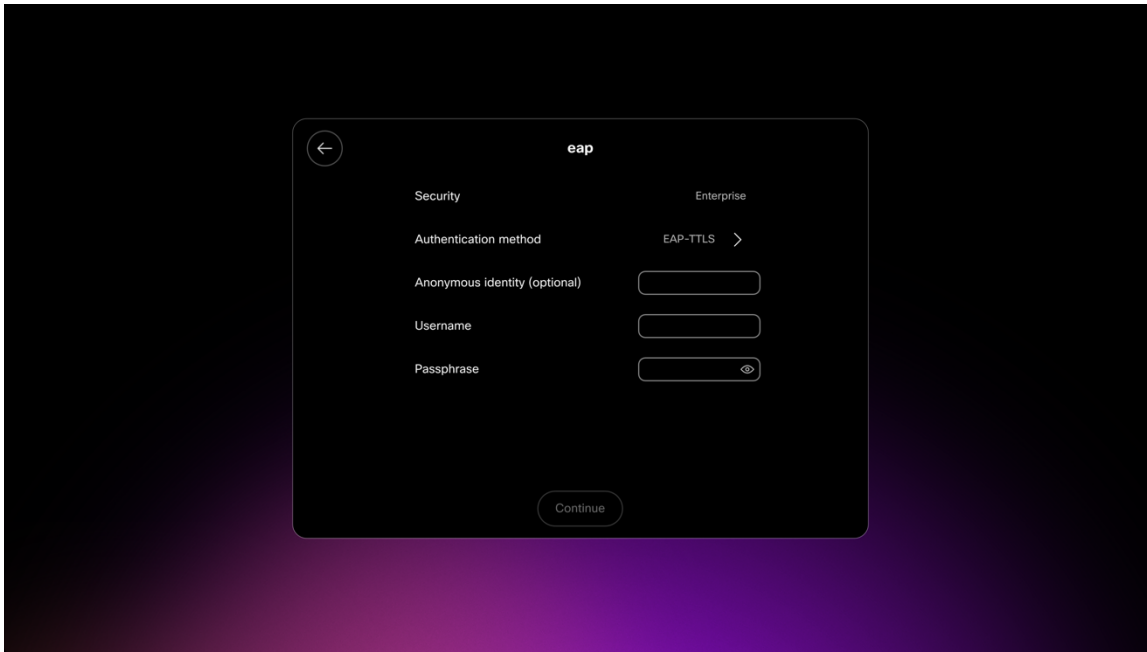


- To connect to an open Wi-Fi network, simply click on the Wi-Fi network name.
- To connect to a PSK enabled Wi-Fi network, click on the Wi-Fi network name, then enter the 8-63 ASCII or 64 HEX **Password**.

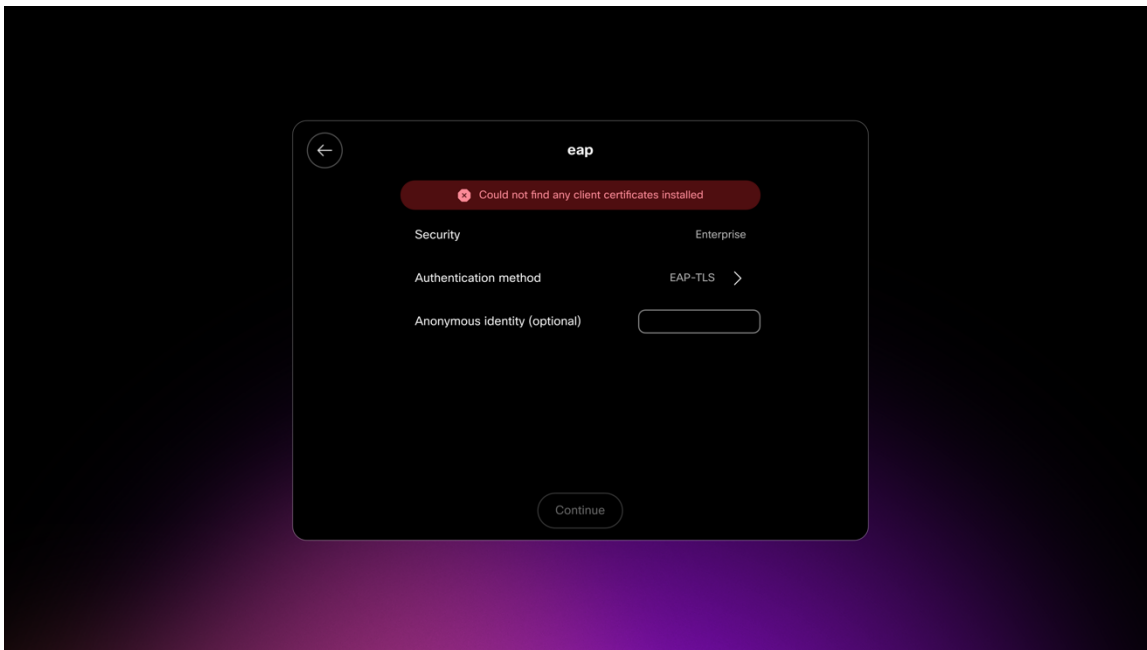


- To connect to an EAP enabled Wi-Fi network, click on the Wi-Fi network name, then select the **Authentication method**.
- If configuring a PEAP, EAP-FAST (FAST), or EAP-TTLS (TTLS) Wi-Fi network, enter the **Username** and **Password**.



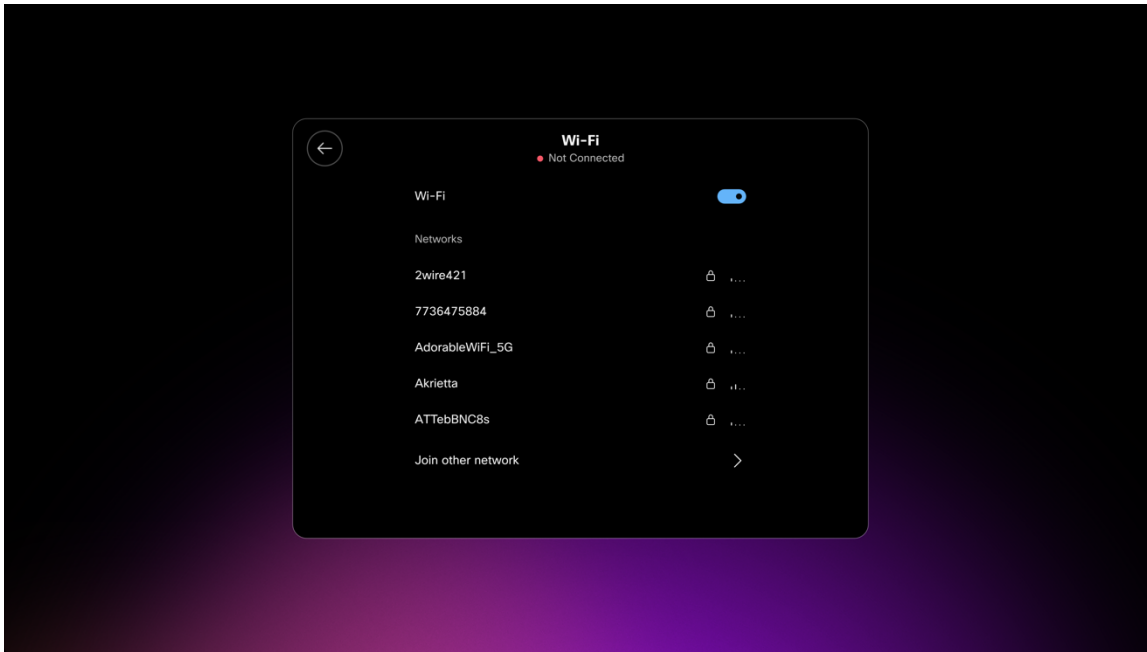


- If configuring an EAP-TLS (TLS) Wi-Fi network, will need to ensure the proper user and CA certificates are installed via the device webpage.

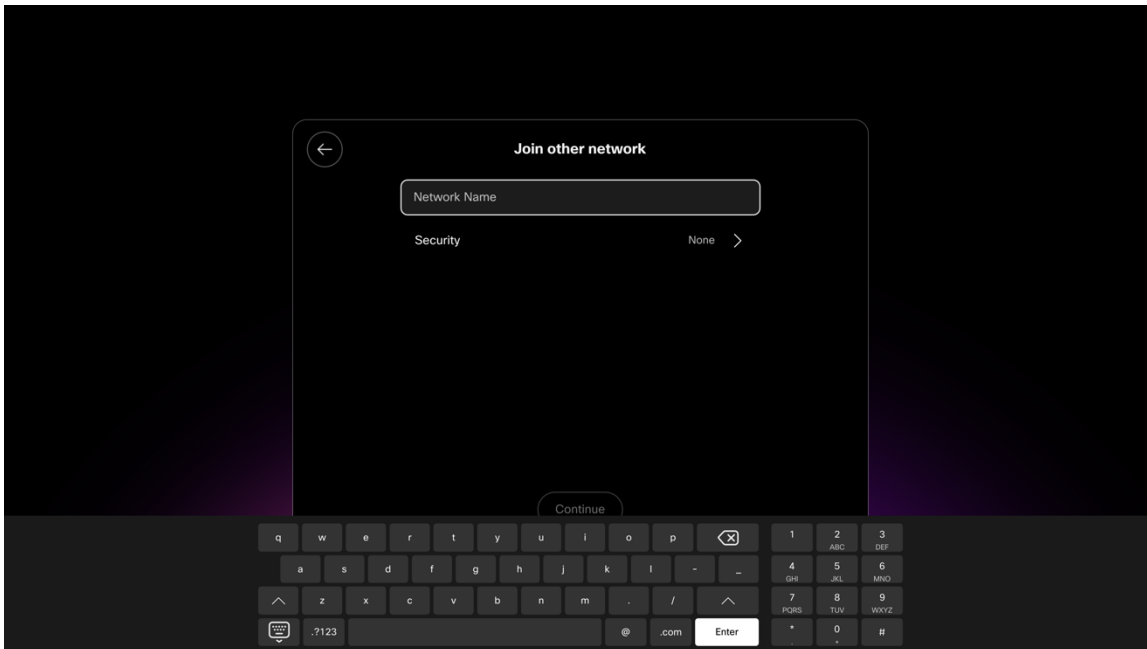


Configuring a Non-Broadcasted Wi-Fi Network

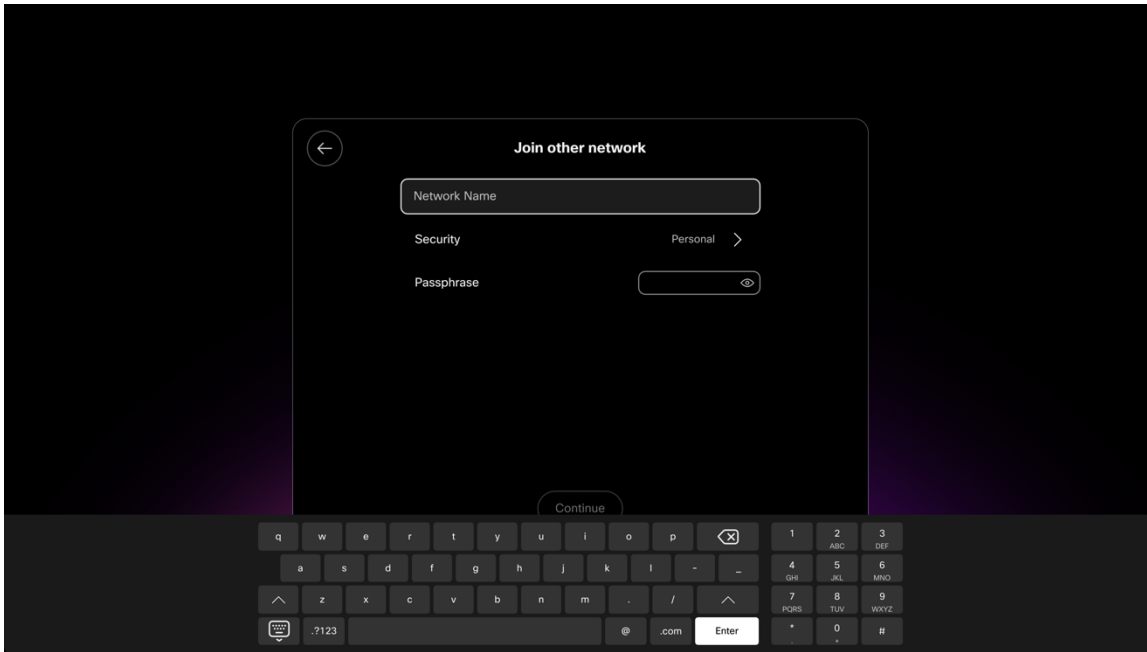
- If manually configuring a non-broadcasted (hidden) Wi-Fi network, select **Join other network**.
- Then configure the **Network name** (SSID), **Security** type, and enter the required credentials depending on the Wi-Fi network's security settings.



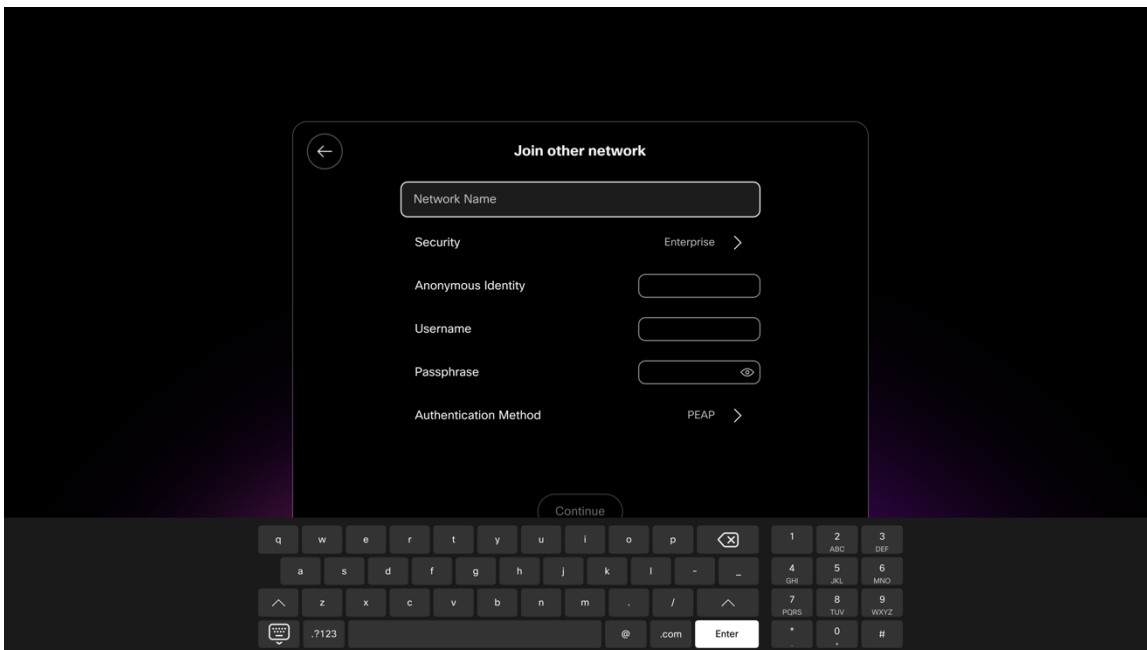
- To connect to an open Wi-Fi network, enter the **Network name**, then set **Security** to **None**.

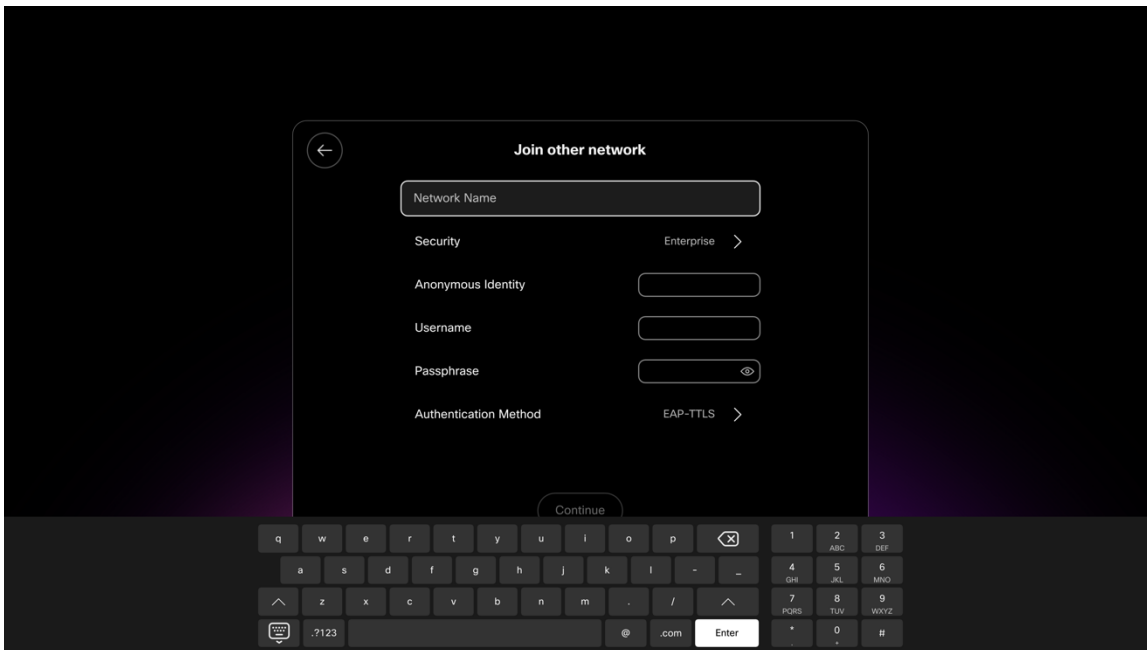
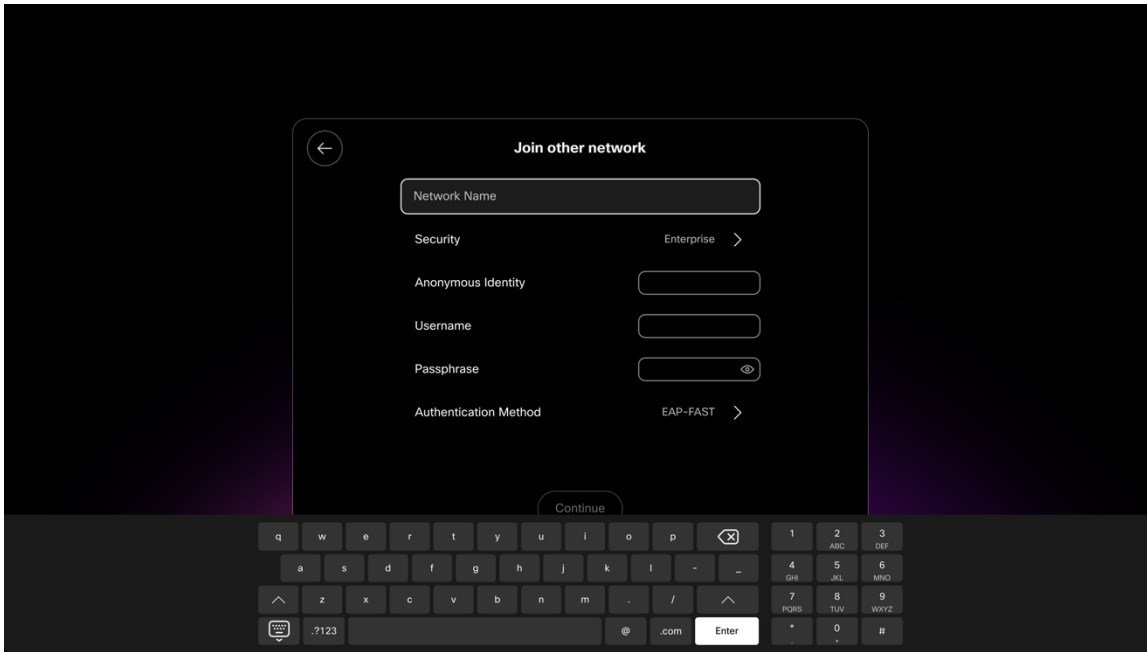


- To connect to a PSK enabled Wi-Fi network, enter the **Network name**, set **Security** to **Personal**, then enter the 8-63 ASCII or 64 HEX **Password**.

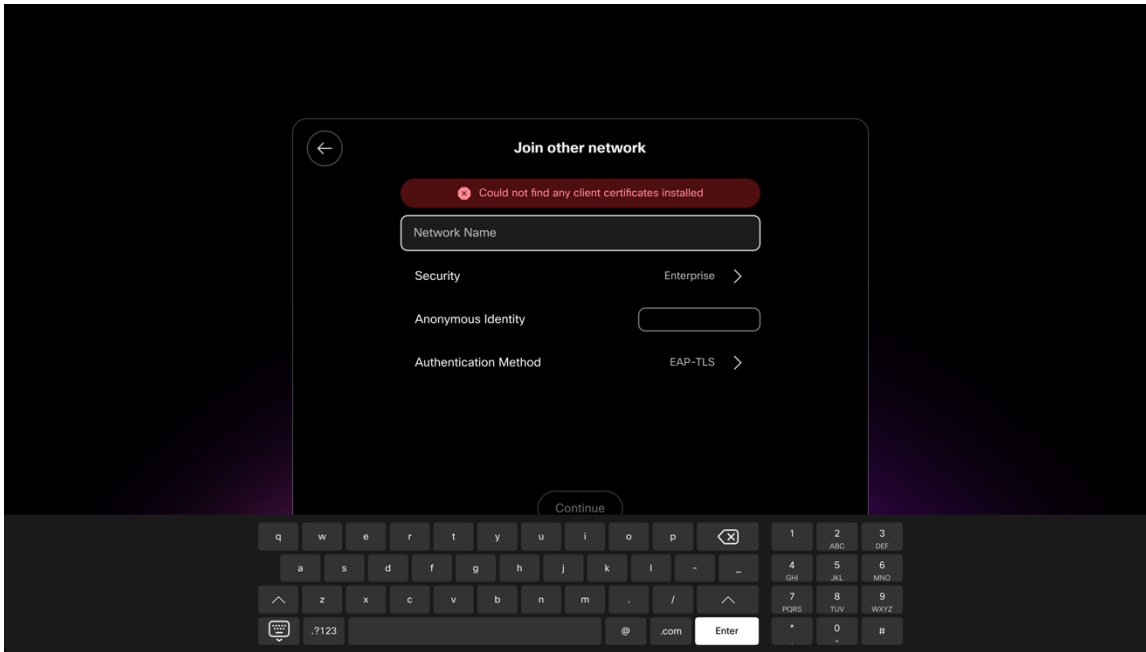


- To connect to an EAP enabled Wi-Fi network, enter the **Network name**, set **Security** to **Enterprise**, then select the **Authentication method**.
- If configuring a PEAP, EAP-FAST (FAST), or EAP-TTLS (TTLS) Wi-Fi network, enter the **Username** and **Passphrase**.



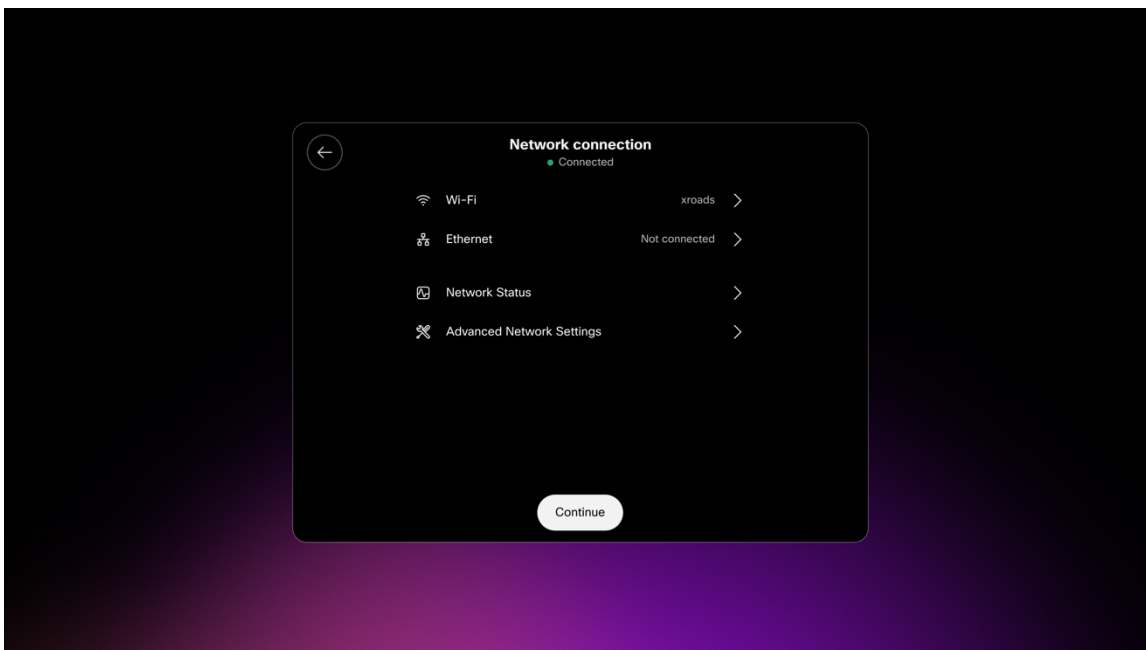


- If configuring an EAP-TLS (TLS) Wi-Fi network, will need to ensure the proper user and CA certificates are installed via the device webpage.



Configuring Advanced Options for the Wi-Fi Network

- **IP Stack, DNS, and Proxy Settings** can be configured in the **Advanced Network Settings** section of the **Network connection** settings.



← **Advanced network settings** Apply

IP Stack

IPv4 and IPv6

IPv4

IPv6

DNS

DNS Domain Name

DNS address 1

DNS address 2

DNS address 3

← **Advanced network settings** Apply

DNS Domain Name

DNS address 1

DNS address 2

DNS address 3

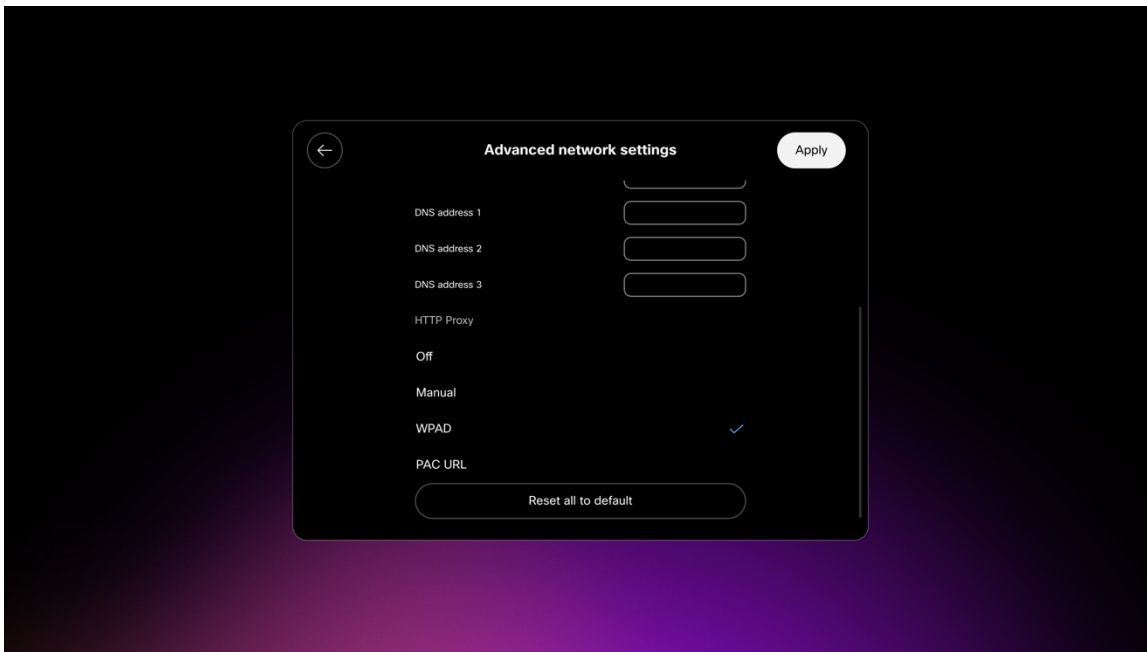
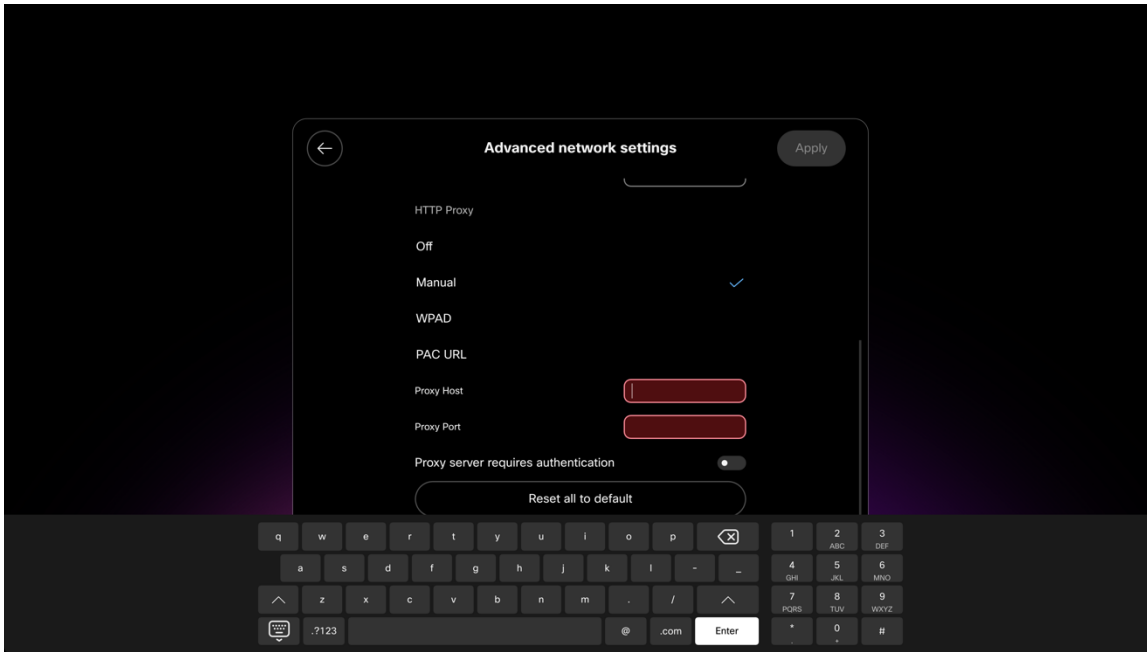
HTTP Proxy

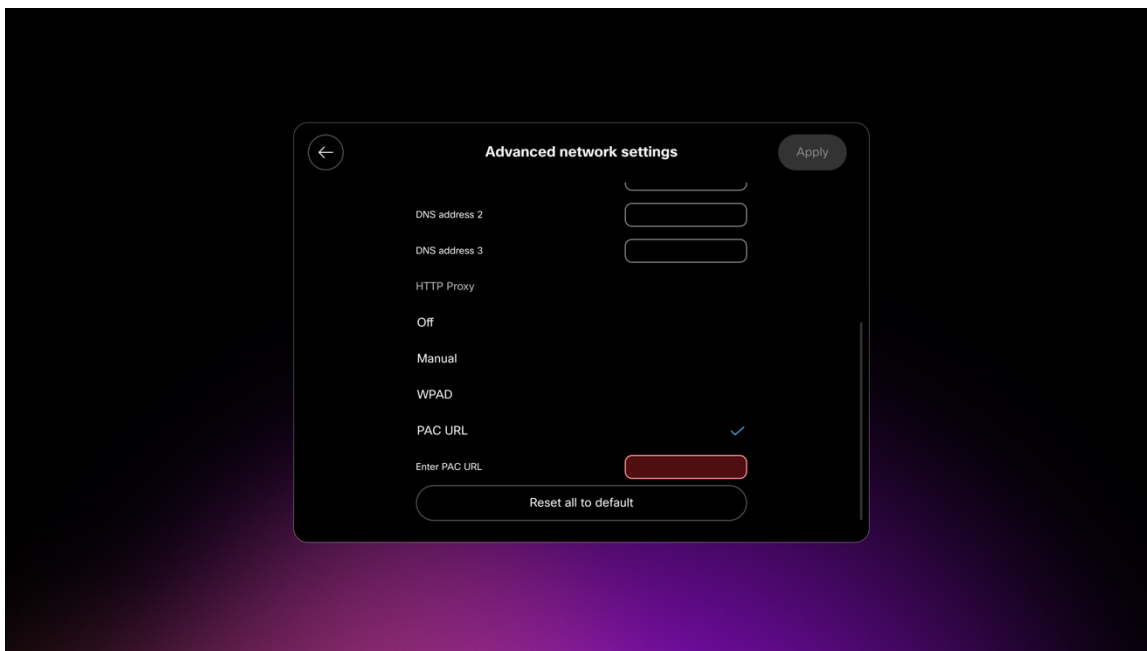
Off

Manual

WPAD

PAC URL





Note: The access point must support AES (CCMP128) as TKIP can only be used as the broadcast/multicast cipher. CCMP256, GCMP128, and GCMP256 encryption ciphers are not supported.

For more information, refer to the **Cisco RoomOS Series Administrator Guide** at this URL:

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html>

Certificate Management

The Cisco RoomOS Series can utilize X.509 digital certificates for **EAP-TLS** or to enable server validation when using **PEAP**, **EAP-FAST**, or **EAP-TTLS**.

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

Only Base-64 (PEM) encoding is acceptable for the client and server certificates (DER encoding is not supported).

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

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

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

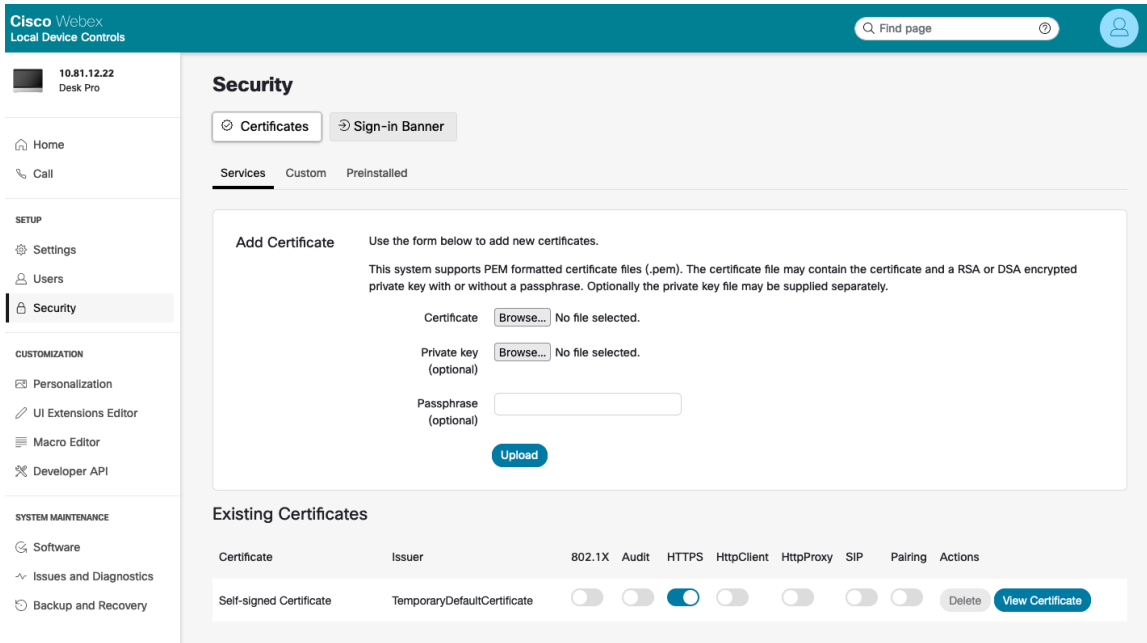
Microsoft® Certificate Authority (CA) servers are recommended. Other CA server types may not be completely interoperable with the Cisco RoomOS Series.

Installing Certificates

Certificates can be installed via the Cisco RoomOS Series webpage.

Automatic certificate enrollment is currently not supported.

To install certificates via the Cisco RoomOS Series webpage, select **Security > Certificates**, then select **Services** or **Custom** depending on whether a user certificate or server certificate (root CA) is to be installed.



A user certificate must be installed to utilize **EAP-TLS**.

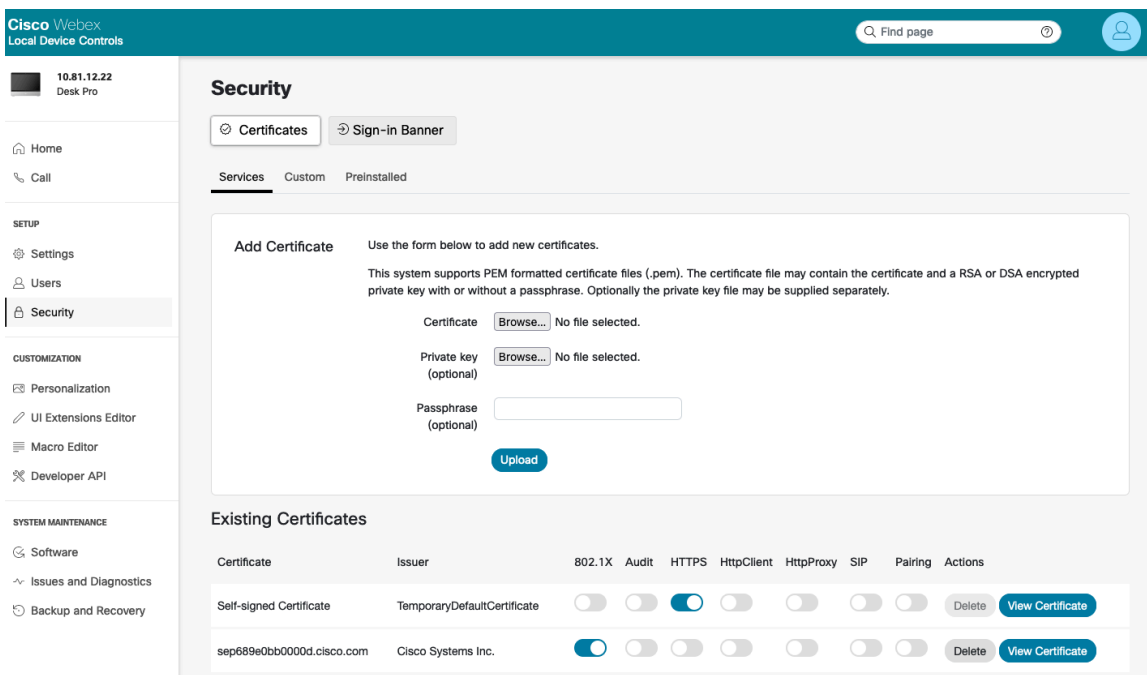
Optionally the private key can be uploaded along with the certificate.

A password may need to be entered to extract the certificates and keys.

Ensure the user certificate is enabled for **802.1X** after it is installed successfully.

Only a single user certificate can be enabled for **802.1X**, therefore that certificate is used automatically as the EAP-TLS user certificate and no additional Wi-Fi profile configuration is required

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



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

Once installed, server validation is automatically enabled and no additional Wi-Fi profile configuration is required.

Security

Certificates Sign-in Banner

Services Custom Preinstalled

Add Certificate Authority Use the form below to add new certificate authorities.
This system supports PEM formatted files (.pem) with one or more CA certificates within the file.

Browse... No file selected.

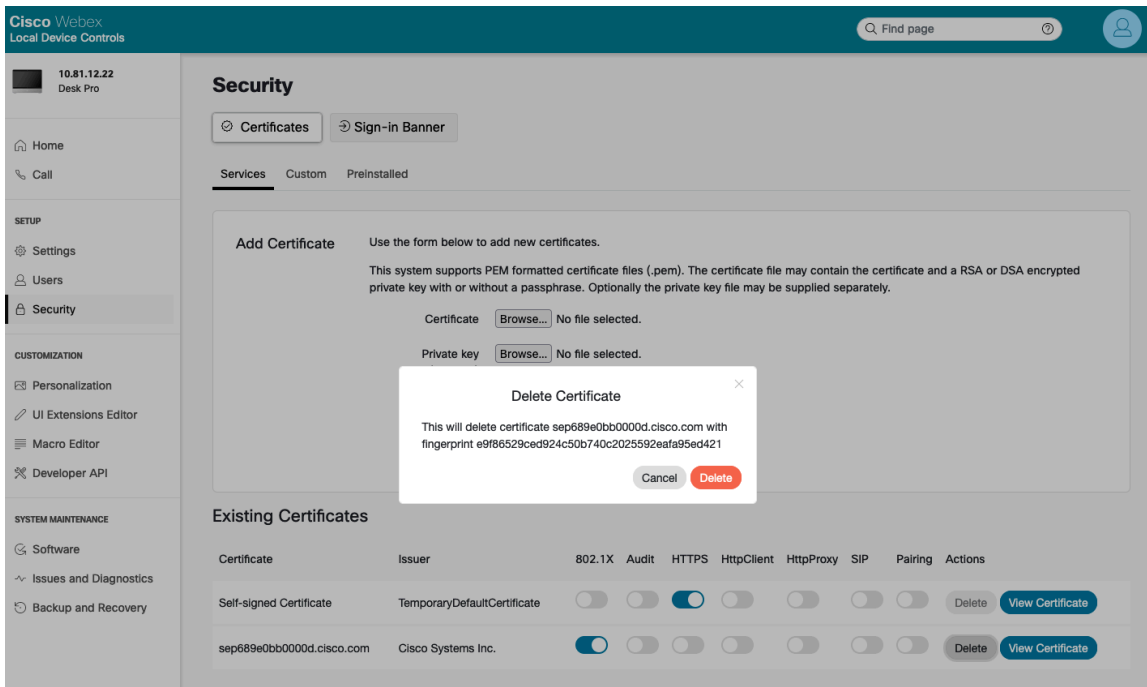
Existing Certificate Authorities

Certificate	Issuer	Details	Actions
IdenTrust Commercial Root CA 1	IdenTrust	View	Delete

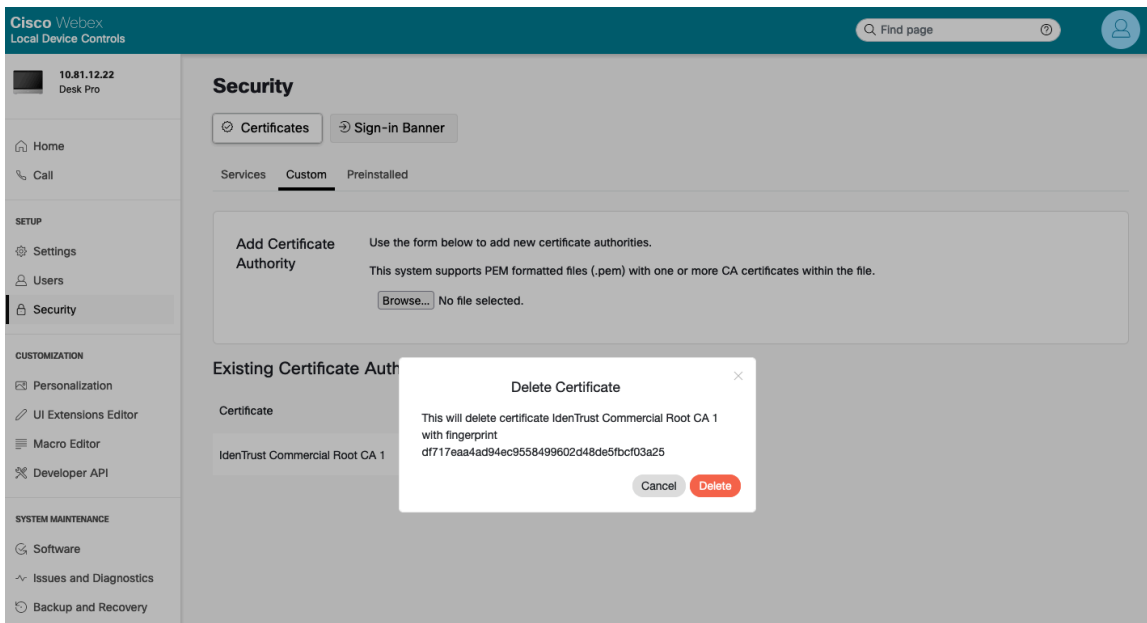
Removing Certificates

Certificates can be removed individually.

To remove an individual user certificate, select **Security > Certificates > Services**, then select **Delete**.



To remove an individual user certificate, select **Security > Certificates > Custom**, then select **Delete**.



For more information, refer to the **Cisco RoomOS Series Administrator Guide** at this URL:

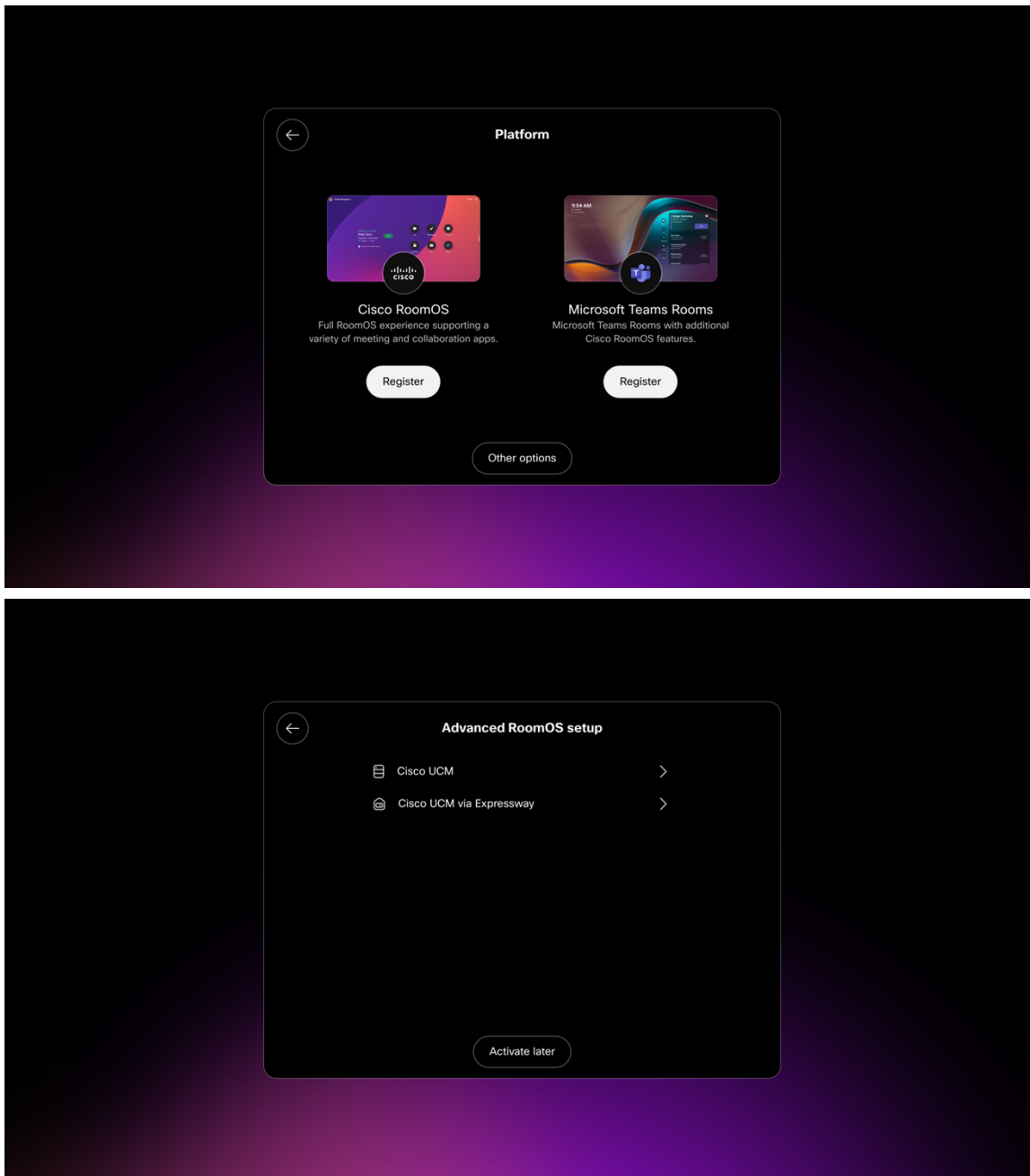
<http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html>

Call Control Configuration

The Cisco RoomOS Series can register to various call control systems.

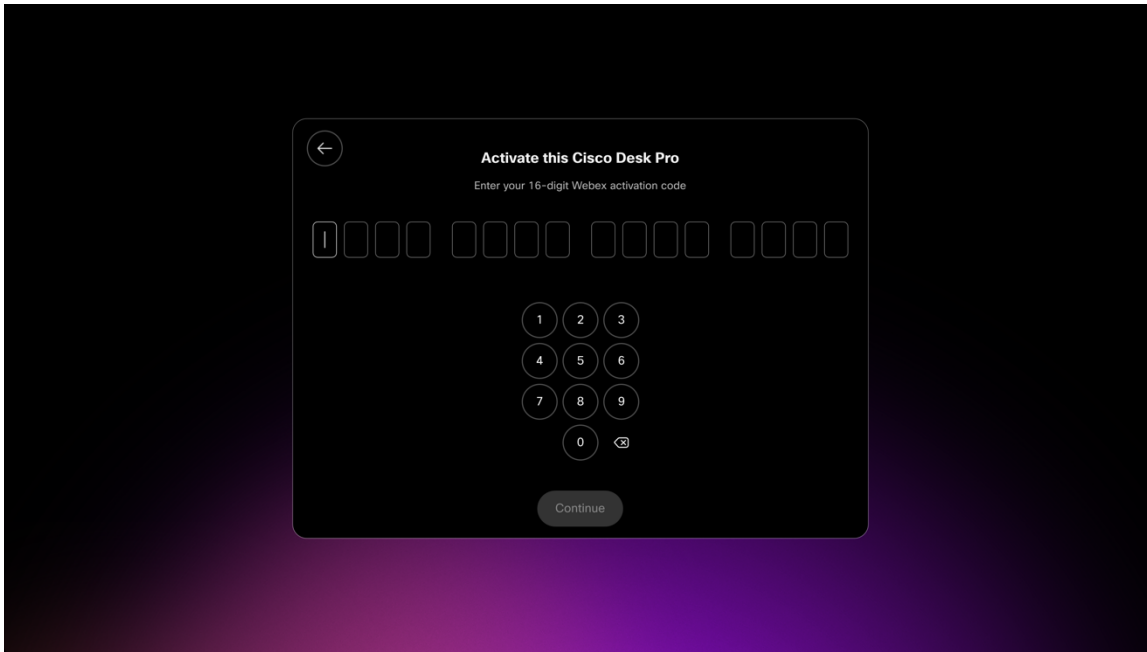
Cisco RoomOS Series Wireless LAN Deployment Guide

Select the desired call control system via the startup wizard.



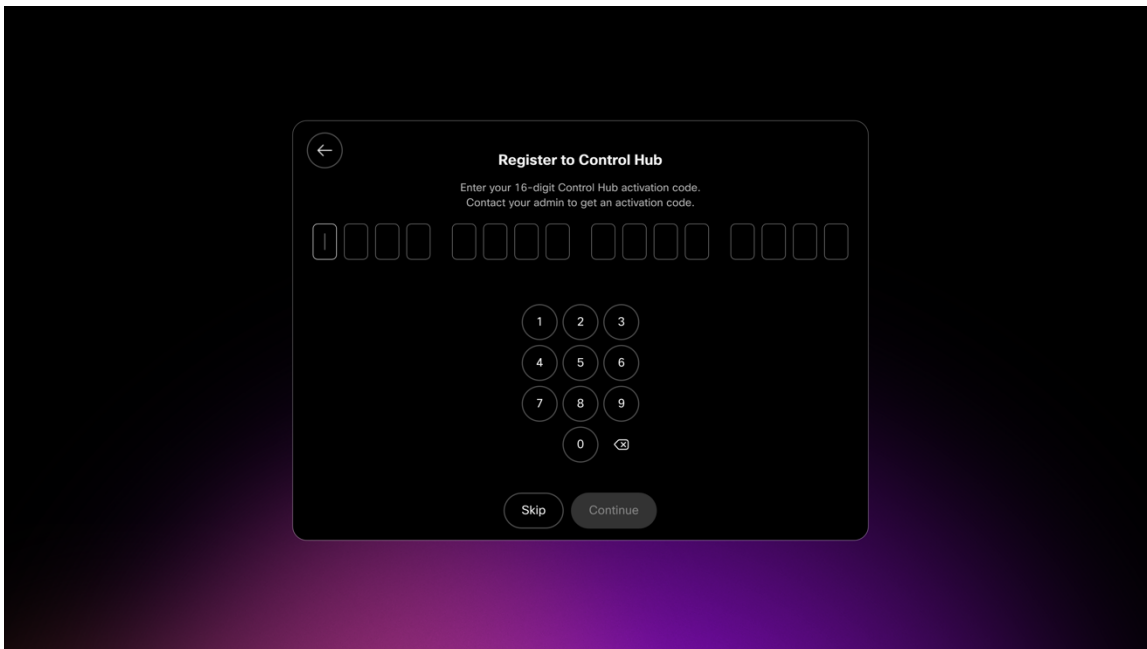
Webex

If **Cisco RoomOS** is selected, enter the 16 digit activation code and configure the proxy options as necessary.



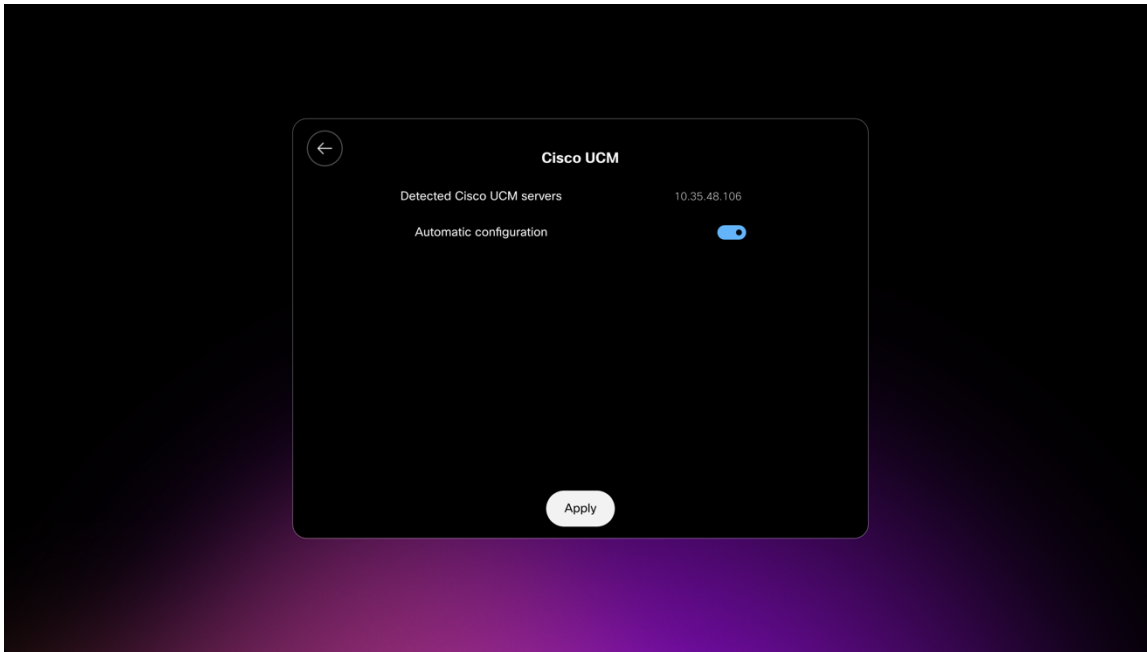
Microsoft Teams Rooms

If **Microsoft Teams Rooms** is selected, enter the 16 digit activation code and configure the proxy options as necessary.



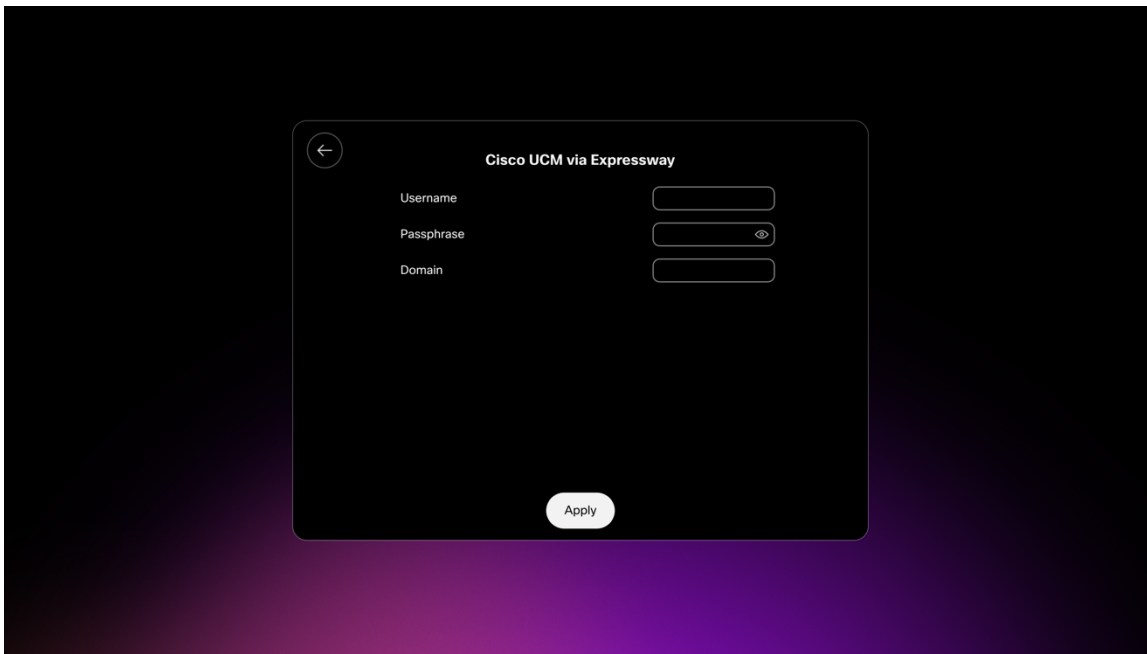
Cisco Unified Communications Manager (UCM)

If **Cisco UCM** is selected under **Other Options**, either use the automatic configuration selection to use the **Cisco UCM server** address provided via the network or enter the **Cisco UCM server** manually.



Cisco Unified Communications Manager (UCM) via Expressway

If **Cisco UCM via Expressway** is selected under **Other Options**, enter the **Username**, **Passphrase**, and **Domain** information.



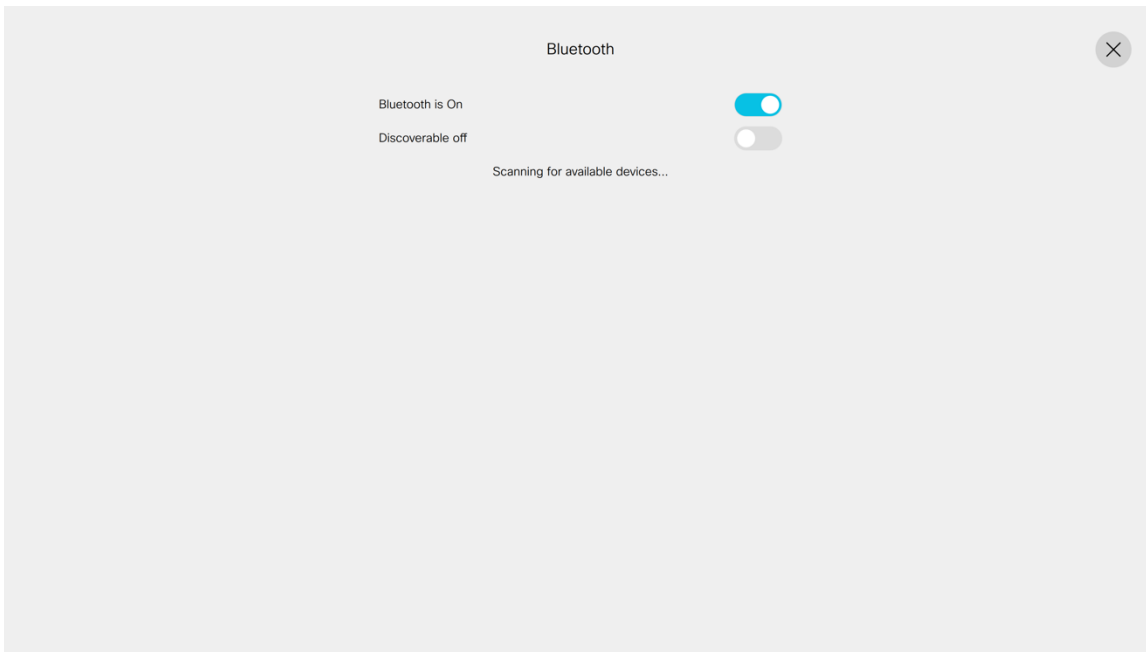
Bluetooth Settings

The Cisco RoomOS Series includes Bluetooth support, which enables hands-free communications.

To pair a Bluetooth headset to the Cisco RoomOS Series, follow the instructions below.

- Navigate to **Settings > Bluetooth**.

- Ensure that **Bluetooth** is set to **On**.



- Ensure the Bluetooth device is in pairing mode.
 - Select the Bluetooth device after it is displayed in the list.
 - The Cisco RoomOS Series will then attempt to pair automatically with the Bluetooth device.
 - If unsuccessful, enter the pin code when prompted.
 - Once paired, the Cisco RoomOS Series will attempt to connect to the Bluetooth device.
- If the Bluetooth device is not displayed, set Discoverable to **On** and select the Cisco RoomOS from the far end device.
- To disconnect the Bluetooth device simply tap on it. Tap it again to connect.
- Select **Unpair** to forget the paired Bluetooth device.

Upgrading Firmware

Webex

The firmware version to be installed on the Cisco RoomOS Series is determined by the configured software upgrade channel in the Webex Control Hub (Stable, Beta, Latest) and is pushed down automatically as new firmware becomes available for that software upgrade channel.

Cisco Unified Communications Manager

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

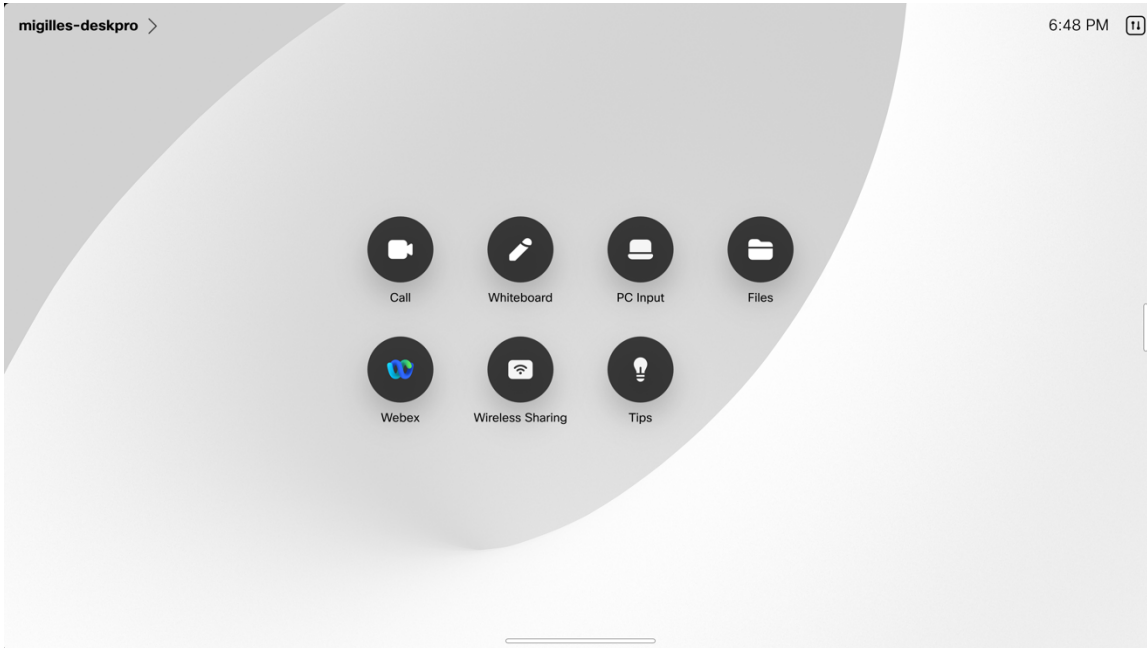
For information on how to install the COP file, refer to the **Cisco Unified Communications Manager Operating System Administration Guide** at this URL:

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

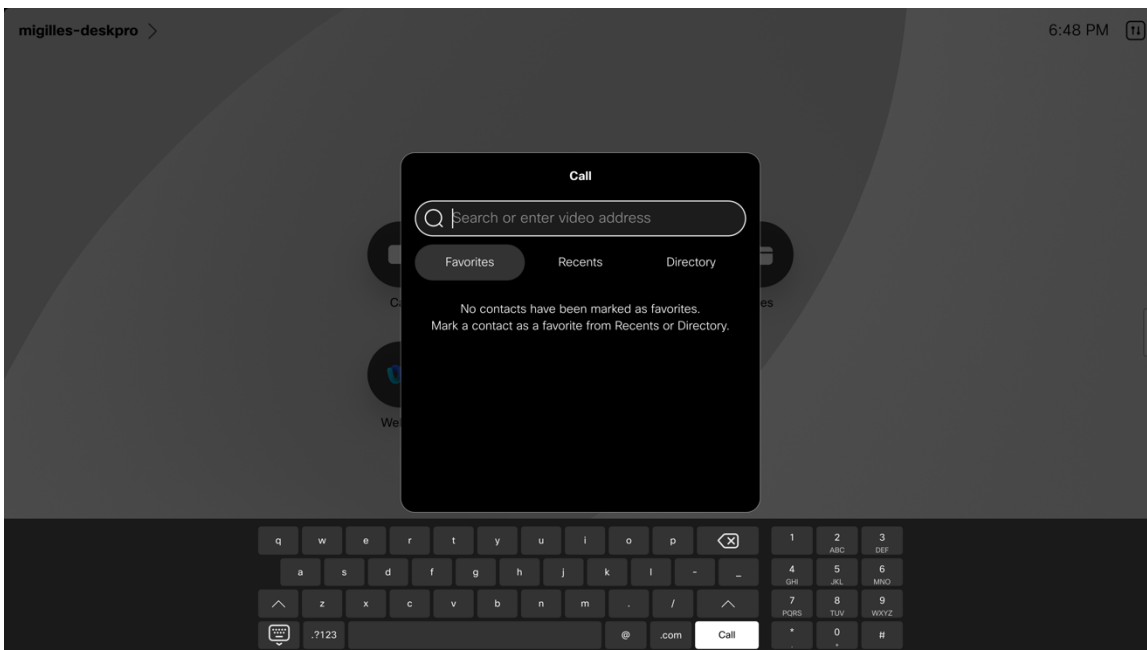
The downloaded device configuration file is parsed and the device load is identified. The Cisco RoomOS Series then downloads the firmware files to flash if it is not running the specified image already.

Using the Cisco RoomOS Series

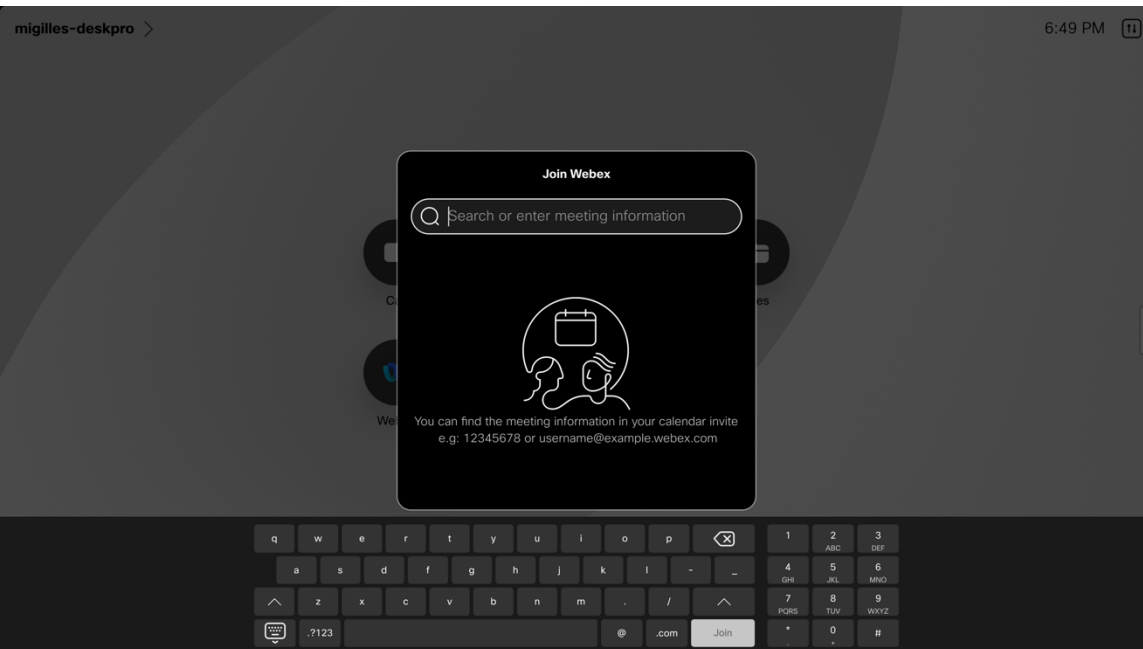
The Cisco RoomOS Series offers various collaboration options including calling and sharing content either locally or via a meeting.



Select the **Call** option to make a call, then enter the name, video address, or phone number.



Select the desired meeting option to join a meeting, then enter meeting information.

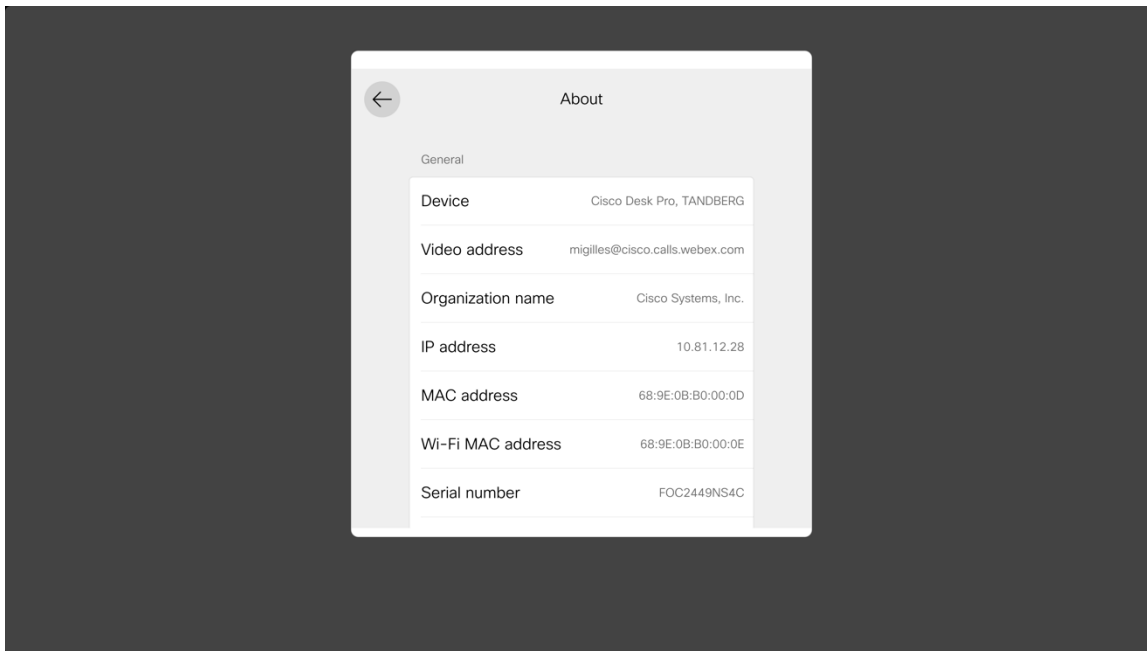


Troubleshooting

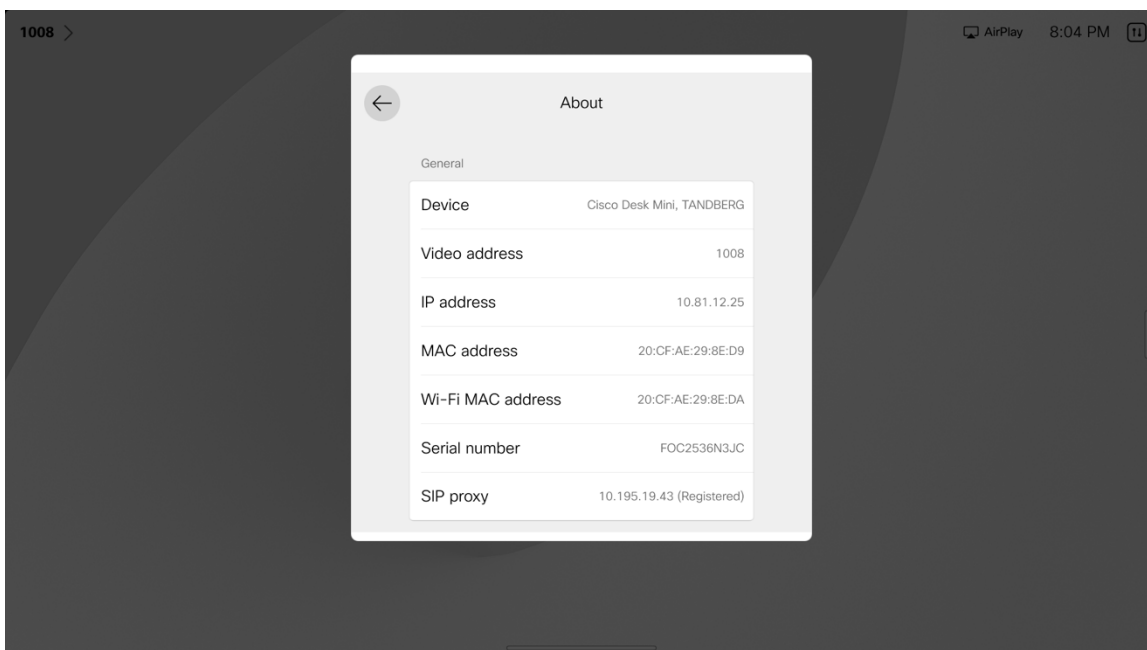
About Device

Video address, IP address, MAC address, serial number, and version information is displayed in **Settings > About this device**.

Webex

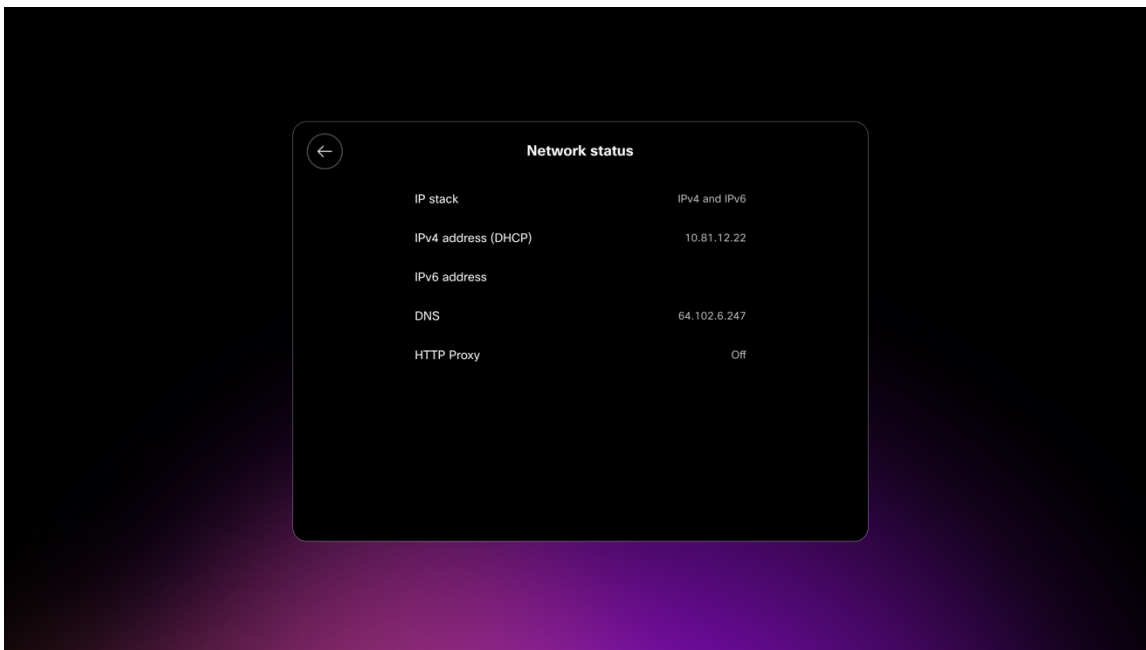
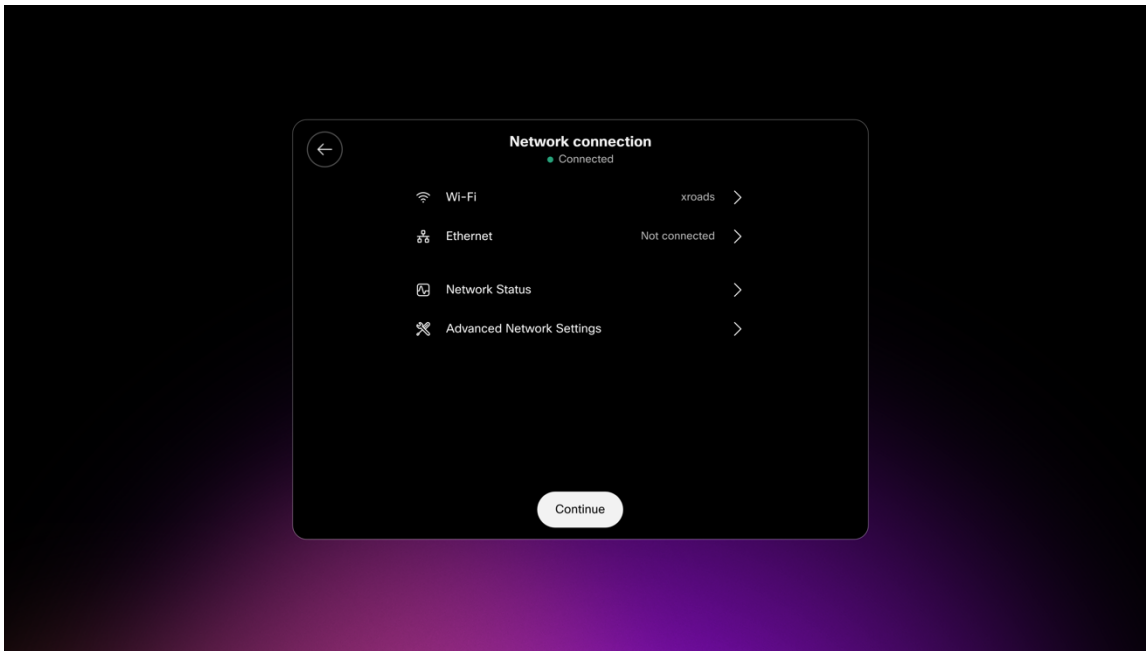


Cisco Unified Communications Manager



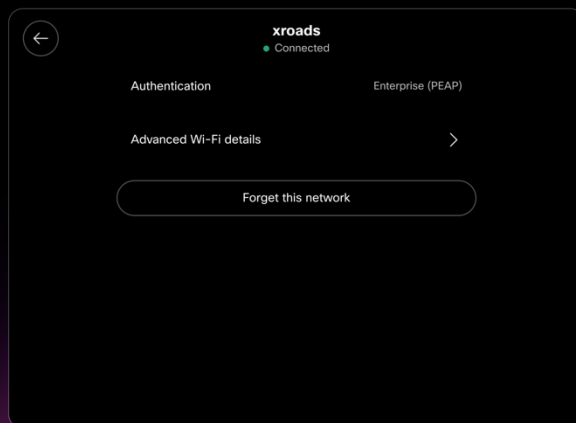
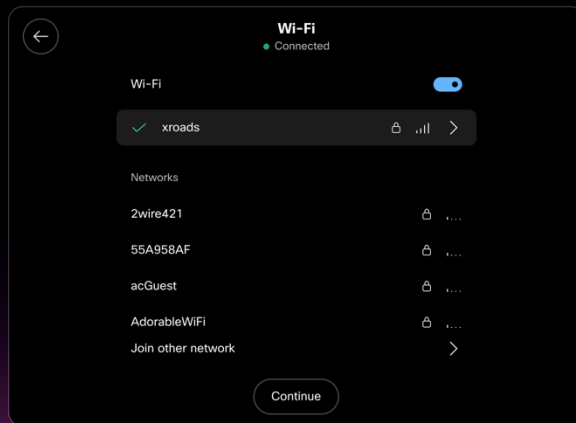
Network Connection Status

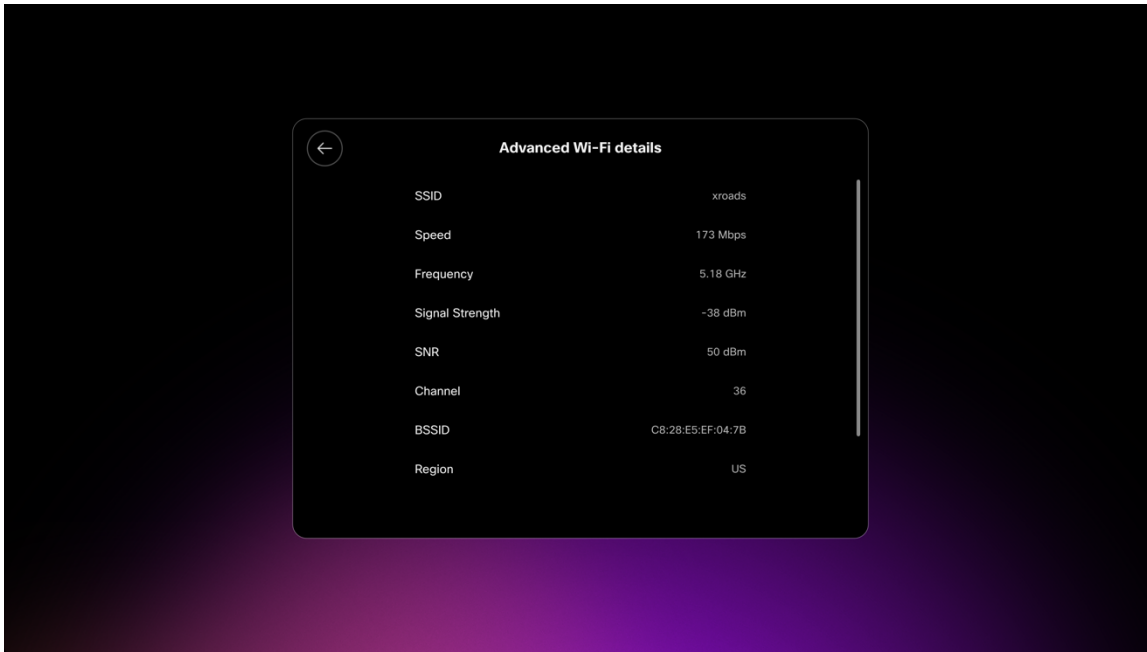
The current network connection status and IP address information is displayed in **Settings > Network connection**.



Advanced Wi-Fi Details

Detailed Wi-Fi connection including SSID, speed / data rate, frequency / channel, signal strength, WLAN MAC address, etc. is displayed when selecting the connected Wi-Fi network when in **Settings > Network connection > Wi-Fi**, then selecting **Advanced Wi-Fi details**.





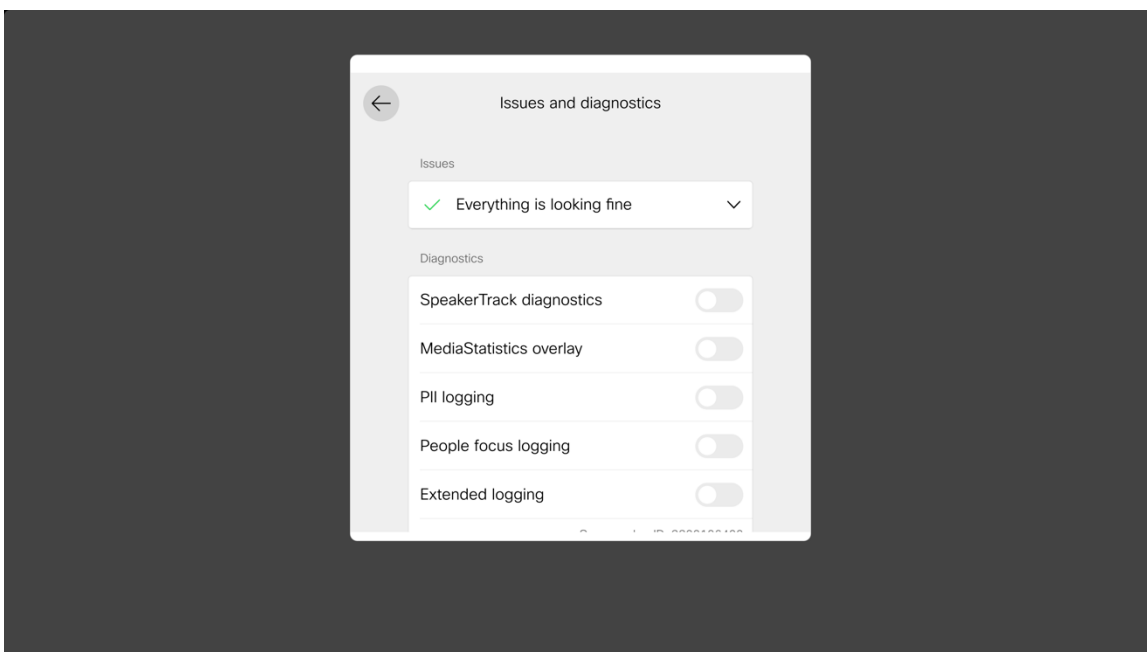
Issues and Diagnostics

Current issues and diagnostic options are displayed when selecting **Settings > Issues and diagnostics**.

Webex

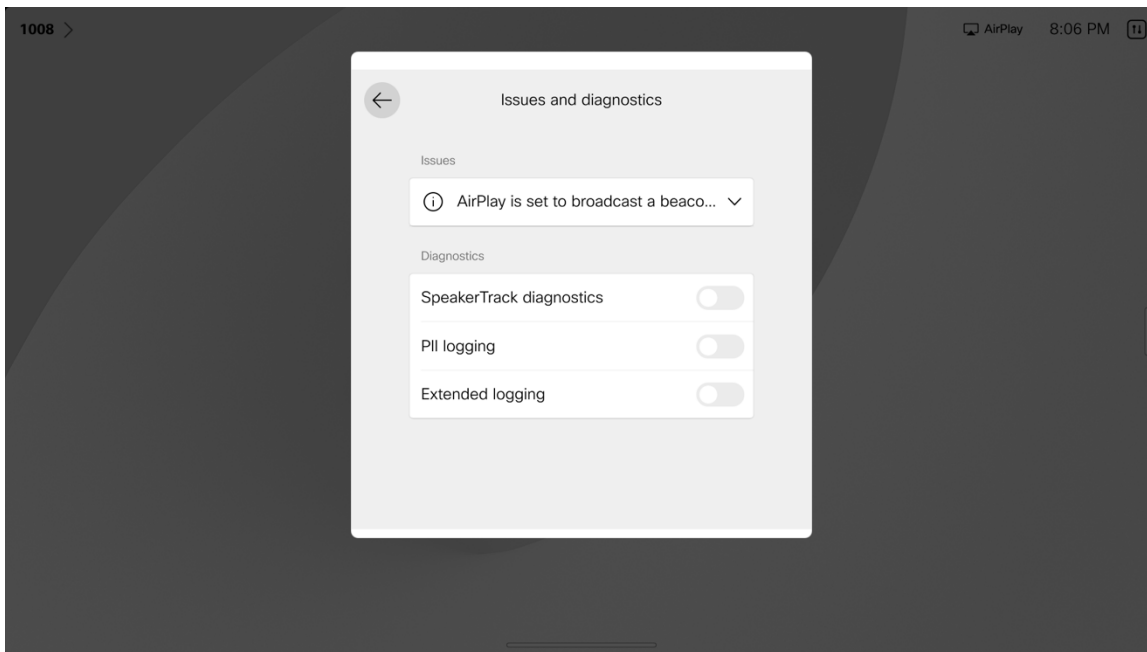
When registered to Webex, device logs can be requested from Webex Control Hub or sent from **Issues and diagnostics** menu. Device logs can then be downloaded from Webex Control Hub or from the Webex Series webpage under **System Maintenance > Issues and Diagnostics > System Logs**.

A Webex connectivity test can also be initiated from the **Issues and diagnostics** menu.



Cisco Unified Communications Manager

When registered to Cisco Unified Communications Manager, device logs can be downloaded from the Cisco RoomOS Series webpage under **System Maintenance > Issues and Diagnostics > System Logs**.



Device Webpages

The Cisco RoomOS Series webpage provides system information, setup, customization, and system maintenance options. To access the webpage, login with the enabled admin account credentials configured in the Cisco RoomOS Series webpage.

System Information

The Cisco RoomOS Series provides system information including network status, IP address, MAC address, serial number, and version information.

Browse to the web interface (<https://x.x.x.x>) of the Cisco RoomOS Series then select **Home** to view this information.

The screenshot displays the Cisco Webex Local Device Controls interface. At the top, the header shows 'Cisco Webex Local Device Controls' on the left, a search bar with 'Find page' in the center, and a user profile icon on the right. Below the header, the main content area is titled 'System Information' and is divided into several sections:

- General:** Displays the IP address '10.81.12.28' (IPv4) and MAC address '68:9E:0B:B0:00:0E'. It also shows the serial number 'FOC2449NS4C' and the active interface 'Wireless'. A 'Normal' temperature status is indicated.
- Software:** Shows the software channel as 'Stable' and the software version as 'RoomOS 11.13.1.5' (2f1a43e2808).
- Issues:** A green checkmark indicates 'Everything is looking fine'.
- Provisioning:** Shows the device is 'Registered' in 'Personal Device Mode'.
- Calendar:** States '0 scheduled meeting(s) found for the next 24 hours' and includes a 'View Scheduled Meetings' button.

A left-hand navigation menu is visible, categorized into 'Home', 'SETUP' (Settings, Users, Security), 'CUSTOMIZATION' (Personalization, UI Extensions Editor, Macro Editor, Developer API), and 'SYSTEM MAINTENANCE' (Software, Issues and Diagnostics, Backup and Recovery).

Setup

The Cisco RoomOS Series provides various configuration options and status information.

Browse to the web interface (<https://x.x.x.x>) of the Cisco RoomOS Series then select the desired option under **Setup** to view this information.

Settings

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Settings

Configurations | Statuses | Send Whiteboard to Email | Audio and Video

Search...

Configuration / SystemUnit

Collapse All | Expand All

Configuration / SystemUnit

BroadcastName	<input type="text"/>	(0 to 256 characters)
CustomDeviceId	<input type="text"/>	(0 to 255 characters)
Name	<input type="text"/>	(0 to 50 characters)

CrashReporting

Advanced	<input type="text" value="On"/>	
Mode	<input type="text" value="Off"/>	
URL	<input type="text"/>	(0 to 255 characters)

SoftwareUpgrade WebCache

Mode	<input type="text" value="Off"/>	
Url	<input type="text"/>	(0 to 255 characters)

- Apps
- Audio
- Bluetooth
- Bookings
- BYOD
- CallHistory
- Cameras
- Conference
- FacilityService
- Files
- HttpClient
- HttpFeedback
- Logging
- Macros
- Mari
- MicrosoftTeams

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Settings

Configurations | Statuses | Send Whiteboard to Email | Audio and Video

Search...

Status / SystemUnit

Collapse All | Expand All

Status / SystemUnit

BroadcastName	Michael Gillespie Desk Pro
DeveloperPreview Mode	Off
Extensions Microsoft Supported	True
LastShutdownReason	Upgrade
LastShutdownTime	2024-02-13T05:57:16Z
ProductId	Cisco Desk Pro
ProductPlatform	Desk Pro
ProductType	Cisco Codec
Uptime	239953

Hardware

DRAM	8
HasWifi	True
Monitoring Temperature Status	Normal
MonitoringSoftware	34
UDI	CS-DESKPRO-K9 V01 FOC2449NS4C

MainBoard

Revision	C
SerialNumber	FOC2448NPJB

- Audio
- Bluetooth
- Bookings
- Cameras
- Capabilities
- Conference
- Diagnostics
- Logging
- MicrosoftTeams
- Network
- NetworkServices
- Peripherals
- Phonebook
- Provisioning
- Proximity

Users

Cisco Webex Local Device Controls 10.81.12.28 Desk Pro

Find page

Users

Create User

Username	Status	Admin	Audit	RoomControl	Integrator	User
admin	Active	✓	✓			✓

Security

Cisco Webex Local Device Controls 10.81.12.28 Desk Pro

Find page

Security

Certificates Sign-in Banner

Services Custom Preinstalled

Add Certificate

Use the form below to add new certificates.

This system supports PEM formatted certificate files (.pem). The certificate file may contain the certificate and a RSA or DSA encrypted private key with or without a passphrase. Optionally the private key file may be supplied separately.

Certificate No file selected.

Private key (optional) No file selected.

Passphrase (optional)

Existing Certificates

Certificate	Issuer	802.1X	Audit	HTTPS	HttpClient	HttpProxy	SIP	Pairing	Actions
Self-signed Certificate	TemporaryDefaultCertificate	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Delete"/> <input type="button" value="View Certificate"/>

Cisco Webex Local Device Controls 10.81.12.28 Desk Pro

Find page

Security

Certificates Sign-in Banner

Services Custom Preinstalled

Add Certificate Authority

Use the form below to add new certificate authorities.

This system supports PEM formatted files (.pem) with one or more CA certificates within the file.

No file selected.

Existing Certificate Authorities

Certificate	Issuer	Details	Actions
No certificates			

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Find page

Security

Certificates Sign-in Banner

Services Custom **Preinstalled**

Preinstalled Certificates

The Certificate Authorities listed below are used to validate the certificates of external servers that the video system communicates with:

- HTTP servers hosting content used by the web views, the `HttpClient` xAPI, Macros, etc.
- SMTP mail servers (on video systems with touch screens)

Certificate Details

Certificate	Issuer	Details	Enabled
AAA Certificate Services	Comodo CA Limited	View	<input checked="" type="checkbox"/>
ACCVRAIZ1	ACCV	View	<input checked="" type="checkbox"/>
Actalis Authentication Root CA	Actalis S.p.A./03358520967	View	<input checked="" type="checkbox"/>
AffirmTrust Commercial	AffirmTrust	View	<input checked="" type="checkbox"/>
AffirmTrust Networking	AffirmTrust	View	<input checked="" type="checkbox"/>

Customization

The Cisco RoomOS Series provides various personalization options as well as other customization options.

Browse to the web interface (<https://x.x.x.x>) of the Cisco RoomOS Series then select the desired option under **Customization** to view this information.

Personalization



10.81.12.28
Desk Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Personalization

- Wallpaper and Halfwake
- Branding
- Virtual Backgrounds
- Ringtones
- Contacts

Halfwake The device enters halfwake after it has been idle for a while.



Default

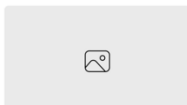
[Upload image](#) Recommended size is 3840*2160 pixels. File format: jpg, png, webp

Turn off display after

10 minutes

[Preview on device](#)

Wallpaper The wallpaper is shown as a background on the home screen.



Custom image



light



night



10.81.12.28
Desk Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Personalization

- Wallpaper and Halfwake
- Branding
- Virtual Backgrounds
- Ringtones
- Contacts

Brand Logo Halfwake logo
Shows brand logo in halfwake

[Upload image](#) Recommended size is 272*272 pixels. File format: png

Home screen logo
Show brand logo on home screen

[Upload image](#) Recommended size is 272*272 pixels. File format: png

Custom Text Custom text displays in the bottom left corner of the main screen.
Example: A help desk number your end users can call for assistance.

Feedback? <https://cs.co/dt> [Apply](#)



10.81.12.28
Desk Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Personalization

Wallpaper and Halfwake

Branding

Virtual Backgrounds

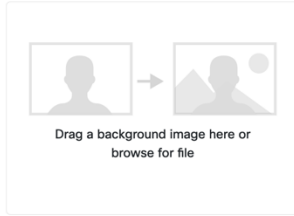
Ringtones

Contacts

Virtual Backgrounds

Upload

You can upload up to three virtual backgrounds to replace the background of your video during a call.



10.81.12.28
Desk Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Personalization

Wallpaper and Halfwake

Branding

Virtual Backgrounds

Ringtones

Contacts

Ringtones

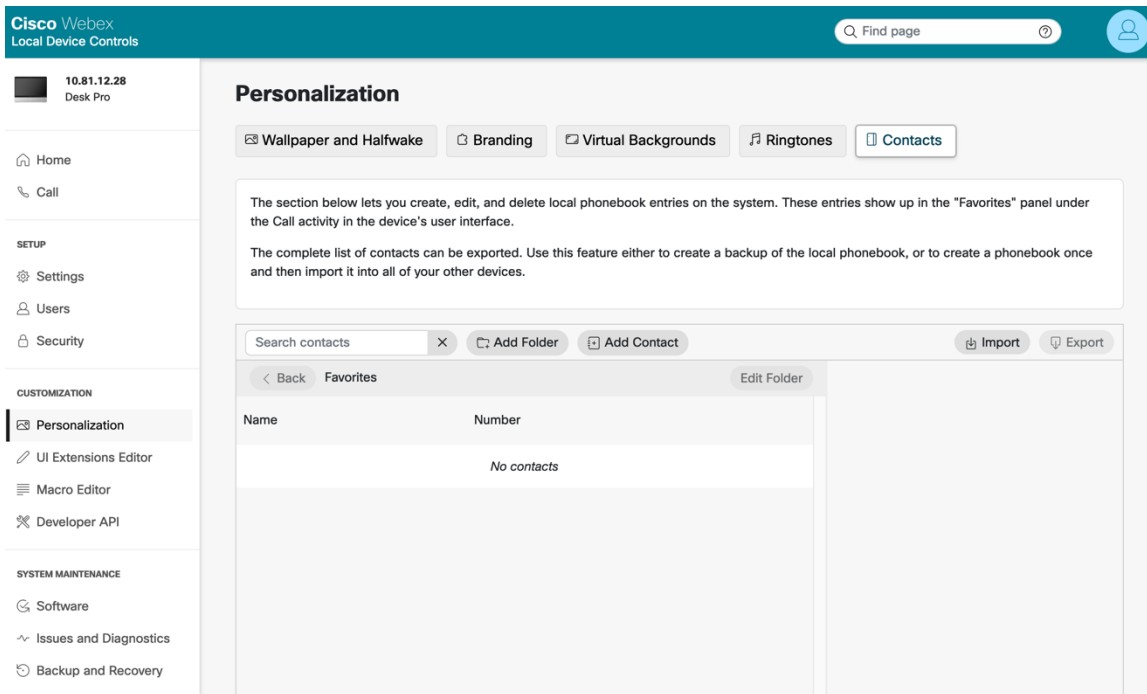
Select Active Ringtone

Please note that the ringtone will play on the video system.

Sunrise

Ringtone volume

50%

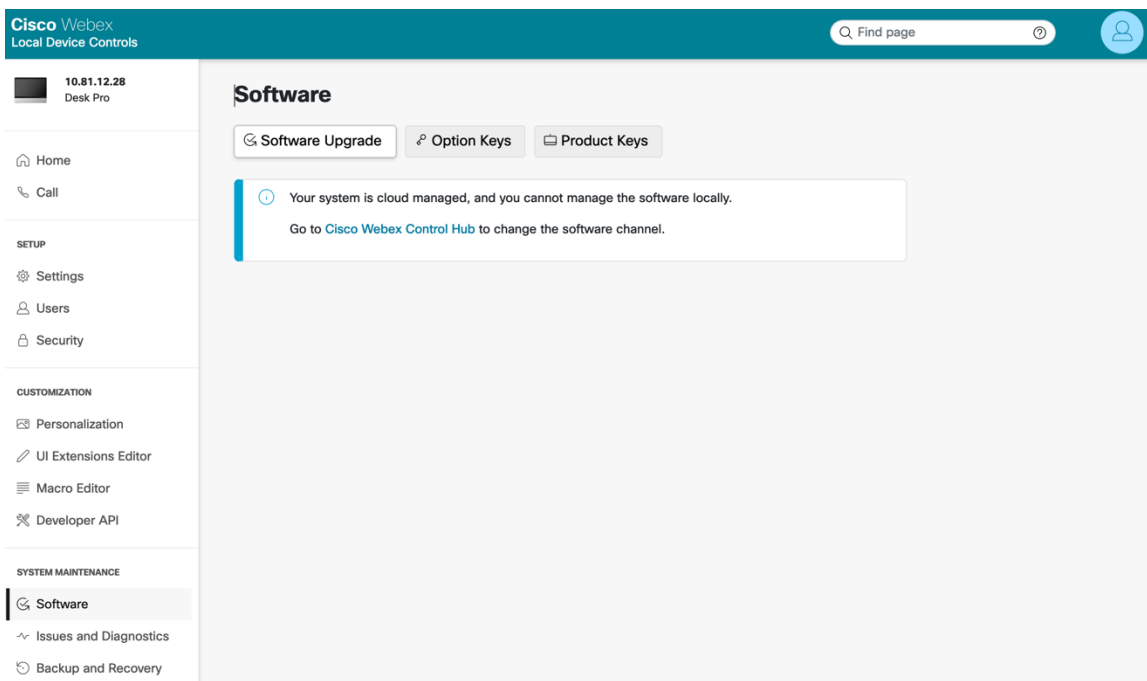


System Maintenance

The Cisco RoomOS Series provides various serviceability options including device logs.

Browse to the web interface (<https://x.x.x.x>) of the Cisco RoomOS Series then select the desired option under **System Maintenance** to view this information.

Software



Issues and Diagnostics

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Home Call

SETUP

- Settings
- Users
- Security

CUSTOMIZATION

- Personalization
- UI Extensions Editor
- Macro Editor
- Developer API

SYSTEM MAINTENANCE

- Software
- Issues and Diagnostics**
- Backup and Recovery

Find page

Issues and Diagnostics

Issues System Logs Call Logs User Interface Screenshots

Diagnostics help identify issues that may cause the system to fail or not work as expected. Rerun

Active Issues

✓ **No Issues Found!**
The system appears to be in working order.

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Home Call

SETUP

- Settings
- Users
- Security

CUSTOMIZATION

- Personalization
- UI Extensions Editor
- Macro Editor
- Developer API

SYSTEM MAINTENANCE

- Software
- Issues and Diagnostics**
- Backup and Recovery

Find page

Issues and Diagnostics

Issues System Logs Call Logs User Interface Screenshots

System Logs

A full archive of the logs on the device is useful for diagnosing problems.

This archive includes all current and historical logs, in addition to current system configuration, system status, packet captures and diagnostics information.

Download logs...

Download logs in legacy format...

Extended Logging

To help diagnose network issues and problems during call setup, the system can enter a timed extended logging mode. This mode is resource intensive, and populates the existing logs with more detailed information.

The extended logging mode can optionally include a full or partial capture of all network traffic. A rolling, full-capture mode is also available.

Start

ⓘ Extended logging is inactive.

Current Logs 🔄

File Name	Size	Last modified
auth.log	22 kB	2024-02-15 19:28
dhclient.log	14 kB	2024-02-15 19:28
dmesg	75 kB	2024-02-13 00:59
eventlog/airplay.log	8 kB	2024-02-15 19:30

Backup and Recovery

Cisco Webex Local Device Controls

10.81.12.28 Desk Pro

Home Call

SETUP

- Settings
- Users
- Security

CUSTOMIZATION

- Personalization
- UI Extensions Editor
- Macro Editor
- Developer API

SYSTEM MAINTENANCE

- Software
- Issues and Diagnostics
- Backup and Recovery**

Backup and Recovery

Backup Restore System Recovery Restart and Shutdown

Download Backup

This page lets you backup a device's configurations. Configurations include xConfigurations, as well as the configurations for other features a device might support, like macros and UI Extensions.

Select items to include in your backup. Leave all items checked to generate a complete backup of the device.

Branding	No items installed
Favorites	No items installed
UI Extensions	No items installed
Macros	No items installed
Sign In Banner	<input checked="" type="checkbox"/> Include
Configuration	<input checked="" type="checkbox"/> Include

The configuration listed below can be modified for a partial backup of the configuration.

Note: Settings such as Network, SIP URI and SystemUnit Name may specifically apply to a certain device. Applying a backup with these settings to a different device may result in it becoming unreachable on the network. To avoid this, consider removing those settings from the list below.

Remove system-specific configurations

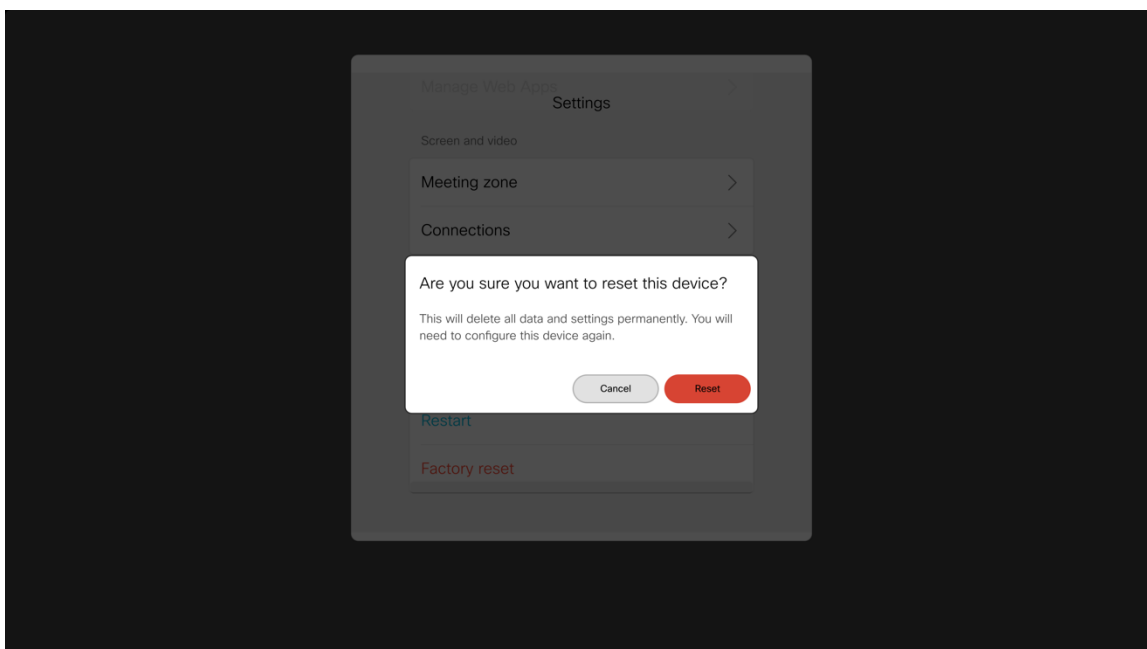
```

Apps WallpaperBundles HalfwakeImage: Auto
Audio DefaultVolume: 50
Audio Input HDMI 1 Level: -5
Audio Input HDMI 1 Mode: 0n
Audio Input HDMI 1 VideoAssociation MuteOnInactiveVideo: 0n

```

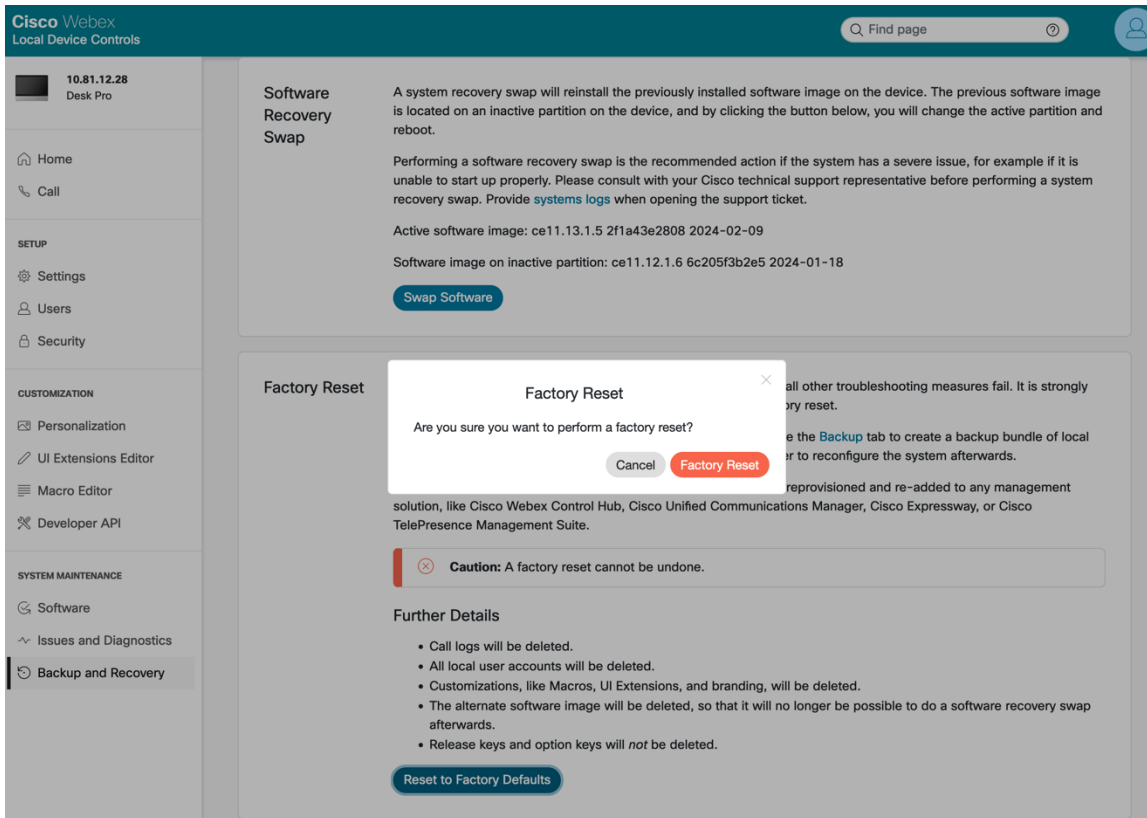
Restoring Factory Defaults

All data can be erased from the Cisco RoomOS Series, by selecting **Factory reset** in **Settings**. A confirmation screen will appear where **Reset** must be selected to proceed with the factory data reset.



A factory reset can also be done from the Cisco RoomOS Series webpage by selecting **Reset to Factory Defaults** under **System Maintenance > Backup and Recovery > System Recovery**.

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



Capturing a Screenshot of the Device Display

The current display of the Cisco RoomOS Series can be captured from the Cisco RoomOS Series webpage.

Browse to the web interface (<https://x.x.x.x>) of the Cisco RoomOS Series then select **OSD Screenshot** under **System Maintenance > Issues and Diagnostics > User Interface Screenshots** to capture a screenshot.



10.81.12.28
Desk Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Issues and Diagnostics

- Issues
- System Logs
- Call Logs
- User Interface Screenshots

Screenshots

Create Screenshot

Taking a screenshot of the touch panel or the on-screen display (OSD) can be useful for creating user manuals, reporting bugs to Cisco, and so on.

Note that any on screen video or presentation will not be captured, and that capturing a screenshot may take a while, depending on image resolution and network bandwidth.

OSD Screenshot

Wake System Up

Use the buttons below to put the system into awake or halfwake state.

Awake

Halfwake

Additional Documentation

Cisco RoomOS Series Data Sheets

<https://www.cisco.com/c/en/us/products/collaboration-endpoints/webex-desk-pro/datasheet-c78-743105.html>

<https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-desk-series/webex-desk-ds.html>

https://assets.ctfassets.net/osq47g2esuw5/74GbQExgrlc1yELb11SOdG/6f86ffcb1cb1bc29e8e54c2f6fb048ea/CM-3239_-_Webex_Mini_Datasheet.pdf

https://www.webex.com/content/dam/wbx/us/data-sheet/desk_hub_datasheet_cm-1560.pdf

Cisco RoomOS Series Administrator Guide

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html>

Cisco RoomOS Series User Guide

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-user-guide-list.html>

Cisco RoomOS Series Quick Reference Guide

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-user-guide-list.html>

Cisco RoomOS Series Release Notes

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html>

Cisco RoomOS Series Software

<https://software.cisco.com/download/home/284711383>

Cisco Unified Communications Manager

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

Cisco Voice Software

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

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_rowlan-srnd.html

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

Cisco RoomOS Series Wireless LAN Deployment Guide

<https://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

Cisco Catalyst IOS XE Wireless LAN Controller Documentation

<https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

Cisco Mobility Express Documentation

<https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-installation-and-configuration-guides-list.html>

Cisco Autonomous Access Point Documentation

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/atnms-ap-8x/configuration/guide/cg-book.html


Cisco Meraki Wireless LAN Documentation

<https://documentation.meraki.com>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Webex, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, Webex, and the Webex logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

 The Bluetooth word mark and logo are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Cisco Systems, Inc., is under license.

© 2024 Cisco Systems, All rights reserved.