

# 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
Models	
Requirements	
Site Survey	8
Call Control	9
Wireless LAN	10
Protocols	
Wi-Fi	
Regulatory	27
Bluetooth	
Languages	
Video Calls	
Device Care	
Wireless LAN Design	31
802.11 Network	
5 GHz (802.11a/n/ac/ax)	
2.4 GHz (802.11b/g/n/ax)	
Signal Strength and Coverage	
Data Kates Rugged Environments	
	20
Extensible Authentication Protocol - Elevible Authentication via Secure Tunneling (EAP-EAST)	
Extensible Authentication Protocol - Transport Laver Security (EAP-TLS)	
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS)	
Protected Extensible Authentication Protocol (PEAP)	41
Quality of Service (QaS)	42
Call Admission Control (CAC)	
Wired QoS	
Roaming	44
Interband Roaming	
Power Management	44
Call Canacity	
Multicast	
Configuring the Cisco Wireless LAN	47
Cisco AireOS Wireless LAN Controller and Lightweight Access Points	
802.11 Network Settings	47
WLAN Settings	
Controller Settings	
Call Admission Control (CAC)	
KF PTOILIES	
Multicast Direct	
OoS Profiles	
Advanced Settings	
Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points	84
802 11 Network Settings	85
002.11 Tetwork Dethilds	

WLAN Settings	
Controller Settings	
Mobility Settings	
Call Admission Control (CAC)	
Multicast	
Advanced Settings	
Sample Configuration	
Cisco Mobility Express and Lightweight Access Points	
Controller Settings	
802.11 Network Settings	
WLAN Settings	
RF Profiles	
Multicast Direct	
Cisco Autonomous Access Points	
802.11 Network Settings	
WLAN Settings	
Call Admission Control (CAC)	
QoS Policies	
Power Management	
Sample Configuration	
Cisco Meraki Access Points	
Creating the Wireless Network	
SSID Configuration	
Radio Settings	
Firewall and Traffic Shaping	
Configuring Cisco Call Control	
Webex	
Personal Usage	
Shared Usage	
Cisco Unified Communications Manager	
Device Enablement	
Device Pools	
Phone Button Templates	
Security Profiles	
SIP Profiles	
QoS Parameters	
Audio and Video Bit Rates.	
Product Specific Configuration Options	
Configuring the Cisco RoomOS Series	241
Wi-Fi Profile Configuration	
Certificate Management	
Installing Certificates	
Removing Certificates	
Call Control Configuration	
Bluetooth Settings	
Ungrading Firmware	
Using the Cisco RoomOS Series	961
	201
Troubleshooting	
About Device	
Network Connection Status	
Cisco RoomOS Series Wireless LAN Deployment Guide	4

Advanced Wi-Fi Details	
Issues and Diagnostics	
Device Webpages	
System Information	
Setup	
Customization	
System Maintenance	
Restoring Factory Defaults	
Capturing a Screenshot of the Device Display	
Additional Documentation	

# **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
01000	1001100	001100	_

Model	Part Number	Peak Antenna Gain	Frequency Ranges	Channel Set (# of channels)	
Cisco Board 55	CS-BOARD55	2.4 GHz = 4.23 dBi	2.412 - 2.472 GHz	1-13 (13)	
		5  GHz = 6.00  dBi	5.180 - 5.240 GHz	36,40,44,48 (4)	
Cisco Board 55s	CS-BOARD55S	2.4 GHz = 4.50 dBi	5.260 - 5.320 GHz	52,56,60,64 (4)	
		5 GHz = 5.80 dBi	5.500 - 5.720 GHz	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	149,133,137,101,103 (3)

### Cisco RoomOS Series 3

Model	Part Number	Part Number Peak Antenna Gain		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%.

#### <u>Noise</u>

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%.

#### <u>Multipath</u>

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

- o 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

- o Webex
- o Cisco Unified Communications Manager (CUCM)

Minimum = 11.5(1)

Recommended = 12.5(1), 14.0(1) and later

#### • Cisco RoomOS Series 3

- o Webex
- o 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	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	Lightweight	Mobility Express	Autonomous
Series									

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

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



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

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

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

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-antennasaccessories/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)
  - o AAC-LD, Opus, G.722, G.711, G.722.1, G.729
  - o 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	Max Tx Power = 20 dBm	6 Mbps	1	OFDM - BPSK
Cisco Board 55s	(Depends on region)	9 Mbps	1	OFDM - BPSK
Cisco Board 70		12 Mbps	1	OFDM - QPSK
Cisco Board 70s		18 Mbps	1	OFDM - QPSK
Cisco Board Pro 55		24 Mbps	1	OFDM - 16 QAM
Cisco Board Pro 75		36 Mbps	1	OFDM - 16 QAM
Cisco Codec Plus		48 Mbps	1	OFDM - 64 QAM
Cisco Codec Pro		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 Dual	Max Tx Power = 19 dBm	7 Mbps (MCS 0)	1	OFDM - BPSK
Cisco Room 70 Single	(Depends on region)	14 Mbps (MCS 1)	1	OFDM - QPSK
Cisco Room 70 Dual		21 Mbps (MCS 2)	1	OFDM - QPSK
Cisco Room 70 Single G2		29 Mbps (MCS 3)	1	OFDM - 16 QAM
Cisco Room 70 Dual G2		43 Mbps (MCS 4)	1	OFDM - 16 QAM
Cisco Room 70 Panorama		58 Mbps (MCS 5)	1	OFDM - 64 QAM
Cisco Room Kit		65 Mbps (MCS 6)	1	OFDM - 64 QAM
Cisco Room Kit Mini		72 Mbps (MCS 7)	1	OFDM - 64 QAM
Cisco Room USB		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	15 Mbps (MCS 0)	1	OFDM - BPSK
	(Depends on region)	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	7 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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 = $18 \text{ dBm}$	15 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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	Modulation
		Streams	
Max Tx Power = 18 dBm	33 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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	Max Tx Power = 19 dBm	1 Mbps	1	DSSS - BPSK
Cisco Board 55s	(Depends on region)	2 Mbps	1	DSSS - QPSK

Cisco Board 70		5.5 Mbps	1	DSSS - CCK
Cisco Board 70s		11 Mbps	1	DSSS - CCK
Cisco Board 85s	2.4 GHz - 802.11g	Data Rate	Spatial	Modulation
Cisco Board Pro 55			Streams	
Cisco Board Pro 75	Max Tx Power = $19  dBm$	6 Mbps	1	OFDM - BPSK
Cisco Desk Pro	(Depends on region)	9 Mbps	1	OFDM - BPSK
Cisco Desk Limited		12 Mbps	1	OFDM OPSK
Cisco Room 55			1	OFDM - QFSK
Cisco Room 55 Dual		18 Mbps	1	OFDM - QPSK
Cisco Room 70 Single		24 Mbps	1	OFDM - 16 QAM
Cisco Room 70 Dual		36 Mbps	1	OFDM - 16 QAM
Cisco Room 70 Single G2		48 Mbps	1	OFDM - 64 QAM
Cisco Room 70 Dual G2		54 Mbps	1	OFDM - 64 QAM
Cisco Room 70 Panorama	2.4 GHz - 802.11n (HT20)	Data Rate	Spatial	Modulation
Cisco Room Panorama			Streams	
Cisco Room Kit	Max Tx Power = 19 dBm	7 Mbps (MCS 0)	1	OFDM - BPSK
Cisco Room Kit Mini	(Depends on region)	14 Mbps (MCS 1)	1	OFDM - QPSK
Cisco Room Kit Plus		21 Mbps (MCS 2)	1	OFDM - QPSK
Cisco Room USB		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	Max Tx Power = 19 dBm	6 Mbps	1	OFDM - BPSK
Cisco Desk Mini	(Depends on region)	9 Mbps	1	OFDM - BPSK
Cisco Room Bar		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	7 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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	15 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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) 300 Mbps (MCS 15)	2	OFDM - 64 QAM
	300 Mbps (MCS 15)	n	
	1 ( )	2	OFDM - 64 QAM
GHz - 802.11ac (VHT20)	Data Rate	Spatial Streams	Modulation
ax Tx Power = 19 dBm	7 Mbps (MCS 0)	1	OFDM - BPSK
epends on region)	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
	130 Mbps (MCS 6) 144 Mbps (MCS 7)	2 2	OFDM - 64 QAM OFDM - 64 QAM
	130 Mbps (MCS 6)           144 Mbps (MCS 7)           173 Mbps (MCS 8)	2 2 2	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM
GHz - 802.11ac (VHT40)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate	2 2 2 Spatial Streams	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation
<b>GHz - 802.11ac (VHT40)</b> ax Tx Power = 18 dBm	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)	2 2 2 Spatial Streams	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK
<b>GHz - 802.11ac (VHT40)</b> ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 1)	2 2 2 Spatial Streams 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)	2 2 2 Spatial Streams 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK
<b>GHz - 802.11ac (VHT40)</b> ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)	2 2 2 <b>Spatial</b> Streams 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM
<b>GHz - 802.11ac (VHT40)</b> ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)	2 2 2 <b>Spatial</b> Streams 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)	2 2 2 Spatial Streams 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 6)	2 2 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 7)	2 2 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 6)         150 Mbps (MCS 7)         180 Mbps (MCS 8)	2 2 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 6)         150 Mbps (MCS 7)         180 Mbps (MCS 8)         200 Mbps (MCS 9)	2 2 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 6)         150 Mbps (MCS 7)         180 Mbps (MCS 8)         200 Mbps (MCS 0)	2 2 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 6)         150 Mbps (MCS 7)         180 Mbps (MCS 8)         200 Mbps (MCS 0)         60 Mbps (MCS 1)	2 2 2 3 Spatial Streams 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6) 144 Mbps (MCS 7) 173 Mbps (MCS 8) Data Rate 15 Mbps (MCS 0) 30 Mbps (MCS 0) 30 Mbps (MCS 1) 45 Mbps (MCS 2) 60 Mbps (MCS 3) 90 Mbps (MCS 4) 120 Mbps (MCS 5) 135 Mbps (MCS 6) 150 Mbps (MCS 7) 180 Mbps (MCS 8) 200 Mbps (MCS 9) 30 Mbps (MCS 0) 60 Mbps (MCS 1) 90 Mbps (MCS 2)	2 2 3 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - 256 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6) 144 Mbps (MCS 7) 173 Mbps (MCS 8) Data Rate 15 Mbps (MCS 0) 30 Mbps (MCS 0) 30 Mbps (MCS 1) 45 Mbps (MCS 2) 60 Mbps (MCS 3) 90 Mbps (MCS 4) 120 Mbps (MCS 5) 135 Mbps (MCS 5) 135 Mbps (MCS 6) 150 Mbps (MCS 7) 180 Mbps (MCS 8) 200 Mbps (MCS 9) 30 Mbps (MCS 1) 90 Mbps (MCS 1) 90 Mbps (MCS 3)	2 2 3 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - BPSK OFDM - QPSK OFDM - QPSK
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6) 144 Mbps (MCS 7) 173 Mbps (MCS 8) Data Rate 15 Mbps (MCS 0) 30 Mbps (MCS 0) 30 Mbps (MCS 1) 45 Mbps (MCS 2) 60 Mbps (MCS 3) 90 Mbps (MCS 4) 120 Mbps (MCS 5) 135 Mbps (MCS 6) 150 Mbps (MCS 7) 180 Mbps (MCS 8) 200 Mbps (MCS 9) 30 Mbps (MCS 1) 90 Mbps (MCS 1) 90 Mbps (MCS 3) 120 Mbps (MCS 3) 180 Mbps (MCS 3)	2 2 3 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - 256 QAM OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 6)         150 Mbps (MCS 7)         180 Mbps (MCS 9)         30 Mbps (MCS 1)         90 Mbps (MCS 1)         90 Mbps (MCS 4)         200 Mbps (MCS 2)         120 Mbps (MCS 4)         200 Mbps (MCS 4)         200 Mbps (MCS 4)         200 Mbps (MCS 4)         200 Mbps (MCS 5)	2 2 3 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM Modulation OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM
GHz - 802.11ac (VHT40) ax Tx Power = 18 dBm epends on region)	130 Mbps (MCS 6)         144 Mbps (MCS 7)         173 Mbps (MCS 8)         Data Rate         15 Mbps (MCS 0)         30 Mbps (MCS 0)         30 Mbps (MCS 1)         45 Mbps (MCS 2)         60 Mbps (MCS 3)         90 Mbps (MCS 4)         120 Mbps (MCS 5)         135 Mbps (MCS 6)         150 Mbps (MCS 7)         180 Mbps (MCS 8)         200 Mbps (MCS 9)         30 Mbps (MCS 1)         90 Mbps (MCS 1)         90 Mbps (MCS 2)         120 Mbps (MCS 3)         180 Mbps (MCS 3)         180 Mbps (MCS 4)         240 Mbps (MCS 5)         270 Mbps (MCS 6)	2 2 3 <b>Spatial</b> <b>Streams</b> 1 1 1 1 1 1 1 1 1 1 1 1 1	OFDM - 64 QAM         OFDM - 64 QAM         OFDM - 256 QAM         Modulation         OFDM - BPSK         OFDM - QPSK         OFDM - QPSK         OFDM - 16 QAM         OFDM - 64 QAM         OFDM - 64 QAM         OFDM - 256 QAM         OFDM - 256 QAM         OFDM - QPSK         OFDM - 64 QAM         OFDM - 64 QAM         OFDM - 16 QAM         OFDM - 256 QAM         OFDM - 256 QAM         OFDM - 16 QAM         OFDM - 0PSK         OFDM - 16 QAM         OFDM - 64 QAM
ax Tx Power = 19 dBm epends on region)	7 Mbps (MCS 0)         14 Mbps (MCS 1)         21 Mbps (MCS 2)         29 Mbps (MCS 3)         43 Mbps (MCS 4)         58 Mbps (MCS 5)         65 Mbps (MCS 6)         72 Mbps (MCS 7)         87 Mbps (MCS 0)         28 Mbps (MCS 1)         43 Mbps (MCS 2)         58 Mbps (MCS 3)         87 Mbps (MCS 4)         14 Mbps (MCS 4)         14 Mbps (MCS 5)	Streams         1         1         1         1         1         1         1         1         1         1         2	OFDM - BPSK OFDM - QPSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 64 QAM OFDM - 256 QAM OFDM - 8PSK OFDM - 8PSK OFDM - QPSK OFDM - 16 QAM OFDM - 16 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	33 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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	Max Tx Power = 22 dBm	1 Mbps	1	DSSS - BPSK
Cisco Desk Mini	(Depends on region)	2 Mbps	1	DSSS - QPSK
Cisco Room Bar		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	6 Mbps	1	OFDM - BPSK
	(Depends on region)	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

# Cisco RoomOS Series 3

## **5 GHz Specifications**

Model	5 GHz - 802.11a	Data Rate	Spatial Streams	Modulation
Cisco Codec EQ	Max Tx Power = 19 dBm	6 Mbps	1	OFDM - BPSK
Cisco Room Bar Pro	(Depends on region)	9 Mbps	1	OFDM - BPSK
		12 Mbps	1	OFDM - QPSK
		18 Mbps	1	OFDM - QPSK
<b>5 GHz - 8</b> Max Tx Pow (Depends on		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	7 Mbps (MCS 0)	1	OFDM - BPSK
	(Depends on region)	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 G	Hz - 802.11n (HT40)	Data Rate	Spatial Streams	Modulation
Max T	x Power = 18 dBm	15 Mbps (MCS 0)	1	OFDM - BPSK
(Depe	nds on region)	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 GH	z - 802.11ac (VHT20)	Data Rate	Spatial Streams	Modulation
Max T	Tx Power = $19 \text{ dBm}$	7 Mbps (MCS 0)	1	OFDM - BPSK
(Depe	nds on region)	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	15 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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	33 Mbps (MCS 0)	1	OFDM - BPSK
(Depends on region)	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	Max Tx Power = 22 dBm	1 Mbps	1	DSSS - BPSK
Cisco Room Bar Pro	(Depends on region)	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	6 Mbps	1	OFDM - BPSK
	(Depends on region)	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	7 Mbps (MCS 0)	1	OFDM - BPSK
	(Depends on region)	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)
Cisco RoomOS Series Wireless LAN	Deployment Guide	

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

# 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:

 $\underline{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-userguide-list.html$ 

# 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).



### **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.



Minimum 20% Overlap

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.



Minimum 20% Overlap

## **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.

₿	cisco Prime Infrastructure			Q ▼ Application Search	🐥 🛿 1 🕴 alpha - ROOT-DOMAIN 🛱
<b>A</b>	Maps / Wireless Maps / Site Ma	ps ( New! ) 🔺			0 S 🖷 🗖
*	Sites / SJ / SJ-21 / 3rd Floor 🔶 5 GHz	Coverage      Recompute Refresh	Q Search on map		Edit Data Charts Segments Tools
Domain Navigato	0 1 50 1 0 1 50 1 0	100 R 21:322:422 (22:322:422 (22:322:423 (22:32) (22:322:423 (22:32) (2	150 R 200 R	200 300R	X           Access Points (43)           Display Label         Name           Image: Constraint of the state of the
	90 S	6500 6(21-320-0021 11-320-0020	6550 6(21-31a-ap2) 6(21-31a-ap2)	9(21-31a-ag24	Map Opacity (%) 0 10 20 30 40 50 60 70 80 90 100 10 10 20 30 40 50 60 70 80 90 100 Show Mobility Express Off
	oom (521-32a-ap25) (5)c21-32a-ap25 (5)c21-3	50 sjc21-32a-ap27	sjc21-31a-ap20	sjc21-31a-ap30	MSE / CMX Settings * Map Properties *
	5050 (jc21-525-sp51) 60.0 (jc21-525-sp57) 61.0	DU0         DU0           jc21:32x-sp32         cjc21:32x-sp33           DU0         cjc21:32x-sp39           21:32x-sp38         cjc21:32x-sp39	000) (j2153n-qp34 (j23 53n-qp34 (j23 53n-qp40 (000) (j23-31-3p41 (j23)	CL0         CL0           S11-ap35         sjc21-51arap36           S12-ap42         SU0           S12-ap42         sjc21-51arap40	

### **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:

### <u>5 GHz</u>

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

## <u>2.4 GHz</u>

802.11 Mode	Mandatory	Supported	Disabled
	Data Rates	Data Rates	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	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
Voice	Webex	EF (46)	5	6	RTP (UDP 5004)
TelePresence	CUCM	CS4 (32)	4	5	RTP (UDP 16384 - 32767)
Video	Webex	AF41 (34)	4	5	RTP (UDP 5004)
Call Control	CUCM	CS3 (24)	3 4 SI		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	<b>Roaming Time</b>
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.

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT C <u>O</u> MM	ANDS HE <u>L</u> P <u>F</u> EEDBACK
Wireless	802.11a Global Parame	ters			
Access Points     All APs     Padios	General			Data Rates**	
Global Configuration	802.11a Network Status	Enabled		6 Mbps	Disabled ᅌ
Advanced	Beacon Period (millisecs)	100		9 Mbps	Disabled ᅌ
Mesh	Fragmentation Threshold (bytes)	2346		12 Mbps	Mandatory ᅌ
AP Group NTP	DTPC Support.	Enabled		18 Mbps	Supported ᅌ
ATF	Maximum Allowed Clients	imum Allowed Clients 100		24 Mbps	Supported ᅌ
RF Profiles	RSSI Low Check	Enabled		36 Mbps	Supported ᅌ
FlexConnect Groups	RSSI Threshold (-60 to -90	-80		48 Mbps	Supported ᅌ
FlexConnect ACI s	dBm)			54 Mbps	Supported ᅌ
FlexConnect VI AN	802.11a Band Status			CCX Location Measu	urement
Templates	Low Band	Enabled		Mada	
Network Lists	Mid Band	Enabled		Mode	
💌 802.11a/n/ac/ax	High Band	Enabled		Interval (seconds)	60
Network RRM				TWT Configuration	***
RF Grouping				Target Waketime	🗹 Enabled
TPC DCA				Broadcast TWT Suppor	t 🗹 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).

.ılı.ılı. cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTRO	OLLER WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11b/g Global Parame	ters					
Access Points All APs Radios	General			Data Rates*	*		
Global Configuration	802.11b/g Network Status	Enabled		1 Mbps		isabled	\$
Advanced	802.11g Support	Enabled		2 Mbps	_ <b>C</b>	isabled	٥
Mesh	Beacon Period (millisecs)	100		5.5 Mbps		isabled	٥
AP Group NTP	Short Preamble	Enabled		6 Mbps		isabled	٥
ATE	Fragmentation Threshold	2346		9 Mbps		isabled	\$
DE Drofilos	DTPC Support.	Enabled		11 Mbps		isabled	\$
ElexConnect Groups	Maximum Allowed Clients	100		12 Mbps	N	landatory	\$
FlexConnect ACLs	RSSI Low Check	Enabled		18 Mbps	s	upported	\$
FlexConnect ACLS	RSSI Threshold (-60 to -90	-80		24 Mbps	s	upported	\$
FlexConnect VLAN Templates	dBm)	00		36 Mbps	S	upported	\$
Network Lists	CCX Location Measureme	nt		48 Mbps	S	upported	\$
802.11a/n/ac/ax	Mode	Enabled		54 Mbps	s	upported	\$
802.11b/g/n/ax	Interval (seconds)	60		TWT Configu	ration ***		
▼ RRM				Target Waketi	ime		🗹 Enabled
RF Grouping TPC				Broadcast TW	T 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

	uluili. cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
W	ireless	802.11a/r	/ac/ax C	isco APs > C	onfigure						
•	Access Points All APs Radios	6						DE Channe			
	802.11a/n/ac/ax	Genera	11					RF Channe	el Assig	nment	
	802.11b/g/n/ax Dual-Band Radios	AP Na	me		rtp9-31a	a-ap1		Current C	nannel		(48,44)
	Global Configuration	Admir	Status		Enable	0		Channel V	/idth *		40 MHz O
Þ	Advanced	Opera	tional Stat	us	UP			* Channel Wi mode	ath can b	e contigurea oni	v when channel configuration is in custom
	Mesh	Slot #			1			Assignme	nt Method		<ul> <li>Global</li> </ul>
Þ	AP Group NTP	11n Pa	rameter	s							Custom
Þ	ATF							Radar Inf	ormatio	n	
	RF Profiles	11n S	upported		Yes						
	FlexConnect Groups	CleanA	ir					Channel		Last Hear	d(Secs)
Þ	FlexConnect ACLs							No radar det	ected cha	nnels	
	FlexConnect VLAN	Clean	Air Capable	•	Yes	_		Ty Dowor		colonmont	
	Templates	Clean	Air Admin S	Status	Enable	0		TX Power	Level A	ssignment	
	Network Lists	- CleanA	ir enable w	nii take eriect oniy	II ICIS enabled	on this band.		Current Ta	Power Le	evel	1
Þ	802.11a/n/ac/ax	Numb	er of Spect	rum Expert	0			Assignme	nt Method		Global
Þ	802.11b/g/n/ax	conne	caons								Custom
Þ	Media Stream	Anteni	na Paran	neters							
Þ	Application Visibility And Control	Anten	na Type		Interna A	I 😂		Performa	nce Pro	file	
	Lync Server	Antenna B 🗸					View and edit Performance Profile for this AP				
	Country				D			Perform	nance Pr	ofile	
	Timers							Noto: Chang		the encoder	causes the Radia to be temperarily disabled
Þ	Netflow							and thus may	result in	loss of connecti	vity for some clients.
•	QoS										

## 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.

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS	<u>S</u> ECURITY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
Wireless	802.11a > RRM > Tx Power Control(TPC)		
Access Points     All APs     Radios	TPC Version		
Global Configuration Advanced Mesh	Ocoverage Optimal Mode (TPCv1) Tx Power Level Assignment Algorithm		
AP Group NTP	Power Level Assignment Method		Automatic Every 600 sec:     On Demand Invoke Rower Undate Once
ATF			
RF Profiles FlexConnect Groups FlexConnect ACLs	Maximum Power Level Assignment (-10 to 30 dBm) Minimum Power Level Assignment (-10 to 30 dBm)		17 11
FlexConnect VLAN Templates	Power Assignment Leader Last Power Level Assignment		463 secs ago
Network Lists	Power Threshold (-80 to -50 dBm)		-65
<ul> <li>802.11a/n/ac/ax</li> <li>Network</li> <li>RRM</li> </ul>	Channel Aware Power Neighbor Count		Denabled
RF Grouping TPC DCA Coverage General			

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	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Wireless	802.11a >	02.11a > RRM > Dynamic Channel Assignment (DCA)								
Access Points     All APs	Dynamic	Channel	Assignment A	lgorithm						
Radios Global Configuration	Channel A	Assignment	Method	<ul> <li>Automatic</li> </ul>	Interval:	10 minutes ᅌ	AnchorTime: 0	\$		
Advanced				Freeze	Invoke	<b>Channel Update</b>	Once			
Mesh				OFF						
AP Group NTP	Avoid For	eign AP int	erference	Enabled						
) ATE	Avoid Cise	co AP load		Enabled						
DE Drofiles	Avoid nor	n-802.11a r	noise	Enabled						
RF Profiles	Avoid Per	sistent Non	-WiFi Interference	Enabled						
FlexConnect Groups	Channel A	Assignment	Leader	RTP9-32A-WL	C3 (10.81.6.7	D)				
FlexConnect ACLs	Last Auto	Channel A	ssignment	556 secs ago						
FlexConnect VLAN Templates	DCA Char	nnel Sensiti	vity	Medium ᅌ	(15 dB)					
Network Lists	Channel V	Width		_20 MHz 🧿	40 MHz ()80	MHz 🔿 160 MHz 🤇	80+80 MHz 0	Best		
802.11a/n/ac/ax	Avoid che	ck for non-	DFS channel	Enabled						
Network RRM	DCA Chan	nel List								
RF Grouping TPC DCA Coverage General Client Roaming Media	DCA Char	nnels	36, 40, 44, 157, 161	48, 52, 56, 60,	64, 100, 153,					

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.

راریاں cısco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11b >	RRM >	Dynamic Cha	nnel Assign	ment (DC	A)			
Access Points     All APs	Dynamic	Channel	Assignment A	lgorithm					
Radios Global Configuration	Channel A	ssignment	Method	<ul> <li>Automatic</li> </ul>	Interval	10 minutes ᅌ	AnchorTime: 0	$\circ$	
Advanced				Freeze	Invoke	Channel Update	Once		
Mesh				OFF					
AP Group NTP	Avoid For	eign AP inte	erference	Enabled					
N ATE	Avoid Cisc	to AP load		Enabled					
RF Profiles	Avoid non	-802.11b r	oise	Enabled					
ElexConnect Groups	Avoid Pers	sistent Non	-WiFi Interference	Enabled					
FlexConnect ACLs	Channel A	ssignment	Leader	RTP9-32A-WL	C3 (10.81.6.7	0)			
Prexconnect Acts	Last Auto	Channel A	ssignment	75 secs ago					
FlexConnect VLAN Templates	DCA Chan	nel Sensiti	vity	Medium ᅌ	(10 dB)				
Network Lists	DCA Chan	nel List							
🕨 802.11a/n/ac/ax									
<ul> <li>802.11b/g/n/ax Network</li> </ul>		1, (	5, 11						
▼ RRM	DCA Chan	nels							
TPC									
DCA					11.				
Coverage									

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.

	uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Wi	reless	802.11a/n	/ac/ax C	isco APs > Co	onfigure						
•	Access Points All APs Radios	Genera	al.					RF Channe	el Assig	nment	
	802.11b/g/n/ax Dual-Band Radios	AP Na Admir	me Status		rtp9-31a Enable	-ap1		Current C Channel V	hannel /idth *		(48,44) 40 MHz 0
Þ	Advanced	Opera	tional State	IS	UP			* Channel wi mode	dth can b	e configured or	nly when channel configuration is in custom
	Mesh	Slot #			1			Assignme	nt Method		Global
Þ	AP Group NTP	11n Pa	rameter	s							Custom
Þ	ATF	110 5	upported		Vec			Radar Inf	ormatio	n	
	RF Profiles	110.5	apported		165						
	FlexConnect Groups	CleanA	ir					Channel		Last Hea	ard(Secs)
Þ	FlexConnect ACLs	0	Al- Constitu					No radar det	ected cha	nnels	
	FlexConnect VLAN Templates	Clean	Air Admin S	itatus	Enable	0		Tx Power	Level A	ssignment	
	Network Lists	* CleanA	ir enable w	ill take effect only	if it is enabled	on this band.		Current Ta	k Power Le	evel	1
×	802.11a/n/ac/ax	Numb	er of Spect ctions	rum Expert	0			Assignme	nt Method		Global
×	802.11b/g/n/ax	Antonr	a Param	otors							Custom
Þ.	Media Stream	Anten	-	leters	(						
Þ	Application Visibility And Control	Anten	na Type		A			Performa	nce Prot	file	
	Lync Server	Anten	na		С			View and	edit Perfo	rmance Profile	for this AP
	Country				D			Perform	nance Pr	ofile	
	Timers							Note: Chang	ing any of	the parameter	rs causes the Radio to be temporarily disabled
Þ.	Netflow							and thus ma	result in	loss of connec	tivity for some clients.
¥.	QoS										

### **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.

ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless									
Access Points     All APs     Radios	General	ile.		Vaice	% Video Ontim	ized 🔼			
Global Configuration  Advanced	Enable Lo	w Latency I	MAC 1						
Mesh AP Group NTP									
▶ ATF	Low latency	Mac feature	e is not supported	for 1140/1250,	/3500 platform	s if more than 3 da	ta rates are enal	oled.	

### 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.

۱۱۱۱۱۱۰ cısco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11h G	Blobal Pa	arameters						
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>Global Configuration</li> </ul> </li> </ul>	Power Co	<b>nstraint</b> er Constrai	int(0-30)	0 de					
Advanced	Channel S	witch A	nnouncement						
Mesh	Channel A	Innouncem	ent	<ul> <li>Image: A start of the start of</li></ul>					
AP Group NTP	Channel S	witch Cour	nt	0					
▶ ATF	Channel C	Quiet Mode							
RF Profiles									
FlexConnect Groups	Radar Bla	cklist							
FlexConnect ACLs	Smart DF	S							

## 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.

	uluulu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDB	АСК	
Wi	ireless	802.11n/a	c/ax (5 (	GHz) Through	put							
*	Access Points All APs	General							MCS (	Data	Rate <sup>1</sup> ) Settings	
	Global Configuration	11n Mode			🗹 Enat	oled <sup>2</sup>			0	(7	Mbps)	Supported
Þ	Advanced	11ac Mod	e		🗹 Enat	oled 3			1	(14	Mbps)	Supported
	Mesh	11ax Mod	e		🗹 Enat	oled ²			2	(21	Mbps)	Supported
Þ	AP Group NTP		Pates						3	(29	Mbps)	Supported
Þ	ATF	VIII MCS	Rates						4	(43	Mbps)	Supported
	RF Profiles	SS1							5	(58	Mbps)	Supported
	FlexConnect Groups	0-8			Enal	oled 4			6	(65	Mbps)	Supported
Þ	FlexConnect ACLs	0-9			🗹 Enat	oled 4			7	(72	Mbps)	Supported
	ElexConnect VI AN								8	(14	Mbps)	Supported
	Templates	552							9	(29	Mbps)	Supported
	Network Lists	0-8			Enat	oled 2			10	(43	Mbps)	Supported
•	802.11a/n/ac/ax	0-9			Enat	oled 2			11	(58	Mbps)	Supported
	Network	SS3							12	(87	Mbps)	Supported
	RF Grouping	0-8			Enat	oled 4			13	( 116	Mbps)	Supported
	TPC	0-9			🗹 Enat	oled 4			14	(130	Mbps)	Supported
	Coverage	664							15	( 144	Mbps)	Supported
	General Client Reaming	554							16	(22	Mbps)	Supported
	Media	0-8			✓ Enat	oled 2			17	(43	Mbps)	Supported
	EDCA Parameters	0-9			Enal	oled 2			18	(65	Mbps)	Supported
	High Throughput	HE MCS R	ates						19	(87	Mbps)	Supported
	(802.11n/ac/ax) CleanAir								20	(130	Mbps)	Supported
	802.11b/g/p/av	SS1			SS2				21	( 173	Mbps)	Supported
į.	Modia Stream	0-7	V E	nabled	0-7	E	nabled		22	(195	Mbps)	Supported
		0-9	V E	nabled	0-9	E	nabled		23	( 217	Mbps)	Supported
Þ	Application visibility And Control	0-11	🗹 Ei	nabled	0-11	<b>V</b> E	nabled		24	(29	Mbps)	Supported
	Lync Server	SS3			SS4				25	(58	Mbps)	Supported
	Country	0-7	✓ Ei	nabled	0-7	V E	nabled		26	(87	Mbps)	Supported
	Timers	0-9	✓ Ei	nabled	0-9	✓ E	nabled		27	( 116	Mbps)	Supported
	Netflow	0-11	🗹 Ei	nabled	0-11	<b>2</b> E	nabled		28	( 173	Mbps)	Supported
	OoS								29	(231	Mbps)	Supported
		SS5			SS6				30	(260	Mbps)	Supported
		0-7	V EI	nabled	0-7	V	nabled		31	(289	Mbps)	Supported

### **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 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 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
Priority 6 Priority 7	Disabled Disabled

#### CleanAir

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



راریان cısco	<u>M</u> ONITOR <u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	_	
Wireless	802.11a/n/ac/ax C	isco APs > C	onfigure							
Access Points All APs Radios 802 11a/p/ac/ay	General					RF Channe	el Assig	nment		
802.11b/g/n/ax Dual-Band Radios	AP Name Admin Status		rtp9-31a Enable	a-ap1		Current Cl Channel V	hannel /idth *		(48,44) 40 MHz 0	
Advanced	Operational State	JS	UP 1			* Channel wi mode	dth can be	e configured only	y when channel configuration is ir	custom
Mesh AP Group NTP	11n Parameter	s	-			Assignme	nt Method		Custom	
RF Profiles	11n Supported		Yes			Radar Inf	ormatio	n		
FlexConnect Groups	CleanAir					Channel		Last Hear	d(Secs)	
<ul> <li>FlexConnect ACLs</li> <li>FlexConnect VLAN</li> <li>Templates</li> </ul>	CleanAir Capable CleanAir Admin S	Status	Yes Enable	0		No radar det	ected char	nnels ssignment		
Network Lists 802.11a/n/ac/ax	* CleanAir enable w Number of Spect connections	<i>ill take effect only</i> rum Expert	if it is enabled 0	on this band.		Current Ta Assignme	k Power Le nt Method	evel	1 Global	
<ul> <li>Media Stream</li> </ul>	Antenna Paran	eters							Custom	
Application Visibility And Control	Antenna Type		Interna A	I 🖸		Performa	nce Prof	ïle		
Lync Server	Antenna		B C D			View and Perform	edit Perfor nance Pro	mance Profile fo	or this AP	
Timers						Note: Chang	ing any of	the parameters	causes the Radio to be temporar	ily disabled
Netflow						and thus may	y result in	loss of connecti	vity for some clients.	

## **Rx Sop Threshold**

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

ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	Rx Sop T	hreshol	d						
Access Points     All APs     Radios     Global Configuration	Rx Sop T Rx Sop T	hreshold 8 hreshold 8	02.11a Defa 02.11b Defa	ult 🗘 O ult 🗘 O	Custom				
<ul> <li>RF Management</li> <li>Flexible Radio</li> <li>Assignment</li> <li>Load Balancing</li> <li>DTLS</li> <li>Band Select</li> <li>Rx Sop Threshold</li> <li>Optimized Roaming</li> <li>Network Profile</li> </ul>	± Rxsop o	nly suppor	ted in Local,Flex,B	ridge and Flex-	-Bridge mode A	ιρs.			

## **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.

۰۱۱۰۰۱۰۰ cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs >	New							
WLANS WLANS Advanced	Type Profile Na SSID ID	ime	WLA voice voice 6	N ᅌ					

ululu cisco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> ON	TROLLER W <u>I</u> RELESS	<u>S</u> ECURITY M <u>A</u> NAGEMENT	C <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
WLANs	WLANs > Edit 'voice'			
WLANs WLANs	General Security	QoS Policy-Mapp	ing Advanced	
▶ Advanced	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface	voice WLAN voice C Enabled [WPA2][Auth(FT 802.1 (Modifications done under 802.11a only C rtp-9 voice C	LX)] security tab will appear after ap	plying the changes.)
	Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID Lobby Admin Access	Enabled Enabled RTP9-32A-WLC3		

### 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.

،، ،،، ،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 2 WPA+WPA2
	Security Type Enterprise
	MAC Filtering 2
	WPA+WPA2 Parameters
	WPA2 Policy 🗹
	WPA2 Encryption CCMP128(AES) TKIP CCMP256 GCMP128 GCMP256
	OSEN Policy
	Fast Transition
	Fast Transition Enable S
	Reassociation Timeout 20 Seconds
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANS	WI ANS > Edit 'voice'
WLANS WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Protected Management Frame
	Authentication Key Management 12
	802.1X-SHA1 C Enable
	802.1X-SHA2 Enable
	FT 802.1X 🗹 Enable
	CCKM Enable
	WPA GTK-randomize State 14 Disable 3



Cisco RoomOS Series Wireless LAN Deployment Guide

.ı ı.ı ı. cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs >	Edit 'v	oice'						
▼ WLANs	General	Secur	rity QoS	Policy-Map	ping Adv	vanced			
WLANS	Protected	l Managem	ent Frame						
Advanced	PMF		Disabled	1 😌					
	Authentic	cation Key	Management <del>19</del>						
	PSK Fo	ormat 21	ASCII	•					
	PSK		🗹 Enable						
	PSK-S	HA2	Enable	e					
	FT PS	<	Enable	2					
	WPA GTK	-randomize S	State 14 Disable	0					

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.

ululu cisco	<u>M</u> ONITOR <u>W</u> L	ANs <u>C</u> ONTROLLER	WIRELESS SECURITY	MANAGEMENT CO	MMANDS HELP	<u>F</u> EEDBACK	
WLANs	WLANs > Edi	t 'voice'					
WLANS WLANS	General	Security QoS	Policy-Mapping Adv	vanced			
	Select AAA s RADIUS Server Apply Cisc Server 1 Server 2 Server 3 Server 4	ervers below to overrivers erver Overwrite interface o ISE Default Settings Authentication Server © Enabled None None None None None	de use of default servers of Enabled Enabled S Accounting Serv S Enabled None None None None None None None	ers © © © ©	EAP Parameters Enable EAPOL Key Timeo EAPOL Key Retrie Identity Request 1 Identity Request 1	ut(200 to 5000 millisec) s(0 to 4) Fimeout(1 to 120 sec) Retries(1 to 20)	400 4 30 2
	Server 5 Server 6	None	None     None	•	Request Timeout(	1 to 120 sec)	30
	Servero	Authorization ACA Ser	ver Accounting ACA	Server	Request Retries(1	to 20)	2

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 QBSS.

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'						
WLANs WLANs	General Security	QoS Policy-Ma	pping Adv	vanced			
▶ Advanced	Quality of Service (QoS) Application Visibility AVC Profile Flex AVC Profile Netflow Monitor Fastlane <b>Override Per-User Ban</b> Average Data Rate	Platinum (voice)  Platinum (voice)  Platinum (voice)  Platinum (voice)  None  Disable  Disable  Disable  DownStream UpS  0  0  0  0  0  0  0  0  0  0  0  0  0	€ € (kbps) <sup>16</sup> tream				
	Burst Data Rate Average Real-Time Rate Burst Real-Time Rate Clear	0 0 0 0 0 0					

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	TROLLER W <u>I</u> REL	ESS <u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'						
WLANS WLANS	General Security Override Per-SSID Ba	QoS Policy- ndwidth Contra	Mapping Ad cts (kbps) <u>16</u>	vanced			
P Advanced	Average Data Rate Burst Data Rate Average Real-Time Rate Durst Real-Time Rate Clear WMM WMM Policy 7920 AP CAC 7920 Client CAC Media Stream	DownStream	UpStream 0 0 0 0				
	Multicast Direct Lync Policy Audio	Silver					

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

Enable Aironet Extensions (Aironet IE).

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

Configure Client Exclusion as necessary.

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

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

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

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

DHCP Address Assignment Required should be disabled.

Management Frame Protection 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.

،، ،،، ،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'voice'
WLANS WLANS	General Security QoS Policy-Mapping Advanced
▶ Advanced	Allow AAA Override       Enabled       DHCP         Coverage Hole Detection       © Enabled       DHCP Server       Override         Enable Session Timeout       © 86400 Session Timeout (secs)       DHCP Addr. Assignment       Required         Aironet IE       © Enabled       Management Frame Protection (MFP)         Diagnostic Channel 11       Enabled       MFP Client Protection 1       Optional ©         Override Interface ACL       IPv4 None ©       IPv6 None ©       MFP Client Protection 1       Optional ©         URL ACL       None ©       P2P Blocking Action       Disabled       802.11a/n (1 - 255)       2       802.11b/g/n (1 - 255)       2       1         Maximum Allowed Clients       0       Static IP Tunneling 11       Enabled       NAC       NAC       NAC State       Nane ©       Static IP Tunneling 11       Enabled       NAC
	Wi-Fi Direct Clients Policy     Disabled     Client Load Balancing       Maximum Allowed Clients     200       Client Band Select



cisco	MONITOR WLANS CONTROLLER WIRELESS SECURIT	Y MANAGEMENT COMMANDS HELP <u>F</u> EEDBACK	
WLANs	WLANs > Edit 'voice'		
WLANS	General Security QoS Policy-Mapping A	dvanced	
Advanced	FlexConnect Local Auth 12 Enabled	PMIP Profile	None ᅌ
	Learn Client IP Address 5 🗸 🗸 Enabled	PMIP Realm	
	Vian based Central	Universal AP Admin Support	
	Switching 13 Enabled	Universal AP Admin	
	Central DHCP Processing Enabled	11v BSS Transition Support	
	Override DNS Enabled	BSS Transition	0
	NAT-PAT Enabled	Disassociation Imminent	
	Central Assoc Enabled	Disassociation Timer(0 to 3000 TBTT)	200
	Lync	Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40
	Lync Server Disabled ᅌ	BSS Max Idle Service	
	11k	Directed Multicast Service	
	Neighbor List Enable	ed Tunneling	
	Neighbor List Dual Band Enable	ed Tunnel Profile	None ᅌ
	Assisted Roaming Prediction Optimization Enable	ed EOGRE Vlan Override	0
	802.11ax BSS Configuration	mDNS	
	Down Link MU-MIMO	ed mDNS Snooping	Enabled

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	C <u>o</u> mmands he <u>l</u> p <u>f</u> eedback	
WLANs	WLANs > Edit 'voice'			
WLANS	General Security QoS	Policy-Mapping Advanced		
WEARs	802.11ax BSS Configuration		mDNS	
P Advanced	Down Link MU-MIMO	Enabled	mDNS Snooping	Enabled
	Up Link MU-MIMO	Enabled	TrustSec	
	Down Link OFDMA	Enabled	Security Group Tag	0
	Up Link OFDMA	Enabled	Umbrella	
			Umbrella Mode	Ignore ᅌ
			Umbrella Profile	None ᅌ
			Umbrella DHCP Override	
			Fabric Configuration	
			Fabric	Enabled
			Mobility	
			Selective Reanchor	Enabled
			U3 Interface	
			U3 Interface	Enabled
			U3 Reporting Interval	30

## **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.

ululu cisco	<u>m</u> onitor <u>w</u> la	Ns <u>C</u> ONT	TROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	AP Groups								
WLANs WLANs	Add New AP G	oup							
Advanced AP Groups	AP Group Name Description	rtp Add	Cancel						

،، ،،، ،، cısco	MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS	<u>S</u> ECURITY M <u>A</u> NAGEMEN	IT C <u>O</u> MMANDS F	IELP <u>F</u> EEDBACK			
WLANs	Ap Groups > Edit 'rtp'						
WLANs	General WLANS RF Profile APs	802.11u Location	Ports/Module	Intelligent Capture			
<ul> <li>Advanced</li> <li>AP Groups</li> </ul>			Apply				
	AP Group Name rtp						
	AP Group Description						
	NAS-ID RTP9-32A-WI	RTP9-32A-WLC3					
	Enable Client Traffic QinQ						
	Enable DHCPv4 QinQ <sup>3</sup>						
	QinQ Service Vlan Id 10 0	0					
	Fabric ACL Template None 🗘						
	CAPWAP Preferred Mode Not-Conf	īgured					
	Custom Web Override-Global 13   Enable						
	External Web auth URL none						
	NTP Auth Enable						
	NTP Server None ᅌ						

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

۱۱۱۱۱۱۰ cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	COMMANDS	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	Ap Group	os > Edit	'rtp'					
WLANs WLANs	General	WLAI	Ns RF Profil	e APs	802.11u	Location	Ports/Module	Intelligent Capture
<ul> <li>Advanced</li> <li>AP Groups</li> </ul>	Add Nev	v						Add New
	WLAN S Interfac /Interfa Group(0	SID ce ce 3)	voice(6) rtp-9 voice		0	1		
	SNMP N	IAC State	Enabled	cel				

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.

ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>a</u> nagement	C <u>O</u> MMANDS	HE <u>L</u> P <u>F</u> EEDBACK	
WLANs	Ap Group	s > Edit	'rtp'						
WLANS WLANS	General	WLA	Ns RF Profil	e APs	802.11u	Location	Ports/Module	Intelligent Capt	ture
Advanced AP Groups							Apply		
	802.11a 802.11b	a none	9	<b>○</b>					

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

Those access points will then reboot.

uluilu cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMEN	r c <u>o</u> mmands	HELP	<u>F</u> EEDBACK		
WLANs	Ap Groups	Groups > Edit 'rtp'									
WLANS WLANS	General	WLAN	s RF Profile	e APs	802.11u	Location	Ports/Module	Inte	lligent Capture		
Advanced AP Groups	APs curre	ntly in th	e Group		Remove APs Add APs to the Group					d APs	
	AP Nan	ne	Ethernet	MAC			ame	Group	Name		
	rtp9-31	a-ap14 a-ap20	00:81:c4:96:78:28 00:81:c4:32:b9:b8								
	rtp9-32	a-ap23	00:81:c4	:96:74:10							

# **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.

ılıılı. cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK							
Controller	General								
General	Name	RTP9-32A-WLC3							
Icons	802.3x Flow Control Mode	Disabled 🗘							
Inventory	LAG Mode on next reboot	Enabled ᅌ							
Interfaces	Broadcast Forwarding	Disabled 📀							
Interface Groups	AP Multicast Mode 1	Multicast 🗘 239.1.1.9 Multicast Group Address							
Multicast	AP IPv6 Multicast Mode <sup>1</sup>	Multicast 📀 ff1e::239:100:100:21 IPv6 Multicast Group Address							
Network Routes	AP Fallback	Enabled							
Fabric Configuration	CAPWAP Preferred Mode	ipv4 😂							
Redundancy	Fast SSID change	Enabled							
Mobility Management	Link Local Bridging	Disabled ᅌ							
Ports	Default Mobility Domain Name	CTG-VoWLAN2							
▶ NTP	RF Group Name	RTP9-VoWLAN2							
E CDP	User Idle Timeout (seconds)	300							
▶ PMIPv6	ARP Timeout (seconds)	300							
Tunneling	ARP Unicast Mode	Disabled 🗘							
F IPv6	Web Radius Authentication	PAP ᅌ							
mDNS	Operating Environment	Commercial (10 to 35 C)							
Advanced	Internal Temp Alarm Limits	10 to 38 C							
I surful Intercention	WebAuth Proxy Redirection Mode	Disabled ᅌ							
Lawrul Interception	WebAuth Proxy Redirection Port	0							
	Captive Network Assistant Bypass	Disabled ᅌ							
	Global IPv6 Config	Disabled ᅌ							
	Web Color Theme 2	Default 🗘							
	HA SKU secondary unit	Disabled ᅌ							
	Nas-Id	RTP9-32A-WLC3							
	HTTP Profiling Port	80							
	DNS Server IP(Ipv4/Ipv6)	171.70.168.183							
	HTTP-Proxy Ip Address(Ipv4/Ipv6)	0.0.0.0							
	WGB Vlan Client	Disabled 📀							
	1. Multicast is not supported with Flex 2.Changes in Web color Theme will ge	«Connect on this platform. Multicast-Unicast mode does not support IGMP/MLD Snooping. Disable Global Multicast first. st updated after browser Refresh.							

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

،،ا،،،ا،، cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller	Multicast								
General Icons Inventory	Enable Glo Enable IG	obal Multica MP Snoopia	ast Mode ng	0					
Interfaces	IGMP Time	eout (30-7	200 seconds)	60					
Interface Groups	IGMP Quer	ry Interval	(15-2400 second:	s) 20					
Multicast	Enable ML	D Snoopin	g						
Network Routes	MLD Time	out (30-72	00 seconds)	60					
Fabric Configuration	MLD Query	y Interval	(15-2400 seconds	) 20					
Redundancy									
Mobility Management									
Ports	Foot Notes								
▶ NTP	Changing Glo	bal Multica	ast configuration p	arameters rem	oves configure	d Multicast VLAN fro	om WLAN.		
▶ CDP									

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.

۱۱۱۱۱۱۰ cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller	Mobility	Anchor (	Config						
General Icons Inventory Interfaces Interface Groups Multicast Network Routes Fabric Configuration Redundancy	Keep Aliv Keep Aliv Symmetr DSCP Val	e Count e Interval ic Mobility 1 ue	(1-30 seconds) Funneling mode	3 10 Enabled 0					
<ul> <li>Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging</li> </ul>									

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.

	uluili. cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIREL	ESS §	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Co	ontroller	Static M	obility Gr	oup Members	5						
	General Icons	Local	Mobility Gro	CTG-Vo	VLAN2						
	Inventory Interfaces	MAC A	ddress	IP Address(Ipv4,	/Ipv6) (	Group N	ame	м	ulticast IP	Status	
	Interface Groups	00:5d:	73:1a:c3:49	10.81.6.70	(	CTG-VoV	/LAN2	0.	0.0.0	Up	
	Multicast										
Þ	Network Routes										
Þ	Fabric Configuration										
Þ	Redundancy										
•	Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging										

# **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.

 cısco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11a(	5 GHz) >	Media						
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> <li>Global Configuration</li> </ul>	Voice Call Adr	Video nission C	Media						
<ul> <li>Advanced</li> <li>Mesh</li> <li>AP Group NTP</li> <li>ATF</li> <li>RF Profiles</li> <li>FlexConnect Groups</li> </ul>	Admiss CAC Me Max RF Reserve Expedit	ion Control athod 4 Bandwidth ad Roaming ad bandwid	(ACM) (5-85)(%) Bandwidth (0-25) Ith	✓ Er Loa 75 (%) 6 ✓	abled d Based 📀				
FlexConnect VLAN Templates	Per-Cal	SIP Ban	dwidth <sup>2</sup>		labled				
Network Lists • 802.11a/n/ac/ax Network • RRM RF Grouping TPC DCA	SIP Con SIP Bar SIP Voi <b>Traffic S</b>	dec ndwidth (kb ce Sample I Stream M	ps) Interval (msecs) I <b>etrics</b>	G.7 64 20	11 ¢				
Coverage General Client Roaming Media	Metrics	Collection							
EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac/ax) CleanAir 802.11b/g/n/ax	Foot Not 1 11a rat 11n rat 2 SIP CA 3 SIP CA 4 Static (	es(Kbps): 6 es(Kbps): 6 C should on C will be sup CAC method	5000,9000,12000, 55000,72200,1300 Iy be used for pho pported only if SIP I is radio based an	18000,24000,3 000,144400,13 nes that suppo snooping is er d load-based C	26000,48000,54 5000,150000,2 rt status code nabled. AC method is c	4000 70000,300000 17 and do not supp channel based.	ort TSPEC-based	admissio	n control.

Admission Control Mandatory for Video should be disabled.

ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11a(5	GHz) >	Media						
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>Global Configuration</li> </ul> </li> </ul>	Voice Call Adm	Video	Media						
<ul> <li>Advanced</li> <li>Mesh</li> <li>AP Group NTP</li> <li>ATF</li> <li>RF Profiles</li> <li>FlexConnect Groups</li> <li>FlexConnect ACLs</li> <li>FlexConnect VLAN</li> <li>Templates</li> <li>Network Lists</li> </ul>	Admissic CAC Met Max RF I Reserver SIP CAC	on Control thod 4 Bandwidth d Roaming Support	(ACM) (5-85)(%) Bandwidth (0-25)	(%) 0	abled				
<ul> <li>S02.11a/n/ac/ax</li> <li>Network</li> <li>RRM</li> <li>RF Grouping</li> <li>TPC</li> <li>DCA</li> <li>Coverage</li> <li>General</li> <li>Client Roaming</li> <li>Media</li> <li>EDCA Parameters</li> <li>DFS (802.11h)</li> <li>High Throughput (802.11h)ac/ax)</li> <li>CleanAir</li> <li>802.11b/g/n/ax</li> </ul>	Foot Note 1 11a rate 11n rate 2 SIP CAC 3 SIP CAC 4 Static Cr	ss(Kbps): 6 s(Kbps): 6 should on will be suj 4C method	000,9000,12000, 5000,72200,1300 ly be used for pho sported only if SIP is radio based an	18000,24000,3 00,144400,13 nes that suppo snooping is en d load-based C	5000,48000,54 000,150000,2 t status code 1 abled. 4C method is c	1000 70000,300000 17 and do not supp hannel based.	ort TSPEC-based	admissio	n control.

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) confi	guration
Voice AC - Admission control (ACM	<b>I</b> ) <b>Enabled</b>
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	(I) 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.

ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11a(5	5 GHz) >	Media						
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>Global Configuration</li> </ul> </li> </ul>	Voice	Video	Media						
Advanced	Unicast	Video Redi	rect						
Mesh	onicase	video itea							
AP Group NTP	Multicas	st Direct	Admission Co	ntrol					
▶ ATF	Maximu	um Media Ba	andwidth (0-85(%	)) 85					
RF Profiles	Client N	1inimum Ph	y Rate 💶	6000	)				
FlexConnect Groups	Maximu	um Retry Pe	rcent (0-100%)	80					
FlexConnect ACLs									
FlexConnect VLAN Templates	Media S	tream - I	Multicast Dire	ct Paramete	rs				
Network Lists	Multica	st Direct En	able						
802.11a/n/ac/ax	Max Str	reams per R	adio	No-	limit ᅌ				
▼ RRM	Max St	reams per C	lient	No-	limit ᅌ				
RF Grouping	Best Ef	fort QoS Ad	mission	🗌 Er	abled				
DCA									
Coverage General									
Client Roaming									
Media									
EDCA Parameters DES (802-11b)	Foot Not	tes							
High Throughput	1 11a rat	es(Kbps): 6	000,9000,12000,	18000,24000,3	6000,48000,54	4000			
(802.11n/ac/ax)	2 SIP CA	es(Kbps): 6 C should on	5000,72200,1300 lv be used for pho	100,144400,13 nes that suppo	000,150000,2 rt status code	70000,300000 17 and do not supp	ort TSPEC-based	admissio	n control.
CleanAir	3 SIP CA	C will be su	oported only if SIP	snooping is er	abled.				
802.11b/g/n/ax	4 Static C	CAC method	is radio based an	d load-based C	AC method is c	hannel based.			

# **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**.

uluılu cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROL	LER.	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile	e > New								
Access Points     All APs	RF Profile	Name		rtp-5						
Radios	Radio Poli	cy		802.	11a ᅌ		_			
Global Configuration	Use defau	It RF Profile	e Template	None	e		٥			
Advanced										
Mesh										
AP Group NTP										
▶ ATF										
RF Profiles										

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.

 cısco	<u>M</u> ONITOR	<u>W</u> LANs		<b>ε w</b> <u>i</u>	RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile	> Edit	'rtp-5'							
Access Points All APs	General	802.1	1 RRM	Hig	h Density	Client	Distribution			
Radios Global Configuration	Data Rat	es <u>1</u>		MCS S	Settings					
Advanced										
Mesh	6 Mbps	Disabled	i 🗘	0	🗹 Supp	orted				
AP Group NTP	9 Mbps	Disabled	i ᅌ	1	🗹 Supp	orted				
ATE	12 Mbps	Mandato	ory ᅌ	2	🗹 Supp	orted				
RF Profiles	18 Mbps	Support	ed ᅌ	3	🗹 Supp	orted				
FlexConnect Groups	24 Mbps	Support	ed ᅌ	4	🗹 Supp	orted				
FlexConnect ACLs	36 Mbps	Support	ed ᅌ	5	🗹 Supp	orted				
FlexConnect VLAN	48 Mbps	Support	ed ᅌ	6	🗹 Supp	orted				
Templates	54 Mbps	Support	ed ᅌ	7	🗹 Supp	orted				
Network Lists				8	🗹 Supp	orted				
🕨 802.11a/n/ac/ax				9	🗹 Supp	orted				
802.11b/g/n/ax				10	🗹 Supp	orted				
Media Stream				11	🗹 Supp	orted				
Application Visibility				12	🗹 Supp	orted				
And Control				13	🗹 Supp	orted				
Lync Server				14	🗹 Supp	orted				
Country				15	🛃 Supp	orted				
Timers				16	🖸 Supp	orted				
Netflow									_	
0.05										

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.
uhuhu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HEL	.p <u>f</u> eedback
Wireless	RF Profile > Edit 'rtp-5'	
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios             <li>Global Configuration</li> </li></ul> </li> </ul>	General 802.11 RRM High Density Client Distribution	overage Hole Detection
Advanced Mesh	Maximum Power Level Assignment (-10 to 30 dBm) 30	Data RSSI(-90 to -60 dBm) -80
AP Group NTP     ATF	Minimum Power Level Assignment (-10 to 30 dBm)         -10         -10           Power Threshold v1(-80 to -50 dBm)         -70         -70	Voice RSSI(-90 to -60 dBm)         -80           Coverage Exception(0 to 100 %)         2
RF Profiles FlexConnect Groups	Power Threshold v2(-80 to -50 dBm) -67 00 DCA Pro	Coverage Level(1 to 200 Clients) 3 ofile Threshold For Traps
FlexConnect VLAN Templates	Avoid Foreign AP Interference         Image: Channel Width         20 MHz         80 MHz         160 MHz         80+80 MHz         Best         Channel Width	Interference (0 to 100%) 10 Clients (1 to 200) 12
Network Lists 802.11a/n/ac/ax		Noise (-127 to 0 dBm)         -70           Utilization (0 to 100 %)         80
<ul> <li>802.11b/g/n/ax</li> <li>Media Stream</li> </ul>	Cit	Connectivity Throughput O Automatic
Application Visibility     And Control     Lync Server	Cit	Craha Onicala
Country Timers	High-Speed Roam	
Netflow     OoS		

cisco	MONITOR WL	ANs <u>C</u> O	NTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	P <u>F</u> EEDBACK
Wireless	RF Profile >	Edit 'rt	p-5'						
Access Points	General	802.11	RRM	High Density	Client	Distribution			
All APs ▶ Radios								Clien	ent Aware
Global Configuration								(	CEnable ODisable
Advanced	High-Speed R	oam							
Mesh	HSR mode						Enabled		
AP Group NTP	Neighbor Ti	meout Facto	or						
▶ ATF	DCA Channe	el List							
RF Profiles									
FlexConnect Groups		36,40	, 44, 48, 52, 61	56, 60, 64, 149	, 153,				
FlexConnect VI AN	DCA Channe	ls							
Templates									
Network Lists					lli.				
802.11a/n/ac/ax	Select	Channel							
802.11b/g/n/ax		36							
Media Stream		40							
Application Visibility		44							
And Control		48							
Country		52							
Timers	Extended U	NII-2 chann	els 🗆 En	abled					
Netflow	Extended of			00100					
N 0.05									

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**.

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile > Edit	'rtp-5'						
Access Points	General 802	.11 RRM	High Density	Client	Distribution			
Radios     Global Configuration     Advanced	High Density Pa	irameters	Multio	cast Param	eters			
Mesh	Maximum Clients	(1 to 200) 200	Mult	icast Data Rate	es² auto ᅌ			
AP Group NTP	Rx Sop Thresho	ld Parameters	<u>5</u>					
RF Profiles	Rx Sop Threshold <sup>6</sup>	Default ᅌ 🛛	Custom					

# **FlexConnect Groups**

Cisco RoomOS Series Wireless LAN Deployment Guide

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

CISCO	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	FlexConn	ect Gro	ups > New						
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios             <li>Global Configuration</li> </li></ul> </li> </ul>	Group Nar	ne rtp	-1						
Advanced									
Mesh									
AP Group NTP									
ATF									
RF Profiles									
FlexConnect Groups									
	NITOR WLANS	CONTROLLE	ER WIRELESS SE	CURITY MANA	GEMENT COMM	IANDS HELP FE	EDBACK		
Wireless Flo	exConnect Grou	ins > Edit	'rtn-1'						
Access Points     All APs     Radios	General Local	Authentica	tion Image Upg	rade ACL Ma	apping Cent		VIAN mapping		VC manning
							· · _ · · · · · · · · · · · · · · · · ·	WLAN A	, concepting
Global Configuration	Group Name		rtp-1					WLANA	
Global Configuration  Advanced  Mesh	Group Name VLAN Template Nam	ne	rtp-1					WLANA	a mapping
Global Configuration Advanced Mesh AP Group NTP	Group Name VLAN Template Nam Enable AP Local Aut	ne hentication <sup>2</sup>	rtp-1					WLANA	
Global Configuration Advanced Mesh AP Group NTP ATF	Group Name VLAN Template Nam Enable AP Local Aut	ne hentication <sup>2</sup>	rtp-1 none 🗘					WLANA	
Global Configuration Advanced Mesh AP Group NTP ATF E RF Profiles	Group Name VLAN Template Nam Enable AP Local Aut lexConnect AP	ne hentication <sup>2</sup>	rtp-1 none ᅌ					WLANA	
Global Configuration Advanced Mesh A P Group NTP ATF E RF Profiles FlexConnect Groups	Group Name VLAN Template Nam Enable AP Local Aut ElexConnect AP HTTP-Proxy	ne hentication <sup>2</sup>	rtp-1					WLANA	
Global Configuration Advanced Mesh A P Group NTP ATF RF Profiles FlexConnect ACLs	Group Name VLAN Template Nam Enable AP Local Aut HERConnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port	ne hentication <sup>2</sup> v6)	rtp-1					WLANA	
Global Configuration Advanced Mesh A AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect ALLs FlexConnect VLAN Templates	Group Name VLAN Template Nam Enable AP Local Aut HERConnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port	ne hentication <sup>2</sup> v6)	rtp-1 none ©					WLAN A	
Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect VLAN Templates Network Lists	Group Name VLAN Template Nam Enable AP Local Aut StexConnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port	ne hentication <sup>2</sup> v6)	rtp-1 none ©					WLAN A	
Global Configuration Advanced Mesh AP Group NTP ATF E RF Profiles FlexConnect Groups FlexConnect ALS FlexConnect VLAN Templates Network Lists S02.11a/n/ac/ax	Group Name VLAN Template Nam Enable AP Local Aut Reaconnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port	ne hentication <sup>2</sup> v6)	rtp-1 none 9					WLAN A	
Global Configuration Advanced Mesh AP Group NTP ATF FlexConnect Groups FlexConnect VLAN Templates Network Lists S02.11a/n/ac/ax Main Straam	Group Name VLAN Template Nam Enable AP Local Aut Electonnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port AAA Server Ip Address	ne hentication <sup>2</sup> v6)	rtp-1 none © 0 Add					WLAN A	
Global Configuration Advanced Mesh AP Group NTP ATF FlexConnect Groups FlexConnect VLAN Templates Network Lists 802.11a/n/ac/ax B02.11b/g/n/ax Configuration	Group Name VLAN Template Nam Enable AP Local Aut Electonnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port AAA Server Ip Address Server Type	ne hentication <sup>2</sup> v6)	rtp-1 none © 0 Add Primary ©					WLAN A	
Global Configuration Advanced Mesh A P Group NTP ATF FlexConnect Groups FlexConnect VLAN Templates Network Lists 802.11a/n/ac/ax 802.11b/g/n/ax Media Stream And Control	Group Name VLAN Template Nam Enable AP Local Aut Electonnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port AAA Server Ip Address Server Type Shared Secret	ne hentication <sup>2</sup> v6)	rtp-1 none © 0 Add Primary ©					WLAN A	
Global Configuration Advanced Mesh A P Group NTP ATF RF Profiles FlexConnect Groups FlexConnect VLAN Fenylates Network Lists 802.11a/n/ac/ax 802.11b/g/n/ax Media Stream And Control Lync Server	Group Name VLAN Template Nam Enable AP Local Aut Execonnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port AAA Server Ip Address Server Type Shared Secret Confirm Shared Sec	ne hentication <sup>2</sup> v6)	rtp-1 none					WLAN A	
Global Configuration Advanced Mesh AP Group NTP ATF FiexConnect Groups FiexConnect VLAN FiexConnect VLAN FiexConnect VLAN S02.11a/n/ac/ax S02.11b/g/n/ax Media Stream Application Visibility And Control Lync Server Country Timeors	Group Name VLAN Template Nam Enable AP Local Aut Execonnect AP HTTP-Proxy Ip Address(Ipv4/Ipv Port AAA Server Ip Address Server Type Shared Secret Confirm Shared Sec Port Number	ne hentication <sup>2</sup> v6)	rtp-1 none © 0 Add Primary © 1812					WLAN A	
Global Configuration Advanced Mesh AP Group NTP ATF FiexConnect Groups FiexConnect VLAN FiexConnect VLAN FiexConnect VLAN B02.11a/n/ac/ax B02.11a/n/ac/ax Media Stream Application Visibility And Control Lync Server Country Timers Nethow	Group Name VLAN Template Nam Enable AP Local Aut Execonnect AP TTP-Proxy Ip Address(Ipv4/Ipv Port AAA Server Ip Address Server Type Shared Secret Confirm Shared Sec Port Number Add	ne hentication <sup>2</sup> v6)	rtp-1 none © 0 Add Primary © 1812					WLAN A	

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

<u>M</u> ONITOR <u>W</u> L/	ANs <u>C</u> ONTROL	LER W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
FlexConnect	Group AP Lis	st						
Group Name			rtp-1					
FlexConnect A	APs							
Add AP Entries 0 - 0 AP MAC Add	of 0 Iress AP Name	S	tatus	AP Mo	de	Тур	ie	Conflict with PnP
	MONITOR WL FlexConnect Group Name FlexConnect / Add AP Entries 0 - 0 AP MAC Add	MONITOR WLANS CONTROL FlexConnect Group AP Lis Group Name FlexConnect APs Add AP Entries 0 - 0 of 0 AP MAC Address AP Name	MONITOR WLANS CONTROLLER WIRELESS FlexConnect Group AP List Group Name FlexConnect APs Add AP Entries 0 - 0 of 0 AP MAC Address AP Name S	MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY       FlexConnect Group AP List     rtp-1       Group Name     rtp-1       FlexConnect APs     rtp-1       Add AP	MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT       FlexConnect Group AP List     rtp-1     FlexConnect APS     rtp-1       FlexConnect APS	MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT     COMMANDS       FlexConnect Group AP List     rtp-1     <	MONITOR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP         FlexConnect Group AP List       rtp-1       rtp	MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT     COMMANDS     HELP     FEEDBACK       FlexConnect Group AP List     rtp-1     rtp-1     rtp-1     rtp-1     rtp-1     rtp-1       FlexConnect APs     Add AP     status     AP Mode     Type

،، ،،، ،، cısco	<u>M</u> ONITOR <u>V</u>	<u>V</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	FlexConne	ct Grou	ıp AP List						
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios             <li>Global Configuration</li> </li></ul> </li> </ul>	Group Nam	ne			rtp-1				
Advanced	FlexConnec	t APs							
Mesh									
AP Group NTP	Add AP								
ATF	Select APs f	rom curr	ent controller						
RF Profiles FlexConnect Groups	Ethernet MA	AC		Add Canc	:el				

# **Multicast Direct**

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

ululu cisco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> ONT	ROLLER W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	Media Stream >Genera	I					
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>Global Configuration</li> </ul> </li> </ul>	Multicast Direct feature Session Message Config	Enabled					
Madvanced	Session announcement State	Enabled					
Mesh	Session announcement URL						
AP Group NTP	Session announcement Emai	1					
MATE	Session announcement Phon	e					
RF Profiles				]			
FlexConnect Groups	Session announcement Note						
FlexConnect ACLs			///				
FlexConnect VLAN Templates							
Network Lists							
🕨 802.11a/n/ac/ax							
🕨 802.11b/g/n/ax							
<ul> <li>Media Stream</li> <li>General</li> <li>Streams</li> </ul>							

Then configure the media streams as necessary.

uluili. cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP
Wireless	Media St	ream > N	lew					
<ul> <li>Access Points         All APs         <ul> <li>Radios</li> <li>Global Configuration</li> </ul> </li> <li>Advanced         Mesh         <ul> <li>AP Group NTP</li> <li>ATF</li> <li>RF Profiles</li> <li>FlexConnect Groups</li> <li>FlexConnect VLAN             <ul> <li>Templates</li> <li>Network Lists</li> <li>802.11a/n/ac/ax</li> <li>802.11b/g/n/ax</li> <li>Media Stream             <ul> <li>General</li> </ul> </li> </ul></li></ul></li></ul>	Stream N Multicast Multicast Maximum Resource Select fro Average F RRC Perior Traffic Pro	ame Destination Destination Expected I Reserva m predefin Packet Size odic update ity (1-8) offile Violatic	Start IP Address( End IP Address() Bandwidth(1 to 35 tion Control(F ed templates (100-1500 bytes)	ipv4/ipv6) 2v4/ipv6) 000 Kbps) <b>RC) Param</b>	solo select 1200 1 best-effort v	~		
Streams								

Once saved, then the media stream will be displayed.

սիսիս cisco	MONITOR WLANs	WIRELESS SECUR	LITY MANAGEMENT	C <u>o</u> mmands he <u>l</u> f	P <u>F</u> EEDBACK	_
Wireless	Media Streams			I	Entries 1 - 1 of 1	
Access Points All APs Radios	Stream Name		Start IP 239.1.1.1	Address(Ipv4/Ipv6)	End IP Address(Ipv4/Ipv6) 239.1.1.1	Operation Status Multicast Direct
Global Configuration  Advanced						
Mesh AP Group NTP						
ATF RF Profiles						
FlexConnect Groups FlexConnect ACLs						
FlexConnect VLAN Templates						
Network Lists 802.11a/n/ac/ax						
<ul> <li>802.11b/g/n/ax</li> <li>Media Stream General Streams</li> </ul>						

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

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ON	troller w <u>i</u> reless	<u>s</u> ecurity m <u>a</u> nagemen	NT C <u>O</u> MMANDS	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'				
<ul> <li>WLANS WLANS</li> <li>Advanced</li> </ul>	General     Security       Override Per-SSID Ba       Average Data Rate       Burst Data Rate       Average Real-Time Rate       Burst Real-Time Rate       Clear       WMM       WMM Policy       7920 AP CAC       7920 Client CAC       Media Stream	QoS     Policy-Map       ndwidth Contracts (       DownStream     UpSt       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0	Advanced (kbps) <sup>16</sup> ream		
	Multicast Direct Lync Policy Audio	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

	արտիս									
	CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIREL	ESS <u>S</u> ECUR	RITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
W	ireless	Edit QoS	Profile							
•	Access Points All APs Radios Global Configuration	QoS Profi	ile Name	platinum For Voice App	lications					
•	Advanced	Description	on							
	Mesh	Per-User	Bandwid	th Contracts (	(kbps)	*				
	AP Group NTP			DownStre	am U	pStream				
•	ATF	Average [	Data Rate	0		)				
	<b>RF Profiles</b>	Burst Dat	a Rate	0		)				
	FlexConnect Groups	Average F	Real-Time R	ate 0		)				
×	FlexConnect ACLs	Burst Rea	al-Time Rate	0		)				
	FlexConnect VLAN Templates	Per-SSID	Bandwid	ith Contracts	(kbps)	*				
	Network Lists			DownStre	am U	pStream				
×	802.11a/n/ac/ax	Average [	Data Rate	0		)				
•	802.11b/g/n/ax	Burst Dat	a Rate	0						
×	Media Stream	Average F	Real-Time R	ate 0		)				
	Application Visibility	Burst Rea	al-Time Rate	0		)				
	And Control	WLAN Qo	S Param	eters						
	Lync Server	Maximum	Priority	voice	~					
	Country	Unicast D	efault Prior	ity besteffor	t v					
	Timers	Multicast	Default Pric	ority besteffor	t v					
•	Netflow									
*	QoS	Wired Qo	S Protoc							
	Roles	Protocol 1	Гуре	None	•					
	Qos Map									

اسان cisco	1. D	MONITOR	<u>W</u> LANs	CONTROLLER	WIRE	LESS <u>S</u> e	CURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Wireless		Edit QoS	Profile							
<ul> <li>Access Poin</li> <li>All APs</li> <li>Radios</li> <li>Global Config</li> </ul>	uts uration	QoS Profi	ile Name on	gold For Video App	olications					
Advanced		Deseripti								
Mesh		Per-User	Bandwid	th Contracts	(kbps)	*				
AP Group N	ТР			DownStre	am U	pStream				
▶ ATF		Average	Data Rate	0		0				
<b>RF</b> Profiles		Burst Dat	ta Rate	0		0				
FlexConnec	t Groups	Average I	Real-Time R	ate 0		0				
FlexConnec	t ACLs	Burst Rea	al-Time Rate	0		0	]			
FlexConnec Templates	t VLAN	Per-SSID	Bandwid	ith Contracts	(kbps)	*				
Network Lis	sts			DownStre	am U	pStream	1			
▶ 802.11a/n/	'ac/ax	Average	Data Rate	0		0	]			
▶ 802.11b/g/	'n/ax	Burst Dat	ta Rate	0		0	]			
Media Streat	ım	Average	Real-Time R	ate 0		0				
Application	Visibility	Burst Rea	al-Time Rate	0		0				
And Contro	I	WLAN Qo	S Param	eters						
Lync Server		Maximum	n Priority	video	~					
Country		Unicast D	efault Prior	ity video	~					
Timers		Multicast	Default Price	video	~					
Netflow		Wined Or	C							
QoS		wirea Qo	S Protoc	01						
Roles		Protocol <sup>-</sup>	Туре	802.1p	<b>~</b>					
Qos Map		802.1p Ta	ag	4						

cisco	MONITOR	<u>w</u> lans	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>a</u> nagement	C <u>O</u> MMANDS	HELP
Wireless	Edit QoS	Profile						
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> <li>Global Configuration</li> </ul>	QoS Profi	ile Name on	bronze For Backgrour	nd				
Advanced								
Mesh	Per-User	Bandwid	th Contracts (	kbps) *				
AP Group NTP			DownStre	am UpStre	am			
▶ ATF	Average [	Data Rate	0	0				
<b>RF Profiles</b>	Burst Dat	ta Rate	0	0				
FlexConnect Groups	Average F	Real-Time R	ate 0	0				
FlexConnect ACLs	Burst Rea	al-Time Rate	0	0				
FlexConnect VLAN Templates	Per-SSID	Bandwid	ith Contracts	(kbps) *				
Network Lists			DownStre	am UpStre	am			
802.11a/n/ac/ax	Average [	Data Rate	0	0				
802.11b/g/n/ax	Burst Dat	ta Rate	0	0				
Media Stream	Average F	Real-Time R	ate 0	0				
Application Visibility	Burst Rea	al-Time Rate	0	0				
And Control	WLAN Qo	S Param	eters					
Lync Server	Maximum	n Priority	backgrou	nd 🗸				
Country	Unicast D	efault Prior	ity backgrou	nd 🗸				
Timers	Multicast	Default Pric	backgrou	nd 🗸				
Netflow								
QoS	wired Qo	S Protoc						
Roles	Protocol 1	Туре	802.1p \					
Qos Map	802.1p Ta	ag	1					

،، ،،، ،، cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Wireless	Edit QoS	Profile						
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> <li>Global Configuration</li> </ul>	QoS Profi	ile Name	silver For Best Effor					
Advanced	Descriptio	on						
Mesh	Per-User	Bandwid	th Contracts (	kbps) *				
AP Group NTP			DownStrea	am UpStre	am			
▶ ATF	Average [	Data Rate	0	0				
<b>RF Profiles</b>	Burst Dat	a Rate	0	0				
FlexConnect Groups	Average F	Real-Time R	ate 0	0				
FlexConnect ACLs	Burst Rea	al-Time Rate	0	0				
FlexConnect VLAN Templates	Per-SSID	Bandwid	th Contracts (	(kbps) *				
Network Lists			DownStrea	am UpStre	am			
802.11a/n/ac/ax	Average [	Data Rate	0					
802.11b/g/n/ax	Burst Dat	a Rate	0					
Media Stream	Average F	Real-Time Ri	ate 0					
Application Visibility And Control	WLAN OO	S Parame	eters	0				
Lync Server	Maximum	Priority	besteffor	· ·				
Country	Unicast D	efault Priori	ty besteffor					
Timers	Multicast	Default Prio	rity besteffor	: •				
Netflow								
▼ QoS	Wired Qo	S Protoco	ol	_				
Profiles Roles	Protocol 1	Гуре	802.1p \	•				
Qos Map	802.1p Ta	ag	0					

# **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**.

،،ا،،،ا،، cısco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	Advance	d EAP							
	Identity R	equest Tim	neout (in secs)						30
▶ RADIUS	Identity re	equest Max	Retries						2
▶ TACACS+	▶ TACACS+ Dynamic WEP Key Index							0	
LDAP Local Net Users	Request T	imeout (in	secs)						30
MAC Filtering	Request N	1ax Retries							2
<ul> <li>Disabled Clients</li> <li>User Login Policies</li> </ul>	Max-Login Ignore Identity Response							enable ᅌ	
AP Policies	EAPOL-Ke	y Timeout	(in milliSeconds)						400
Password Policies EAPOL-Key Max Retries									4
Local EAP	EAP-Broadcast Key Interval(in secs)							3600	
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	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

Cisco RoomOS Series Wireless LAN Deployment Guide

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

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

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

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

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

#### Auto-Immune

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

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

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

(Cisco Controller) > show wps summary

Auto-Immune

Auto-Immune..... Disabled

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

Signature Policy Signature Processing...... Enabled

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

(Cisco Controller) >config wps auto-immune disable

## **Rogue Policies**

Cisco RoomOS Series Wireless LAN Deployment Guide

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

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
Security	Rogue Policies	
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> </ul>	Rogue Detection Security Level       Low       High       Critical       Image: Critical         Rogue Location Discovery Protocol       Disable       Image: Critical       Image: Critical </td <td>Custom</td>	Custom
AP Policies Password Policies	Polling Interval     0     Seconds       Validate rogue clients against MSE     Enabled	
Advanced EAP	Detect and report Ad-Hoc Networks     Image: Comparison of the second seco	
Certificate     Access Control Lists	Rogue Detection Minimum RSSI (-70 to -128)     -90       Rogue Detection Transient Interval (0, 120 to 1800 Sec)     0	
Wireless Protection Policies	Rogue Client Threshold (0 to disable, 1 to 256)     0       Rogue containment automatic rate selection     Enabled	
General Rogue Rules	Auto Contain	
Friendly Rogue Standard Signatures Custom Signatures Signature Events	Auto Containment Level     1       Auto Containment only for Monitor mode APs     Enabled       Auto Containment on FlexConnect Standalone     Enabled	
Client Exclusion Policies AP Authentication Management Frame Protection	Rogue on Wire     Enabled       Using our SSID     Enabled       Valid direct on Rogue AR     Enabled	
Veb Auth	AdHoc Rogue AP Enabled	
TrustSec		
<ul> <li>Umbrella</li> </ul>		

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.

Cisco Catalys	st 9800-40 Wireless Controller Welcome alpha 🐐 📽 🖺 🏟 🖗 🗭 Search APs and Clients Q 🗈
Q Search Menu Items	Configuration - > Radio Configurations - > Network
Dashboard	5 GHz Band 2.4 GHz Band
Monitoring >	General 🗄 Apply
Configuration >	5 GHz Network Status
() Administration >	▲ Please disable 5 GHz Network Status to configure Beacon Interval, Fragmentation Threshold, DTPC Support.
X Troubleshooting	Beacon Interval* 100
	Fragmentation 2346 Threshold(bytes)*
	DTPC Support
	CCX Location Measurement
	Mode
	Data Rates
	Please disable 5 GHz Network Status to configure Data Rates
	6 Disabled v9 Disabled v12 Mandatory v
	18 Supported v24 Supported v36 Supported v
	48 Supported v54 Supported v Mbps Mbps

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).

Cisco Cata	alyst 9800-40 Wireless C	Controller Welcom	e alpha 🔺 🕏 🖺	* * • • 2	Search APs and Clients Q	•
Q Search Menu Items	Configuration * > Radio Con	figurations * > Network				
🔜 Dashboard	5 GHz Band 2.4 GHz B	and				
Monitoring >	General					
Configuration >	2.4 GHz Network Status	$\checkmark$				
<ul> <li>⊘ Administration →</li> <li>&gt; X Troubleshooting</li> </ul>	Please disable 2.4 GHz 802.11g Network Status, Be Fragmentation Thre	Network Status to configure acon Interval, Short Preamble, shold, DTPC Support.				
- -	802.11g Network Status	<b>~</b>				
	Beacon Interval*	100				
	Short Preamble	<ul> <li>Image: A start of the start of</li></ul>				
	Fragmentation Threshold(bytes)*	2346				
	DTPC Support					
	CCX Location Measure	ment				
	Mode					
	Interval*	60				
	Data Rates					
	A Please disable 2.4 GHz Ne Ra	etwork Status to configure Data ates				
	1 Mbps	• 2 Mbps Disabled •	5.5 Disabled v	]		
	6 Disabled Mbps	• 9 Disabled •	11 Disabled v	]		
	12 Mandatory	• 18 Supported •	24 Supported v	]		
	36 Supported Mbps	• 48 Supported •	54 Supported v	]		

# 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 Cata	alyst 9800-40 Wireless	Controller Welcome a	lpha 🔺 🜾 🖺 🄅 🍇	Search APs	and Clients Q
Q Search Menu Items	Configuration - > Radio Co	onfigurations - > High Throu	ughput		
	5 GHz Band 2.4 GHz	Band			
	❤ 11n				
Administration →     Administration →	Ena	ble 11n 🔽		Select All	
X Troubleshooting	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate	)
	_0/(7Mbps)	[]/(14Mbps)	2/(21Mbps)	3/(29Mbps)	
	4/(43Mbps)	5/(58Mbps)	_6/(65Mbps)	[7]/(72Mbps)	
	-8/(14Mbps)		0/(43Mbps)	√1/(58Mbps)	
	2/(87Mbps)	3/(116Mbps)	√4/(130Mbps)	√15/(144Mbps)	
	√16/(22Mbps)	√]7/(43Mbps)	_18/(65Mbps)	]9/(87Mbps)	
	_20/(130Mbps)	_21/(173Mbps)	_22/(195Mbps)	23/(217Mbps)	
	_24/(29Mbps)	25/(58Mbps)	26/(87Mbps)	21/(116Mbps)	
		23/(231Mphs)		(203Mbbs)	
	✓ 11ac				
		🛦 The D	ata rates are for 20MHz channels and S	Short Guard	
			Interval		
	Enable 13	IC		Select All	
	SS/MCS	SS/MCS	SS/MCS	SS/MCS	
	/8/(86.7Mbps)	🗸 1/9/(n/a)	2/8/(173.3Mbps)	🗸 2/9/(n/a)	
	3/8/(260.0Mbps)	✓ 3/9/(288.9Mbps)	4/8/(346.7Mbps)	🗸 4/9/(n/a)	
	✓ 11ax				
	Enable 11:	av 🗸		Select All	
	Multiple	sid		ooloot Air	
	SS/MCS	SS/MCS	SS/MCS	SS/MCS	
		✓ 1/9	√ 1/11	2/7	
	2/9	2/11	3/7	3/9	
		✓ 4/7	✓ 4/9	4/11	
		5/9	5/11	6/7	
	<u>~</u> 8\a	6/11		✓ //9	
	<u>√</u> 7/11	8/7	8/9	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.

Cisco RoomOS Series Wireless LAN Deployment Guide

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

Cisco Cataly	yst 9800-40 Wireless Controller Welcome alpha 🛛 🏘 🧒 🖺 🎄 🖄 🚱 🎜 Search Afs and Clerifs 🔍	•
Q Search Menu Items	Configuration - > Radio Configurations - > Parameters	
📻 Dashboard	5 GHz Band 2.4 GHz Band	
Monitoring >	EDCA Parameters	
Configuration >		
() Administration >	EDCA Profile optimized-video-v	
💥 Troubleshooting	DFS (802.11h)	
	▲ DTPC Support is enabled. Please disable it at Network to configure Power Constraint	
	Power Constraint* 0	
	Channel Switch 🔽 Status	
	Channel Switch Quiet • Announcement Mode	
	Smart DFS <	

#### 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.

Cisco Cat	alyst 9800-40 Wireless Controller Welcome alpha	00040	C Search APs and Clients Q	
Q Search Menu Items	Configuration - > Radio Configurations - > RRM			
📷 Dashboard	5 GHz Band 2.4 GHz Band FRA			
Monitoring >	General Coverage DCA TPC RF Grouping			
	Power Assignment Method	Power Assignment Leader	RCDN6-21A-WLC5 (10.201.81.9)	
() Administration >		Transmit Power Update	600 second(s)	
X Troubleshooting	<ul> <li>Automatic</li> </ul>	Last Run:	365 second(s) ago	
ΨΨ.	On Demand Invoke Power Update Once	Power Neighbor Count:	3	
	) Fixed			
	Max Power Level Assignmen 17			
	Min Power Level Assignmen 11			
	Power Threshold* -70			

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 RoomOS Series Wireless LAN Deployment Guide

Cisco Catalys	st 9800-40 Wireless Contro	oller Welcome alpha 🖌 📽 🛱 🖗 🖗 🖉 🎜 Search APs and C	ients Q
Q Search Menu Items	Configuration * > Radio Configuration	ions * > RRM	
Dashboard	5 GHz Band 2.4 GHz Band	FRA	
Monitoring >	General Coverage DCA	A TPC RF Grouping	
Configuration >	Dynamic Channel Assignment	it Algorithm	
$\bigcirc$ Administration $\rightarrow$ $\%$ Troubleshooting	Channel Assignment Mode	Automatic     Freeze     Invoke Channel Update Once     Off	
	Interval Anchortime	10 minutes •	
	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 Channel Width	medium 20 MHz  0 40 MHz  80 MHz  160 MHz  Best	
	Auto-RF Channel List		
	✓     ✓     ✓     ✓     ✓     ✓       36     40     44     48     52     56     64     100       ✓     ✓     ✓     ✓     ✓     ✓       140     144     149     153     157     161     165	V V V	
	Event Driven RRM		
	EDRRM		

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

Cisco Cata	lyst 9800-40 Wireless Controll	ller Welcome alpha 🖌 🗞 🖺 🏟 🖗 🗭 Search APs and Clie	nts Q 🗭
Q Search Menu Items	Configuration * > Radio Configuration	ons* > RRM	
m Dashboard	5 GHz Band 2.4 GHz Band	FRA	
Monitoring >	General Coverage DCA	TPC RF Grouping	
Configuration >	Dynamic Channel Assignment A	Algorithm	
() Administration >	Obarral Assistant Mada		
X Troubleshooting	Channel Assignment Mode	Automatic     Freeze     Invoke Channel Lindele Once	
		○ Off	
	Interval	10 minutes v	
	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	531 second(s) ago	
	DCA Channel Sensitivity	medium 🔹	
	Auto-RF Channel List		
	✓         ✓         ✓		
	9 10 11		
	Event Driven RRM		
	EDRRM		

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.

Cisco Cat	alyst 9800-40 Wirel	less Controller	Welcome alpha 🛛 🐔 🗖	8 * 8 0 2	Search APs and Clients Q
Q Search Menu Items	Configuration - > W	Edit Radios 5 GHz Ban	d		×
_		Configure Detail			
Dashboard	All Access Pe	General		RF Channel Assignmen	nt
$\bigcirc$ Monitoring $\rightarrow$	Number of AP(s): 1	AP Name	rcdn6-22a-ap1	Current Channel	149
Configuration >	AP 🗸 AP Name Model	Admin Status		Channel width	40 MHz v
() Administration >	rcdn6-22a- ap1	CleanAir Admin Status	ENABLED	Assignment Method	Global
	H 4 1 ⊨	Antenna Parameters		Tx Power Level Assign	ment
		Antenna Type	Internal	Current Tx Power Level	2
	✓ 5 GHz Radios	Antenna Mode	Omni	Assignment Method	Global
	Number of AP(s): 1	Antenna A			
	AP v Slot Name No	Antenna B			
	rcdn6-22a- 1	Antenna C			
	⊣	Antenna D			
	> 2.4 GHz Radi	Antenna Gain	10		
	> Dual-Band R	Download Core Dump to b	bootflash		
	> Country				
	> LSC Provisio				
		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.



# **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 operates 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.

	nyst 5000 40 Wileless Controlle	VVelcome a	ibuo III do El	Search APs and Clients Q	
Search Menu Items	Configuration - > Tags & Profiles - >	Edit WLAN			×
		General Security Advanced			
Dashboard		Layer2 Layer3 AAA			
Monitoring >	Number of WLANs selected : 0	Layer 2 Security Mode	WPA + WPA2 +	East Transition Enabled	
	Status: Name Vilo	MAC Filtering		Over the DS	
() Administration →	Data 2	Protected Management Frame		Reassociation Timeout 20	
💥 Troubleshooting	H 4 1 ⊨ H 10 ¥ items p				
		PMF	Disabled v		
		WPA Parameters			
		MDA Dollow			
		WPA Policy			
		WPA2 Encryption	AES(CCMP128)		
			CCMP256		
			GCMP256		
		MPSK			
		Auth Key Mgmt	802.1x		
			CCKM		
			FT + 802.1x		
			802.1x-SHA256		
			PSK-SHA256		
		"D Cancel		Update & Apply to Devic	æ
					_
CISCO CISCO Cata	lyst 9800-40 Wireless Controlle	er Welcome a	lipha 🔗 🕏 🖺	O C Search APs and Clients Q	•
Q. Search Menu Items	llyst 9800-40 Wireless Controlle Configuration * > Tags & Profiles * >	er Welcome a Edit WLAN	alpha 🛛 希 🕏 🖺	One of the second APs and Clients Q	€ ×
Q Search Menu Items	lyst 9800-40 Wireless Controlle	er Welcome a Edit WLAN General Security Advanced	alpha 🖌 🏶 🖺	🏶 随 🖌 🎜 Search APs and Clients 🔍 🗌	×
Q. Search Menu Items	Configuration > Tags & Profiles > < Add < Delete Cnable WLAP	Edit WLAN General Security Advanced Layer2 Layer3 AAA	ulpha 🛛 🖀 🤻 🖺	Search APs and Clients Q	<b>x</b>
Cisco Cisco Cata     Is.122     O. Search Menu Rems     Dashboard     Monitoring	Ilyst 9800-40 Wireless Controlle Configuration - > Tags & Profiles - > Add Delote Enable WLAN Number of WLANs selected : 0	Edit WLAN General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode	wpa + wpa2 •	Image: Search APs and Cleves     Image: Q       Image: Search APs and Cleves     Q       Image: Search APs and Aps and Cleves     Q <t< th=""><th>*</th></t<>	*
Cisco Cisco Cata Cisco Cisco Cisco Cata Cisco	Number of WLANs selected : 0	Edit WLAN General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering	WPA + WPA2 •	Image: Search APs and Cleres     Image: Cleres       Fast Transition     Enabled       Over the DS	×
Cisco Cisco Cata Cisc	Number of WLANs selected : 0 Status- Name V ID Status- Name 2 Voice 1 Status- 2 Status- 2 Sta	Edit WLAN  General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering  Protected Management Frame	ulpha 🔮 📽 🖺	Ceerch APs and Cleves      Ceerch APs and C	×
Cisco Cisco Cate Cisco Cisco Cate Cisco Cat	Add Delete Enable WLAN Number of WLANs selected : 0 Status: Name UD O Dota 2 H 4 1 + H 10 + Rems p	er Welcome a Edit WLAN General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering Protected Management Frame	WPA + WPA2 •	Image: Search APs and Cleves       Image: Cleves <td< th=""><th>×</th></td<>	×
Cisco Claco Cata Cisco Claco Claco Cisco Claco Cisco Claco Claco Cisco Claco C	Alyst 9800-40 Wireless Controlle Configuration * > Tags & Profiles * > * Add > Delete Feable WLAP Number of WLANs selected : 0 Status: Name VID Voice 1 O Data 2 14 4 1 + 11 10 • Rems p	er Welcome a Edit WLAN General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering Protected Management Frame PMF	Mpha 🕷 📽 🖺	Image: Search APs and Cleres	×
Cisco Cisco Cata Cisco Cisco Cata Cisco Cata Cisco Content Cisco Conten	Number of WLANs selected : 0	er Welcome a Edit WLAN General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering Protected Management Frame PMF WPA Parameters	WPA + WPA2 • Disabled •	Image: Search APs and Cleves	×
Cisco Cisco Cisco Cate Cisco Cisco Cisco Cate Cisco Cat	Add Delete Enable WLAN Number of WLANs selected : 0 Status: Name UD Otice 1 Otice 2 H d 1 > H 10 + Rems p	er Welcome a Edit WLAN General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering Protected Management Frame PMF WPA Parameters	Npha R R R	Coerch APs and Clevis      C	×
Cisco Claco Cate Cate Cisco Claco Cate Cate Cate Cate Cate Cate Cate Cate	Add Palets Controlle Configuration - > Tags & Profiles - > Add Palets Enable WLAN Number of WLANs selected : 0 Status Name ID O Voice 1 O Data 2 H 4 1 P H 10 Parets F	er Welcome a Edit WLAN General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering Protected Management Frame PMF WPA Parameters WPA Policy	Inpha R R R	Image: Search APs and Cleres     Image: Search	×
Cisco Claudiana Control Contr	Number of WLANs selected : 0	er Welcome a Edit WLAN  General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering  Protected Management Frame  PMF  WPA Parameters  WPA Policy WPA2 Policy WPA2 Policy WPA2 Policy	Mpha R R R	Image: Search APs and Clients	×
Cisco Cisco Cate Cisco Cisco Cate Cisco Cisco Cate Cis	Add Delete Enable WLAN Number of WLANs selected : 0 Status: Name UD Otice 1 Otice 2 H d 1 × H 10 + Rems p	er Welcome a Edit WLAN  General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering Protected Management Frame PMF WPA Parameters WPA Policy WPA2 Encryption	AES(CCMP128)	Coerch APs and Cleris      C	×
Cisco Cisco Cate Cisc	Alyst 9800-40 Wireless Controlle Configuration * > Tags & Profiles * > Add Delete Enable WLAN Number of WLANs selected : 0 Status Name ID O Voice 1 O Data 2 H 4 1 P H 10 Rems p	er Welcome a Edit WLAN  General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering  Protected Management Frame  PMF  WPA Parameters  WPA Policy WPA2 Encryption	Impha       Impha       Impha       Impha       Impha         Impha       Impha       Impha       Impha       Imph       Imph         Impha	Fast Transition     Cover the DS     Reassociation Timeout     20	×
Cisco Clauding Cisco Clauding Cisco Clauding Configuration Configuratio	Alyst 9800-40 Wireless Controlle Configuration * > Tags & Profiles * > * Add Pelete Proble WAA Number of WLANs selected : 0 Voice 1 O Data 2 10 • Rems p	er Welcome a Edit WLAN  General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering  Protected Management Frame  MPA Parameters  WPA Policy WPA2 Policy WPA2 Policy MPSK	Mpha WPA + WPA2 • Disabled • AES(CCMP128) • GCMP128 • GCMP128 • GCMP256 •	Image: Content APs and Clients	×
Cisco Cisco Cate Cisco Cisco Cate Cate Cisco Cate Cate Cisco Cate Cate Cate Cisco Cate Cisco Cate Cate Cate Cate Cate Cate Cate Cate	Add Delete Enable WLAN Number of WLANs selected : 0 Status- Name UD O Data 2 H 4 1 > H 10 , Rems p	er Welcome a Edit WLAN	Mpha & R & R WPA + WPA2 • Disabled • Disabled • AES(CCMP128) / CCMP256 GCMP128 • GCMP128 • GCMP128 • GCMP128 • GCMP128 • GCMP128 • GCMP128 •	Image: Control of the state of the stat	×
<ul> <li>Cisco Cisco Cate</li> <li>Cisco Cisco Cate</li> <li>Configuration</li> <li>Configuration</li> <li>Administration</li> <li>Troubleshooting</li> </ul>	Add Deicts Controlle Configuration * > Tags & Profiles * > Add Deicts Enable WLAN Number of WLANs selected : 0 Status Name UD Otice 1 Data 2 H 4 1 > H 10 r Rems p	er Welcome a Edit WLAN  General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering  Protected Management Frame  PMF  WPA Parameters  WPA Policy WPA2 Encryption  MPSK Auth Key Mgmt	Impha       Impha       Impha       Impha       Impha         Impha       Impha       Impha       Impha       Impha       Impha         Impha       I	Image: Control APs and Clients	×
Cisco Cisco Cate   Cisco Cisco Cate   Cisco Cate   Configuration   Configuration   Administration   Could be booting	Alyst 9800-40 Wireless Controlle Configuration * > Tags & Profiles * > Add Peters Frable WLAN Number of WLANs selected : 0 Voice 1 O Data 2 H 4 1 P H 10 Peters p	er Welcome a  Edit WLAN  General Security Advanced Layer2 Layer3 AAA  Layer 2 Security Mode  MAC Filtering  Protected Management Frame  PMF  WPA Parameters  WPA Policy WPA2 Encryption  MPSK Auth Key Mgmt	Mpha	Image: Content APs and Clients	×
Cisco Cisco Cate Cisco C	Alyst 9800-40 Wireless Controlle Configuration * > Tags & Profiles * > * Add Polete Pouloe WUA Number of WLANs selected : 0 Voice 1 O Data 2 16 1 1 0 terms p	er Welcome a Edit WLAN   General Security Advanced  Layer2 Layer3 AAA  Layer2 Security Mode  MAC Filtering  Protected Management Frame  WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption  MPSK Auth Key Mgmt	Mpha	Fast Transition     Enabled     Over the DS     Reassociation Timeout     20	×
Cisco Cisco Cate Cisco Cisco Cate Cate Cisco Cate Cate Cate Cate Cate Cate Cate Cate	Add Delete Enable WLAN Number of WLANs selected : 0 Status Name 0 O Data 2 H 4 1 > H 10 terms p	er Welcome a Edit WLAN  General Security Advanced Layer2 Layer3 AAA Layer 2 Security Mode MAC Filtering Protected Management Frame WPA Parameters WPA Policy WPA2 Encryption MPSK Auth Key Mgmt	Mpha	Fast Transition   Court he DS   Reassociation Timeout   20	
Cisco Cisco Cate     Cisco Cate     Cisco Cate     Cisco Cate     Configuration     Administration     Administration     Troubleshooting	Add Delete Configuration * > Tags & Profiles * > Add Delete Enable WLAN Number of WLANs selected : 0 Voice 1 O Data 2 H 4 1 P H 10 Prems p	er Welcome a  Edit WLAN  General Security Advanced Layer2 Layer3 AAA  Layer 2 Security Mode MAC Filtering  Protected Management Frame  MPA Parameters  WPA Policy WPA2 Policy WPA2 Encryption  MPSK Auth Key Mgmt  PSK Format	Impha       Impha       Impha       Impha       Impha         Impha       Impha       Impha       Impha       Impha       Impha         Impha       Imph       Impha       Impha	Coarch APs and Cleves      Coarch APs and C	
Cisco Used Cate Is 22a  Cisco C	Alyst 9800-40 Wireless Controlle Configuration * > Tags & Profiles * > * Add Polete Poulde WUA Number of WLANs selected : 0 Voice 1 O Data 2 10 • Rems p	er Welcome a  Edit WLAN  General Security Advanced Layer2 Layer3 AAA  Layer2 Security Mode MAC Filtering  Protected Management Frame  WPA Policy WPA2 Policy WPA2 Encryption  MPSK Auth Key Mgmt  PSK Format  PSK Format  C Cancel	Image: WPA + WPA2 →         WPA + WPA2 →         Image: WPA + WPA	Coach APs and Cleric      C	

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.

e	cisco	Cisco 16.12.2s	Catal	alyst 9800-40 Wireless Controller					Welco	me alpha	*	6 8	0.0	0 0	s and Clients	Q	()		
٩	Search Menu II	erra	Ľ	Conf	iguratio	n -> Tag	is & Profile	15 ° >	Edit WLAN										×
	Dashboard							• 11LA	General	Security	Adva	nced							
٢	Monitoring			Numb	er of WL	ANs select	ed : O		Layerz	Layers									
Z,	Configurat	ion	>		Status	Name	×	D	Authenticat	ion List		authentica	ition_dot1	× •					
ŵ	Administra	tion	•		0	Voice Deta		2	Local EAP /	Authentication									
×	Troublesho	oting		н	< 1	P 10	10 ¥	items g											
									D Cancel								🗄 Update & A	Apply to Dev	(ce

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 enabled defer priority for queues 4-6.

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

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

Ensure Load Balance and Band Select are disabled.

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

Cisco Cat	alyst 9800-40 Wireless Controller	Welcome alpha 🛛 😤 🔞	🖺 🏟 🔞 🥝 🎜 Search APs and Clients Q
Q Search Menu Items	Configuration * > Tags & Profiles * > WLANs	Edit WLAN	×
		General Security Advanced	
Dashboard		Coverage Hole Detection	Universal Admin
Monitoring      →	Number of WLANs selected : 0	Aironet IE	Load Balance
الم الم Configuration ک	Status v Name v: ID v SSID	P2P Blocking Action Disabled +	Band Select
Administration →	Voice 1 voice	Multicast Buffer	IP Source Guard
∽ ∑ Troubleshooting	H 4 1 F H 10 F Items per page	Media Stream Multicast-	WMM Policy Required +
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		Max Client Connections	mDNS Mode Bridging +
			Off Channel Scanning Defer
		Per WLAN 0	
		Per AP Per 0 WLAN	Defer 0 1 2 Priority
		Per AP Radio 200	3 🗸 4 5
		114 BCC Transition Connect	6 7
		TTV B35 Transition Support	Scan Defer 100 Time
		BSS Transition	Assisted Roaming (11k)
		Disassociation Imminent(0 200 to 3000 TETT)	
		Optimized Roaming 40	Prediction Dptimization
		Disassociation Timer(0 to	Neighbor List
		BSS Max Idle Service	Dual Band Neighbor
		BSS Max Idle Protected	DTIM Period (in beacon intervals)
		Directed Multicast Service	
		11ax	5 GHz Band (1-255) 2
		Develop OFDMA	2.4 GHz Band (1-255) 2
		Linink OFDMA	
		Cancel	Update & Apply to Device

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.

Cisco Cat	alyst 9800-40 Wire	less Controller We	come alpha 🛛 🐔 🕵	B 🌣 🖄 Ø S	Search APs and Clients Q
Q Search Menu Items	Configuration - > T	Edit Policy Profile			×
📰 Dashboard	+ Add X Dele	General Access Policies	QOS and AVC Mob	ility Advanced	
Monitoring >	Status v Pol		ig in enabled state will result in lo	ss of connectivity for clients a	ssociated with this profile.
🔾 Configuration >	Dat	Name*	Voice	WLAN Switchi	ng Policy
() Administration >	□ Ø defa	Description	Enter Description	Central Switching	ENABLED
☆ Troubleshooting	ia a <b>1</b> ⊳ ⊨i	Status		Central Authentio	eation ENABLED
		Passive Client	DISABLED	Central DHCP	ENABLED
		Encrypted Traffic Analytics	DISABLED	Central Associat	on ENABLED
		CTS Policy		Flex NAT/PAT	DISABLED
		Inline Tagging			
		SGACL Enforcement			
		Default SGT	2-65519		
		Cancel			Update & Apply to Device

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

Cisco Cata	alyst 9800–40 Wi	reless Controller Welco	me alpha 🛛 🏠 🌾 🖺 🕻	0 10	Search	APs and Clients Q
Q Search Menu Items	Configuration - > E	Edit Policy Profile				×
_		General Access Policies	QOS and AVC Mobility	Advanced		
E Dashboard	+ Add X D	RADIUS Profiling			WLAN ACL	
Monitoring >	Status 🗸 F	Local Subscriber Policy Name	Search or Select 🔻		IPv4 ACL	Search or Select 🔻
Configuration >		WLAN Local Profiling			IPv6 ACL	Search or Select
() Administration >	□ Ø ¢	Global State of Device Classification	Disabled (i)		URL Filters	
% Troubleshooting	⊨ ⊲ 1 ⊳	HTTP TLV Caching			Pre Auth	Search or Select 🔻
		DHCP TLV Caching			Post Auth	Search or Select 🗸
		VLAN				
		VLAN/VLAN Group	VLAN0500			
		Multicast VLAN	Enter Multicast VLAN			
	(	"D Cancel			[	Tupdate & Apply to Device

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

Cisco Catal	lyst 9800-40 Wir	reless Controlle	Welcome alpha	* • •		Search APs and Clients Q
Q Search Menu Items	Configuration - > E	dit Policy Profile				×
	+ Add × D	General Acc	ess Policies QOS and	AVC Mobility	Advanced	
		Auto QoS	None v		Flow Monitor	IPv4
Monitoring >	Status V F	QoS SSID Policy			Egress	Search or Select 🚽
Configuration >		Egress	platinum x v		Ingress	Search or Select 🔻
(O) Administration >		Ingress	platinum-up x v		Flow Monitor	IPv6
X Troubleshooting		QoS Client Policy	/		Egress	Search or Select
		Egress	Search or Select 🔻		Ingress	Search or Select
		Ingress	Search or Select 🚽			
		SIP-CAC				
		Call Snooping				
		Send Disassociate				
		Send 486 Busy				
		Cancel				Update & Apply to Device

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.

¢	Cisco Cisco C 16.12.2s	ataly	st 9800-40 W	/ireless Controller We	elcome alpha	<b>%</b> 🖹 🔇	8 0 C	Search APs and Clients Q
٩	Search Menu Items	(	Configuration - >	Edit Policy Profile				×
	Dashboard			General Access Policies	QOS and AVC	Mobility	Advanced	
	Dashboard			WLAN Timeout			Fabric Profile	Search or Select
٢	Monitoring	>	Status v F	Session Timeout (sec)	86400		Umbrella Parameter Map	Not Configured 🔻
Z	Configuration	>		Idle Timeout (sec)	300		mDNS Service	default-mdns-service 🔻
ক্টি	Administration	>	□ Ø ¢	Idle Threshold (bytes)	0		Policy	Clear
×	Troubleshooting		⊲ ⊲ 1 ⊳	Client Exclusion Timeout (sec)	60		WLAN Flex Po	licy
				DHCP			VLAN Central Sw	vitching
				IPv4 DHCP Required			Split MAC ACL	Search or Select 🔻
				DHCP Server IP Address			Air Time Fairne	ess Policies
				Show more >>>			2.4 GHz Policy	Search or Select
				AAA Policy			5 GHz Policy	Search or Select
				Allow AAA Override				
				NAC State				
				Policy Name	default-aaa-policy x	,		
				Accounting List	Search or Select	,		
				Cancel				Update & Apply to Device

## **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.

¢	Cisco 16.12.2s	Cataly	yst 98	800-40	Wireless Controller		Welcome <i>alpha</i>	*	<b>F</b>	* 🕸 0	<b>c</b> (		Q	¢
Q	Search Menu Items		Config	guration -	> Tags & Profiles - > RF									
	Dashboard		+ A	Add										
	Monitoring	>		State 🖂	RF Profile Name	~.	Band	~	Descripti	on				~
Z	Configuration	>		Ø	Low_Client_Density_rf_5gh		5 GHz		pre config	jured Low Client	Density rf			
$\sim$				O	High_Client_Density_rf_5gh		5 GHz		pre config	ured High Client	Density r			
Ś	Administration	> .	Add R	RF Profile	1							×		
×	Troubleshooting		Ge	neral	802.11 RRM Adva	nced								
			Nam	ne*	Enter Name									
			Radi	io Band	5 GHz Band	•							1 - 6 of 6 ite	
			Stat	us	DISABLE									
			Des	cription	Enter Description									
			D Ca	ancel						Apply 1	o Device			

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

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

Cisco Catalyst 9800-40 Wireless Controller Welcome alpha 🖌 🎓 🖺 🏟 🖄 🛛 🌫 Search APs and Clerits Q								
Q Search Menu Items	Configuration	Tags & Profiles - > RF	:					
🔜 Dashboard	+ Add							
Monitoring	> State ~	RF Profile Name	<ul> <li>✓ Band</li> </ul>	- Description			~	
	, 🗆 o	Low_Client_Density_rf_5gh	5 GHz	pre configure	d Low Client Density rf			
~~		High_Client_Density_rf_5gh	5 GHz	pre configure	d High Client Density r			
(O) Administration	> Add RF Profil	le				•		
% Troubleshooting	General	802.11 RRM Adva	nced			-		
	Operational	I Rates	802.11n	MCS Rates				
	6 Mbps	Disabled •	Enabled Da	ata Rates:		1 - 6 of f		
	9 Mbps	Disabled 🔻	[0,1,2,3,4,5,6	,7,8,9,10,11,12,13,14,15,16,	17,18			
	12 Mbps	Mandatory v	,19,20,21,22,	23,24,23,20,27,20,29,30,31]				
	18 Mbps	Supported 👻	Enable	MCS Index V				
	24 Mbps	Supported v		0				
	36 Mbps	Supported 🔻		1				
	48 Mbps	Supported v		2				
	54 Mbps	Supported v		3				
				4				
				5				
				6				
				7				
				8				
			$\checkmark$	9				

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 RoomOS Series Wireless LAN Deployment Guide

Cisco Cata	lyst 9800-40 Wireless Controller	Welcome alpha	📽 🖺 🏟 🔞 🥹 🎜 Search APs and Clients Q
Q Search Menu Items	Configuration • > Tags & Profiles • > RF		
Dashboard	+ Add C Delete		
Monitoring >	State 🤟 RF Profile Name 🗸	Band ~	Description ~
	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf
Goomgaration	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r
() Administration →	Add RF Profile		×
💥 Troubleshooting	General 802.11 RRM Advanced		
	General Coverage TPC DCA		
	Coverage Hole Detection		1 - 6 of 6 items
	Minimum Client Level (clients)*	3	
	Data RSSI Threshold (dBm)*	-80	
	Voice RSSI Threshold (dBm)*	-80	
	Exception Level(%)*	25	
	Cancel		Apply to Device

Cisco Catalys	st 9800-40 Wireless Controller Welcome alpha	🕷 🏗 🖺 🏟 👰 🧭 🎜 🛛 Search AP's and Clients 🔍 🗌
Q Search Menu Items	Configuration - > Tags & Profiles - > RF	
Dashboard	+ Add	
Monitoring >	State v RF Profile Name v Band	<ul> <li>Description</li> </ul>
Configuration >	Low_Client_Density_rf_5gh 5 GHz	pre configured Low Client Density rf
~	High_Client_Density_rf_5gh 5 GHz	pre configured High Client Density r
()   Administration   >	dd RF Profile	×
X Troubleshooting	General 802.11 RRM Advanced	
	Constal Courses TPC DCA	
	General Coverage TPC DCA	
	Transmit Power Control	1 - 6 of 6 items
	Maximum Power Level(dBm)* 30	
	Minimum Power Level(dBm)* -10	
	Power Threshold V1(dBm)* -70	
	D Cancel	Apply to Device

Cisco Catal	yst 9800-40 Wireless Control	ler Welcome alpha 🖀	S G Ø Ø Ø Ø Ø	Search APs and Clients Q
Q Search Menu Items	Configuration • > Tags & Profiles • >	RF		
📰 Dashboard	+ Add × Delete			
$\bigcirc$ Monitoring $\rightarrow$	State 🖂 RF Profile Name	<ul> <li>Band</li> </ul>	Description	~
	Low_Client_Density_rf_5g	jh 5 GHz	pre configured Low Client Density rf	
~	High_Client_Density_rf_5	gh 5 GHz	pre configured High Client Density r	
(O) Administration >	Add RF Profile		×	
X Troubleshooting	General 802.11 RRM	Advanced		
	0	201		
	General Coverage IPC	DCA		
	Dynamic Channel Assignment			1 - 6 of 6 items
	Avoid AP Foreign AP Interference			
	Channel Width	20 MHz 40 MHz 80 MHz Best	0 160 MHz	
	DCA Channels	✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓       ✓	✓ ✓ ✓ ✓ ✓ ✓ 104 108 112 116 120 124 	
	High Speed Roam			
	Mode Enable			
	Neighbor Timeout*	5		
	Client Network Preference	Default 🔻		
	D Cancel		Apply to Device	

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

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

Cisco Ca	talyst 9800-40 Wireless Control	ler Welcome alpha 🛛 🌴 🧒 🛱 🦉 🦉 Construct Aths and C	lents Q
Q Search Menu Items	Configuration • > Tags & Profiles • >	RF	
📻 Dashboard	+ Add × Delete		
$\bigcirc$ Monitoring $\rightarrow$	State 🖂 RF Profile Name	V Band V Description	×.
المراجع (Configuration )	Low_Client_Density_rf_5	gh 5 GHz pre configured Low Client Density rf	
	Add DE Drofile	igh 5 GHz pre configured High Client Density r	
	Add RF Profile		
X Troubleshooting	General 802.11 RRM	Advanced	
	High Density Parameters		
	Max Clients*	200	
	Multicast Data Rate (Mbps)	Auto 🗸	
	Rx Sop Threshold (dbm)	auto v	
	Client Distribution		
	Load Balancing Window*	5	
	Load Balancing Denial Count*	3	
	AIF Configuration		
	Status	DISABLED	
	Bridge Client Access	DISABLED	
	Airtime Allocation	5	
	FRA		
	Client Aware		

## **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.

¢	Cisco Catalyst 98	800-40 Wireless Cont	roller Welcome alpha	• • • • •	2 Search APs and Clients Q
Q Se	earch Menu Items	uration - > Tags & Profiles	· > Flex		
D	ashboard + A	dd X Delete			
( N	<sup>Ioni</sup> Add Flex Profile				×
್ಸಿ c	Conf General Local Au	thentication Policy ACL	VLAN		▶ of 1 items
()] A	.dm <sub>Name*</sub>	Enter Name	Fallback Radio Shut		
Ж Т	roul Description	Enter Description	Flex Resilient		
	Native VLAN ID	1	ARP Caching		
	HTTP Proxy Port	0	Efficient Image Upgrade		
	HTTP-Proxy IP Address	0.0.0	Office Extend AP		
	CTS Policy		Join Minimum Latency		
	Inline Tagging				
	SGACL Enforcement				
	CTS Profile Name	default-sxp-profile x			
	ා Cancel				Apply to Device

# 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.

Cisco Catalyst	9800-40 Wireless Controller	Welcome alpha	🎼 💾 🏟 🔯 🥝 🎜 🛛 Searc	h APs and Clients Q
Q Search Menu Items	onfiguration - > Tags & Profil Edit Policy	Tag		×
📰 Dashboard	Policy Site RF A	Changes may result in loss of conne	activity for some clients that are associated	to APs with this Policy Tag.
Monitoring >	+ Add × Delete Name*	default-policy-tag		
Configuration >	Policy Tag Name	default policy-tag		
() Administration >	default-policy-tag VLA	N-POLICY Maps: 2		
X Troubleshooting	H - 1 - H 10 + Add			
	WLA	N Profile	<ul> <li>Policy Profile</li> </ul>	¥.
	Data		Data	
	Uoice		Voice	
	H H	1 ► ► 10 ¥ items pe	r page	1 - 2 of 2 items
	Map WL	N and Policy		
	WLAN Prof	Voice	Policy Profile*	Voice 🔻
	> RLA	N-POLICY Maps: 0		
	່ວ Cancel	]		Update & Apply to Device

## 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**.

Cisco Catalyst 9800	-40 Wireless Controller Welcome alpha	0 Ø Ø & B <b>7</b> %	Search APs and Clients Q
Q. Search Menu Items	ion - > Tags & Profiles - > Tags		
Dashboard Policy	Site RF AP		
Monitoring	× Delete		
Configuration > site	e Tag Name	< Description	×
Administration	ault-site-tag	default site tag	
			1 - 1 of 1 items
Name*	Enter Name		
Description	Enter Description		
AP Join Profile	default-ap-profile 🔻		
Flex Profile	default-flex-profile		
Control Plane Name	<b>•</b>		
Enable Local Site			
Cancel			Apply to Device

#### <u>RF Tag</u>

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.

¢	Cisco Cisco C	atalys	st 9800-40 Wireless Contr	roller Welcome alpha		Search APs and Clients Q	•
Q Sea	irch Menu Items	C	Configuration - > Tags & Profiles	• > Tags			
📰 Da	shboard		Policy Site RF AP				
(2) Mo	onitoring	>	+ Add X Delete				
್ಸಿ ರಂ	onfiguration	>	RF Tag Name	, v	Description		
ۍ ک	Iministration	>	default-rf-tag		default RF tag		
≫ Tro	oubleshooting		Add RF Tag		×	1 - 1 of 1 items	
			Name*	Enter Name			
			Description	Enter Description			
			5 GHz Band RF Profile	Global Config 🗸			
			2.4 GHz Band RF Profile	Global Config 🔹			
			Cancel		Apply to Device		

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

Cisco Cat     Cisco Cat     Cisco Cat     Cosco Cat	configuration • >	reless Controller Edit AP	Welcome alpha 🛛 🏠 📢		Search APs and Clients Q
Dashboard	✓ All Access	General Interfaces	High Availability Inver	ntory ICap Advanced	
) Monitoring	Number of AP(s): 1	AP Name*	rcdn6-22a-ap1	Primary Software Version	16.12.2.132
Configuration >	AP × AP Name Mo	Location*	rcdn6-22	Predownloaded Status	N/A
Administration >	rcdn6-22a- AP	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
C Troubleshooting	B-K	Ethernet MAC	00a7.42b7.cb1a	Next Retry Time	N/A
		Admin Status	ENABLED	Boot Version	1.1.2.4
	> 5 GHz Rac	AP Mode	Local 👻	IOS Version	16.12.2.132
		Operation Status	Registered	Mini IOS Version	0.0.0.0
	2.4 GHz R	Fabric Status	Disabled	IP Config	
	> Dual-Banc	LED State		CAPWAP Preferred Mode IPv	4
	Country	LED Brightness Level	8 🔻	DHCP IPv4 Address 10.	201.81.125
		CleanAir NSI Key		Static IP (IPv4/IPv6)	
	LSC Provis	Tags		Time Statistics	
		Policy	default-policy-tag	Up Time	10 days 18 hrs 16 mins 54 secs
		Site	default-site-tag 🔻	Controller Association Latency	2 mins 4 secs
		RF	default-rf-tag 🔻		
		ී Cancel			Update & Apply to Device

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

Cisco Cataly	vst 9800-40 W	ireless Controller	Welcome alpha	• 🖹 💠 🖄 O C 💿	earch APs and Clients Q
Q Search Menu Items	Configuration - > E	Edit AP			×
Dashboard	<ul> <li>All Acces</li> </ul>	General Interfaces	High Availability Inven	tory ICap Advanced Version	
Monitoring >	Number of AP(s): 1	AP Name*	rcdn6-22a-ap1	Primary Software Version	16.12.2.132
Configuration >	AP × A Name M	Location*	rcdn6-22	Predownloaded Status	N/A
() Administration >	rcdn6-22a- Al	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
X Troubleshooting	H H 1	Ethernet MAC	00a7.42b7.cb1a	Next Retry Time	N/A
		Admin Status		Boot Version	1.1.2.4
	> 5 GHz Ra	AP Mode	Flex v	IOS Version	16.12.2.132
	2 4 GHz I	Operation Status	Registered		0.0.0.0
	2.4 GHZ I	Fabric Status	Disabled	IP Config	
	Dual-Bar	LED State		CAPWAP Preferred Mode IPv4	
	> Country	LED Brightness Level	8 •	DHCP IPv4 Address 10.2	201.81.125
		CleanAir <u>NSI Key</u>		Static IP (IPv4/IPv6)	
	LSC Prov	Tags		Time Statistics	
		Policy	default-policy-tag	Up Time	0 days 0 hrs 10 mins 1 secs
		Site	Flex v	Controller Association Latency	10 secs
		RF	default-rf-tag 🗸		
	ſ	5 Cancel			
		Joancer			Device

# **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.

Cisco Cata	alyst 9800-40 Wireless Controller Welcome alpha 🛛 🏶 🖺 🏟 🕲 C Search APs and Clients Q 🖗
Q Search Menu Items	Configuration - > Wireless - > Mobility
🚃 Dashboard	Global Configuration Peer Configuration
Monitoring >	Mobility Group Name* CTG-VoWLAN3
Configuration >	Multicast IPv4 Address 0.0.0
√ ∴ Administration →	Multicast IPv6 Address ::
NG Traublachastics	Keep Alive Interval (sec)* 10
Troubleshooting	Mobility Keep Alive Count* 3
	Mobility DSCP Value* 48
	Mobility MAC Address* 706d.153d.b50b
Cisco Catal	yst 9800-40 Wireless Controller Welcome alpha 🖌 📽 🖺 🏟 🔯 🥹 📿 Search APs and Clients Q 🔅
Q Search Menu Items	
Dashboard	Global Configuration Peer Configuration
Monitoring >	<ul> <li>Mobility Peer Configuration</li> </ul>
🔾 Configuration >	+ Add × Delete
() Administration >	MAC Address         v         IP Address         v         Public IP         v         Group Name         v         Multicast IPv4         v         Status         v         PMTU         v
X Troubleshooting	706d.153d.b50b 10.201.81.9 N/A CTG-VoWLAN3 0.0.0 N/A N/A
	H         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I         I
	> Non-Local Mobility Group Multicast Configuration

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

Cisco Cata	alyst 9800-40 Wireless Controller	Welcome alpha 🛛 🐔 🜾	8000	Search APs and Clients Q
Q Search Menu Items	Configuration - > Interface - > Wireless			
Dashboard	+ Add X Delete			
Monitoring >	Interface Name 🗸 Interface Type 🗸 Tr	rustpoint Name 🗸 VLAN ID	V. IP Address V.	IP Netmask v MAC Address v
Configuration >	Vlan310     Management       Id     ◄       Id     ►       Id     ■	310	10.201.81.9	255.255.255.240 70:6d:15:3d:b5:0b
() Administration >				
💥 Troubleshooting				

# **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.

Cisco Catalyst 9800-40 Wireless Controller Welcome alpha 🛛 🏶 🖺 🖗 🖗 🧭 Search APs and Clients Q									
Q Search Meru Items Configuration - > Radio Configurations - > Media Parameters									
Dashboard	5 GHz Band 2.4 GHz Bar	nd							
Monitoring >									
Configuration >	Media			Voice					
() Administration >	General			Call Admission Control (0	CAC)				
X Troubleshooting	Unicast Video Redirect			Admission Control (ACM)					
	Multicast Direct Admission Control			Load Based CAC					
	Media Stream Admission	edia Stream Admission		Max RF Bandwidth (%)*	75				
	Control (ACM)	5	1	Reserved Roaming Bandwidth (%)*	6				
	bandwidth (%)*	5	]	Expedited Bandwidth					
	Maximum Media Bandwidth (%)*	85		SIP CAC and Bandwidth					
	Client Minimum Phy Rate (kbps)	6000	¥	SIP CAC Support					
	Maximum Retry Percent (%)*	80	]	Traffic Stream Metrics					
	Media Stream - Multicast I Parameters	Direct		Metrics Collection					
				Stream Size*	84000				
	Multicast Direct Enable			Max Streams*	2				
	Max streams per Radio	No Limit	<b>•</b>	Inactivity Timeout					
	Max streams per Client	No Limit	•						
	Best Effort QOS Admission								

#### **Multicast**

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

Cisco Ca 16.12.2s     Cisco Ca 16.12.2s	Configuration • > S	ervices - > Multicast	Welcome alpha 🖌 🐔 <table-cell> 🦉</table-cell>	02	earch APs and Clients Q
<ul> <li>Dashboard</li> <li>Monitoring </li> </ul>	Global Wireless Multicast Mode	ENABLED	IGMP Snooping		🖺 Apply
Configuration >	Wireless mDNS Bridging		Disabled	Enabled	Q Search
Administration >	IP Multicast	DISABLED	Status VLAN ID Name	Status	VLAN ID Name
Troubleshooting	Wireless Broadcast	DISABLED		O	1 default 🗲
	AP Capwap	Unicast v		Θ	310 VLAN0310 🗲
	Multicast			0	400 VLAN0400 🗲
	MLD Snooping	DISABLED	No Vlan available	O	500 VLAN0500 🗲
	IGMP Snooping Querier	DISABLED			
	IGMP Snooping	ENABLED			
	Last Member Querier Interval (milliseconds)	1000			Disable All
	> Wireless E	Proadcast and Wireless	Non-IP Multicast		

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

Cisco Cata	lyst 9800-40 Wireless Controller Welcome alpha 🖌 🕷 🕲 🏟 🕲 🕫 Search APs and Clients Q	•
Q Search Menu Items	Configuration - > Wireless - > Media Stream	
Dashboard	General Streams	
Monitoring >	Multicast Direct Enable 🔽	Apply
	Session Message Config	
() Administration >	Session Announcement	
☆ Troubleshooting	Session Announcement URL	
	Session Announcement Email	
	Session Announcement Phone	
	Session Announcement Note	

Then configure the media streams as necessary.

Cisco Cisco	Catalyst 9800-4	0 Wireless Controller Welcome	alpha 🔺 🕏 🛦 🛛	B * @ 0 C [	Search APs and Clients Q	Eeedback
Q Search Menu Items	Configuration	Wireless     Media Stream				
Dashboard	General S	Streams				
	>	Si Add Media Stream		×	▼ Status	T No items to display
Image: Administration         Image: Construction         Image: Construction	>	Stream Name* Multicast Destination Start IPv4/IPv6				
X Troubleshooting		Address* Multicast Destination End IPv4/IPv6 Address*				
Walk Me Through >		Maximum Expected Bandwidth (Kbps)* Resource Reservation Control (RRC) P	1000 arameters			
		Average Packet Size*	1200			
		Policy Priority	admit v			
		QOS	Video Drop 🔻			
		Cancel		Apply to Device		

Once saved, then the media stream will be displayed.

Cisco Cisco C	Catalyst 9800-40	) Wireless Controlle	r	Welcome alpha	<b>* *</b>	<b>A</b> [	a 🌣 🕅	0 0	Search APs ar	d Clients Q	Feedback y <sup>A</sup>
Q Search Menu Items	Configuration	> Wireless - > Media	Stream								
📻 Dashboard	General S	treams									
	+ Add	× Delete									
		Stream Name	Ŧ	Start IP Address		Ŧ	End IP Addre	SS	Т	Status	Ŧ
-A		10.195.19.27		239.1.1.1			239.1.1.1			Enabled	
O Administration	> 1	▶ 10 ¥									1 - 1 of 1 items
C Licensing											
💥 Troubleshooting											

And enable Multicast Direct in the WLAN configuration.

Cisco Cata	alyst 9800-40 W	ireless Controller Welcome alpha	🗣 🖹 🏶 🖄 😧 🎜 Search APs and Clients Q
Q Search Menu Items	Configuration - >	Edit WLAN	×
Dashboard	+ Add × C	General Security Advanced Coverage Hole Detection	Universal Admin
Monitoring	Number of WLANs s	Aironet IE	Load Balance
Configuration >	Status Name	P2P Blocking Action Disabled •	Band Select
(○) Administration →	Voić.	Multicast Buffer DISABLED	IP Source Guard
☆ Troubleshooting		Media Stream Multicast-	WMM Policy Required •
ww -		Max Client Connections	mDNS Mode Bridging v
			Off Channel Scanning Defer
		Per WLAN 0 Per AP Per 0 WLAN	Defer 0 1 2 Priority
		Per AP Radio 200 Per WLAN	□ 3
		11v BSS Transition Support	Scan Defer 100 Time
		BSS Transition	Assisted Roaming (11k)
		Disassociation Imminent(0 200 to 3000 TBTT)	Prediction Optimization
		Optimized Roaming 40 Disassociation Timer(0 to 40 TBTT)	Neighbor List
		Cancel	Update & Apply to Device

# **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.

Cisco RoomOS Series Wireless LAN Deployment Guide

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.

Cisco Ca	Cisco Catalyst 9800-40 Wireless Controller Welcome alpha 🛛 🕸 🕲 🖗 🖄 🚱 <table-cell> Search APs and Clerits Q</table-cell>						
Q. Search Menu Items	Configuration - > Wireless - > Advanced						
📻 Dashboard	Load Balancing Band Select Optimized Roaming High Density Preferred Calls						
Monitoring >							
Configuration >	Rx Sop Threshold						
() Administration >	Rx Sop Threshold 5 GHz (dbm)						
₩ Troubleshooting	Rx Sop Threshold 2.4 GHz (dbm)						
	Multicast Data Rate						
	Multicast Data Rate 5 GHz (Mbps)						
	Multicast Data Rate 2.4 GHz (Mbps)						

#### **Rogue Policies**

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

Cisco Cisco Cat	alyst 9800-40 Wireless Cont	roller	Welcome alpha	<b>* </b>	B 🗘 🕅	02	Q
Q Search Menu Items	Configuration - > Security - > V	/ireless Prote	ection Policies				
🔜 Dashboard	Rogue Policies RLDP R	ogue AP Rules	Client Exclusion	Policies			
Monitoring >	Rogue Location Discovery Protocol	Disable	¥				
Configuration >	Retry Count	1					
() Administration >	Schedule RLDP						
💥 Troubleshooting	Day Star	Time	End Time				
	Monday	G	©				
	Tuesday	G	G				
	Wednesday	G	G				
	Thursday	G	G				
	Friday	G	S				
	Saturday	G	G				
	Sunday	G	G				

### **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
۱
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
1
address-family ipv6
exit-address-family
۱
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
1
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
١
subscriber templating
parameter-map type webauth global
virtual-ip ipv4 1.1.1.6
flow exporter wireless-local-exporter
destination local wlc
۱
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
1
crypto pki trustpoint TP-self-signed-3110682001
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3110682001
revocation-check none
rsakeypair TP-self-signed-3110682001
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
١
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 1 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 ١

```
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
۱
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
١
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 vtv 0 4
transport input ssh
line vtv 515
transport input ssh
١
ntp server 10.81.254.202
ntp server 10.115.162.212
۱
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<sup>2</sup>M 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

Cisco RoomOS Series Wireless LAN Deployment Guide

- 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.

æ	Monitoring	Cisco Cisco Airon	et 1850 Serie:	Q 🛦 💿 🖹 💳 😫 🌣	
\$	Wireless Settings ≫ wLANs	CCESS POINTS ADMIN	IISTRATION		
		Access Points 2			
	Access Points Groups	Search		General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u	Global AP Configuration Convert to ME Q Convert to CAPWAP Q
	📽 WLAN Users				
	管 Guest WLANs			System Name WI C1850-1	er 12 Primary Controller and Preferred Master 12 Preferred Master
		Refresh			
	∜ Mesh	Sele Mana Type	Location	GUI access will be disrupted when IP Configuration is changed.	Up Time AP Model
÷.	Management	🖇 🗆 🛄 ME Cap	able default loc	IP Address 10.0.0.30	0 days, 14 h 13 m 31 s AIR-AP1852I-A-K9
an C	Services	8 🗆 🛀 capwai	P default loc	Subnet Mask 255.255.0	0 days, 14 h 13 m 31 s AIR-AP1852I-B-K9
Ł	Advanced			Gateway 10.0.0.1	
				Country United States ( •	
				Changing country code requires controller reset.	
				O Apply & Cano	

# 802.11 Network Settings

It is recommended to have the Cisco RoomOS Series operates 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.

æ	Monitoring	Advanced BE Parameters	
	Monitoring	2.4 GHz Band	
•	Wireless Settings	5.0 GHz Band	
ġ.	Management	Automatic Elexible Badio Assignment	
¢	Services	2.4 GHz Optimized Roaming	
*	Advanced	5 GHz Optimized Roaming	
	✤ SNMP	Event Driven RRM	
	🗟 Logging	CleanAir detection	
	I RF Optimization	5.0 CUz Channel Width	
	I RF Profiles	5.0 GHz Channel Width	40 MHz •
	✗ Controller Tools		Lower Density Higher Density
	Security Settings	2.4 GHz Data Rates	1 2 55 6 9 11 12 18 24 36 48 54
			802.11b devices not supported
			Lower Density Higher Density
		5.0 GHz Data Rates	6 9 12 18 24 36 48 54
			Some legacy devices not supported
		Select DCA Channels	2.4 GHz □ <u>1</u> 2 3 4 5 <u>6</u> 7 8 9 10 <u>11</u>
			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**.

<b>æ</b>	Monitoring	Cisco Aironet 1850	Series Mobility Express	Q	A	٩	B	₽	$\geq$	٥	
•	Wireless Settings										
ġ.	Management	RF OPTIMIZATION									
æ	Services	Il RF Optimization Enab	ed								
*	Advanced ✔ SNMP										
	🗟 Logging	RF Optimization	Enabled	• 😯							
	I RF Optimization	Client Density	Low Typical	High 😯							
	I RF Profiles	Traffic Type	Voice and Data	• 😯							
	& Controller Tools										
	Security Settings		Apply								
	🛙 СМХ										

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. Cisco RoomOS Series Wireless LAN Deployment Guide 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.

🖚 Monitoring	9	.1 1.1 CISC	O Cisc	o Aironet 18	350 Series Mobility Exp	ress			Q	A	٩	Ð	₽	$\geq$	¢
Wireless Settings	ACC	ESS P	OINTS .	ADMINISTI	RATION										
2 Access Points	010	Access	s Points	2											
Access Points Groups	Q, Sei	arch						Global AP	Configuration	Conve	rt to ME	0	Convert to C	CAPWAP	0
<sup>थ</sup> WLAN Users													-		
쓸 Guest WLANs								Primary Controller P	rimary Contr	oller and P	referred	d Master	Pref	erred Ma	ster
DHCP Server															
- 51101 001101		efresh													
* Mesh		efresh Sele	Mana	Туре	Location	Name	IP Address	AP Mac	Up Time			AP Mod	lel		
<ul> <li>Mesh</li> <li>Management</li> </ul>		Sele	Mana	Type ME Capable	Location default location	Name AP1850-1	IP Address 10.0.0.100	AP Mac 38:ed:18:c8:1b:78	Up Time 0 days, 14	h 37 m 44 s		AP Mod	lel 8521-A-K9		
<ul> <li>Mesh</li> <li>Management</li> <li>✓ Services</li> </ul>	8	Sele	Mana	Type ME Capable CAPWAP	Location default location default location	Name AP1850-1 AP1850-2	IP Address 10.0.0.100 10.0.0.101	AP Mac 38:ed:18:c8:1b:78 38:ed:18:ca:28:40	Up Time 0 days, 14 0 days, 14	h 37 m 44 s h 37 m 44 s		AP Mod	lel 8521-A-K9 8521-B-K9		



æ	Monitoring	Cisco Aironet 1850 Series Mobility Express	Q & ⊕ ≞ ≌ ¢
\$	Wireless Settings ৯ wLANs	ACCESS POINTS ADMINIS General Badio 1/2.4 GHz) Badio 2 (56Hz) 802.114	
	Access Points	Access Points 2	
	Access Points Groups	Admin Mode Enabled	obel AP Configuration Convert to ME O Convert to CAPWAP O
	營 WLAN Users	Channel Automatic V 802.11b/g/n	
	📽 Guest WLANs	Channel Width 20 MHz +	Primary Controller and Preferred Master     Up Preferred Master
	DHCP Server	Refresh Transmit Power Automatic V	
	⁵ Mesh	Solect Mana Type	c Up Time AP Model
ġ.	Management	C ME Capable	8:c8:1b:78 0 days, 13 h 15 m 06 s AIR-AP1852I-A-K9
J.C.	Services	CAPWAP default location AP1850-2 10.0.0.101 38:er	d:18:ca:28:40 0 days, 13 h 15 m 06 s AIR-AP1852I-B-K9
*	Advanced		
æ	Monitoring	Cisco Aironet 1850 Series Mobility Express	Q ▲ ③ ≞ ≓ ■ ✿
\$	Wireless Settings		
	ッ WLANs	ACCESS POINTS AP1850-2	×
		Access Point	
	Access Points Groups	General Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u	ntion Convert to ME Q Convert to CADWAP Q
	📽 WLAN Users	Admin Mode Enabled -	
	📽 Guest WLANs	Channel Automatic	Controller and Preferred Master D Preferred Master
	DHCP Server	Refresh 802.11a/n/	'ac
	∮ Mesh	Channel Width 20 MHz V	c Up Time AP Model
ň.	Management	Transmit Power Automatic V	8:c8:1b:78 2 days, 23 h 44 AIR-AP1852I-A-K9
<u>م</u>			
•	Services	C C Cancel Control Con	8:ca:28:40 2 days, 23 h 38 AIR-AP1852I-B-K9

# **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.

<b>8</b>	Monitoring	Gisco Aironet 1850 Series Mobility Express	Q	A	٢	Ð	11	\$
\$	Wireless Settings ⋒ wLANs	WLAN/RLAN CONFIGURATION						
	🕍 Access Points							
	Access Points Groups	General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling						
	📽 WLAN Users							
	📽 Guest WLANs	Add n						
	ℬ DHCP Server			Policy		Radio	Policy	
	<sup>\$</sup> Mesh	Type WLAN T				0 0112	Unity	
ġ.	Management	Profile Name * voice						
6		SSID * voice						
-	Services	WLANs with same SSID can be configured, unless layer-2 security settings are different.						
*	Advanced	Admin State Enabled <b>v</b>						
		Radio Policy 5 GHz only v						
		Broadcast SSID						
		Local Profiling 🔵 ?						
			_					
		O Apply O Cance	ol					

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

		Add new WLAN/RLAN		>	) ≓ ⊠ ≎
- 639 - 75	Monitoring	General WLAN Security VLAN & Firewall Traffic Sha	ping Advanced 802.11u Hotspot2.0 Schedu	uling	
	WLANS 앱 Access Points Groups 양 WLAN Users 양 Guest WLAN	Guest Network 💽 🖓 Captive Network Assistant 💽 🖗 MAC Filtering 💭 Security Type WPA2Enterprise v Authentication Server External Radius v	0		
÷	⊗ DHCP Server ∜ Mesh Management	Radius Profiling 🕜 🖓 BYOD 🚺 RADIUS Server			dio Policy SHz only
*	Services Advanced	Authentication Caching			
			Parisa ID Address	Part	
		X Enabled	10.0.0.20	1812	
		Add RADIUS Accounting Server	Server IP Address	Port	
		X Enabled	10.0.0.20	1813	

<b>B</b>	Monitoring		Cisco Aironet 1850 Serie	es Mobility Exp	ress			Q	A	٩		•
\$	Wireless Settin	ngs										
	NULANs	Add new WLAN/RLAN										
	🗳 Access Points											
	Access Points Groups	General WLAN Security	VLAN & Firewall Traffic Shap	ng Advanced	802.11u Ho	tspot2.0	Scheduling					
	📽 WLAN Users	Guest Network										
	📽 Guest WLANs	Captive Network Assistant										
	DHCP Server	MAC Filtering									adio Policy	
	7 Mesh	Security Type	Personal 🔻									
÷.	Management	WPA2	WPA3									
"C	Services	AutoConfig iPSK	0									
÷	Advanced	Passphrase Format	ASCII									
	Advanced	Passphrase *	•••••									
		Confirm Passphrase *										
			Show Passphrase									
										Cancel		

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

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

			Add new WLAN/RLAN		ά α	A	٩	B	≓	$\leq$	•
æ	Monitoring	Cisc	General WLAN Security VLAN & Firewal	Traffic Shaping Advanced 802.11u Hotspot2.0							
\$	Wireless Settings ⋒	WLAN/RLA	Scheduling								
	🚔 Access Points	Active	Allow AAA Override								
	Access Points Groups		Maximum Allowed Clients	Unlimited(Default) v 🕜							
	쑿 WLAN Users		Maximum Allowed Clients Per AP Radio	200 8							
	📽 Guest WLANs	Add new WL	802.11k	Disabled •		-					
	DHCP Server	(3 ×	802.11r	Disabled •	sourity	Policy		5 GHz o	nly		
	7 Mesh		802.11v	Disabled •							
ġ.	Management		CCKM								
æ	Services		Client Band Select								
*	Advanced		Client Load Balancing								
			Umbrella Profile	None •							
			Umbrella Mode	Ignore •							

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

		Add new WLAN/RLAN			>	; ≓	•
88 •	Monitoring	General WLAN Security VLAN & Firewall Traffic Shaping	Advanced 802.11u Hotspot2	.0 Scheduling			
<b>\$</b>	Wireless Setti						
	access Points	Guest Network					
	Access Points	MAC Filtering					
	앱 WLAN Users	Security Type WPA2Enterprise V					
	🛎 Guest WLANs	Authentication Server External Radius 🔹 🕜					
	DHCP Server	Radius Profiling 🔵 💡				idio Policy	
	4 Mesh	BYOD				and only	
ġ.	Management	RADIUS Server					
se.	Services						
Ł	Advanced	Authentication Caching					
		Add RADIUS Authentication Server					
		State Serv	er IP Address	Port			
		K Enabled 10.0.	0.20	1812			
		Add RADIUS Accounting Server					
		State Serv	er IP Address	Port			
		Enabled 10.0	0.20	1813			
æ	Monitoring	CISCO Cisco Aironet 1850 Series Mobility Exp	ress				
٥	Wireless Setting	ADMIN ACCOUNTS					
ġ.	Management						
	• Access						
	O Time						
	✤ Software Update	Management User Priority Order Local Admir	Accounts TACACS+	RADIUS Auth Cached Users			
æ	Services	Authentication Call Station ID Type AP MAC Ad	dress:SSID +				
*	Advanced	Authentication MAC Delimiter Hyphen	•				
		Accounting Call Station ID Type IP Address	•				
		Accounting MAC Delimiter Hyphen	•				
		Fallback Mode Passive	•				
		Username cisco-probe					
		Interval 300	© Second	s			
		AP Events Accounting					
		Apply					
æ	Monitoring	Add RADIUS Authentication Server					
۵	Wireless Setti	gS Action Server Index Network User	Management	State Server IP Address	Shared Key	Port	
ġ.	Management			10.0.0.20		1812	
	• Access						
	😁 Admin Accour	s					
	O Time	Add RADIUS Accounting Server					
	• Software Upda	Action Server Index Network User	Management	State Server IP Address	Shared Key	Port	
~	Services			10.0.20	*****	1813	
	Advanced						

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

Monitoring	Cisco Aironet 1850 Series Mobility Express	(	α, ×	A	٩		#	\$
Wireless Settings	Add new WLAN/RLAN General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Schedu	lling						
Access Points Groups	Client IP Management Network(Default) • Peer to Peer Block							
알 WLAN Users Addr	Native VLAN ID 1		Pol	licy		Radio Po	licy	
ণ্ড DHCP Server 🛛 🕝 🗙 গ Mesh	DHCP Scope Name • VLAN ID * 3 •					5 GHz onl	у	
<ul> <li>Management</li> <li>Services</li> </ul>	No DHCP Scope associated with VLAN ID Enable Firewall No •							
Advanced	VLAN ACL Map							
	Add New VLAN							
	VLAN Name VLAN Id	_	1					
	Image: Contract of the second seco							
	H         4         1         Image         1 - 2	of 2 items						
	VLAN and Firewall configuration apply to all WLANs and RLANs configured with same VLAN	Cancel						

Ensure Platinum (Voice) is selected for QoS.

		Add new WLAN/RLAN	⇒	¢
<b>62</b> 0	Monitori	General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling		
*	Wireless			
	M WLANS	QoS Platinum (Voice) v		
	L Access F	Average and time bandwidth limit about he attend Average bandwidth limit		
	Groups	Rate limits per client		
	양 WLAN U	Average downstream bandwidth limit 0 kbps 🥑		
	Guest W	Average real-time downstream bandwidth 0 kbps 🕜	lcy	
	B DHOF 3	Average upstream bandwidth limit 0 kbps	1	
<u>.</u>	7 Mesn	Average real-time upstream bandwidth limit 0 kbps		
	Manager			
1 contraction of the second	Services	Rate limits per BSSID		
*	Advance	Average downstream bandwidth limit 0 kDps 🥜		
		Average real-time downstream bandwidth 0 kbps 🕜		
		Average upstream bandwidth limit 0 kbps 🥑		
		Average real-time upstream bandwidth limit		

æ	Monitori			Fastlane	Disabled	•				
\$	Wireless				Enabling Fast	lane will update (	QoS value to platinum.			
	WLANs		Ap	plication Visibility Control	Enabled	•				1
	Access I			AVC Profile	voice					
	Access F Groups	Add Rule								
	양 WLAN U		s	Application		Action		Average Rate	Burst Rate	
	📽 Guest V									
	THCP S									1
	∜ Mesh									

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

		Add new V	VLAN/HLAN								
æ			Active	Add new WLAN/RLAN			Security Policy	Radio Policy			
	Monitoring	l≤ ×	Enabled	General WLAN Security VLAN & Firewal	I Traffic Shaping Advanced 802	.11u Hotspot2.0		5 GHz only			
\$	Wireless Settings <sub>WLANs</sub>			Scheduling							
	Access Points			Allow AAA Overside							
	Access Points Groups			Maximum Allowed Clients	Unlimited(Default) v						
	管 WLAN Users			Maximum Allowed Clients Per AP Radio	200 🕄						
	📽 Guest WLANs			802.11k	Disabled •						
				802.11r	Enabled •						
	∜ Mesh			802.11v	Disabled •						
ġ.	Management			сскм	0						
æ	Services			Client Band Select							
Ł	Advanced			Client Load Balancing							
				Umbrella Profile	None 🔻						
				Umbrella Mode	Ignore 🔻						
				Umbrella DHCP Override							
				mDNS							
				mDNS Profile	None 🔻						
				Passive Client	0						
				Please enable Globa when Global Multica	l Multicast in Services->Media Stream. Pass st is disabled.	sive Client will not work					
				Multicast IP	239.1.1.1						
				Multicast Direct	0						

# **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.

<b>8</b> 2	Monitoring	Cisco Aironet 1860 Series Mobility Express		Q	A	٩	Ħ	٥
\$	Wireless Settings ৯ <sub>WLANs</sub>	ACCESS POINT GROUP						
	🖞 Access Points	Access Points Groups						
		Add new group						
	管 WLAN Users	Q. Search General WLANs Access Points RF Profile Ports Intelligent Capture						
	🖆 Guest WLANs	Add new group Refre						
		AP Group ni AP Group name express-1	AP count					
	∲ Mesh	AP Group description	0					
÷.	Management	Les detault-grou NAS-ID	2					
an C	Services	Venue Group UNSPECIFIED +						
Ł	Advanced	Venue Type UNSPECIFIED +						
		Add New Venue						
		Language Venue Name						
		@ Apply						

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

æ	Monitoring		sco Cisco Airone	t 1850 Series	Mobility Express						Q	A	٩	Ð	#	٥
\$	Wireless Settings ৯ <sub>WLANs</sub>	ACCESS	9 POINT GROUP													
	🕍 Access Points	Acces	s Points Groups	-1												
				Add new g	roup				Ŷ							
	알 WLAN Users	Q Search		General WL	ANs Access Point	ts RF Profile	Ports Intelli	igent Capture								
	📽 Guest WLANs	Add new	group Refresh													
			AP Group name	⊕ Add nev	v WLAN/RLAN					AP count						
	∜ Mesh	8 ×	express-1	ту	Add new WLAN	I/RLAN				0						
ń.	Management	ľ	default-group	×w		Type WLAP	N 🔻			2						
J.C.	Services				Profil	le Name voice	· •									
*	Advanced						<b>⊘</b> Update	Cancel								

<b>ев</b> м	lonitoring		Cisco Airone		ries Mobility Express				Q	A	٩	Ð	#	0
wi 🗱 Wi	ireless Settings <sup>WLANs</sup>	ACCESS	POINT GROUP											
<u>010</u> A	Access Points	Access	Points Groups	-										
ير <u>تن</u> م				Add ne	aw group			×						
10 <sup>1</sup>	WLAN Users	Q Search		General	WLANs Access Points	RF Profile Ports In	elligent Capture							
쓭	Guest WLANs	Add new g	group Refresh											
® (			AP Group name	⊕ Ad	d new WLAN/RLAN			AP c	ount					
∱ N	Mesh	8 ×	express-1		Туре	Profile Name	Status	0						
<b>й-</b> Ма	anagement		default-group	×	WLAN	voice	Enabled	2						
🖋 Se	ervices													
📥 Ac	dvanced													
		H 4 1	1 » H 10 V	1										
				н ч	1 1 × H 10 ¥	tems per page	1 - 1 of 1 items							
							Apply     Scancel							

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

Those access points will then reboot.

<b>8</b> 36	Monitoring		o Cisco	o Aironet 1850 S	eries Mobility Express					Q	A	٩	B	₽	\$
\$	Wireless Settings ৯ <sub>WLANs</sub>	ACCESS P	Add n	ew group											
	별 Access Points 별 Access Points Groups	Access P	General	WLANS Access	Points RF Profile Ports	Int	telligent Capture								
	볼 WLAN Users 볼 Guest WLANs	Q. Search Add new grou	Q Searc	ch					Refresh						
	ঔ DHCP Server ⊁ Mesh	8 ×	APs in	n <b>"express-1"</b> group AP Name	MAC Address			AP Group	All v						
њ. "С	Management Services			AP1850-1 AP1850-2	38:ed:18:c8:1b:78 38:ed:18:ca:28:40										
+1	Advanced						*								
		H K 1 1	H 4	1 1 × H	1 - 2 of 2 item	5		 00 -	No items to display						
								(	⊘ Apply ⑧ Cancel						

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

æ	Monitoring	Cisco Aironet 1850 Series Mobility Express	Q	A	٢	Ð	≓	٥
\$	Wireless Settings ৯ <sub>WLANs</sub>	ACCESS POINT GROUP						
	Access Points	Access Points Groups						
	쓸 WLAN Users	Q Search						
	뿔 Guest WLANs	Add new group Refresh						
		AP Group name AP count						
	⁵ Mesh	Add new group 0						
ň.	Management	General WLANs Access Points RF Profile Ports Intelligent Capture						
J.C.	Services							
*	Advanced	2.40Hz None • SGHz None • C Cancel						

# **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.

<b>æ</b>	Monitoring		Cisco Aironet 1850 Serie	s Mobility Express				Q	A	٩	Ð	#	•
\$	Wireless Settings												
÷.	Management	RF Profile	S										
se .	Services	RF prof	ile 6										
*	Advanced ✔ SNMP	Q Search											
		() Add ne	w RF Profile	Add RF Profile									
			RF profile	General 802.11 RRM Cli	ent Distribution		Applied						
		2 × 3	express-1										
	& Controller Tools	ß	High-Client-Density-802.11a	RF profile name	express-1	1	No						
	*	C	High-Client-Density-802.11bg	BE profile description			No						
	V Security Settings		Low-Client-Density-802.11a				No						
	CMX		Low-Client-Density-802.11bg	Band	5GHz ¥		No						
		R	Typical-Client-Density-802.11bg	Maximum clients per radio	200		No						
				Rx SOP Threshold	Auto 🔻								
				Multicast datarates	Auto 🔻								
		н н 1	1 ► H 10 ▼ items per page		O Apply O C	Cancel							

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

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

🚳 Monitoring	Gisco Alronet 1860 Series Mobility Express	۹	A	٢	Ð	₽	٥
Wireless Settings							
ሱ Management	RF Profiles						
Services	RF profile 6						
Advanced	Q, Search						
🗟 Logging	Add new RF Profile						
I RF Optimization							
RF Profiles	Add RF Profile						
	General 802.11 RRM Client Distribution						
🛱 Security Settings							
🖾 СМХ	Data rates	54					
	MCS settings						
	v 1 4 3 4 5 6 7 6 9 10 11 12 13 14 15 18 17 18 19 20 21 22 23 24 25 28 27 28 29	30 31					
	O Apply O Car	icel					

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

🍘 Monitoring		sco Cisco Aironet	1850 Series Mobility Ex	kpress			Q	A	٩	Ð	#		٥
🍄 Wireless Settings													
ሱ Management	RF Profile	es											
🖋 Services	RF pro	file 6											
Advanced	Q Search												
🗟 Logging	⊕ Add n	ew RF Profile	Add RF Profile										
I RF Optimization		RF profile				Applied							
II RF Profiles	@ ×	express-1	General 802.11 RRM	Client Distribution									
Controller Tools	ß	High-Client-Density-802				No							
	C	High-Client-Density-802	Channel Wie	dth 40 MHz 🔻		No							
Security Settings	C	Low-Client-Density-802	Select DCA Channels	Select All  36 40 44 48 52 56 60 64	100 104 108	No							
🖾 СМХ	C	Low-Client-Density-802		112 116 120 124 128 132 136 14	0 144 149 153	No							
	Ø	Typical-Client-Density-8		157 161 165		No							
	ß	Typical-Client-Density-6		Some of the channels are not allowed to configure as enabled. These channels can be enabled in RF Optimi At least one Channel Number should be selected	they are not ization screen.	No							
	H 4 1	1 ► H 10 ▼ it										7 of 7 ite	

Cisco RoomOS Series Wireless LAN Deployment Guide

# **Multicast Direct**

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

Then configure the streams.

æ			Cisco Aironet 1850 Se	ries Mobility	Express		Q	▲	٩	Ð	≓	$\geq$	٥
•	Monitoring												
٠	Wireless Settings	Media Str	ream Settings										
ġ.	Management		is Streen Disabled										
r	Services	Un meu	Disabled										
	C Media Stream												
	<b>♥</b> TLS		Global Multicast										
	<b>♥</b> mDNS		Multicast Direct										
	Network Assurance		Multicast Direct										
	🚔 Webhook	Ses	sion Announcement State										
	Intelligent Capture	Se	ssion Announcement URL	URL									
	🗅 Umbrella	Ses	sion Announcement Email	Email									
Ł	Advanced	Sess	ion Announcement Phone	Phone									
		Ses	ssion Announcement Note	Note	li.								
		Add New S	Stream										
		Action	Stream Name		Start IP Address	End IP Address		Operation	Status				
		×	10.0.0.40		239.1.1.40	239.1.1.40	5	Aulticast-c	lirect				

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.

		Add new	WLAN/HLAN					
æ			Active	Add new WLAN/RLAN			Security Policy	Radio Policy
	Monitoring	3 ×	Enabled	General WLAN Security VLAN & Firewal	I Traffic Shaping Advanced 802.11u	Hotspot2.0		5 GHz only
-	Wireless Settings			Scheduling				
	M WLANS							
	Access Points			Allow AAA Override				
	Access Points Groups			Maximum Allowed Clients	Unlimited(Default)			
	📽 WLAN Users			Maximum Allowed Clients Per AP Radio	200 3			
	📽 Guest WLANs			802.11k	Disabled •			
				802.11r	Enabled			
	⁵ Mesh			902 11.	Disabled			
ġ.	Management			COKM				
J.C.	Services			Client Band Select				
÷	Advanced			Client Load Balancing				
	Advanced			Client Load Balancing				
				Umbrella Profile	None v			
				Umbrella Mode	Ignore 🔻			
				Umbrella DHCP Override				
				mDNS				
				mDNS Profile	None 🔻			
				Passive Client	0			
				Please enable Globs when Global Multics	il Multicast in Services->Media Stream. Passive Clien ist is disabled.	nt will not work		
				Multicast IP	239.1.1.1			
				Multicast Direct	<b>()</b> 0			

# **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 802.11a/n/ac network status is Enabled.

cisco	<u>H</u> OME	<u>N</u> ETWORK	ASSOCIATIO	N W <u>I</u> RELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e ( <u>M</u> ANAGEMENT	Configuration	Ping Logout	<u>R</u> efresl
NETWORK	Host	name ap-1					ap-1	uptime is 1 day	/, 4 hours, 51 mi	nutes
Summary	Net	work Interfac	es: Summary							
Adjacent Nodes	Sys	tem Settings								
NETWORK INTERFACE	IP A	ddress (Static	;)		10.9.0.9					
Summary	IP S	ubnet Mask			255.255.255.0					
IP Address	Defa	ault Gateway			10.9.0.2					
Radio0-802.11N 2.4GHz	MAG	C Address			18e7.281b.3f54					
Radio1-802.11AC 5GHz	Inte	rface Status		GigabitEthernet		Radio0-802.1	1N <sup>2.4GHz</sup>	Radio1-802.1	11AC <sup>5GHz</sup>	
	Soft	ware Status			Enabled		Disabled	ŀ	Enabl	ed 🏫
	Hard	dware Status			Up î		Down	ŀ	ι	Jp 🏫
	Inter	rface 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.

Cisco RoomOS Series Wireless LAN Deployment Guide

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.



- я	9.3-2Mb/sec	Require	• Enable	
MCS Rates: 0 1	2 3 4	5 6 7 8 9 1		18 19 20 21 22 23
Enable O				
Disable 💿 🔿	0000			00000
Transmitter Power (dBm):		015 012 09 06	6 🔾 3 💿 Max	Power Translation Tab (mW/dBm)
Client Power (dBm):		OLocal ○15 ○12	9 6 3 Max	
DefaultRadio Channel:		Channel 36 - 5180 MH	iz Channel 36 5180	) MHz
Dynamic Frequency Selec	tion Bands:	Band 1 - 5.150 to 5.250	GHz	
		Band 2 - 5.250 to 5.350 Band 3 - 5.470 to 5.725 Band 4 - 5.725 to 5.820	5 GHz	
Channel Width:		Below 40 MHz 2	0 MHz	
World Mode		O Disable	C Legacy	<ul> <li>Dot11d</li> </ul>
Country Code:			Quitdoor	
,,				
Radio Preamble		<ul> <li>Short</li> </ul>		
Antenna:		🔾 a-antenna	ab-antenna Oabc-antenna	<ul> <li>abcd-antenna</li> </ul>
Internal Antenna Configur	ration:	<ul> <li>Enable</li> </ul>	O Disable	
		Antenna Gain(dBi):	0 (-128 - 128)	
	()	0.5.11		
Gratuitous Probe Respons	se(GPR):	Enable		
		Transmission Space	GABLED (10-255)	
		mansmission opee		
Traffic Stream Metrics:		Enable	<ul> <li>Disable</li> </ul>	
Aironet Extensions:		<ul> <li>Enable</li> </ul>	O Disable	
Ethernet Encapsulation T	ransform:	RFC1042	○ 802.1H	
Reliable Multicast to WGE	3:	<ul> <li>Disable</li> </ul>	Enable	
Public Secure Packet For	warding:	PSPF must be set per	VLAN. See VLAN page	
Beacon Privacy Guest-Mo	ode:	<ul> <li>Enable</li> </ul>	<ul> <li>Disable</li> </ul>	
Beacon Period:	100	(20-4000 Kusec)	Data Beacon Rate (DTIM)-	2 (1-100)
Max. Data Retries:	64	(1-128)	RTS Max Retries	64 (1-128)
Eragmontation Threshold		(256,2246)	PTS Threshold:	04 (1-120)
ragmentation inreshold	2346	(200-2040)	Rio mesnolu:	234/ (0-234/)
Root Parent Timeout:		0	(0-65535 sec)	
Root Parent MAC 1 (optio	nal):		(НННН.НННН.НННН)	
Root Parent MAC 2 (optio	nal):		(НННН.НННН.НННН)	
Root Parent MAC 3 (optio	nal):		(НННН.НННН.НННН)	
iteett arent in te e (epne				
Root Parent MAC 4 (optio	nal):		(НННН.НННН.НННН)	

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.

							Sa <u>v</u> e	Configuration	<u>P</u> ing Logout	<u>R</u> efr	
cisco	<u>H</u> OME	<u>N</u> ETWORK	ASSOCIATION	WIRELESS	SECURITY	<u>S</u> ERVICES	<u>M</u> ANAGEMENT	<u>S</u> OFTWARE	EVENT LOG		
Security											
	Hostr	name ap-1					ap-	1 uptime is 1 da	iy, 4 hours, 33 mi	nutes	
Admin Access	Security: Global SSID Manager										
SSID Manager	SSI	D Properties									
Dot11u Manager	<b>C</b>	ment CCID L in									
Server Manager	Cur	Frent SSID LIS	τ								
AP Authentication	dat	a sa			SSID:		voice	-			
Intrusion Detection	VOI	ce			VLAN:		3 Backup 1:	Define VLA	<u>Ns</u>		
Local RADIUS Server							Backup 1: Backup 2:				
Advance Security							Backup 3:				
					Band-Select	:	Band Se	lect			
					Universal Ad	dmin Mode:	Universa	al Admin Mode			
					Interface:		Radio0-8	02.11N <sup>2.4GHz</sup>			
							Radio1-8	02.11AC <sup>5GHz</sup>			
		Network ID:	(0-40	)96)							
		Delete									
	Client Authentication Settings										
	Methods Accepted:										
	Open Authentication: with EAP     Over Authentication     Web Authentication     Web Pass										
		🗆 Sh	ared Authenticatio	n: < NC	ADDITION>		0				
		🗹 Ne	twork EAP:	< NC	ADDITION >	٥					
		Sonyor Brid	aritiae:								
		545 4						•			
	EAP Authentication Servers					MAC Authentication Servers					
		💿 Us	e Defaults Define	Defaults		Use Defaults <u>Define Defaults</u>					
	Customize Priority 1: << NONE >  Priority 2: << NONE >				◯ Customize						
					Priority 1: <a>NONE</a> <a>C</a> <a>Priority 2: <a>NONE</a> <a>C</a></a>						
		P	nonty 3: < NONE	× ×			Priority 3:	NUNE >			
	Clier	nt Authenticat	ted Key Managem	ient							
		Key Manad	ement:	Mand	atory ᅌ		CCKM 🔽 Ena	ble WPA wr	Av2 dot11r		
					· -						

11. O	itoy.		ASCII  Hexadecimal
The Configuration	n:	Disable ᅌ	
11w Association-	comeback:	1000	(1000-20000)
11w Saquery-retr	y:	100	(100-500)
DS Client MFP			
Enable Client	MFP on this S	SID: Optional	0
AP Authentication			
Credentials:		< NONE >	Define Credentials
Authentication Meth	nods Profile:	< NONE >	Define Authentication Methods Profiles
Accounting Settings			
Enable Accou	unting		Accounting Server Priorities:
			Ouse Defaults Define Defaults
			◯ Customize
			Priority 1: <pre> &lt; NONE &gt; </pre>
			Priority 2: < NONE > 3
			Priority 3: <pre> &lt; NONE &gt; </pre>
Rate Limit Parameters			
Rate Limit Parameters Limit TCP:			
Rate Limit Parameters Limit TCP:	Rate:	Burst-Si	ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output:	Rate: Rate:	Burst-Si Burst-Si	ze: (0-500000) ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP:	Rate: Rate:	Burst-Si Burst-Si	ze: (0-500000) ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input:	Rate: Rate: Rate:	Burst-Si Burst-Si Burst-Si	ze: (0-500000) ze: (0-500000) ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: Output:	Rate: Rate: Rate: Rate:	Burst-Si Burst-Si Burst-Si Burst-Si	ze: (0-500000) ze: (0-500000) ze: (0-500000) ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: Output: General Settings	Rate: Rate: Rate: Rate:	Burst-Si Burst-Si Burst-Si Burst-Si	ze: (0-500000) ze: (0-500000) ze: (0-500000) ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Input: Input: Output: Coutput: General Settings Advertise Exter	Rate: Rate: Rate: Rate: nded Capabilite	Burst-Si Burst-Si Burst-Si Burst-Si s of this SSID	ze: (0-500000) ze: (0-500000) ze: (0-500000) ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Exter	Rate: Rate: Rate: Rate: nded Capabilite	Burst-Si Burst-Si Burst-Si Burst-Si s of this SSID	ze: (0-500000) ze: (0-500000) ze: (0-500000) ze: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Exter	Rate: Rate: Rate: Rate: nded Capabilite Advertise t	Burst-Si Burst-Si Burst-Si Burst-Si s of this SSID lireless Provisi his SSID as a Se	ze: (0-500000) ze: (0-500000) ze: (0-500000) ze: (0-500000) se: (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Exter Enable IP Redia	Rate: Rate: Rate: Rate: Advertise V	Burst-Si Burst-Si Burst-Si Burst-Si s of this SSID /ireless Provisi his SSID as a So	ze: (0-500000) ze: (0-500000) ze: (0-500000) ze: (0-500000) se: (0-500000)

Association Limit	(optional): (1-255)	
EAP Client (option	al):	
	Username: Password:	
Multiple BSSID Beacon	Settings	
Multiple BSSID Be	acon	
	Set SSID as Guest Mode	
	Set DataBeacon Rate (DTIM): DISABLED (1-100)	
		Apply
Guest Mode/Infrastructu	re SSID Settings	
Radio0-802.11N <sup>2.4GHz</sup> :		
Set Beacon Mode:	○ Single BSSID Set Single Guest Mode SSID: < NONE > < < > < < > < < > < < > < < > < < > < < > < < > < < > < < > < < > < < < < > < < < < < > < < < < < > < < < < < > < < < < < < < < < < < < < < < < < < < <	
	O Multiple BSSID	
Set Infrastructure SSID:	< NONE > 3 Force Infrastructure Devices to associate only to this SSID	
Radio1-802.11AC <sup>5GHz</sup> :		
	⊖ Single BSSID Set Single Guest Mode SSID: < NONE > 🗘	
Set Beacon Mode:		
Set Beacon Mode:	Multiple BSSID	
Set Beacon Mode: Set Infrastructure SSID:	Multiple BSSID <pre></pre>	

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.

						Sa <u>v</u> e (	Configuration	Ping Logout <u>R</u> efresh		
CISCO	<u>H</u> OME <u>N</u> ETWORK	ASSOCIATION	WIRELESS	SECURITY	<u>S</u> ERVICES	<u>M</u> ANAGEMENT	<u>S</u> OFTWARE	<u>E</u> VENT LOG		
Services	Hostname ap-1					a	o-1 uptime is 1 (	day, 4 hours, 48 minutes		
Telnet/SSH										
Hot standby	Services: VLAN									
CDP	Global VLAN Properties									
DNS										
Filters	Current Native VLAN: VLAN 10									
нттр	Assigned VLANs									
QOS	Current VLAN L	ist	Create			Define SSID	s			
Stream			orouto				-			
SNMP	VLAN 2	_								
SNTP	VLAN 3 VLAN 10		VLA	AN ID:		3	(1-409	4)		
VLAN			VLA	VLAN Name (optional):						
ARP Caching		Delete		Native VL	AN					
Band Select				Enable Pu	Iblic Secure F	acket Forwarding	4			
Auto Config				Radio0-80	2 11N2.4GHz	•				
	<ul> <li>Radio0-802.11N<sup>2-sGR2</sup></li> <li>Radio1-802.11AC<sup>5GHz</sup></li> <li>Management VLAN (If non-native)</li> </ul>									
								Apply Cancel		
	VLAN Informatio	n								
	View Information for: VLAN 2 3									
		GigabitEtherne	t Packets Radio0-802.11N <sup>2.4GHz</sup>			Packets	Radio1-802.11AC <sup>5GHz</sup> Packets			
	Received		65884					65884		
	Transmitted	5462						5462		
								Refresh		

Ensure **AES** is selected for encryption type.
،، ،،، ،، cısco	HOME NETWORK ASSOCIATION	WIRELESS SECUR	ity <u>s</u> ervices	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configuration	Ping   Logout	<u>R</u> efres
Security	Hostname ap-1			ap-1	l uptime is 1 day	r, 4 hours, 32 mir	nutes
Admin Access Encryption Manager	Security: Encryption Manager						
SSID Manager	Set Encryption Mode and Keys for	VLAN:		3 ᅌ		Define VLA	Ns
Server Manager	Encryption Modes						
AP Authentication	◯ None						
Local RADIUS Server	Optional	\$					
Advance Security	Cisco Compl	iant TKIP Features: (	Enable Message	e Integrity Check (N	IIC)		
	• Cipher AES CCMP	0		in the second			
	Encryption Keys						
		Transmit Key	Encryptio	n Key (Hexadecin	nal)	Key Size	
	Encryption Key 1:	0				128 bit ᅌ	
	Encryption Key 2:	0				128 bit ᅌ	
	Encryption Key 3:	0				128 bit 📀	
	Encryption Key 4:	0				128 bit 😺	
	Global Properties						
	Broadcast Key Rotation Interval:	<ul> <li>Disable R</li> </ul>	otation				
		C Enable R	tation with Interva	DISABLED (10-	-10000000 sec)		
	WPA Group Key Update:	Enable Gr	oup Key Update O	n Membership Terr	mination		
		Enable Gr	oup Key Update C	n Member's Capab	ility Change		
	L					Apply Ca	incel

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

				Save Configuration   Ping   Logout   <u>R</u> efres
cisco	<u>Home N</u> etwork <u>A</u> ssoci	ATION WIRELESS SECUR	RITY <u>S</u> ERVICES <u>M</u> ANA	GEMENT <u>S</u> OFTWARE <u>E</u> VENT LOG
ecurity	SERVER MANAGER		TIES	
Admin Access	Hostname ap-1			ap-1 uptime is 1 day, 4 hours, 42 minutes
Encryption Manager	Security: Server Manager			
SSID Manager	Backup RADIUS Server			
Dot11u Manager	IP Version:			
Server Manager	Backup RADIUS Server Na			
AP Authentication	Backup RADIUS Server In		(Hesterne e	
Intrusion Detection	Backup RADIUS Server:		(Hostname of	TP Address)
Local RADIUS Server	Shared Secret:			
Advance Security				Apply Delete Cancel
	Corporate Servers			
	Current Server List			
	RADIUS			
		IP Version:	○IPV4 ○IPV6	
	10.0.0.20	Server Name:	10.0.0.20	
	10.9.0.9	Server:	10.0.0.20	(Hostname or IP Address)
		Shared Secret:	•••••	
				-
	Delete	Authentication Port (option	nal): 1812 (0-6553	5)
		Accounting Port (optional)	1813 (0-6553	5)
				Apply Cancel
	Default Server Priorities			
	EAP Authentication	MAC Authe	ntication	Accounting
	Priority 1: 10.0.0.20 ᅌ	Priority 1:	< NONE > 🔅	Priority 1: 10.0.0.20 😒
	Priority 2: < NONE > 🗘	Priority 2:	< NONE > 💲	Priority 2: < NONE > ᅌ
	Priority 3: < NONE > ᅌ	Priority 3:	< NONE > 😒	Priority 3: < NONE > 😳
	Admin Authentication (RA	DIUS) Admin Auth	entication (TACACS+)	
	Priority 1: < NONE > 📀	Priority 1:	< NONE > 📀	
	Priority 2: < NONE > 📀	Priority 2:	< NONE > 📀	
	Priority 3: < NONE > 文	Priority 3:	< NONE > 😳	
				Appiy Cancel

#### 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).

 cısco	Save Configuration Ping Logout Refresh HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Wireless Services	WDS STATUS         GENERAL SET-UP         SERVER GROUPS           Hostname ap-1         ap-1 uptime is 1 day, 4 hours, 50 minutes
WDS	Wireless Services: WDS/WNM - General Set-Up WDS - Wireless Domain Services - Global Properties
	<ul> <li>Use this AP as Wireless Domain Services</li> <li>Wireless Domain Services Priority: 255 (1-255)</li> <li>Use Local MAC List for Client Authentication</li> </ul>
	WNM - Wireless Network Manager - Global Configuration
	Configure Wireless Network Manager Wireless Network Manager Address: DISABLED (IP Address or Hostname)
	Apply Cancel

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.

							Sa <u>v</u> e	Configuration	Ping Logout	<u>R</u> efres
CISCO	<u>H</u> OME	NETWORK	ASSOCIATION	WIRELESS	SECURITY	<u>S</u> ERVICES	<u>M</u> ANAGEMENT	<u>S</u> OFTWARE	EVENT LOG	
ervices	Hostna	ame ap-1					a	p-1 uptime is 1	day, 4 hours, 48	minutes
elnet/SSH										
lot standby	Servi	ices: VLAN								
CDP	Glob	al VLAN Pro	perties							
DNS										
ilters	Cur	rent Native V	LAN: VLAN 10							
ITTP	Assi	gned VLANs								
los	Curr	rent VLAN Li	st	Create	VLAN		Define SSID	)s		
Stream				oreate			0000	-		
NMP	VLA	N 2								
INTP	VLA VLA	N 3 N 10		VLA	AN ID:		10	(1-409	4)	
/LAN				VLA	AN Name (opt	tional):				
ARP Caching			Delete		Native VL	AN				
Band Select					C Enable Pu	Iblic Secure F	Packet Forwardin	a		
Auto Config						0 44N2 4GHz		5		
					Radiou-au	2.11N				
					Radio1-80	2.11AC <sup>5GHz</sup>				
					Managem	ent VLAN (If I	non-native)			
								(	Apply Car	ncel
	VLAN	N Information	ı							
	View	Information	for: VLAN 2 ᅌ							
			GigabitEthern	et Packets	Radio0	-802.11N <sup>2.4GHz</sup>	Packets	Radio1-802.	11AC <sup>5GHz</sup> Packe	ts
	Recei	ved		65884						65884

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.

iliilii cisco	Save Configuration   Ping   Logout   Refres
Wireless Services	WDS STATUS GENERAL SET-UP SERVER GROUPS
AP	Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 51 minutes
WDS	Wireless Services: WDS - Server Groups
	Server Group List
	Server Group Name: WDS       WDS       Group Server Priorities: Define Servers       Delete       Priority 1: 10.90.9
	Priority 2: < NONE > 0 Priority 3: < NONE > 0
	Use Group For: <ul> <li>Infrastructure Authentication</li> </ul>
	◯ Client Authentication
	Authentication Settings SSID Settings
	EAP Authentication     Apply to all SSIDs
	MAC Authentication SSID: DISABLED Add
	Default (Any) Authentication
	Apply Cancel

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.

 cisco	HOME NETWORK ASSOCIATION WIRELESS	SECURITY SERVICES MANA	Save Configuration	Ping Logout Refresh
Wireless Services	U WDS STATUS	L SET-UP	ER GROUPS	
AP	Hostname ap-1		ap-1 uptime is 2 da	ys, 2 hours, 31 minutes
WDS	Wireless Services: WDS - Server Groups			
	Server Group List			
	< NEW > WDS	Group Name: Clients		
	Clients	Server Priorities: Define Servers		
	Delete	iority 1: 10.0.0.20 ᅌ		
	P	iority 2: < NONE > ᅌ		
	P	iority 3: < NONE > ᅌ		
	Use Group For: O Infrastructure Authentication			
	Client Authentication			
	Authentication Settings	SSID Settings	De	
	<ul> <li>LEAP Authentication</li> </ul>	Restrict SSIDs	(Apply only to listed SSIDs	)
	MAC Authentication	SSID: DIS	ABLED Add	1
	Default (Any) Authentication		Ren	nove

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.

،، ،،، ،، cısco	<u>H</u> OME <u>N</u> E	twork <u>a</u> sso	CIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configuration	Ping   Logout	<u>R</u> efresh
Security		STATISTICS		GENER	AL SET-UP		EAP-FAST SET-UP			
Admin Access	Hostname	ap-1					ap-1	l uptime is 1 da	y, 4 hours, 43 mi	nutes
Encryption Manager	Security:	Local RADIUS S	Server - Ge	eneral Set-Up						
SSID Manager	Local Rad	dius Server Auth	entication	Settings						
Dot11u Manager	Enable A	Authentication P	rotocols:	🗹 E4	AP FAST					
Server Manager				🗸 LE	AP					
Intrusion Detection				M	AC					
Local RADIUS Server				_				A	Apply Cancel	
Advance Security	Natural			- 4 - 1						
	Network	Access Servers	(AAA Cliei	nts)						
	Current	Network Access	Servers							
	< NEW > 10.9.0.9	_			Network Acc	ess Server:	10.9.0.9		(IP Address)	
					Shared Secre	et:			1	
		te								
	Dere	ne							analu Canad	
									Cance	
	Individua	l Users								
	Current	Users								
	< NEW >			Username:		wds				
	wds			Password:		•••••		🔿 Text 💿 N	T Hash	
				Confirm Pas	ssword:					
	Dele	ete		Group Nam	e:	< NONE >	0			
							uthentication Only			
								•	Apply Cancel	
	User Grou	ups								
	Current	liser Groups								
	Current	user Groups	Crew	n Nome						
	< NEW >		Grou	p Name.						
			Sess	ion Timeout (	optional):			(	1-4294967295 s	ec)
			0000				L			
	Dele	te	Faile	d Authenticat	ions before L	.ockout (opti	onal):	(1-4294967295	5)	
			Lock	out (optional)	:		Infinite			
							Interval	(1-4	294967295 sec)	
				D (orfine)					·····	
			VLAN	(optional)				r	Add	
			SSID	(optional):					Add	
									Delete	
									Apply Cance	ł

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.

،، ،،، ،، cısco	HOME NETWORK ASSOCIATION WIRELE	Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh SS <u>SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG</u>
Wireless Services	Hostname ap-1	ap-1 uptime is 1 day, 4 hours, 50 minutes
WDS	Wireless Services: AP Participate in SWAN Infrastructure:	• Enable 🔿 Disable
	WDS Discovery:	Auto Discovery     Specified Discovery: 10.9.0.9     (IP Address)
	Username:	wds
	Password: Confirm Password:	
	Authentication Methods Profile:	< NONE > Define Authentication Methods Profiles
		Apply Cancel

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.

ululu cisco	<u>H</u> OME <u>N</u> ETWORK <u>A</u>	SSOCIATION WIR	ELESS	SECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	e Configui <u>S</u> OFT	ration <u>P</u> ing WARE <u>E</u> Vi	Logout   <u>R</u> efresh ENT LOG
Wireless Services	WDS STATU Hostname ap-1	s	GENER	AL SET-UP	Ĭ	SERVER GROU	IPS ap-1 up	otime is 1 day	, 5 hours, 1 minute
WDS	Wireless Services: WDS Information	VDS - Wireless Doma	ain Servi	ices - Status					
	MAC Address	IPv4 Address		IPv6 Addre	155	Priority		State	
	18e7.281b.3f54	10.9.0.9		::		255		Administrat	vely StandAlone
	WDS Registration								
	APs: 1			Mobile Nod	es: 0				
	AP Information								
	Hostname	MAC Address		IPv4 Addre	955	IPv6 Address		CDP Neighbor	State
	ap-1	18e7.281b.3f54		10.9.0.9		::		Switch-2.gil	REGISTERED
	Mobile Node Information	ation							
	MAC Address	IP Address	State			SSID	VLAN I	D BSS	ID
	Wireless Network M	anager Information							
	IP Address	Authentication State	IS						
									Refresh

### **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.

Cisco RoomOS Series Wireless LAN Deployment Guide

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

., <b> </b> ,,, <b> </b> ,, сіsco <u>н</u> оме	<u>N</u> ETWORK <u>A</u> SSO	CIATIO	N WIRELESS <u>S</u> EC	URITY <u>S</u> ERVICES M	Sa <u>v</u> e Configura IANAGEMENT <u>S</u> OFTW	ition   <u>P</u> ing   Logout   <u>R</u> e VARE <u>E</u> VENT LOG
ervices	QoS POLICIES	R	ADIO0-802.11N <sup>2.4GHZ</sup>	RADIO1-802.11AC <sup>5</sup>	GHZ ADVAN	CED
Telnet/SSH Hos	tname an-1				an-1 untime in	s 1 day 4 hours 47 minutes
lot standby					ap-1 uptime is	s ruay, 4 nours, 47 minutes
CDP Se	rvices: QoS Policies -	Acces	s Category			
DNS Ac	case Catagory Definit	lion				
ilters	cess category bennin					
ттр	Access Category		Background	Best Effort	Video	Voice
os			(003 1-2)	(003 0,3)	(CO3 4-5)	(003 0-7)
tream M	in Contention	AP	4	4	3	2
NMP (2	×-1; x can be 0-10)	Client	4	4	3	2
NTP	ev Contontion		10			2
LAN	/indow			0	4	3
RP Caching (2	<sup>x</sup> -1; x can be 0-10)	Client	10	10	4	3
and Select		AP	7	3	1	1
uto Config (0	ixed Slot Time					
	,	Client	7	3	2	2
T	ransmit Opportunity	AP	0	0	3008	1504
(C	-65535 µS)	Client	0	0	3008	1504
Ad	mission Control for V	'ideo ar	nd Voice	Optimized Voice	WFA Default	Apply Cancel
	Video(CoS 4-5)	Admis	sion Control			
	Voice(CoS 6-7)					
		Admis	sion Control			
		Max Ch	annel Capacity (%):	75		
	1	Roam C	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.

rvices		RADIO0-802.11N <sup>2.4GHZ</sup>	RADIO1-802.11AC <sup>5GHZ</sup>	
einet/SSH		ACCESS CATEGORIES	ACCESS CATEGORIES	
ot standby	Hostname ap-1		ap-1 u	ptime is 1 day, 4 nours, 44 minu
)P	Services: QoS Policies			
IS	Create/Edit Policies			
ters				
ТР	Create/Edit Policy:	Voice ᅌ		
S				
ream	Policy Name:	Voice		
MP				
	Classifications:	DSCP - COS Controlled Load (4)		
AN R Caching		DSCP - COS Video < 100ms Later DSCP - COS Voice < 10ms Latero	ncy (5) ;y (6)	
nd Select				
to Config		Delete Classification		
	Match Classification	ns:	Apply Class of S	Service
	IP Precedence:	Routine (0)	Best Effort (0)	Add
	IP DSCP:	<ul> <li>Best Effort</li> </ul>	Best Effort (0)	Add
		0	0-63)	
	IP Protocol 119		Best Effort (0)	C Add
	Filter:	No Filters defined. Define Filters.		
	Default Classificat	ion for Packets on the VLAN:	Best Effort (0)	C Add
	Rate Limiting:			
	Bits per Sec.:	(8000-20000000	00) Burst Rate (Bytes):	(1000-512000000)
	Conform Action:	Transmit ᅌ	Exceed Action: Drop ᅌ	Add
	Apply Policies to Interfa	ace/ VLANs		Apply Delete Cancel
	VLAN 2	Radio0-802.11N <sup>2.4GHz</sup>	Radio1-802.11AC <sup>5GHz</sup>	GigabitEthernet0
	Incoming		Data	Data ᅌ
	Outgoing		Data	Data ᅌ
	VLAN 3	Padia0 802 11124GHz	Padia1-902 44 & 05GHz	GigabitEthernet0
	Incoming	Raul00-002.11N	Voice	Voice
	Outgoing			
	Cargoing			
	VLAN 10	Radio0-802.11N <sup>2.4GHz</sup>	Radio1-802.11AC <sup>5GHz</sup>	GigabitEthernet0
	Incoming		< NONE > ᅌ	< NONE > ᅌ
	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.

ululu cisco	Save Configuration Ping Logout Refresh
Services	QoS POLICIES RADIO0-802.11N2 <sup>4GHZ</sup> ACCESS CATEGORIES ACCESS CATEGORIES
Telnet/SSH	Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 47 minutes
Hot standby	
CDP	Services: QoS Policies - Advanced
DNS	IP Phone
Filters	QoS Element for Wireless Phones : O Enable I Dot11e
QOS	
Stream	
SNMP	IGMP Snooping
SNTP	Snooping Helper: 🧿 Enable 🔿 Disable
VLAN	
ARP Caching	
Band Select	AVVID Priority Mapping
Auto Config	Map Ethernet Packets with CoS 5 to CoS 6: O Yes O No
	WiFi MultiMedia (WMM)
	Enable on Radio Interfaces:
	Radio0-802.11N <sup>2.4GHz</sup>
	Radio1-802.11AC <sup>5GHz</sup>
	Apply Cancel

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.

RADIO0-802.11N <sup>2.4</sup> GHZ	RADIO1-802.	andling	Max Retries for Pa NO DISCARD	ap cket Discard (0-128)	-1 uptime is 1 d	lay, 4 hours, 48 m	ninutes
tname ap-1  rvices: Stream  acket Handling per User Prior User Priority  oS 0 (Best Effort)  oS 1 (Background)  oS 2 (Spare)  oS 3 (Excellent)	prity: Packet Ha Reliable Reliable Reliable	andling	Max Retries for Pa NO DISCARD NO DISCARD	ap cket Discard (0-128)	-1 uptime is 1 d	lay, 4 hours, 48 m	ninutes
rvices: Stream acket Handling per User Prio User Priority oS 0 (Best Effort) oS 1 (Background) oS 2 (Spare) oS 3 (Excellent)	Packet Ha Packet Ha Reliable Reliable Reliable	andling O	Max Retries for Pa NO DISCARD	cket Discard (0-128)			
rvices: Stream acket Handling per User Prio User Priority oS 0 (Best Effort) oS 1 (Background) oS 2 (Spare) oS 3 (Excellent)	Prity: Packet Ha Reliable Reliable Reliable	andling C	Max Retries for Pa NO DISCARD NO DISCARD	cket Discard (0-128)			
acket Handling per User Prio User Priority oS 0 (Best Effort) oS 1 (Background) oS 2 (Spare) oS 3 (Excellent)	Packet Ha Reliable Reliable Reliable	andling C	Max Retries for Pa NO DISCARD NO DISCARD	cket Discard (0-128)			
User Priority oS 0 (Best Effort) oS 1 (Background) oS 2 (Spare) oS 3 (Excellent)	Packet Ha Reliable Reliable Reliable	andling C	Max Retries for Pa	(0-128)			
oS 0 (Best Effort) oS 1 (Background) oS 2 (Spare) oS 3 (Excellent)	Reliable Reliable Reliable	0	NO DISCARD	(0-128)			
oS 1 (Background) oS 2 (Spare) oS 3 (Excellent)	Reliable Reliable	0	NO DISCARD				
oS 2 (Spare) oS 3 (Excellent)	Reliable	<b>v</b>	NO DISCARD	223 A 21213			
oS 2 (Spare) oS 3 (Excellent)	Reliable			(0-128)			
oS 3 (Excellent)		<b>\$</b>	NO DISCARD	(0-128)			
	Reliable	٥	NO DISCARD	(0-128)			
oS 4 (Controlled Load)	Reliable	0	NO DISCARD	(0-128)			
-0.5.0.64)	Kellable		NO DISCARD	(0-120)			
05 5 (Video)	Reliable	<b>\$</b>	NO DISCARD	(0-128)			
oS 6 (Voice)	Reliable	\$	NO DISCARD	(0-128)			
oS 7 (Network Control)	Reliable	٥	NO DISCARD	(0-128)			
ow Latency Packet Rates:							
6.0Mb/sec :	Nominal	O Non-Nominal	<ul> <li>Disable</li> </ul>				
9.0Mb/sec :	Nominal	Non-Nominal	<ul> <li>Disable</li> </ul>				
12.0Mb/sec :	Nominal	Non-Nominal	Disable				
18.0Mb/sec :		Non-Nominal	Disable				
24 0Mb/sec :			Disable				
26.0Mb/see :							
30.0WD/SBC :	<ul> <li>Nominal</li> </ul>	<ul> <li>Non-Nominal</li> </ul>	Disable				
48.0Mb/sec :	Nominal	Non-Nominal	<ul> <li>Disable</li> </ul>				
54.0Mb/sec :	Nominal	Non-Nominal	<ul> <li>Disable</li> </ul>				
					(	Apply Can	icel
	6.0Mb/sec : 9.0Mb/sec : 12.0Mb/sec : 18.0Mb/sec : 24.0Mb/sec : 36.0Mb/sec : 48.0Mb/sec : 54.0Mb/sec :	6.0Mb/sec : Nominal 9.0Mb/sec : Nominal 12.0Mb/sec : Nominal 18.0Mb/sec : Nominal 24.0Mb/sec : Nominal 36.0Mb/sec : Nominal 48.0Mb/sec : Nominal 54.0Mb/sec : Nominal	6.0Mb/sec : Nominal Non-Nominal 9.0Mb/sec : Nominal Non-Nominal 12.0Mb/sec : Nominal Non-Nominal 18.0Mb/sec : Nominal Non-Nominal 24.0Mb/sec : Nominal Non-Nominal 36.0Mb/sec : Nominal Non-Nominal 48.0Mb/sec : Nominal Non-Nominal 54.0Mb/sec : Nominal Non-Nominal	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	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	6.0Mb/sec: Nominal Non-Nominal Disable 9.0Mb/sec: Nominal Non-Nominal Disable 12.0Mb/sec: Nominal Non-Nominal Disable 13.0Mb/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	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 54.0Mb/sec : Nominal Non-Nominal Disable

#### **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.



#### **Sample Configuration**

```
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname ap-1
logging rate-limit console 9
aaa new-model
۱
aaa group server radius rad eap
server name 10.0.0.20
۱
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
1
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
1
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
۱
crypto pki trustpoint TP-self-signed-672874324
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-672874324
revocation-check none
rsakeypair TP-self-signed-672874324
crypto pki certificate chain TP-self-signed-672874324
certificate self-signed 01
 30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 36373238 37343332 34301E17 0D313630 38303332 33303533
 385A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
 532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3637 32383734
 33323430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
 CB155DD1 3421B13F CD121F42 7A62D9F5 38EBC966 4420F38A 38DFAFF2 D43CD3B9
 5F5A1B75 7910F9F5 6E9EDEF4 730942C7 17DC4CBC E5AE3E49 0AF79419 0BEF34BC
 5DCEB4E2 FF2978CB C34D5AEE ED1DFB58 C7BF6592 61C1AD25 3EF87205 15EA58C2
 0A5E2B15 7F08FAEA 5DA2BFA7 95E56C60 22C229C7 024A91D7 A4FEB50B 5425357F
 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
 23041830 168014FC 2FE6CF0E E0380A40 11381459 5D596E3E A684DA30 1D060355
 1D0E0416 0414FC2F E6CF0EE0 380A4011 3814595D 596E3EA6 84DA300D 06092A86
 4886F70D 01010505 00038181 0053F55B 5EBB1FE2 C849BC45 47D0E710 0200404E
 A8B174BC A46EB56A 857166C3 B9FD71DF 7264F5AF DC804A67 16BD35A2 4F39AFD7
 0BD24F71 BAF916AC E984343C A54B7395 E5D15237 8897D436 A150BFB2 DC23E8D3
 AFF0A51C B6253153 C4E2C022 66F1E361 B2EE49E2 763FCBC7 6381E7F7 61B6E14D
 60CDF947 2C044617 37211E5F CE
     quit
username <REMOVED> privilege 15 password 7 <REMOVED>
class-map match-all class Voice0
match ip dscp cs3
class-map match-all class Voice1
match ip dscp af41
class-map match-all class Voice2
match ip dscp cs4
class-map match-all class Voice3
match ip dscp ef
!
policy-map Voice
class class Voice0
 set cos 4
```

Cisco RoomOS Series Wireless LAN Deployment Guide

```
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
١
encryption vlan 2 mode ciphers aes-ccm
encryption vlan 3 mode ciphers aes-ccm
١
ssid data
ssid voice
۱
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 gos class voice local
  admission-control
  admit-traffic narrowband max-channel 75 roam-channel 6
!
```

dot11 gos class voice cell admission-control ۱ 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 ۱ interface GigabitEthernet0.10 encapsulation dot1Q 10 native

```
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
۱
interface BVI1
mac-address 18e7.281b.3f54
ip address 10.9.0.9 255.255.255.0
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ip default-gateway 10.9.0.2
ip forward-protocol nd
no ip http server
ip http authentication aaa
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
 nas 10.9.0.9 key 7 <REMOVED>
 user wds nthash 7 <REMOVED>
!
radius-server attribute 32 include-in-access-reg format %h
radius server 10.0.0.20
address ipv4 10.0.0.20 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
radius server 10.9.0.9
address ipv4 10.9.0.9 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
access-list 111 permit tcp any any neq telnet
bridge 1 route ip
!
wlccp ap username wds password 7 <REMOVED>
wlccp ap wds ip address 10.9.0.9
wlccp authentication-server infrastructure method WDS
wlccp authentication-server client eap method Clients
wlccp authentication-server client leap method Clients
wlccp wds priority 255 interface BVI1
!
line con 0
access-class 111 in
line vty 04
access-class 111 in
transport input all
!
sntp server 10.0.0.2
sntp broadcast client
end
```

# **Cisco Meraki Access Points**

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

- 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**.

ululu cisco Meraki	Q Search Dashboard								
NETWORK	Create network								
Meraki MX64 🚽 👻									
	Setup network								
Network-wide	Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization. ①								
Security & SD-WAN	Network name Scranton Branch Office								
Organization									
	Network type Wireless - 🖲								
	Network configuration O Default Meraki configuration								
	Bind to template No templates to bind to ()								
	Clone from existing network Select a 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?



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



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

cisco Meraki	<b>Q</b> Search Dashboard										
NETWORK	Add access points										
Meraki WLAN 👻	Add access points from your or devices in the order will be adde	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 inve	entory. Once in your inventory, you	can add devid	es to your network(s).							
Network-wide	Search inventory										
Wireless	MAC address	Serial number	Model *	Claimed on							
	✓ 88:15:44:60:18:8c	Q2MD-MWQS-J9K7	MR53	4/29/2020 2:59 PM							
Organization											
	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.

'uluulu' Meraki	Q Search Dashboard										
NETWORK	Configuration ov	Configuration overview									
Meraki WLAN 👻	SSIDs	Showing 4 of 15 SSIDs	SIDs. Show all my SSIDs.								
			meraki-voice								
	Enabled		enabled 🗘								
Network-wide	Name		rename								
	Access control		edit settings								
Wireless	Encryption		802.1X with Meraki RADIUS								
	Sign-on method		None								
Organization	Bandwidth limit		unlimited								
	Client IP assignment		Local LAN								
	Clients blocked from us	ing LAN	no								
	Wired clients are part o	f 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.

ululu Gisco Meraki	<b>Q</b> Search Dashboard	
NETWORK Meraki WLAN 👻	Access control	•
Network-wide	Network access Association requirements	Open (no encryption) Any user can associate
<b>Wireless</b> Organization		<ul> <li>Pre-shared key (PSK)         Users must enter a passphrase to associate</li> <li>MAC-based access control (no encryption)         RADIUS server is queried at association time</li> <li>Enterprise with Meraki Cloud Authentication          Liser credentials are validated with 802.1X at association time</li> </ul>
	WPA encryption mode	WPA2 only (recommended for most deployments)
	802.11r 🛈	Disabled 📴
	802.11w 🕲	Disabled (never use)
	Splash page	• None (direct access) Users can access the network as soon as they associate

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.

dialu cisco Meraki	<b>Q</b> Search Dashboard				
NETWORK	User management p	oortal			
Meraki WLAN 👻	SSID: meraki-voice	with Meraki authentication. Thes	e 802.1X accounts are n	nanaged separately from Administrator o	or Guest accounts.
	Authorization - Remove Users	Search			
Network-wide	Description	Email (Username)	Account type	Authorized for SSID *	Authorized by
Wireless					
Organization			(5)	Save Changes or <u>cancel</u>	
			(Pi	ease allow 1-2 minutes for changes to take effect.	.)
		Create user Account type: Merak	i 802.1X		×
		Description:			
		Email (Username):			
		Password:	Ge	nerate	
		Authorized: No ᅌ			
				Close Print Creat	te user

Cisco RoomOS Series Wireless LAN Deployment Guide

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

ululu uso Meraki	Addressing and traff	fic
NETWORK	Client IP assignment	<ul> <li>NAT mode: Use Meraki DHCP Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the <u>SSID frewall settings</u> permit.</li> </ul>
Meraki WLAN 👻		Bridge mode: Make clients part of the LAN Meraki devices operate transparently (no NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and wireless cameras.
Network-wide		Layer 3 roaming Clients receive DHCP leases from the LAN or use static IPs, similar to bridge mode. If the client mams to an AP where their
Wireless		original bubbet is not available, then the client's traffic will be forwarded to an achor AP on their original subnet. This allows the client to keep the same IP address, even when traversing IP subnet boundaries.
Organization		<ul> <li>Layer 3 roaming with a concentrator</li> <li>Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.</li> </ul>
		<ul> <li>VPN: tunnel data to a concentrator</li> <li>Meraki devices send traffic over a secure tunnel to an MX concentrator.</li> </ul>
	VLAN tagging (1) Bridge mode and layer 3 roaming only	Use VLAN tagging
	VLAN ID ()	AP tags VLAN ID Actions
		All other APs 3
		Add VLAN
	Content filtering  (1) NAT mode only	Don't filter content 0
	Bonjour forwarding  Bridge mode and layer 3	Enable Bonjour Gateway
	roaming only	There are no Bonjour forwarding rules on this network. Add a Bonjour forwarding rule

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.

Cisco RoomOS Series Wireless LAN Deployment Guide

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

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



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

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

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

ululu cisco Meraki	<b>Q</b> Search Dashboard	
NETWORK	SSID availability	
Meraki WLAN 👻	SSID: meraki-voice	0
	Visibility	Advertise this SSID publicly
Notwork-wide	Per-AP availability 0	This SSID is enabled on all APs
Network-wide	Scheduled availability	disabled 😳
Wireless		
Organization		

## **Radio Settings**

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

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

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

cisco Meraki	Q Search Dashboard											
NETWORK	Radio settings											
Meraki WLAN 👻	Overview RF profiles											
Network-wide	BAND     CHANNEL     AP TAG     RF PROFILE     REGULATORY DOMAIN       5     ~     All     ~     All     ~											
Wireless	Search by AP name Update auto channels Edit settings •											
Organization	Taract power Traggit power											
	Image: power     Image: power     Image: power     Image: power       Image											
	MR53         36 (Auto)         20         8 - 30         8         Basic Indoor Profile											

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**.

cisco Meraki	Q Search Dashboard
NETWORK	RF PROFILES Edit Basic Indoor Profile
Meraki WLAN 👻	
	General 2.4 GHz 5 GHz
Network-wide	General
Wireless	Band selection Per SSID
Organization	The Access Points configured to use this profile will follow the band selection set on the <u>Access Control page</u> for the respective SSID. date.
	Minimum bitrate configuration       Per band         Set the minimum bitrates for the 2.4 & 5 GHz radios separately below.         Per SSID         The Access Points configured to use this profile will follow the minimum bitrate selection set on the <u>Access Control page</u> for the respective SSID. Per SSID minimum bitrate selection will be moved to RF profiles at a later date.
	Client balancing On Off Client Balancing uses information about the state of the network and wireless client probes to steer the client to the best available access point during association. Read more about client balancing <u>here</u> .

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.

Cisco RoomOS Series Wireless LAN Deployment Guide

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	General 2.4 GHz 5 GHz	<u></u>
NETWORK	5 GHz radio settings	
Meraki WLAN -	Turn off 5GHz radio	See band selection above.
Network-wide	Channel width	Auto Manual
Wireless		Manual 5 GHz channel width
Organization		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 Radio transmit power range (dBm)	AutoChannel will assign radios to channels with low interference. Change channels used by AutoChannel Transmit shorter distance 7 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 5 9 12 18 24 35 48 54

ululu Moraki	General 2.	4 GHz	5 GHz														_
CISCO MIGTARI		Chang	e 5 GHz (	channels u	used by A	utoChann	el										×
NETWORK	5 GHz rad	ad Available channels for Auto Channel															
	Turn off 5GHz	off SGHz 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 UNII-3										ISM				
Network-wide		20 MHz	36 40	44 48	52 56	60 64	100	104 10	8 112	116 12	124	128	132 <b>136</b>	140 144	149 153	157 161	165
Wireless		40 MHz	38	46	54	62	102		110	118	126	6	134	142	151	159	
		80 MHz		12	5	8	106		122			138		155			
			DF3 channels Deselect DFS channels														
																Cancel	Done
				For low to	medium d	ensity deple	oyments.										
				80 MHz (5	channels)												
				For low de bandwidtl problems	ensity area: h and data	s with few o rates for mo	or zero nei odern dev	ghboring ices. Inc	g networ reases r	rks. Higher isk of interf	arence						

## **Firewall and Traffic Shaping**

On the **Wireless > Configure > Firewall & traffic shaping** page, firewall and traffic shaping rules can be defined. Cisco RoomOS Series Wireless LAN Deployment Guide 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.

cisco Meraki	<b>Q</b> Search Dashboard							
NETWORK Meraki WLAN 🗢	Firewall & traffic s	shap	oing o					
Network-wide	Block IPs and ports Layer 2 LAN isolation	Disab	oled ᅌ (br	ridge mode	only)			
Wireless	Layer 3 firewall rules (1)	# P	Policy	Protocol	Destination	Port	Comment	Actions
" Organization		) م <u>Add a</u>	Allow 🔉	Any Any rewall rule	Local LAN Any	Any Any	Wireless clients accessing LAN Default rule	
	Block applications ar	nd co	ntent ca	ategories	S			
	Layer 7 firewall rules	There Add a	e are no ru <u>a layer 7 f</u> i	les defined rewall rule	for this SSID.			
	Traffic shaping rules Per-client bandwidth limit	unlimi	ited	details	Enable Sp	peedBu	rst 🛈	
	Per-SSID bandwidth limit	Unlimi Contraction Shape	e traffic on th	details his SSID	0			

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.

Cisco Webex Control Hub			4° ⊚ ⊆
∩ Overview	Overview		
MONITORING	Organization Health () (BETA)	Devices 1,029 Total Devices Online: 29	Onboarding 147 Total Users There is no CSV upload within 180 days
MANAGEMENT 요 Users 이 Worksbaces	4 of 9 action items complete You can provide a better experience for your end users View All Action Items	Online with Issues: 182 Offline: 93	- Inactive 0% - Not Verified 12% - Verified 2% - Active 86%
Devices	Webex Services ALL ONLINE	Expired: 693 Unknown: 32	Potential New Users 1 Delayed Conversions 0
Account  Organization Settings  ERVICES	Messenger Webex Calling Meetings Hybrid Services Control Hub	What's New	Review Enable Directory Sync
⊖ Messaging ⊒ Meeting ⊾ Calling ⊖ Hybrid	Oeveloper API     Room Devices     Contact Center     O     UCM Cloud	Cisco Webex +	Quick Links Cisco COVID-19 Webex Response Resources Learn More
	Hybrid Services ALL ONLINE 6 INCOMPLETE Calendar Calendar (Office Calendar (Google) 265) (Exchange)	Meetings, Moderated Unnue for Video Devices, Pea- Meeting, Loby for Schedule Meetings, Enhancements to the Guest Join Experience and much more. Prevent Users from Using Unmanaged Apps Feb 10, 2021 Force Authentication for Users When Changing Passwords Jun 5, 2021	<ul> <li>Admin Capabilities</li> <li>Manage Subscriptions</li> <li>Organization Tasks</li> <li>Audit Log</li> <li>Manage Auto-License Template</li> </ul>
	Call Message Video Mesh		Onboarding Report

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**.

Cisco Webex Control Hub		
G Overview	C Add Device	×
MONITORING	Assign to a user or a workspace?	
♡ Organization Health	Devices for personal usage should be assigned to a specific user. A workspace represents a physical local owned by a specific user, such as a meeting room with a Webex Board 55 or a reception with a shared ph	ion containing a device not one.
ol Analytics		
~ Troubleshooting		
MANAGEMENT	L A C	
은 Users		
⑦ Workspaces		
📋 Devices	Existing User Worksp	ace
BB Apps	Personal Usage Shared U	sage
🗎 Account		
Organization Settings	Multiple Cisco IP Phones: To bulk activate devices, Import/Upload CSV file.	
SERVICES		
Messaging		
📋 Meeting		
% Calling		
🛆 Hybrid		Cancel Next

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

Cisco Webex Control Hub		
G Overview	C Add Device	×
MONITORING	Which user will this device belong to?	
♡ Organization Health	Search for a user	
Doll Analytics	0.0	
-√ Troubleshooting		
MANAGEMENT		
은 Users		e
⑦ Workspaces		
📋 Devices		
88 Apps		
🛅 Account		
Organization Settings		
SERVICES		
O Messaging		
📋 Meeting		
℅ Calling		
Hybrid	Back	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.

Cisco Webex		
Control Hub		
G Overview	Add De	evice
MONITORING	Assign to a user or a workspace?	
♡ Organization Health	Devices for personal usage should be assigned to a specific user. A w owned by a specific user, such as a meeting room with a Webex Boar	vorkspace represents a physical location containing a device not d 55 or a reception with a shared phone.
nalytics		
~ Troubleshooting		
MANAGEMENT	$\Omega$	$\bigcirc$
요 Users	$\langle \rangle$	
() Workspaces		
Devices	Existing User	Workspace
BB Apps	Personal Usage	Shared Usage
Account		
Organization Settings	Multiple Cisco IP Phones: To bulk activate devices, Impo	ort/Upload CSV file.
SEDVICES		
SERVICES		
Messaging		
Meeting		
℅ Calling		
Hybrid		Cancel

#### Select either Existing Workspace or New Workspace.

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

Add Device	
	×
MONITORING Assign to an existing workspace or a new workspace?	ĺ
Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a works	pace.
If you add multiple devices in a workspace that are not designed to work together, it may create interference issues.	
Analysis     Oc	
A Users	
0 Workspaces	
Devices Existing Workspace New Workspace	
88 Apps	
The Account	
Organization Settings     Which Workspace will the device be assigned to?     Weddeeseese containing devices that are not Clean ID Discose will not be about an activities that are not Clean ID Discose will not be about an activities in a	
services workspace.	
O Messaging Search for a Workspace	
Meeting	
% Calling	
○ Hybrid	
Back	Next
Cisco Webex	
	×
G Overview C Add Device	×
Add Device Assign to an existing workspace or a new workspace?	×
Overview     C     Add Device     Add Device     Assign to an existing workspace or a new workspace?     Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a work     Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a work	× pace.
Overview     Add Device     Add Device     Assign to an existing workspace or a new workspace?     Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues.     If you add multiple devices in a workspace that are not designed to work together, it may create interference issues.	× pace.
Overview       C       Add Device         MONITORING       Assign to an existing workspace or a new workspace?         Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues.         Analytics       O c         Troubleshooting       O c	X pace.
Overview     Add Device     Add Device     Assign to an existing workspace or a new workspace?     Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace     f you add multiple devices in a workspace that are not designed to work together, it may create interference issues.	pace.
Overview       C       Add Device         MONTORING       Assign to an existing workspace or a new workspace?       Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a work if you add multiple devices in a workspace that are not designed to work together, it may create interference issues.         MANAGEMENT       Oc	pace.
Add Device     MONITORING     Organization Health     Analytics     Or     MANAGEMENT     Users     Device     Add Device     Assign to an existing workspace or a new workspace?   Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace that are not designed to work together, it may create interference issues.	pace.
Add Device     MONITORING     Organization Health     Analytics     Or     MANAGEMENT     Users   Workspaces     Cubers     O Workspaces     Cubers     Cubers <td< td=""><td>× pace.</td></td<>	× pace.
Add Device   MONTORING   Organization Health   Analytics   Troubleshooting   MANAGEMENT   Users   Workspaces   Devices   Existing Workspace   New Workspaces   Existing Workspace	pace.
Add Device   MONTTORING   Organization Health   Analytics   Analytics   Vortubleshooting   MANAGEMENT   Users   Vorkspaces   Devices   States a device   Existing Workspace   New Workspace   New Workspace	× pace.
Add Device     MONTORING     Organization Health     Analytics     Organization Health     In Analytics     Organization Health     In Analytics     Organization Health     In Analytics     Organization Health     In Devices     Existing Workspace     New Workspace     New Workspace     New Workspace     In Devices     Account     Organization Existing this device here here here there here here there here	× pace.
Add Device   MONTORING   Organization Health   Analytics   Troubleshooting   MANAGEMENT   Jesers   Vorkspaces   Pevices   Apps   Account   Organization Settings   Where will this device be located? What would you like to call the Workspace that this device will be assigned to?	pace.
Overview C   MONFORMUS   Organization Health   Analytics   Troubleshooting   MANAGEMENT   Users   Vorkspaces   Devices   Apps   Account   Organization Settings   SERVICES      Account Services Interview	pace.
Overview C   MONFORMS   MONFORMS   MONFORMS   Organization Health   Analytics   Troubleshooting   MANAGEMENT   Queries   Devices   Account   Organization Stettings   Where will this device be located?   Where will this device be located?   What would you like to call the Workspace that this device will be assigned to?   Insert name of device location, e.g. 'Reception' or 'Bo.	× pace.
Add Device   MONTRONNE   Organization Health   Analytics   Troubleshooting   MANAGEMENT   Users   Vorkspaces   Devices   Apps   Account   Organization Settings   Where will this device be located?   Where will this device be located?   Where will this device be located?   What would you like to call the Workspace to?   Insert name of device location, e.g. 'Reception' or 'Bo.	×
Overview C   MONTRORING   MONTRORING   Organization Health   Analytics   Troubleshooting   MANAGEMENT   Users   Overview   Devices   Statisting Workspace   Devices   Statisting Workspace   Devices   Statisting Workspace   New Workspace   New Workspace   New Workspace   Where will this device be located?   What would you like to call the Workspace that his device will be assigned to?   Insert name of device location, e.g. 'Reception' or 'Bo.	×

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

Cisco Webex Control Hub				
	C	Add D	evice	$\times$
MONITORING	[ [	What kind of device do you want to set up in this	workspace?	
$\bigcirc$ Organization Health				
nol Analytics	0.0		۰	
~ Troubleshooting	00			
MANAGEMENT			⊖ <u>∎</u>	
요 Users		Cisco Webex Rooms device	Cisco IP Phone	
⑦ Workspaces		e.g. Cisco Webex Board, Room, and Desk series,	e.g. Cisco 8845, 8865, 8800 and Analog Telephone	
📋 Devices		and Webex Share.	Adapter ports	
88 Apps				
🗎 Account				
Organization Settings				
SERVICES				
○ Messaging				
📋 Meeting				
℅ Calling				
→ Hybrid			Back	xt

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

Cisco Webex Control Hub					
G Overview	C		Add Device	×	( )
MONITORING	ŀ	Which services are	needed in this Workspace?		
<ul><li>in Analytics</li><li></li></ul>	0 c		Cisco Webex Calling Free Calling features with additional PSTN service provided through Webex.		
MANAGEMENT					e
<ul> <li>☑ Users</li> <li>♡ Workspaces</li> </ul>		E Calendar	Calendar service enables One Button To Push for this Workspace.		
Devices					
<ul> <li>Account</li> <li>Organization Settings</li> </ul>					
SERVICES					
<ul> <li>Messaging</li> <li>Meeting</li> </ul>					
<ul><li>S Calling</li><li>△ Hybrid</li></ul>				Back 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/productsmaintenance-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		
Device is trusted MAC Address *		]
Description		1
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*		Default	
Cisco Unified Communications Ma	nager Group*	Default	<b>O</b>
Calling Search Space for Auto-reg	istration	< None >	٥
Adjunct CSS		< None >	٥
Reverted Call Focus Priority		Default	٥
Intercompany Media Services Enro	olled Group	< None >	٥
Roaming Sensitive Settings			
Date/Time Group*	CMLocal		
Region*	Default		0
Media Resource Group List	< None >		0
Location	< None >		0
Network Locale	< None >		0
SRST Reference*	Disable		0
Connection Monitor Duration ***			
Single Button Barge*	Default		0
Join Across Lines*	Default		0
Physical Location	< None >		0
Device Mobility Group	< None >		0
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.

Γ	Phone Button Template Information								
	Button Template Name * Standard Cisco Webex Desk Pro								
Γ	Button Information								
l	Button	Feature							
	1 L	ine **	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*	None	٢	
Packet Capture Duration	0		
BLF Presence Group*	Standard Presence group	0	
MTP Preferred Originating Codec*	711ulaw	٥	
Device Security Profile*	Cisco Webex Desk Pro - Standard SIP Non-Secure	٢	
Rerouting Calling Search Space	< None >	٢	
SUBSCRIBE Calling Search Space	< None >	٢	
SIP Profile*	Standard SIP Profile	٢	View Details
Digest User	< None >	0	
Media Termination Point Require	red		
Unattended Port			
Require DTMF Reception			
L			

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	0					
Transport Type*	TCP+UDP 🕒						
Enable Digest Authentication							
TFTP Encrypted Config							
Exclude Digest Credentials in Configuration File							
Phone Security Profile CAPF Information							
Authentication Mode*	By Null String	•					
Key Order*	RSA Only	0					
RSA Key Size (Bits)*	2048	•					
EC Key Size (Bits)	< None >	٥					
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	0	
Packet Capture Duration	0		
BLF Presence Group*	Standard Presence group	0	
MTP Preferred Originating Codec*	711ulaw	0	
Device Security Profile*	Cisco Webex Desk Pro - Standard SIP Non-Secure	٢	
Rerouting Calling Search Space	< None >	0	
SUBSCRIBE Calling Search Space	< None >	٢	
SIP Profile*	Custom Webex Desk Pro SIP Profile	٢	View Details
Digest User	< None >	٢	
Media Termination Point Requir	red		
Unattended Port			
Require DTMF Reception			
L			

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		0					
Dial String Interpretation*	Phone number consists of	of characters 0-9, *, #, an	0					
Confidential Access Level Headers*	Disabled		0					
Redirect by Application								
Disable Early Media on 180								
Outgoing T.38 INVITE include audio mline								
Offer valid IP and Send/Receive mode only for T.38 Fax Relay								
Use Fully Qualified Domain Name in SIP F	lequests							
Assured Services SIP conformance								
Enable External QoS**								
SDP Information								
SDP Session-level Bandwidth Modifier for Ea	arly Offer and Re-invites $^{*}$	TIAS and AS		0				
SDP Transparency Profile		Pass all unknown SDP attr	ibutes	<b>©</b>				
Accept Audio Codec Preferences in Received	Default		0					
Require SDP Inactive Exchange for Mid-Call Media Change								
Allow RR/RS bandwidth modifier (RFC 3	556)							
Parameters used in Phone								
Timer Invite Expires (seconds)*	180							
Timer Register Delta (seconds)*	30							
Timer Register Expires (seconds)*	3600							
Timer T1 (msec)*	500							
Timer T2 (msec)*	4000							
Retry INVITE*	6							
Retry Non-INVITE*	10							
Media Port Ranges	• Common Port Range for Audio and Video							
Separate Port Ranges for Audio and Video								
Start Media Port* 16384								
DSCP for Audio Callis       Use System Default       G         DSCP for Video Callis       Use System Default       G         DSCP for Audio Portion of Video Callis       Use System Default       G         DSCP for Audio Portion of Video Callis       Use System Default       G         DSCP for Audio Portion of Video Callis       Use System Default       G         DSCP for Audio Portion of TelePresence Calls       Use System Default       G         Call Pickup Group Other URI*       x-cisco-serviceuri-pickup       G         Call Pickup Group Other URI*       x-cisco-serviceuri-pickup       G         Meet Me Service URI*       x-cisco-serviceuri-meetme       G         User Info*       Nome       G       G         DTMF DB Level*       Nominal       G       G         Call Hold Ring Back*       Off       G       G         Call Hold Ring Back*       Off       G       G         Do Not Disturb Control*       User       G       G         Inner Subscribe Expires (seconds)*       300       G       G         Timer Subscribe Expires (seconds)*       15       G       G         Maximum Redirections*       70       G       G       G         Generatione Transfer      cic	Stop Media Port*	32766						
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------	-----------------------------	---					
DSCP for Video Calls     Use System Default     Image: Call State System Default     Image: Call System Default State System Default     Image: Call System Default State System Default State System Default     Image: Call System Default State System Stat	DSCP for Audio Calls	Use System Default						
DSCP for Audio Portion of Video Calis       Use System Default       ©         DSCP for TelePresence Calis       Use System Default       ©         DSCP for Audio Portion of TelePresence Calis       Use System Default       ©         Call Pickup UR1*       x-cisco-serviceuri-pickup       ©         Call Pickup Group UR1*       x-cisco-serviceuri-opickup       ©         Meet Me Service UR1*       x-cisco-serviceuri-meetme       ©         DTMF DB Level*       Nome       ©         DTMF DB Level*       Off       ©         Anonymous Cali Block*       Off       ©         Cali Hold Ring Back*       Off       ©         Do Not Disturb Control*       User       ©         Do Not Disturb Control*       User       ©         Telnet Level for 7940 and 7960*       Disabled       ©         Resource Priority Namespace       < None >       ©         Timer Kuep Alive Expires (seconds)*       300       ©         Timer Subscribe Deta (seconds)*       15       Maximum Redirections*       70         Off Hook To First Digit Timer (milliseconds)*       15000       ©       Cali Forward UR1*       x-cisco-serviceuri-dfwdail         Speed Dial (Abbreviated Dial) UR1*       x-cisco-serviceuri-dfwdail       ©       ©	DSCP for Video Calls	Use System Default						
DSCP for TelePresence Calls       Use System Default       S         DSCP for Audio Portion of TelePresence Calls       Use System Default       S         Call Pickup UR!*       x-cisco-serviceuri-pickup       Call Pickup Group Other UR!*       x-cisco-serviceuri-opickup         Call Pickup Group UR!*       x-cisco-serviceuri-opickup       Call Pickup Group UR!*       x-cisco-serviceuri-opickup         Call Pickup Group UR!*       x-cisco-serviceuri-meetme       S         User Info*       None       S         DTMF DB Level*       Nominal       G         Call Hold Ring Back*       Off       G         Anonymous Call Block*       Off       G         Do Not Disturb Control*       User       G         Telnet Level for 7940 and 7960*       Disabled       G         Resource Priority Namespace       < None >       G         Timer Subscribe Deta (seconds)*       300       G         Timer Subscribe Deta (seconds)*       15       Maximum Redirections*       To0         Call Forward URI*       x-cisco-serviceuri-ofwdail       S       S       S         Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial       G       G         Growser Priority How Space       Service Priority Audit       S       S	DSCP for Audio Portion of Video Calls	Use System Default						
DSCP for Audio Portion of TelePresence Calls       Use System Default       G         Call Pickup UR1*       x-cisco-serviceuri-pickup       G         Call Pickup Group UR1*       x-cisco-serviceuri-opickup       G         Call Pickup Group UR1*       x-cisco-serviceuri-opickup       G         Meet Me Service UR1*       x-cisco-serviceuri-opickup       G         User Info*       None       G         DTMF DB Level*       Noninal       G         Call Hold Ring Back*       Off       G         Caller DB Blocking*       Off       G         Do Not Disturb Control*       User       G         Teinet Level for 7940 and 7960*       Disabled       G         Resource Priority Namespace       < None >       G         Timer Subscribe Expires (seconds)*       300       G         Timer Subscribe Delta (seconds)*       15       G         Maximum Redirections*       70       G         Off Hook To First Digit Timer (milliseconds)*       15000       G         Call Abbreviated Dial) UR1*       x-cisco-serviceuri-cfwdall       x-cisco-serviceuri-cfwdall         Speed Dial (Abbreviated Dial) UR1*       x-cisco-serviceuri-cfwdall       x-cisco-serviceuri-cfwdall         Speend Natended Transfer       -       -	DSCP for TelePresence Calls	Use System Default	3					
Call Pickup UR1*       x-cisco-serviceuri-opickup         Call Pickup Group Other UR1*       x-cisco-serviceuri-opickup         Call Pickup Group UR1*       x-cisco-serviceuri-opickup         Meet Me Service UR1*       x-cisco-serviceuri-meetme         User Info*       None         DTMF DB Level*       Nominal         Call Hold Ring Back*       Orf         Call Hold Ring Back*       Orf         Caller DB locking*       Orf         Caller DB locking*       Off         Do Not Disturb Control*       User         Caller DF Job Level (Seconds)*       Job         Do Not Disturb Control*       User         Caller Kep Kepires (seconds)*       Joo         Timer Keep Alive Expires (seconds)*       Joo         Timer Subscribe Expires (seconds)*       Joo         Timer Subscribe Delta (seconds)*       Joo         Call Forward UR1*       x-cisco-serviceuri-cfwdail         Speed Dial (Abbreviated Dial) UR1*       x-cisco-serviceuri-abbrdial         Conference Join Enabled       -         Cander Transfer       -         Inable VAD       -         Semi Attended Transfer       -         Inable VAD       -         Mutter Message Walting       - <t< td=""><td>DSCP for Audio Portion of TelePresence Calls</td><td>Use System Default</td><td>3</td></t<>	DSCP for Audio Portion of TelePresence Calls	Use System Default	3					
Call Pickup Group UR!*       x-cisco-serviceuri-opickup         Meet Me Service UR!*       x-cisco-serviceuri-meetme         User Info*       None         DTMF DB Level*       Nominal         Call Hold Ring Back*       Off         Anonymous Call Block*       Off         Caller D Blocking*       Off         Do Not Disturb Control*       User         Resource Priority Namespace       < None >         Timer Subscribe Expires (seconds)*       300         Timer Subscribe Expires (seconds)*       300         Timer Subscribe Expires (seconds)*       15         Maximum Redirections*       70         Off Hook To First Digit Timer (milliseconds)*       15000         Caller Forward UR1*       x-cisco-serviceuri-dfwalil         Speed Dial (Abbreviated Dial) UR1*       x-cisco-serviceuri-abbrdial         © Semi Attended Transfer       -         Inable VAD       -         Statter Message Waiting       -         Mutter Message Waiting       -         Mutter Message Waiting       -         Numelization Script       Konne >	Call Pickup URI*	x-cisco-serviceuri-pickup						
Call Pickup Group URI*       x-cisco-serviceuri-gpickup         Meet Me Service URI*       x-cisco-serviceuri-meetme         User Info*       None         DTMF DB Level*       Nominal         Call Hold Ring Back*       Off         Call Hold Ring Back*       Off         Caller ID Blocking*       Off         Do Not Disturb Control*       User         Do Not Disturb Control*       User         Teinet Level for 7940 and 7960*       Disabled         Resource Priority Namespace       < None >         Timer Subscribe Expires (seconds)*       300         Timer Subscribe Delta (seconds)*       15         Maximum Redirections*       70         Off Hook To First Digit Timer (milliseconds)*       15000         Call Forward URI*       x-cisco-serviceuri-abbrdial         Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial         Speed Dial (Abbreviated Transfer       Isable VAD         Sutter Message Waiting       Imale X-disco-serviceuri-abbrdial         Stuter Message Waiting       Imale X-disco-serviceuri-abbrdial         Numelization Script       Knone         Normalization Script       Knone	Call Pickup Group Other URI*	x-cisco-serviceuri-opickup						
Meet Me Service URI* x-cisco-serviceuri-meetme   User Info* None   DTMF DB Level* Nominal   Call Hold Ring Back* Off   Call Hold Ring Back* Off   Caller ID Blocking* Off   D Not Disturb Control* User   D Not Disturb Control* User   Teinet Level for 7940 and 7960* Disabled   Resource Priority Namespace < None >   Timer Keep Allve Expires (seconds)* 300   Timer Subscribe Expires (seconds)* 300   Timer Subscribe Delta (seconds)* 15   Maximum Redirections* 70   Off Hook To First Digit Timer (milliseconds)* 15000   Call Forward URI* x-cisco-serviceuri-abbrdial   Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial   © Semi Attended Transfer	Call Pickup Group URI*	x-cisco-serviceuri-gpickup						
User Info*       None       9         DTMF DB Level*       Nominal       9         Call Hold Ring Back*       Off       9         Anonymous Call Block*       Off       9         Caller ID Blocking*       Off       9         Do Not Disturb Control*       User       9         Telnet Level for 7940 and 7960*       Disabled       9         Resource Priority Namespace       < None >       9         Timer Subscribe Expires (seconds)*       300       9         Timer Subscribe Delta (seconds)*       15       9         Maximum Redirections*       70       9         Off Hook To First Digit Timer (milliseconds)*       15000       9         Call Forward UR1*       x-cisco-serviceuri-cfwdall       x-cisco-serviceuri-abbrdial         Speed Dial (Abbreviated Dial) UR1*       x-cisco-serviceuri-abbrdial       9         Conference Join Enabled       FRC 2543 Hold       9       9         Semi Attended Transfer       5       9       9         Isuter Message Waiting       -       9       9         MuPP User Authorization       -       9       9         Normalization Script       -       9       9         Normalization Script	Meet Me Service URI*	x-cisco-serviceuri-meetme						
DTMF DB Level*       Nominal       G         Call Hold Ring Back*       Off       G         Anonymous Call Block*       Off       G         Caller ID Blocking*       Off       G         Caller ID Blocking*       Off       G         Do Not Disturb Control*       User       G         Do Not Disturb Control*       User       G         Teinet Level for 7940 and 7960*       Disabled       G         Resource Priority Namespace       < None >       G         Timer Keep Alive Expires (seconds)*       300       G         Timer Subscribe Expires (seconds)*       300       G         Timer Subscribe Delta (seconds)*       15       Maximum Redirections*         70       Off Hook To First Digit Timer (milliseconds)*       15000         Call Forward URI*       x-cisco-serviceuri-cfwdall       x-cisco-serviceuri-abbrdial         Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial       Sconference Join Enabled         RFC 2543 Hold       Semi Attended Transfer       Semi Attended Transfer       Semi Attended Transfer         Enable VAD       Stutter Message Waiting       WIMPP User Authorization       Normalization Script         Normalization Script       Normalization Script       Normali Attendescript Script	User Info*	None						
Call Hold Ring Back* Off Off Off Off Caller ID Blocking* Off User Caller ID Blocking* Off User Caller ID Blocking* Off Off Off Off Off Caller ID Blocking* Off Off Off Caller ID Blocking* Off Off Caller ID Blocking* Caller ID Blocking* Off Caller ID Blocking* Cal	DTMF DB Level*	Nominal						
Anonymous Call Block* Off G Caller ID Blocking* Off C Caller ID Blocking* C Caller ID	Call Hold Ring Back*	Off	3					
Caller ID Blocking* Off   Do Not Disturb Control* User   Telnet Level for 7940 and 7960* Disabled   Resource Priority Namespace < None >   Timer Keep Allve Expires (seconds)* 300   Timer Subscribe Expires (seconds)* 300   Timer Subscribe Delta (seconds)* 300   Timer Subscribe Delta (seconds)* 15   Maximum Redirections* 70   Off Hook To First Digit Timer (milliseconds)* 15000   Call Forward URI* x-cisco-serviceuri-cfwdall   Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial   Conference Join Enabled RFC 2543 Hold   Semi Attended Transfer Enable VAD   Stutter Message Waiting MLPP User Authorization	Anonymous Call Block*	Off	3					
Do Not Disturb Control* User   Telnet Level for 7940 and 7960* Disabled   Resource Priority Namespace < None >   Timer Keep Alive Expires (seconds)* 300   Timer Subscribe Expires (seconds)* 300   Timer Subscribe Delta (seconds)* 15   Maximum Redirections* 70   Off Hook To First Digit Timer (milliseconds)* 15000   Call Forward URI* x-cisco-serviceuri-cfwdall   Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial   Conference Join Enabled RFC 2543 Hold   Semi Attended Transfer Enable VAD   Stutter Message Waiting MLPP User Authorization	Caller ID Blocking*	Off	3					
Telnet Level for 7940 and 7960* Disabled   Resource Priority Namespace < None >   Timer Keep Alive Expires (seconds)* 300   Timer Subscribe Expires (seconds)* 300   Timer Subscribe Delta (seconds)* 15   Maximum Redirections* 70   Off Hook To First Digit Timer (milliseconds)* 15000   Call Forward URI* x-cisco-serviceuri-cfwdall   Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial   Conference Join Enabled RFC 2543 Hold   Semi Attended Transfer Enable VAD   Stutter Message Waiting MLPP User Authorization	Do Not Disturb Control*	User	9					
Resource Priority Namespace < None >   Timer Keep Alive Expires (seconds)* 300   Timer Subscribe Expires (seconds)* 300   Timer Subscribe Delta (seconds)* 15   Maximum Redirections* 70   Off Hook To First Digit Timer (milliseconds)* 15000   Call Forward URI* x-cisco-serviceuri-cfwdall   Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial   Conference Join Enabled RFC 2543 Hold   Semi Attended Transfer Enable VAD   Stutter Message Waiting MLPP User Authorization	Telnet Level for 7940 and 7960*	Disabled	3					
Timer Keep Alive Expires (seconds)* 300   Timer Subscribe Expires (seconds)* 300   Timer Subscribe Delta (seconds)* 15   Maximum Redirections* 70   Off Hook To First Digit Timer (milliseconds)* 15000   Call Forward URI* x-cisco-serviceuri-cfwdall   Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial   Conference Join Enabled RFC 2543 Hold   @ Semi Attended Transfer Enable VAD   Stutter Message Waiting MLPP User Authorization	Resource Priority Namespace	< None >	3					
Timer Subscribe Expires (seconds)*       300         Timer Subscribe Delta (seconds)*       15         Maximum Redirections*       70         Off Hook To First Digit Timer (milliseconds)*       15000         Call Forward URI*       x-cisco-serviceuri-cfwdall         Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial         © Conference Join Enabled       RFC 2543 Hold         © Semi Attended Transfer       Enable VAD         Stutter Message Waiting       MLPP User Authorization         Normalization Script       Normalization Script         Normalization Script       Stute	Timer Keep Alive Expires (seconds)*	300						
Timer Subscribe Delta (seconds)*       15         Maximum Redirections*       70         Off Hook To First Digit Timer (milliseconds)*       15000         Call Forward URI*       x-cisco-serviceuri-cfwdall         Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial         Conference Join Enabled       RFC 2543 Hold         Semi Attended Transfer       Enable VAD         Stutter Message Waiting       MLPP User Authorization         Normalization Script       Normalization Script	Timer Subscribe Expires (seconds)*	300						
Maximum Redirections*       70         Off Hook To First Digit Timer (milliseconds)*       15000         Call Forward URI*       x-cisco-serviceuri-cfwdall         Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial         Conference Join Enabled       RFC 2543 Hold         Semi Attended Transfer       Enable VAD         Stutter Message Waiting       MLPP User Authorization         Normalization Script       Normalization Script	Timer Subscribe Delta (seconds)*	15						
Off Hook To First Digit Timer (milliseconds)*       15000         Call Forward URI*       x-cisco-serviceuri-cfwdall         Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial         © Conference Join Enabled       RFC 2543 Hold         © Semi Attended Transfer       Enable VAD         Stutter Message Waiting       MLPP User Authorization         Normalization Script       None >	Maximum Redirections*	70						
Call Forward URI* x-cisco-serviceuri-cfwdall Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial C Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization Normalization Script Normalization Script	Off Hook To First Digit Timer (milliseconds)*	15000						
Speed Dial (Abbreviated Dial) URI*       x-cisco-serviceuri-abbrdial         Image: Conference Join Enabled       RFC 2543 Hold         Image: Conference Join	Call Forward URI*	x-cisco-serviceuri-cfwdall						
Conference Join Enabled RFC 2543 Hold Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization Normalization Script Normalization Script	Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrdial						
RFC 2543 Hold     Semi Attended Transfer     Enable VAD     Stutter Message Waiting     MLPP User Authorization  Normalization Script Normalization Script	Conference Join Enabled							
Semi Attended Transfer Enable VAD Stutter Message Waiting MLPP User Authorization Normalization Script Normalization Script	RFC 2543 Hold							
Enable VAD  Stutter Message Waiting  MLPP User Authorization  Normalization Script  Normalization Script  Normalization Script	Semi Attended Transfer							
Stutter Message Walting MLPP User Authorization Normalization Script Normalization Script	Enable VAD							
Mormalization Script Normalization Script	Stutter Message Waiting							
Normalization Script	MLPP User Authorization							
Normalization Script < None >	Normalization Script							
	Normalization Script < None >	٥						

Enable Trace				
Parameter Name	Parameter Value			
1				
_ Incoming Requests FROM URI Settings				
Caller ID DN				
Caller Name				
Trunk Specific Configuration				
Reroute Incoming Request to new Trunk based on $\ensuremath{^{\ast}}$	Never			
Resource Priority Namespace List	< None >			
SIP Rel1XX Options*	Disabled 🗘			
Video Call Traffic Class*	Mixed			
Calling Line Identification Presentation*	Default			
Session Refresh Method *	Invite			
Early Offer support for voice and video calls*	Disabled (Default value)			
Enable ANAT				
Deliver Conference Bridge Identifier				
Allow Passthrough of Configured Line Device Cal	er 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 st	atus for Trunks with Service Type "None (Default)"			
Ping Interval for In-service and Partially In-service	Trunks (seconds)* 60			
Ping Interval for Out-of-service Trunks (seconds)*	120			
Ping Retry Timer (milliseconds)*	500			
Ping Retry Count*	6			
SUP Information				
Send send-receive SDP in mid-call INVITE				
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.

- Enterprise Parameters Configuration		
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)
		100
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	• 64 kbps (G.722, G.711) kbps	<ul> <li>Keep Current</li> <li>Setting</li> <li>Use System</li> <li>Default</li> <li>None</li> <li>2000 kbps</li> </ul>	Keep Current Setting     Use System Default     None     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 La	yout		
?	Parameter Va	lue	Override Enterprise/Common Phone Profile Settings
Room Name (from Exchange(R))			
Web Access*	Disabled	0	
SSH Access*	Disabled	0	
Default Call Protocol*	SIP	0	
Quality Improvement Server			
Multipoint Mode*	Use Endpoint	0	
Telnet Access*	Off	0	
Microphone Unmute On Disconnect*	On	0	
Call Logging Mode*	On	0	
OSD Encryption Indicator*	Auto	0	
Alternate phone book server type*	UDS	0	
Alternate phone book server address			
Default Volume	70		
Max Total Downstream Rate	15000		
Max Total Upstream Rate	10000		
Load Server			
WiFi Allowed*	On	0	
System Name			
Wake-up On Motion Detection*	On	3	
Custom Message			
Settings Menu Mode*	Unlocked	0	
Accessibility Call Notification*	Default	0	
Configuration Control Mode*	Unified CM and Endpoint	0	
Webex Devices Onboarding Token			
Easy Webex join*	Auto	0	
⊢ Far End Camera Control Setting	5		
Far End Camera Control*	On		8
Far End Camera Control Signaling C	apability* On		8
- Eacility Service Settings			
Facility Service Type*	ek	0	
Facility Service Name	эл.		
Facility Service Number			
Facility Service Number		_	
Video			

Standby Settings						
Standby Mode* On			3			
Standby Delay 10						
Serial Port Settings						
Serial Port*	Or	n		0		
Serial Port Login Requ	uired* Or	1		0		
Admin username an	d passwo	ord —				
Admin Username						
Admin Password						
Proximity						
Proximity Mode*			On			0
Call Control*			Disabled			Θ
Proximity Content Sha	are From C	lients*	Disabled			0
Proximity Content Sha	are To Clie	nts*	Disabled			0
LDAP User Managen	nent					
LDAP Mode*		Off			0	
LDAP Server Address						
LDAP Server Port		0				
LDAP Attribute						
LDAP Base DN						
LDAP Encryption*		LDAPS			0	
LDAP Minimum TLS Ve	ersion*	TLSv1.	2		0	
LDAP Verify Server Ce	ertificate*	Off			0	
LDAP Admin Filter						
LDAP Admin Group						
Customization Provi	isioning-					
Customization File						
Customization Hash T	vpe* SH	A512		6	_	
Customization Hash		- SIL				
SMTP Provisioning -	0#			0		
SMTP Server	UII					
SMTP Port	0					
SMTP Security type*	None					
SMTP Username						
SMTP Password						
SPITE Password						
SMTP From address						

Field Name	<b>Description</b>
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

Cisco RoomOS Series Wireless LAN Deployment Guide

	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 username to be used.

#### Cisco Desk Pro Configuration Options (versions 12.5 and later)

Product Specific Conf	iguration Layout	
?	Parameter Value	Pull xConfig. from device
i-Note: Endpoints runn These parameters are in	ning software versions earlier than CE 9. dicated below with the # symbol.	8 only support provisioning a limited set of parameters from Cisco Unified CM.
Audio	General Settings	
Bluetooth	DefaultVolume	50 #
	Microphones Mute Enabled*	True 🗸
BYOD	Ultrasound MaxVolume	70
CallHistory	Input	
Cameras	HDMI 1	
	Level	0
Conference	Mode*	On v
FacilityService	MicrophoneMode*	Focused v
	USBC 1	
	Level	0
HttpFeedback	Mode*	On v
Logging	SoundsAndAlerts	
Massas	RingTone	Sunrise
	RingVolume	50
NetworkServices		
Phonebook	KeyClickDetector	
	Enabled*	True 🗸
RoomAnalytics	Attenuate*	True v
RoomScheduler		

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

# <u>Audio</u>

General Settings	
DefaultVolume	50
Microphones Mute Enabled*	True 🗸
Ultrasound MaxVolume	70
Input	
HDMI 1	
Level	0
Mode*	On v
MicrophoneMode*	Focused V
USBC 1	
Level	0
Mode*	On v
SoundsAndAlerts	
RingTone	Sunrise
RingVolume	50
-	
KeyClickDetector	
Enabled*	True 🗸
Attenuate*	True

#### <u>Bluetooth</u>

General Settings		
Allowed*	True	~
Enabled*	False	~
Enabled*	False	~

#### <u>BYOD</u>

General Settings		
HidForwarding Enabled*	False	<b>v</b>
TouchForwarding Enabled*	True	<b>v</b>

# Call History

General Settings		
Mode*	On	*

#### <u>Cameras</u>

alse v	
'rue 🗸	
Auto 🗸	
Auto 🗸	
20	
Auto 🗸	
)	
	alse v rue v uto v uto v auto v

#### **Conference**

DefaultCall		
Protocol*	Sip	*
Rate	6000	
DoNotDisturb DefaultTimeout	60	
Encryption Mode*	BestEffort	~
FarendMessage Mode*	Off	<b>v</b>
MaxReceiveCallRate	6000	
MaxTotalReceiveCallRate	15000	<i>#</i>
MaxTotalTransmitCallRate	15000	*
MaxTransmitCallRate	6000	
MicUnmuteOnDisconnect Mode*	On	✓ *
Multipoint Mode*	Auto	✓ 🕫
FarEndControl		
Mode*	On	~ ₽
SignalCapability*	On	✓ *

# Facility Service

Service 1		
CallType*	Video 🗸	ø
Name	Live Support	#
Number		#
Type*	Helpdesk v	)¢
Service 2		
CallType*	Video 🗸	)
Name		
Number		
Type*	Helpdesk v	)
- Service 3		
CallType*	Video	1
Name		
Number		
Type*	Helpdesk	1
.,,,,,		,
Service 4		
CallType*	Video 🗸	)
Name		
Number		
Type*	Helpdesk v	)
Service 5		
CallTune*	Video	1
Name	Video	
Name	L	
Number		
Type*	Helpdesk v	J

#### HTTP Client

General Settings		
Mode*	Off	<b>v</b>
AllowInsecureHTTPS*	False	~
AllowHTTP*	True	~
UseHttpProxy*	On	~

#### HTTP Feedback

General Settings			
TIsVerify*	On	~	
UseHttpProxy*	On	<b>v</b>	

#### Logging

General Settings			
<b>j</b> -			
CloudUpload Mode*	Off	~	
Internal Mode*	On	~	
External			
external			
Mode*	Off	~	
Protocol*	SyslogTLS	~	
TIsVerify*	On	<b>v</b>	
Server			
Address			
Port	514		

#### <u>Macros</u>

General Settings		
	<u></u>	
AutoStart*	On	v
Mode*	Off	~
UnresponsiveTimeout	5	

#### **Network Services**

General Settings		
H323 Mode*	Off	~
UPnP Mode*	On	<b>v</b>
Websocket*	Off	<b>v</b>
WelcomeText*	On	<b>v</b>
Wifi Allowed*	True	<b>v</b>
НТТР		
Mode*	Off	✓ <sup>#</sup>
Proxy		
Mode*	Off	<b>v</b>
Url		
LoginName		
Password		
PACUrl		
HTTPS-		
VerifyClientCertificate*	Off	<b>v</b>
StrictTransportSecurity*	Off	▼
Server		
MinimumTLSVersion*	TLSv1.1	<b>v</b>
_ SNMP		
Sime -		
CommunityName		
Mode -	Off	<u> </u>
SystemContact		
SystemLocation		
SSH		
HostKeyAlgorithm*	RSA	<b>v</b>
Mode*	Off	v)*
SMTP		
Mode*	Off	*
Server		*
Port	0	#
Security*	StartTls	✓ <sup>#</sup>
Username		#
Password		#
From		#

# <u>Phone Book</u>

Server 1		
ID		
Type*	CUCM	✓ )#
URL		#
Pagination*	Enabled	~
TIsVerify*	On	~

#### **Room Analytics**

General Settings		
PeopleCountOutOfCall*	Off	~
PeoplePresenceDetector*	Off	<b>v</b>
AmbientNoiseEstimation —		
Mode*	Off	~
Interval	10	

#### Room Scheduler

General Settings		
Enabled*	False v	

# <u>SIP</u>

General Settings		
MinimumTLSVersion*	TLSv1.0	<b>v</b>

#### <u>Security</u>

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

#### Serial Port

. .

I

General Settings		
BaudRate*	115200	•
LoginRequired *	On v	1
Mode*	On v	)

## <u>Standby</u>

General Settings			
BootAction*	RestoreCameraPosition	~	
Control*	On	~ *	
Delay	10	*	
StandbyAction*	PrivacyPosition	~ *	
WakeupAction*	RestoreCameraPosition	~	
WakeupOnMotionDetection*	On	~ *	
Signage			
Url			

on		
Mode*	Off	~
InteractionMode*	NonInteractive	~
RefreshInterval	0	
Audio*	Off	~

#### System Unit

General Settings Name	*
CrashReporting Mode*	Off
URL	¢

# User Interface

#### General Settings Accessibility IncomingCallNotification Default v # Bookings Visibility Title\* × Auto ContactInfo Type\* Auto $\mathbf{v}$ Diagnostics Notifications\* Auto × Branding AwakeBranding Colors\* × Auto KeyTones Mode\* Off × SoundEffects Mode\* On × Proximity Notifications\* Auto V CustomMessage # Whiteboard ActivityIndicators\* On × Assistant Mode\* On $\mathbf{v}$ Security Mode\* Normal ×

- Features		
HideAll*	False	✓
Call		
Start*	Auto	<b>v</b>
MidCallControls*	Auto	<b>v</b>
End*	Auto	<b>v</b>
JoinWebex*	Auto	<b>v</b> #
Keypad*	Auto	<b>v</b>
MusicMode*	Hidden	×
Share		
Start*	Auto	<b>v</b>
Whiteboard		
Start*	Auto	<b>v</b>
030		
EncryptionIndicator*	Auto	<b>∨</b> ] <sup>#</sup>
Output*	1	<b>v</b>
HalfwakeMessage		
Mode*	Auto	▼
Phonebook		
Mode*	ReadWrite	~
DefaultSearchFilter*	All	~

SettingeMenu			
SettingsHend			
Mode*	Unlocked	*	
Visibility*	Auto	~	

# Peripherals

General Settings		
InputDevice Mode*	Off v	
Pairing CiscoTouchPanels RemotePairing <sup>*</sup>	On •	
Profile		
TouchPanels*	0 ~	
Cameras*	0 ~	
ControlSystems*	NotSet v	

# <u>Proximity</u>

General Settings		
Mode*	Off	♥ *
Services		
ContentShare		
ToClients*	Disabled	*
FromClients*	Enabled	*
CallControl*	Disabled	v)#

#### <u>User Management</u>

# <u>Video</u>

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*	Auto	~	
Resolution*	3840_2160_60	v	
Connector 2			
MonitorRole*	Auto	~	
RGBQuantizationRange*	Full	~	
Resolution*	Auto	~	
Location			
HorizontalOffset	1		
VerticalOffset	0		
CEC			
Mode*	On	~	
Presentation			
DefaultSource*	2	~	
Priority*	Equal	~	
Selfview			
Default			
FullscreenMode*	Current	~	
Mode*	Current	~	
OnMonitorRole*	Current	~	
PIPPosition *	Current	<b>v</b>	
OnCall			
Duration	10		
Mode*	On	~	

#### Voice Control

General Settings			
Wakeword Mode*	On	~	
	-		

#### <u>Web Engine</u>

Off	v
Off	~
On	v
	Off Off On

#### <u>Webex</u>

General Settings		
CloudProximity Mode*	Off v	j

# Room Cleanup

AutoRun			
HourOfDay	0		
ContentType			
Whiteboards*	Daily	~	
WebData*	Daily	~	

# <u>Bookings</u>

v

#### **Miscellaneous**

General Settings		
Configuration Control Mode*	Unified CM and Endpoint	
Room Name (from Exchange(R))		#
LoadServer		#
Webex Devices Onboarding Token		#
- Admin username and password-		
Autoria abernanie ana passitora		_
Admin Username	admin	#
Admin Password		#
Customization Provisioning		
customization Provisioning		
Customization File		#
Customization Hash Type*	SHA512 v	
Customization Hash		#

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

Product Specific Confi	iguration Layout		
?	Parameter Value		Pull xConfig. from device
i-Note: Endpoints runn These parameters are in	ing software versions earlier than CE dicated below with the # symbol.	9.8 only support provisioning a limited set of p	arameters from Cisco Unified CM.
Audio	General Settings		
	DefaultVolume	50	#
Bluetooth	Ultrasound MaxVolume	70	
BYOD	USB Mode*	SpeakerAndMicrophone	~
CallHistory			
Cameras	HDMI 1		
	Level	0	
Conference	Mode*	On	~
FacilityService	MicrophoneMode*	Focused	~
HttpClient	USBC 1		
	Level	0	
HttpFeedback	Mode*	On	~
Logging	Microphones		
Macros	Mute		
NetworkServices	Enabled *	True	~
Phonebook	NoiseRemoval	Manual	
RoomAnalytics	Mode	manual	
RoomScheduler	PingTone	Suprise	
SIP	RingVolume	50	
Security	- KevClickDetector		
SerialPort	Enabled*	False	~
	Attenuate*	True	~
Standby			
Systemonic			
UserInterface			
Peripherals			
Proximity			
UserManagement			
Video			
VoiceControl			
WebEngine			
Webex			
RoomCleanup			
Bookings			
Miscellaneous			

#### <u>Audio</u>

General Settings		
DefaultVolume	50 #	
Ultrasound MaxVolume	70	
USB Mode*	SpeakerAndMicrophone v	
Input		
HDMI 1		
Level	0	
Mode*	On v	
MicrophoneMode*	Focused v	
USBC 1		
Level	0	
Mode*	On v	
Microphones		
Enabled*	True v	
NoiseRemoval		
Mode*	Manual v	
SoundsAndAlerts		
RingTone	Sunrise	
RingVolume	50	
KeyClickDetector		
Enabled*	False v	
Attenuate*	True v	

#### <u>Bluetooth</u>

General Settings		
Allowed*	True ~	
Enabled*	False v	

#### <u>BYOD</u>

HidForwarding Enabled* False	~	
TouchForwarding Enabled* True	<b>v</b>	

#### Call History

General Settings		
Mode*	On	, ¢

#### **Cameras**

Background			
background			
Enabled*	False	~	
UserImagesAllowed*	True	~	
PowerLine Frequency*	Auto	~	
SpeakerTrack Mode*	Auto	<b>~</b>	
Camera			
Brightness			
DefaultLevel	20		
Mode*	Auto	~	
ExposureCompensation			
Level	0		

#### **Conference**

- DefaultCall			
Delautean			
Protocol*	Sip	~ <i>*</i>	
Rate	6000		
DoNotDisturb DefaultTimeout	60		
Encryption Mode*	BestEffort	~	
FarendMessage Mode*	Off	~	
MaxReceiveCallRate	6000		
MaxTotalReceiveCallRate	15000	×	
MaxTotalTransmitCallRate	15000	<i>#</i>	
MaxTransmitCallRate	6000		
MicUnmuteOnDisconnect Mode*	On	v )#	
Multipoint Mode*	Auto	~ *	
FarEndControl			
Mode*	On	*	
SignalCapability*	On	~ *	

#### **Facility Service**

Service 1		
CallType*	Video	▼ <sup>#</sup>
Name	Live Support	#
Number		#
Туре*	Helpdesk	*
Service 2		
CallType*	Video	<b>v</b>
Name		
Number		
Type*	Helpdesk	v
Service 3		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	<b>v</b>
Service 4		
CallType*	Video	<b>v</b>
Name		
Number		
Type*	Helpdesk	•
Service 5		
CallType*	Video	<b>v</b>
Name		
Number		
Type*	Helpdesk	<b>v</b>

# HTTP Client

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

# HTTP Feedback

General Settings			
TIsVerify*	On	~	
UseHttpProxy*	On	~	

# <u>Logging</u>

General Settings			
CloudUpload Mode*	Off	~	
Internal Mode*	On	~	
External			
Mode*	Off	~	
Protocol*	SyslogTLS	~	
TIsVerify*	On	~	
Server			
Address			
Port	514		

#### <u>Macros</u>

General Settings		
AutoStart*	On v	)
Mode*	Off v	)
UnresponsiveTimeout	5	

#### **Network Services**

General Settings		
H323 Mode*	Off	~
UPnP Mode*	On	<b>v</b>
Websocket*	Off	<b>v</b>
WelcomeText*	On	<b>v</b>
Wifi Allowed*	True	<b>v</b>
НТТР		
Mode*	Off	✓ <sup>#</sup>
Proxy		
Mode*	Off	<b>v</b>
Url		
LoginName		
Password		
PACUrl		
HTTPS-		
VerifyClientCertificate*	Off	<b>v</b>
StrictTransportSecurity*	Off	▼
Server		
MinimumTLSVersion*	TLSv1.1	<b>v</b>
_ SNMP		
Sime -		
CommunityName		
Mode -	Off	<u> </u>
SystemContact		
SystemLocation		
SSH		
HostKeyAlgorithm*	RSA	<b>v</b>
Mode*	Off	v)*
SMTP		
Mode*	Off	*
Server		*
Port	0	#
Security*	StartTls	✓ <sup>#</sup>
Username		#
Password		#
From		#

# <u>Phone Book</u>

Server 1		
ID		
Type*	CUCM	✓ )#
URL		#
Pagination*	Enabled	~
TIsVerify*	On	~

#### **Room Analytics**

General Settings		
PeopleCountOutOfCall*	Off	~
PeoplePresenceDetector*	Off	~
AmbientNoiseEstimation		
Mode*	Off	~
Interval	10	

#### Room Scheduler

General Settings		
Enabled*	False v	

# <u>SIP</u>

General Settings		
MinimumTLSVersion*	TLSv1.0	<b>v</b>

#### <u>Security</u>

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

#### Serial Port

. .

\_

General Settings		
BaudRate*	115200	•
LoginRequired *	On v	1
Mode*	On v	)

## <u>Standby</u>

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

Url		
Mode*	Off	~
InteractionMode*	NonInteractive	~
RefreshInterval	0	
Audio*	Off	~

#### System Unit

General Settings	
CustomDeviceId	
Name	#
CrashReporting	
Mode*	Off v
URL	#

# User Interface

#### General Settings Accessibility IncomingCallNotification Default v # Bookings Visibility Title\* × Auto ContactInfo Type\* Auto $\mathbf{v}$ Diagnostics Notifications\* Auto × Branding AwakeBranding Colors\* × Auto KeyTones Mode\* Off × SoundEffects Mode\* On × Proximity Notifications\* Auto V CustomMessage # Whiteboard ActivityIndicators\* On × Assistant Mode\* On $\mathbf{v}$ Security Mode\* Normal ×

Features			
HideAll*	False	~	
Call			
Start*	Auto	~	
MidCallControls*	Auto	~	
End*	Auto	~	
JoinWebex*	Auto	~ *	
Keypad*	Auto	~	
MusicMode*	Hidden	~	
Share			
Start*	Auto	~	
Whiteheard			
Stort*	Auto		
Start	Auto		
OSD			
EncryptionIndicator*	Auto	*	
Output*	1	~	
HalfwakeMessage			
Mode*	Auto	~	
Phonebook			
Mode*	ReadWrite	~	
DefaultSearchFilter*	All	<b>~</b>	
SettingeMenu			

# SettingsMenu Mode\* Unlocked Visibility\*

#### **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 v
Services	
ContentShare	
ToClients*	Disabled v #
FromClients*	Enabled v#
CallControl*	Disabled v#

#### <u>User Management</u>

LDAP	
Mode*	(Off ~ )#
Encryption*	LDAPS v
VerifyServerCertificate*	Off v
BaseDN	¢
Attribute	R
MinimumTLSVersion*	TLSv1.2 v
Server	
Address	<i>#</i>
Port	0 #
Admin	
Group	ð
Filter	#
PasswordPolicy	
ReuseLimit	12
MaxLifetime	0
Complexity	
MinimumLength	8
MinimumUppercase	0
MinimumLowercase	0
MinimumDigits	0
MinimumSpecial	0

# <u>Video</u>

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	<b>~</b>	
Mode*	Off	~	
CEC			
Mode*	On	~	
Monitors*	Auto	~	
DefaultMainSource*	1	~	

Output	
Connector 1	
BrightnessMode*	Auto v
Resolution *	3840_2160_60 ~
Connector 2	
MonitorRole*	Auto
RGBQuantizationRange*	Full v
Resolution *	Auto v
Location	
HorizontalOffset	1
VerticalOffset	0
CEC	
Mode*	On v
Presentation	
DefaultSource*	2
Polosta *	
Priority *	Equal
Selfview	
Default	
FullscreenMode*	Current v
Mode*	Current v
OnMonitorRole*	Current ~
PIPPosition*	Current v
OnCall	
Duration	10
Mode*	On v

# Voice Control

General Settings			
Wakeword Mode*	On	v	

#### <u>Web Engine</u>

General Settings	
Mode*	Off v
RemoteDebugging*	Off ~
UseHttpProxy*	On v
MinimumTLSVersion*	TLSv1.1 v

# <u>Webex</u>

General Settings			
Meetings JoinProtocol*	SIP	~	
CloudUpgrades Mode*	Off	~	
CloudProximity			
Mode*	Off	~	
GuestShare*	Auto	~	

#### Room Cleanup

AutoRun			
HourOfDay	0		
ContentType			
Whiteboards*	Daily	×	
WebData*	Daily	~	

# <u>Bookings</u>

General Settings		
ProtocolPriority*	Auto	J

# <u>Miscellaneous</u>

General Settings		
ouncial occurigo		
Configuration Control Mode*	Unified CM and Endpoint	
Room Name (from Exchange(R))		*
LoadServer		*
Webex Devices Onboarding Token		*
- Admin username and password-		
Admin username and password—		
Admin Username	admin	*
Admin Password		#
Customization Provisioning		
_		
Customization File		Ŧ
Customization Hash Type*	SHA512 v	
Customization Hash		*
### Cisco Desk Configuration Options (versions 12.5 and later)

Parameter Value		
		Pull xConfig. from device
ning software versions earlier than CE dicated below with the # symbol.	9.8 only support provisioning a limited set of	f parameters from Cisco Unified CM.
General Settings		
DefaultVolume	50	#
Input MicrophoneMode*	Focused	~
Ultrasound MaxVolume	70	
USB Mode*	SpeakerAndMicrophone	~
Microphones		
Mute Enabled *	True	~
NoiseRemoval	Manual	
Mode	Мапцаі	•
SoundsAndAlerts		
RingTone	Sunrise	
RingVolume	50	
	General Settings DefaultVolume Input MicrophoneMode* Ultrasound MaxVolume USB Mode* Microphones Mute Enabled * NoiseRemoval Mode* SoundsAndAlerts RingTone RingVolume	dicated below with the # symbol.          General Settings       50         Input MicrophoneMode*       Focused         Ultrasound MaxVolume       70         USB Mode*       SpeakerAndMicrophone         Microphones       Mute         Enabled*       True         NoiseRemoval       Mode*         Mode*       Sunrise         RingTone       Sunrise         RingVolume       50

#### <u>Audio</u>

General Settings	
DefaultVolume	50 #
Input MicrophoneMode*	Focused
Ultrasound MaxVolume	70
USB Mode*	SpeakerAndMicrophone V
Missonhauss	
Microphones	
Mute	
Enabled *	True v
NoiseRemoval	
Mode*	Manual v
SoundsAndAlerts	
RingTone	Sunrise
RingVolume	50

#### <u>Bluetooth</u>

General Settings			
Allowed*	True	~	
Enabled*	False	~	

### Call History

General Settings		
Mode*	On v	ø

#### <u>Cameras</u>

Background			
Enabled*	True	~	
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	6000	#
MaxTotalTransmitCallRate	6000	Ŧ
MaxTransmitCallRate	6000	
MicUnmuteOnDisconnect Mode*	On	*
Multipoint Mode*	Auto	*
-FarEndControl		
Mode*	On	*
SignalCapability *	On	*

#### Facility Service

.

Service 1		
CallType*	Video	*
Name	Live Support	#
Number		#
Туре*	Helpdesk	<b>∼</b> )#
Service 2		
CallType*	Video	~
Name		
Number		
Туре*	Helpdesk	~
Service 3		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	<b>v</b>
Service 4		
CallType*	Video	<b>v</b>
Name		
Number		
Туре*	Helpdesk	<b>v</b>
Service 5		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	v

#### HTTP Client

General Settings		
Mode*	Off	~
AllowInsecureHTTPS*	False	~
AllowHTTP*	True	<b>v</b> )
UseHttpProxy*	On	~

### HTTP Feedback

General Settings			
TIsVerify*	On	~	
UseHttpProxy*	On	<b>v</b>	

### Logging

General Settings			
<b>j</b> -			
CloudUpload Mode*	Off	~	
Internal Mode*	On	~	
External			
external			
Mode*	Off	<b>v</b>	
Protocol*	SyslogTLS	~	
TIsVerify*	On	<b>v</b>	
Server			
Address			
Port	514		

#### <u>Macros</u>

1	General Settings		
	AutoStart*	On v	
	Mode*	Off v	
	UnresponsiveTimeout	5	

#### **Network Services**

General Settings		
H323 Mode*	Off	~
UPnP Mode*	On	~
Websocket*	FollowHTTPService	~
WelcomeText*	On	~
Wifi Allowed*	True	~
Mode*	Off	*
Broxy		
Mode*	Off	~
Url		
LoginName		
PACUrl		
HTTPS		
VerifyClientCertificate*	Off	~
StrictTransportSecurity*	Off	~
Server		
MinimumTLSVersion *	TLSv1.1	~
SNMP		
CommunityName		
Mode*	Off	<b>v</b>
SystemContact		
SystemLocation		
SSH		
HostKeyAlgorithm*	RSA	~
Mode*	Off	✓ +
SMTP		
Mode*	Off	✓ )#
Server		#
Port	0	#
Security*	StartTis	*
Username		#
From		#

### <u>Phone Book</u>

Server 1		
ID		
Type*	CUCM	v )#
URL		*
Pagination*	Enabled	~
TIsVerify*	On	~

### **Room Analytics**

Cisco RoomOS Series Wireless LAN Deployment Guide

- General Settings-			
Ceneral Dettings			
PeopleCountOutOfCall*	Off	~	
PeoplePresenceDetector*	Off	~	
AmbientNoiseEstimation			
Mode*	Off	~	
Interval	10		
ReverberationTime			
Mode*	Off	~	
Interval	1800		

### Room Scheduler

General Settings			
Enabled*	False	~	

### <u>SIP</u>

General Settings		
MinimumTLSVersion*	TLSv1.0	0

### <u>Security</u>

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

#### <u>Serial Port</u>

General Settings		
BaudRate*	115200	~
LoginRequired*	On	v)#
Mode*	On	~ *

# <u>Standby</u>

General Settings		
BootAction*	DefaultCameraPosition	~
Control*	On	♥ #
Delay	10	#
StandbyAction *	PrivacyPosition	✓ #
WakeupAction *	RestoreCameraPosition	~
WakeupOnMotionDetection*	Off	✓ #

Signage			
Url			
Mode*	Off	~	
RefreshInterval	0		
Audio*	Off	~	

### <u>System Unit</u>

General Settings	
CustomDeviceId	
Name	#
CrashReporting	
Mode*	Off v
URL	#

### User Interface

- General Settings		
Accessibility IncomingCallNotification *	Default v)*	
Bookings Visibility Title*	Auto	
ContactInfo Type*	Auto	
Diagnostics Notifications*	Auto	
Branding AwakeBranding Colors*	Auto	
KeyTones Mode*	On 🗸	
SoundEffects Mode*	On v	
Proximity Notifications*	Auto	
CustomMessage	#	
Whiteboard ActivityIndicators*	On v	
Assistant Mode*	On 🗸	
Security Mode*	Normal	
Features		
HideAll*	False v	
Call		
Start*	Auto	
MidCallControls*	Auto	
End*	Auto	
VideoMute*	Auto	
JoinWebex*	Auto v#	
Keypad*	Auto	
MusicMode*	Hidden v	
Chare		
Start*	Auto	
2.2.1		
Whiteboard		
Start*	Auto	
- OSD		
EncryptionIndicator*	Auto v	
Output*	↓	
HalfwakeMessage		
Mode*	Auto	
Phonebook		
Mode*	PaadWrite	
DefaultSearchFilter*		
SettingsMenu		
Mode*	Unlocked v	
Visibility*	Auto	

#### **Peripherals**

-General Settings			
General Settings			
InputDevice Mode*	Off	~	
Pairing CiscoTouchPanels	On	~	
RemotePairing*			
Profile			
Frome			
TouchPanels*	0	~	
- *			
Cameras*	Minimum1	~	
ControlSystems*	NotSet	× I	
Controisystems	NOLSEL	•	

#### **Proximity**

General Settings		
Mode* AlternatePort Enabled*	Off False	*
Services		
ContentShare		
ToClients*	Disabled	✔ #
FromClients*	Enabled	*
CallControl*	Disabled	✓ #

# User Management

LDAP		
Mode*	Off v	
Encryption*	LDAPS v	
VerifyServerCertificate*	Off v	
BaseDN		#
Attribute		#
MinimumTLSVersion*	TLSv1.2 v	
Server		
Address		<i>#</i>
Port	0	ð.
Admin		_
Group		ð
Filter		ð.
- PasswordPolicy		
ReuseLimit	12	]
MaxLifetime	0	]
Complexity		
MinimumLength	8	
MinimumUppercase	0	
MinimumLowercase	0	
MinimumDigits	0	
MinimumSpecial	0	

### <u>Video</u>

-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*	2	<b>v</b>
Priority*	Equal	~
- Selfview		
FullscreenMode*	Current	~
Mode*	Current	~
OnMonitorRole*	Current	<b>v</b>
PIPPosition*	Current	~
0.0.0		
OnCall		
Duration	10	
Mode*	Off	~

#### Voice Control

Γ	General Settings		
	Wakeword Mode*	(On v)	

#### Web Engine

General Settings		
Mode*	Off	~
RemoteDebugging*	Off	~
UseHttpProxy*	On	~
MinimumTLSVersion*	TLSv1.1	~

### <u>Webex</u>

General Settings			
Meetings JoinProtocol* CloudUpgrades Mode*	SIP	<b>v</b>	
CloudProximity			
Mode*	Off	▼	
GuestShare*	Auto	<b>v</b>	

### Room Cleanup

AutoRun		
HourOfDay	0	
ContentType		
Whiteboards*	Daily	
WebData *	Daily	

#### <u>Bookings</u>

General Settings			
ProtocolPriority*	Auto	~	

### <u>Miscellaneous</u>

- General Settings		
Seneral Sectings		
Configuration Control Mode*	Unified CM and Endpoint	
Room Name (from Exchange(R))		#
LoadServer		*
Webex Devices Onboarding Token		*
- Admin username and nassword-		
Autim username and password		
Admin Username	admin	#
Admin Password		*
		<u> </u>
Customization Provisioning		
customization revisioning		_
Customization File		#
Customization Hash Type*	SHA512 v	
Customization Hash		*

### Cisco Desk Mini Configuration Options (versions 12.5 and later)

Product Specific Con	figuration Layout		
?	Parameter Value		Pull xConfig. from device
i-Note: Endpoints run These parameters are in	ning software versions earlier than CE ndicated below with the # symbol.	9.8 only support provisioning a limited set of pa	rameters from Cisco Unified CM.
Audio	General Settings		
Bluetooth	DefaultVolume	50	#
	Input MicrophoneMode*	Focused	~
CallHistory	Ultrasound MaxVolume	70	
Cameras	USB Mode*	SpeakerAndMicrophone	×
Conference	Microphones		
FacilityService	Mute Enabled *	True	~
HttpClient	NoiseRemoval		
HttpFeedback	Mode*	Manual	~
Logging	SoundsAndAlerts		
Macros	RingTone	Sunrise	
	RingVolume	50	
NetworkServices			

# <u>Audio</u>

-General Settings	
General Settings	
DefaultVolume	50 #
Input MicrophoneMode*	Focused v
Ultrasound MaxVolume	70
USB Mode*	SpeakerAndMicrophone v
Microphones	
Mute	
Enabled*	True 🗸
NoiseRemoval	
Mode*	Manual v
SoundsAndAlerts	
o o un us ran un de las	
RingTone	Sunrise
RingVolume	50

#### <u>Bluetooth</u>

-General Settings		
Allowed*	True	~
Enabled*	False	~

# Call History

General Settings		
Mode*	On	✓ <sup>#</sup>

### <u>Cameras</u>

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 v
ConnectorDetection	
Mode*	Auto 🗸
CameraRight	2
CameraLeft	1

### <u>Conference</u>

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		#
Туре*	Helpdesk	<b>∼</b> )#
Service 2		
CallType*	Video	~
Name		
Number		
Туре*	Helpdesk	~
Service 3		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	<b>v</b>
Service 4		
CallType*	Video	<b>v</b>
Name		
Number		
Туре*	Helpdesk	<b>v</b>
Service 5		
CallType*	Video	~
Name		
Number		
Type*	Helpdesk	v

#### HTTP Client

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

### HTTP Feedback

General Settings			
TIsVerify*	On	~	
UseHttpProxy*	On	~	

### Logging

General Settings			
<b>j</b> -			
CloudUpload Mode*	Off	~	
Internal Mode*	On	~	
External			
external			
Mode*	Off	~	
Protocol*	SyslogTLS	~	
TIsVerify*	On	<b>v</b>	
Server			
Address			
Port	514		

#### <u>Macros</u>

General Settings		
	<u></u>	
AutoStart*	On	v
Mode*	Off	~
UnresponsiveTimeout	5	

#### **Network Services**

General Settings		
H323 Mode*	Off	~
UPnP Mode*	On	~
Websocket*	FollowHTTPService	~
WelcomeText*	On	~
Wifi Allowed*	True	~
Mode*	Off	*
Broyv		
Mode*	Off	~
Url		
LoginName		
PACUrl		
HTTPS		
VerifyClientCertificate*	Off	~
StrictTransportSecurity*	Off	~
Server		
MinimumTLSVersion *	TLSv1.1	~
SNMP		
CommunityName		
Mode*	Off	<b>v</b>
SystemContact		
SystemLocation		
SSH		
HostKeyAlgorithm*	RSA	~
Mode*	Off	✓ +
SMTP		
Mode*	Off	✓ )#
Server		#
Port	0	#
Security*	StartTis	*
Username		#
From		#

### <u>Phone Book</u>

Server 1		
ID		
Type*	CUCM	v )#
URL		*
Pagination*	Enabled	~
TIsVerify*	On	~

### **Room Analytics**

Cisco RoomOS Series Wireless LAN Deployment Guide

- General Settings			
General Dectings			
PeopleCountOutOfCall*	Off	~	
PeoplePresenceDetector*	Off	~	
AmbientNoiseEstimation ——			
Mode*	Off	~	
Interval	10		
ReverberationTime			
Mode*	Off	~	
Interval	1800		

### Room Scheduler

General Settings			
Enabled*	False	~	

### <u>SIP</u>

General Settings			
MinimumTLSVersion*	TLSv1.0	~	

### <u>Security</u>

Audit		
Logging		
Mode*	Internal	~
OpError		
Action*	Tapara	
Action	Ignore	<b>`</b>
Server		
Address		
Port	514	
PortAssignment*	Auto	~
Fips Mode*	Off	~
Saccion		
Session		
InactivityTimeout	0	
ShowLastLogon*	Off	v
MaxTotalSessions	20	
MaxSessionsPerUser	20	
MaxFailedLogins	0	
FailedLoginsLockoutTime	60	

#### <u>Serial Port</u>

General Settings		
BaudRate*	115200	~
LoginRequired*	On	v)#
Mode*	On	<b>~</b> ]#

# <u>Standby</u>

General Settings		
BootAction*	DefaultCameraPosition	~
Control*	On	♥ #
Delay	10	#
StandbyAction *	PrivacyPosition	✓ #
WakeupAction *	RestoreCameraPosition	~
WakeupOnMotionDetection*	Off	✓ #

Signage			
Url			
Mode*	Off	~	
RefreshInterval	0		
Audio*	Off	~	

### <u>System Unit</u>

General Settings	
CustomDeviceId	
Name	#
CrashReporting	
Mode*	Off v
URL	#

### User Interface

- General Settings		
Accessibility IncomingCallNotification *	Default v)*	
Bookings Visibility Title*	Auto	
ContactInfo Type*	Auto	
Diagnostics Notifications*	Auto	
Branding AwakeBranding Colors*	Auto 🗸	
KeyTones Mode*	On v	
SoundEffects Mode*	On v	
Proximity Notifications*	Auto	
CustomMessage	#	
Whiteboard ActivityIndicators*	On v	
Assistant Mode*	On 🗸	
Security Mode*	Normal	
Features		
HideAll*	False v	
Call		
Start*	Auto	
MidCallControls*	Auto	
End*	Auto	
VideoMute*	Auto	
JoinWebex*	Auto v#	
Keypad*	Auto	
MusicMode*	Hidden v	
Chare		
Start*	Auto	
2.2.1		
Whiteboard		
Start*	Auto	
- OSD		
EncryptionIndicator*	Auto v	
Output*	↓	
HalfwakeMessage		
Mode*	Auto	
Phonebook		
Mode*	PaadWrite	
DefaultSearchFilter*		
SettingsMenu		
Mode*	Unlocked v	
Visibility*	Auto	

### **Peripherals**

-General Settings			
General Settings			
InputDevice Mode*	Off	~	
Pairing CiscoTouchPanels	On	~	
RemotePairing*			
Profile			
Frome			
TouchPanels*	0	~	
- *			
Cameras*	Minimum1	~	
ControlSystems*	NotSet	× I	
Controisystems	NOLSEL	•	

#### **Proximity**

General Settings		
Mode* AlternatePort Enabled*	Off False	*
Services		
ContentShare		
ToClients*	Disabled	✔ #
FromClients*	Enabled	*
CallControl*	Disabled	✓ #

# User Management

LUAP		
Mode*	Off v	
Encryption*	LDAPS v	
VerifyServerCertificate*	Off v	
BaseDN		#
Attribute		#
MinimumTLSVersion*	TLSv1.2 v	
Server		
Address		)#
Port	0	<i>#</i>
Admin		
Group		ð.
Filter		ø
PasswordPolicy		
ReuseLimit	12	]
MaxLifetime	0	]
Complexity		
MinimumLength	8	
MinimumUppercase	0	]
MinimumLowercase	0	
MinimumDigits	0	
MinimumSpecial	0	]

### <u>Video</u>

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 v	]
Mode*	Current v	]
OnMonitorRole*	Current	]
PIPPosition*	Current V	]
OnCall		
Duration	10	
Mode*	Off v	)

#### Voice Control

General Settings			
Wakeword Mode*	On	~	

### <u>Web Engine</u>

#### General Settings

Mode*	Off v
RemoteDebugging*	Off v
UseHttpProxy*	On v
MinimumTLSVersion*	TLSv1.1 ~

#### <u>Webex</u>

General Settings		
Meetings JoinProtocol*	SIP	~
CloudUpgrades Mode*	Off	~
CloudProximity		
Mode*	Off	~
GuestShare*	Auto	~

# Room Cleanup

AutoRun		
HourOfDay	0	
ContentType		
Whiteboards*	Daily	~
WebData *	Daily	~

#### <u>Bookings</u>

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	*
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.

 $\underline{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}$ 

# **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.

Welcome
English
English (United States) Norwegian Norsk
German Deutsch French
Français (France) Arabic
Start
← Use the old onboarding

- 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	AES
		WPA2-PSK-SHA256	ТКІР
		WPA2-PSK	
Enterprise	FAST	WPA3-802.1X-SHA256	AES
	PEAP	WPA2-802.1X-SHA256	ТКІР
	TLS	WPA2-802.1X	
	TTLS		

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

$\left( \leftarrow \right)$		Network connecti • Not Connected	on	
	((1-	Wi-Fi	Not connected	>
	8	Ethernet	Not connected	>
	2	Network Status		>
	*	Advanced Network Settings		>
		Continue without netwo	ork	

#### 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.

( <del>c</del> )	<b>₩i-Fi</b> ● Nat Connected	
	Wi-Fi	
	Networks	
	2wire421	
	7736475884	
	AdorableWiFi_5G	
	Akrietta	
	ATTebBNC8s	
	Join other network	>

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

	$\leftarrow$				Enter	the pa	<b>psk</b> assphra	ase for p	sk							
										0						
											1	2 ABC 5	3 DEF			
~ ~	z 2.?123	×		9						Enter	GHI 7 PQRS *	зкі 8 тич 0 +	9 WXYZ #			

- 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.

$\leftarrow$	eap		
	Security	Enterprise	
	Authentication method	PEAP >	
	Anonymous identity (optional)		
	Username		
	Passphrase	٢	
$\left( \leftarrow \right)$	eap		
	Security	Enterprise	
	Authentication method	EAP-FAST	
	Anonymous identity (optional)		
	Username		
	Passphrase		
	Continue		

$\leftarrow$	eap	
	Security	Enterprise
	Authentication method	EAP-TTLS
	Anonymous identity (optional)	
	Username	
	Passphrase	٢

• 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.

$(\leftarrow)$	eap		
	<ul> <li>Could not find any client certific</li> </ul>	ates installed	
	Security	Enterprise	
	Authentication method	EAP-TLS	
	Anonymous identity (optional)		

#### 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.

$\left( \leftarrow \right)$	Wi-Fi • Not Connected		
	Wi-Fi		
	Networks		
	2wire421		
	7736475884		
	AdorableWiFi_5G		
	Akrietta		
	ATTebBNC8s		
	Join other network	>	

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

	$\leftarrow$		Join	other net	work						
		Network Na	me								
		Security				None 📏					
	w e					₽ X		2	3		
							<b>4</b> GHI	5 JKL	6 MNO		
							7 PORS	8 TUV	9 wxyz		
.?						om Enter	*				

• 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**.

	÷				Join	other ne	etwork	<b>,</b>							
		Ne	twork N	lame											
		Se	curity					Pers	onal >						
		Pa	ssphras	se			(		0						
									$\boxtimes$		2 ABC	3 DEF			
										4 GHI	5 JKL	6 MNO			
									^	7 PQRS	8 TUV	9 wxyz			
ê									Enter						

- 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.

( <del>&lt;</del> )	Join other net	twork			
	Network Name				
	Security	Enterprise >			
	Anonymous Identity				
	Username				
	Passphrase				
	Authentication Method	PEAP			
		• • ×	1 2 ABC	3 DEF	
			4 5 GHI JKL 7 8	6 мю 9	
.?123		@ .com Enter	PQRS TUV * 0	WXX7Z #	

$\left( \leftarrow \right)$	Join other networ	ĸ		
	Network Name		)	
	Security	Enterprise >		
	Anonymous Identity			
	Username			
	Passphrase			
	Authentication Method	EAP-FAST		
		° X	1 2 ABC	3 DEF
			4 5 GHI JKL	6 MINO
	c v b n m . @	.com Enter	PQRS TUV	wxrz #
(<)	Join other networ	k		
	Network Name		)	
	Security	Enterprise 📏	/	
	Anonymous Identity			
	Username			
	Passphrase			
	Authentication Method	EAP-TTLS		
	r t y u i o	▶ 🔇	1 2 	3 DEF
			4 5 GHI JKL	6 MNO
∧ z ×	cvbnm.	.com Enter	7 8 PQRS TUV * 0	9 wxvz #
<b>~</b> 1				

• 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.

(<)	Join other ne	etwork			
	Could not find any client				
	Network Name				
	Security	Enterprise >			
	Anonymous Identity				
	Authentication Method	EAP-TLS			
	r t y u i				
		k I	4 5 GHI JKL	6 MINO	
			7 8 PQRS TUV	9 MXYZ	
.?123		@ .com Enter			

#### **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.

¢	Networ	<b>'k connection</b> Connected	
ę	Wi-Fi	xroads	>
**	Ethernet	Not connected	>
6	Network Status		>
*	Advanced Network	Settings	>
		Continue	

$\leftarrow$	Advanced network	Apply Apply	
	IP Stack		
	IPv4 and IPv6		
	IPv4		
	IPv6		
	DNS		
	DNS Domain Name		
	DNS address 1		
	DNS address 2		
	UNIS addrace 3		
	Advanced natwork	v cattings	
( <del>c</del> )	Advanced network	< settings Apply	
<ul> <li>••</li> </ul>	Advanced network נוזע טטחשות Name DNS address 1	c settings Apply	
¢	Advanced network UNS Jomain Name DNS address 1 DNS address 2	x settings Apply	
( <del>``</del>	Advanced network	c settings Apply	
( <del>(</del>	Advanced network URS Domain Name DNS address 1 DNS address 2 DNS address 3 HTTP Proxy	c settings Apply	
( <del>c</del> )	Advanced network	Apply	
( <del>(</del>	Advanced network URS Umain Name DNS address 1 DNS address 2 DNS address 3 HTTP Proxy Off	Apply	
( <del>``</del>	Advanced network UNS Jomain Name DNS address 1 DNS address 2 DNS address 3 iTTTP Proxy Off Manual WPAD	Apply	

	$\left( \leftarrow \right)$	Advanced network settings	Apply	
	HTTP Proxy			
	Off			
	Manual			
	WPAD			
	PAC URL			
	Proxy Host			
	Proxy Port			
	Proxy serve	er requires authentication		
		Reset all to default		
		y u i o p 🗙	1 2 ABC	3 DEF
	a s d f g		4 5 GHI JKL	6 MINO
^ 	z x c v	b n m . / A	PQRS TUV	worz #
~				
		Advanced potwork pattings	Apply	
	÷	Advanced network settings	Apply	
	C DNS address	Advanced network settings	Apply	
	C DNS address : DNS address :	Advanced network settings	Apply	
	C DNS address : DNS address : DNS address :	Advanced network settings	Apply	
	C DNS address : DNS address : DNS address : HTTP Proxy	Advanced network settings	Apply	
	C DNS address : DNS address : DNS address : HTTP Proxy Off	Advanced network settings	Apply	
	C DNS address DNS address DNS address HTTP Proxy Off Manual	Advanced network settings	Apply	
	C DNS address : DNS address : DNS address : HTTP Proxy Off Manual WPAD	Advanced network settings	Apply	
	CNS address DNS address DNS address DNS address DNS address I DNS address I HTTP Proxy Off Manual WPAD PAC URL	Advanced network settings	Apply	
	C DNS address DNS address DNS address UNS address HTTP Proxy Off Manual WPAD PAC URL	Advanced network settings	Apply	
	C DNS address 3 DNS address 3 DNS address 3 DNS address 3 ONS address 3 ONS address 3 ONS address 3 ONS address 3 DNS address 3	Advanced network settings	Apply	
	CNS address : DNS address : DNS address : DNS address : DNS address : HTTP Proxy Off Manual WPAD PAC URL	Advanced network settings	Apply	
	C DNS address DNS address DNS address UNS address HTTP Proxy Off Manual WPAD PAC URL	Advanced network settings	Apply	

(~)	Advanced netwo	ork settings	Apply
	DNS address 2		
	DNS address 3		
	HTTP Proxy		
	Off		
	Manual		
	WPAD		
	PAC URL		
	Enter PAC URL		
	Reset all to d	default	

**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:

 $\underline{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html}$ 

### **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.

Cisco Webex Local Device Controls		Q Find page 💿 🙎
10.81.12.22 Desk Pro	⊘ Certificates     ∋ Sign-in Banner	
S₀ Call SETUP ⊕ Settings ⊖ Users ⊖ Security	Services         Custom         Preinstalled           Add Certificate         Use the form below to add new certificates.           This system supports PEM formatted certificate files (.pem). The certificate private key with or without a passphrase. Optionally the private key file ma Certificate           Certificate         Browse	a file may contain the certificate and a RSA or DSA encrypted y be supplied separately.
CUSTOMIZATION C3 Personalization C UI Extensions Editor T Macro Editor C Developer API	Private key Browse No file selected. (optional) Passphrase (optional) Upload	
SYSTEM MAINTENANCE	Existing Certificates	
<ul> <li>∿ Issues and Diagnostics</li> <li>⊙ Backup and Recovery</li> </ul>	Certificate Issuer 802.1X Audit HTTPS HttpClie Self-signed Certificate TemporaryDefaultCertificate	Delete View Certificate

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.

Cisco Webex Local Device Controls						Q Find page	)	0	2
10.81.12.22 Desk Pro	Security								
G Home	⊘ Certificates ⊕ Sigr	-in Banner							
% Call	Services Custom Preins	talled							
SETUP	Add Certificate U Ti Pi	se the form below to add new ce his system supports PEM formatt ivate key with or without a passp Certificate Browse Private key Browse (optional) Passphrase (optional)	rtificates. ed certificate files (.p. hrrase. Optionally the No file selected.	em). The certific: private key file n	ate file may contai	in the certificate a	nd a RSA or	r DSA encrypted	
SYSTEM MAINTENANCE	Existing Certificates								
G Software	Certificate	Issuer	802.1X Audit	HTTPS HttpC	Client HttpProxy	SIP Pairing	Actions		
<ul> <li>Backup and Recovery</li> </ul>	Self-signed Certificate	TemporaryDefaultCertificate					Delete	View Certificate	
	sep689e0bb0000d.cisco.com	Cisco Systems Inc.					Delete	View Certificate	

Cisco RoomOS Series Wireless LAN Deployment Guide

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.

Cisco Webex Local Device Controls			Q Find page	0	2
10.81.12.22 Desk Pro	⊘ Certificates				
☆ Home % Call	Services Custom Preinstalled				
serup Settings Users Security	Add Certificate Use the form below to add new cer Authority This system supports PEM formatte Browse No file selected.	tificate authorities. d files (.pem) with one or more CA certificates v	within the file.		
CUSTOMIZATION	Existing Certificate Authorities				
UI Extensions Editor	Certificate Issuer	Details Actions			
Macro Editor     Neveloper API	IdenTrust Commercial Root CA 1 IdenTrust	View Delete			
SYSTEM MAINTENANCE					
G Software					
<ul> <li>∽ Issues and Diagnostics</li> <li>⊙ Backup and Recovery</li> </ul>					

## **Removing Certificates**

Certificates can be removed individually.

To remove an individual user certificate, select **Security > Certificates > Services**, then select **Delete**.

Cisco Webex Local Device Controls								QF	ind page		0	2
10.81.12.22 Desk Pro	Security											
ကြ Home % Call	Certificates     Sign- Services Custom Preinsta	in Banner										
SETUP	Add Certificate Us Thi prin	e the form below to add new cert s system supports PEM formattec vate key with or without a passphi Certificate Browse M Private key Browse M Delete C This will delete certificate so fingerprint e9f86529ccd924	ficates. I certificate ase. Optio Io file sele- Io file sele- Certificate p689e0bb c50b740c2	files (.p. nally the cted. cted. 00000d.cls 025592e Can	em). The private ke	certificate fil ay file may be x /ith 21 klete	e may contai	in the cei	rtificate an	id a RSA oi	r DSA encrypted	
SYSTEM MAINTENANCE	Existing Certificates											
G Software	Certificate	Issuer	802.1X	Audit	HTTPS	HttpClient	HttpProxy	SIP	Pairing	Actions		
<ul> <li>Backup and Recovery</li> </ul>	Self-signed Certificate	TemporaryDefaultCertificate								Delete	View Certificate	
	sep689e0bb0000d.cisco.com	Cisco Systems Inc.								Delete	View Certificate	

To remove an individual user certificate, select **Security > Certificates > Custom**, then select **Delete**.

Cisco Webex Local Device Controls			Q Find page	0	2
10.81.12.22 Desk Pro	Security				
G Home	⊘ Certificates	Banner			
℅ Call	Services Custom Preinstalled	i			
setup Settings Users Security	Add Certificate Use th Authority This sy Brow	e form below to add new certificate authorities. stern supports PEM formatted files (.pem) with one or more CA cert rse No file selected.	aficates within the file.		
CUSTOMIZATION   Personalization  UI Extensions Editor	Existing Certificate Auth	Delete Certificate			
Macro Editor % Developer API	IdenTrust Commercial Root CA 1	with fingerprint df717eaa4ad94ec3558499602d48de5fbcf03a25 Cancel Delete			
SYSTEM MAINTENANCE					
Software					
<ul> <li>Backup and Recovery</li> </ul>					

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

 $\label{eq:http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html$ 

## **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.

Register to Control Hub         Enter your 16-digit Control Hub activation code.         Contact your admin to get an activation code.         1       2         4       5         6         7       8
Enter your 16-digit Control Hub activation code.     Contact your admin to get an activation code.      1 2 3     4 5 6     7 8 9
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$
(4)(5)(6)       (7)(8)(9)
Skip Continue
Skip Continue

## **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.

(F)	Cisco U	Ю	
	Detected Cisco UCM servers	10.35.48.106	
	Automatic configuration		
	Apply	4	

## Cisco Unified Communications Manager (UCM) via Expressway

If Cisco UCM via Expressway is selected under Other Options, enter the Username, Passphrase, and Domain information.

Cisco UCM via Expressway Username Passphrase	
Username Passphrase	
Domain	
Apply	

## **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.

Cisco RoomOS Series Wireless LAN Deployment Guide

• Ensure that **Bluetooth** is set to **On**.

Bluetooth	×
Bluetooth is On	
Discoverable off	
Scanning for available devices	

- Ensure the Bluetooth device is in pairing mode.
  - Select the Bluetooth device after it is displayed in the list.
  - o The Cisco RoomOS Series will then attempt to pair automatically with the Bluetooth device.
  - If unsuccessful, enter the pin code when prompted.
  - o 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/productsmaintenance-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.

migilles-deskpro >	6	:49 PM 🖽
	Join Webex Q Bearch or enter meeting information es	
	Wc You can find the meeting information in your calendar invite e.g: 12345678 or username@example.webex.com	
	qwertyuiop 🐼 123 asdfghjki456 <sub>014</sub> Juliu	
	x         x         v         b         n         n         /         ∧         7         8         9         9         www.z           (m)         .         /         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .         .<	

# Troubleshooting

## **About Device**

Video address, IP address, MAC address, serial number, and version information is displayed in **Settings > About this device**.

## <u>Webex</u>



## **Cisco Unified Communications Manager**

1008 >				😱 AirPlay	8:04 PM 11
	$\leftarrow$		About		
		General			
		Device	Cisco Desk Mini, TANDBERG		
		Video address	1008		
		IP address	10.81.12.25		ſ
		MAC address	20:CF:AE:29:8E:D9		J
		Wi-Fi MAC address	20:CF:AE:29:8E:DA		
		Serial number	FOC2536N3JC		
		SIP proxy	10.195.19.43 (Registered)		

## **Network Connection Status**

The current network connection status and IP address information is displayed in **Settings > Network connection**.

$(\leftarrow)$	Network connection	on	
(í÷	Wi-Fi	xroads	
8	Ethernet	Not connected	
2	Network Status	>	
*	Advanced Network Settings	>	
	Continue		
$\left( \leftarrow \right)$	Notwork status		
	Network status		
	Network status		
IP	stack	IPv4 and IPv6	
IP IP	stack 4 address (DHCP)	IPv4 and IPv6 10.81.12.22	
IP IP	4 address (DHCP)	IPv4 and IPv6 10.81.12.22	
IP IP: IP:	feaddress (DHCP)	IPv4 and IPv6 10.81.12.22	
91 191 191 10	4 address (DHCP) 16 address 18	IPv4 and IPv6 10.81.12.22 64.102.6.247	
91 191 191 10 11 11 11	4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9]  4   4	4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9]  4   4   4   6   1   1   1	Address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9]  4   4   4   6	retwork status stack 4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9] 19] 19] 10 10 11 11	retwork status stack 4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9] 14] 14] 16 17] 17]	Herwork status stack 4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9] 19] 19] 10 10 11 11 11 11 11 11 11 11 11 11 11	stack 4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9] 19] 19] 10] 11] 11] 11] 11] 12] 12] 12] 12] 12] 12	stack 4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9] 19] 19] 11] 11] 11]	stack 4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	
9   4  	stack 4 address (DHCP) 6 address IS TP Proxy	IPv4 and IPv6 10.81.12.22 64.102.6.247 Off	

## **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**.

<b>(</b>	Wi-Fi • Connected		
	Wi-Fi		
	✓ xroads	< In. A	
	Networks		
	2wire421		
	55A958AF		
	acGuest		
	AdorableWiFi		
	Join other network	>	
	Continue		
( <del>\</del>	xroads • Conpected		
( <del>¢</del> )	xroads • Connected Authentication	Enterprise (PEAP)	
(e)	xroads • Connected Authentication	Enterprise (PEAP)	
( <del>¢</del> )	xroads • Connected Authentication Advanced Wi-Fi details	Enterprise (PEAP)	
(<)	xroads • Connected Authentication Advanced Wi-Fi details Forget this netw	Enterprise (PEAP)	
( <del>¢</del> )	xroads • Connected Authentication Advanced Wi-FI details Forget this netwo	Enterprise (PEAP)	
	xroads • Connected Authentication Advanced Wi-Fi details Forget this netw	Enterprise (PEAP)	
( <del>(</del>	xroads • Connected Authentication Advanced Wi-Fi details Forget this netw	Enterprise (PEAP)	
E and the second sec	xroads • Connected Authentication Advanced Wi-Fi details Forget this netw	Enterprise (PEAP)	

SSIDxroadsSpeed173 MbpsFrequency5.18 GHzSignal Strength-38 dBmSNR50 dBmChannel36BSSIDC8-28:E5:EF:-04:7BRegionUS	SSIDxroadsSpeed173 MbpsFrequency5.18 GHzSignal Strength-38 dBmSNR50 dBmChannel36BSSIDC8:28:E5:EF:04:7BRegionUS	SSIDxroadsSpeed173 MbpsFrequency5.18 GHzSignal Strength-38 dBmSNR50 dBmChannel36BSSIDC8:28:E5:EF:04:7BRegionUS	<del>(</del>	A	dvanced Wi-Fi details	
Speed173 MbpsFrequency5.18 GHzSignal Strength-38 dBmSNR50 dBmChannel36BSSIDC8:28:E5:EF:04:7BRegionUS	Speed173 MbpsFrequency5.18 GHzSignal Strength-38 dBmSNR50 dBmChannel36BSSIDC8:28:E5:EF:04:7BRegionUS	Speed173 MbpsFrequency5.18 GHzSignal Strength-38 dBmSNR50 dBmChannel36BSSIDC8:28:£5:EF:04:78RegionUS		SSID	xroads	
Frequency5.18 GHzSignal Strength-38 dBmSNR50 dBmChannel36BSSIDC8-28:E5:EF:-04:7BRegionUS	Frequency     5.18 GHz       Signal Strength     -38 dBm       SNR     50 dBm       Channel     36       BSSID     C8:28:E5:EF:04:78       Region     US	Frequency     5.18 GHz       Signal Strength     -38 dBm       SNR     50 dBm       Channel     36       BSSID     C8:28:E5:EF:04:7B       Region     US		Speed	173 Mbps	
Signal Strength     -38 dBm       SNR     50 dBm       Channel     36       BSSID     C8:28:E5:EF:04:7B       Region     US	Signal Strength     -38 dBm       SNR     50 dBm       Channel     36       BSSID     C8:28:E5:EF:04:7B       Region     US	Signal Strength     -38 dBm       SNR     50 dBm       Channel     36       BSSID     C8:28:E5:EF:04:78       Region     US		Frequency	5.18 GHz	
SNR 50 dBm Channel 36 BSSID C8-28:E5:EF:04:7B Region US	SNR     50 dBm       Channel     36       BSSID     C8:28:E5:EF:04:78       Region     US	SNR 50 dBm Channel 36 BSSID C8:28:E5:EF:04:78 Region US		Signal Strength	-38 dBm	
Channel     36       BSSID     C8:28:E5:EF:04:7B       Region     US	Channel     36       BSSID     C8:28:E5:EF:04:7B       Region     US	Channel 36 BSSID C8:28:E5:EF:04:78 Region US		SNR	50 dBm	
BSSID C8-28:E5:EF:04:7B Region US	BSSID C8:28:E5:EF:04:78 Region US	BSSID C8:28:E5:EF:04:7B Region US		Channel		
Region US	Region US	Region US		BSSID	C8:28:E5:EF:04:7B	l
				Region		

## **Issues and Diagnostics**

Current issues and diagnostic options are displayed when selecting **Settings > Issues and diagnostics**.

#### <u>Webex</u>

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.

$\leftarrow$	Issues and diagnostics	
	Issues	
	<ul> <li>Everything is looking fine</li> </ul>	$\sim$
	Diagnostics	
	SpeakerTrack diagnostics	
	MediaStatistics overlay	
	PII logging	
	People focus logging	
	Extended logging	
	0 1 10 0	~~~~~

## **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.

1008 >		д AirPlay	8:06 PM 1
	- Issues and diagnostics		
	Issues		
	(i) AirPlay is set to broadcast a beaco V		
	SpeakerTrack diagnostics		
	PII logging		
	Extended logging		

## **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.

Cisco Webex Local Device Controls				Q Find page	<u> </u>
10.81.12.28 Desk Pro	System Informat	ion			
☆ Home	General		Is	sues	
% Call	10.81.12.28 IPv4	68:9E:0B:B0:00:0E MAC Address	Ø	) Everything is looking fine	
SETUP					
Settings	IPv6		P	rovisioning	
A Users	FOC2449NS4C	ି Wireless		Webey O Personal	
🔒 Security	Serial Number	Active Interface	Ø	Registered Device Mode	Details
CUSTOMIZATION	Normal				
Personalization	Temperature		C	alendar	<b>\$</b>
UI Extensions Editor	7e75011a-0740-5813-8	3949-4d1cde1d477f@broadcloud.or	g _	0 scheduled meeting(s) found for the next 3	24 hours.
Macro Editor	migilles@cisco.calls.web	ex.com		Last updated: Thursday 3:59 PM	
Developer API	Cloud SIP Address			Views	Scheduled Meetings
SYSTEM MAINTENANCE	Software		\$		
😪 Software	Stable	RoomOS 11.13.1.5			
	Software Channel	2f1a43e2808			
S Backup and Recovery		Sontware version			

## Setup

The Cisco RoomOS Series provides various configuration options and status information.

Browse to the web interface (<u>https://x.x.x.x</u>) of the Cisco RoomOS Series then select the desired option under **Setup** to view this information.

## <u>Settings</u>

Cisco Webex ocal Device Controls								
10.81.12.28 Desk Pro	Settings							
A Home	Configurations	General Statuses	Send Whiteboard	to Email	ଝି Audio and Vide	0		
le Call	Search	Configura	tion / SystemUn	it			Collapse All	Expand All
SETUP	Apps							
Settings	Audio							
Q Users	Bluetooth	BroadcastN	ame (				(0 to 256 ch	aracters)
Security	Bookings	CustomDev	iceld (i				(0 to 255 ch	aracters)
CUSTOMIZATION	BYOD	Name	(				(0 to 50 cha	acters)
Personalization	CallHistory							
✓ UI Extensions Editor	Cameras	CrashRepo	orting					-
Macro Editor	Conference	Advanced	(	On		~		
Ceveloper API	FacilityService	Mode	(	Off		~		
YSTEM MAINTENANCE	Files	URL	(				(0 to 255 ch	aracters)
Software	HttpClicot							
<ul> <li>Issues and Diagnostics</li> </ul>		Softwarel	narada WahCacha					
Backup and Recovery	HttpFeedback	Softwareo	pgrade webcache					•
	Logging	Mode	(	Off		~		
	Macros	Url	Q				(0 to 255 ch	aracters)
<b>tisco</b> Webex	Macros Mari MicrosoftTeams	Uri	۵			Q Find page	(0 to 255 ch	aracters) ව
tisco Webex ocal Device Controls	Macros Mari MicrosoftTeams	Un	G			Q Find page	(0 to 255 ch	aracters)
tisco Webex scal Device Controls 10.81.12.28 Desk Pro	Macros Mari MicrosoftTeams	Uri	G Send Whiteboard	to Email	ହ Audio and Vide	Q Find page	(0 to 255 ch	aracters) ত
isco Webex ocal Device Controls 10.81.12.28 Desk Pro ∂ Home	Macros Mari MicrosoftTeams Settings © Configurations	Uri	∑ Send Whiteboard	to Email	€ Audio and Vide	Q Find page	(0 to 255 ch	aracters)
isco Webex ceal Device Controls 10.81.12.28 Desk Pro G Home G Call	Macros Mari MicrosoftTeams Settings © Configurations Search	Uri Statuses Status / S	⊠ Send Whiteboard ystemUnit	to Email		Q Find page	(0 to 255 ch	3     Expand All
isco Webex scal Device Controls 10.81.12.28 Desk Pro	Macros Mari MicrosoftTeams Settings © Configurations Search Audio	Uri Statuses Status / S	⊠ Send Whiteboard	to Email	Q Audio and Vide	Q Find page	(0 to 255 ch	aracters)       Joint Control of Contr
isco Webex ocal Device Controls ■ 10.81.12.28 Desk Pro → Home ← Call ETUP ② Settings	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth	Uri Statuses Status / S Broadcasth	Send Whiteboard ystemUnit	to Email		Q Find page	(0 to 255 ch	<ul> <li>Tracters)</li> <li>Expand Al</li> </ul>
isco Webex cal Device Controls Desk Pro	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings	Uri Statuses Status / S Broadcasth DeveloperPar	Send Whiteboard ystemUnit lame review Mode	to Email Michael Gill Off		Q Find page	(0 to 255 ch	Texpand All
isco Webex scal Device Controls Desk Pro Desk Pro Call ETUP S Settings 2 Users 3 Security	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bluetooth Bluetooth Bookings Cameras	Uri Statuses Status / S Broadcasth DeveloperP Extensions LastShutdo	Send Whiteboard ystemUnit lame review Mode Microsoft Supported wnReason	to Email Michael Gill Off True Upgrade	Paudio and Vide	Q Find page	(0 to 255 ch	Image: Second All Second Al
isco Webex cal Device Controls 10.81.12.28 Desk Pro A Home Call Etrup Settings Q Users Security Sustomization	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings Cameras Capabilities	Uri Statuses Status / S BroadcastN DeveloperP Extensions LastShutdo Productid	Send Whiteboard ystemUnit Iame review Mode Microsoft Supported wwReason wmTime	to Email Off True Upgrade 2024-02-1 Cisco Desk	Audio and Vide     espie Desk Pro     3T05:57:16Z     Pro	Q Find page	(0 to 255 ch	aracters)       D       Expand Al
Isco Webex         Docal Device Controls         Iocal Jevice Controls         Desk Pro         A Home         Call         Settings         Users         Security         Sustantian         Sustantian         Security         Sustantian	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bookings Cameras Capabilities Conference	Uri Statuses Status / S Broadcasth Developerions LastShutdo LastShutdo ProductPlan	Send Whiteboard ystemUnit Iame review Mode Microsoft Supported wmReason wmTime	to Email Off Tugrade 2024-02-1 Cisco Desk Desk Pro	Q Audio and Vide  espie Desk Pro  3T05:57:16Z Pro	Q Find page	(0 to 255 ch	Texpand Al
isco Webex scal Device Controls 10.81.12.28 Desk Pro Call ETUP S Settings 2 Users 3 Settings 3 Settings 3 Settings 3 Settings 3 Settings 3 Settings 3 Settings 4 Users 3 Settings 4 Users 5 Settings 4 Users 5 Settings 5 Settings	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bluetooth Bluetooth Bookings Cameras Capabilities Conference	Uri Statuses Status / S Status / S Broadcasth DeveloperP Extensions LastShutdo ProductId ProductId ProductId ProductId ProductId	Send Whiteboard ystemUnit uame review Mode Microsoft Supported wnReason wnTime form e	to Email Off True Upgrade 2024-02-1 Cisco Code Desk Pro Cisco Code 239953	Audio and Vide  espie Desk Pro  TO5:57:16Z  Pro  c	Q Find page	(0 to 255 ch Collapse All	Image: Second All Second Al
isco Webex cal Device Controls 10.81.12.28 Desk Pro Call Call Security Security Users Security Users Security Users Security Users Security Users Security Users Security Users Security Users Security Users Security Users Security Users Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Sec	Macros Mari MicrosoftTeams Settings Search Audio Bluetooth Bluetooth Bluetooth Cameras Capabilities Canference Diagnostics	Uri Statuses Status / S Broadcasth DeveloperP Extensions LastShutdo LastShutdo ProductPlat ProductPlat ProductIppime	Send Whiteboard ystemUnit Iame review Mode Microsoft Supported wmReason wmTime form e	to Email Off True Upgrade 2024-02-1 Cisco Desk Desk Pro Cisco Code 239953	Q Audio and Vide     espie Desk Pro     3T05:57:16Z     Pro     c	Q Find page	(0 to 255 ch	aracters)       D       Expand All
isco Webex         bcal Device Controls         10.81.12.28         Desk Pro         A Home         Call         Settings         Users         Security         Security         Supersonalization         UI Extensions Editor         Macro Editor         Verein Editor         Verein Editor         Verein Editor	Macros Mari MicrosoftTeams Settings Search Audio Bluetooth Bookings Cameras Cameras Cameras Canference Diagnostics	Uri Statuses Status / S Status / S BroadcastN Developerit LastShutdo LastShutdo ProductPlat ProductPlat ProductTyp Uptime Hardware	Send Whiteboard Send Whiteboard ystemUnit lame review Mode Microsoft Supported wmReason wmReason wmTime e	to Email Off Tupe 2024-02-1 Cisco Desk Desk Pro Cisco Code 239953	Q Audio and Vide espie Desk Pro 3T05:57:16Z Pro ac	Q Find page	(0 to 255 ch	Transmission
isco Webex scal Device Controls 10.81.12.28 Desk Pro Call Call Call Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Sec	Macros Mari MicrosoftTeams Settings © Configurations Search Audio Bluetooth Bluetooth Bluetooth Bluetooth Cameras Capabilities Canference Diagnostics Logging MicrosoftTeams	Uri Statuses Status / S Status / S Broadcasth DeveloperP Extensions LastShutdo ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId ProductId P	Send Whiteboard ystemUnit Iame review Mode Microsoft Supported wnReason wnTime form e	to Email Michael Gill Off True Upgrade 2024-02-1 Cisco Code 239953	Audio and Vide espie Desk Pro Tro to	Q Find page	(0 to 255 ch	Texpand All
isco Webex         cal Device Controls         10.81.12.28         Desk Pro         Desk Pro         A Home         Call         Security         Security         Security         Security         UI Extensions Editor         Macro Editor         Macro Editor         Developer API         VISTEM MAINTENANCE         Software	Macros Mari MicrosoftTeams Settings Search Audio Bluetooth Bluetooth Bluetooth Bluetooth Cameras Capabilities Capabilities Canference Diagnostics Logging MicrosoftTeams Network	Uri Statuses Status / S Broadcasth DeveloperP Extensions LastShutdo LastShutdo LastShutdo ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPla	Send Whiteboard ystemUnit Iame review Mode Microsoft Supported wmReason wmTime form e	to Email Off True Upgrade 2024-02-1 Cisco Desk Desk Pro Cisco Code 239953 8 True Nameri	Q Audio and Vide espie Desk Pro 3T05:57:16Z Pro c	Q Find page	(0 to 255 ch	aracters)       D       Expand Al       -
Disco       Webex         Docal Device Controls         Device Controls         Desk Pro         Desk Pro         A Home         Call         Setury         Settings         Users         Security         Superside         Versonalization         U Extensions Editor         Macro Editor         Developer API         System MAINTENANCE         Software         Sustantic Superside	Macros         Mari         MicrosoftTeams         Settings         Search         Audio         Bluetooth         Bookings         Cameras         Canference         Diagnostics         Logging         MicrosoftTeams         Network         NetworkServices	Uri Statuses Status / S BroadcastN DeveloperP Extensions LastShutdo Productid ProductiVpa Uptime Hardware DRAM HasWifi MonitoringS	Send Whiteboard ystemUnit Iame review Mode Microsoft Supported wmReason wmTime form e Temperature Status	to Email Off True Upgrade 2024-02-1 Cisco Desk Desk Pro Cisco Code 239953 8 True Normal 34	Q Audio and Vide espie Desk Pro 3T05:57:16Z Pro xc	Q Find page	(0 to 255 ch	aracters)       The second
Disco       Webex         Docal Device Controls         I       0.81.12.28         Desk Pro         I       Security         I       Security         I       Dersonalization         I       UI Extensions Editor         I       Macro Editor         I       Developer API         INSTEM MAINTENANCE       Image: Software         V       Issues and Diagnostics         ID       Backup and Recovery	Macros         Mari         MicrosoftTeams         Settings         Search         Audio         Bluetooth         Bookings         Cameras         Canference         Diagnostics         Logging         MicrosoftTeams         Network         Peripherals	Uri Statuses Status / S Status / S BroadcastN Developerions LastShutdo ProductIV ProductIV ProductIV ProductIV ProductIV Interventions LastShutdo ProductIV Interventions LastShutdo ProductIV Interventions LastShutdo ProductIV Interventions LastShutdo ProductIV Interventions LastShutdo ProductIV Interventions LastShutdo Interventions LastShutdo ProductIV Interventions Uptime	Send Whiteboard Set W	to Email Michael Gill Off True Upgrade 2024-02-1 Cisco Code 239953 8 True Normal 34 CS-DESKPI	Audio and Vide  espie Desk Pro  Tro  Tro  RO-K9 V01 FOC2449	Q Find page o	(0 to 255 ch Collapse All	The second and the s
isco Webex cal Device Controls 10.81.12.28 Desk Pro 2 Home Call ETUP Settings 3 Users 3 Settings 3 Settings 3 Security USTOMIZATION 3 Personalization 4 UI Extensions Editor 5 Macro Editor 5 Developer API VSTEM MANTENANCE 3 Software F Issues and Diagnostics 5 Backup and Recovery	Macros Mari MicrosoftTeams Settings Search Audio Bluetooth Bluetooth Bluetooth Bluetooth Cameras Capabilities Canference Diagnostics Logging MicrosoftTeams Network NetworkServices Peripherals	Uri Statuses Status / S Status / S BroadcastN DeveloperP Extensions LastShutdo ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat ProductPlat RasWifi MonitoringS UDI MainBoi	Send Whiteboard ystemUnit ame review Mode wnReason wnTime form e form e	to Email Off True Upgrade 2024-02-1 Cisco Desk Desk Pro Cisco Code 239953 8 True Normal 34 CS-DESKP	Audio and Vide espie Desk Pro 3T05:57:16Z Pro ec RO-K9 V01 FOC2449	Q Find page	(0 to 255 ch Collapse All	aracters)       D       Expand All       -
isco Webex cal Device Controls Desk Pro Desk Pro Call Call Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings S	Macros Mari MicrosoftTeams Settings Search Audio Bluetooth Bluetooth Bluetooth Bluetooth Cameras Capabilities Capabilities Capabilities Canference Diagnostics Logging MicrosoftTeams Network Peripherals Phonebook	Uri Statuses Status / S Broadcasth DeveloperP Extensions LastShutdo LastShutdo ProductPlat ProductPlat ProductPlat ProductPlat ProductTyp Uptime Hardware DRAM HasWifi Monitorings UDI MainBo. Revision	Send Whiteboard ystemUnit ame review Mode Microsoft Supported wwReeson wmTime form e torm e	to Email Michael Gill Off True Upgrade 2024-02-1 Cisco Desk Desk Pro Cisco Code 239953 8 True Normal 34 CS-DESKPI C	Q Audio and Vide espie Desk Pro 3T05:57:16Z Pro vc RO-K9 V01 FOC2449	Q Find page	(0 to 255 ch	Transmission

## <u>Users</u>

Cisco Webex Local Device Controls					Q Find	page	0	2
10.81.12.28 Desk Pro	Users						Create	User
A Home	Username	Status	Admin (i)	Audit (j)	RoomControl (j)	Integrator (j)	User (i)	
% Call	admin	Active	$\checkmark$	$\checkmark$			$\checkmark$	

## <u>Security</u>

Cisco Webex Local Device Controls	Q Find page 💿	2
10.81.12.28 Desk Pro ∩ Home % Call	Security          O Certificates          • Sign-in Banner         Services       Custom       Preinstalled	
SETUP  Settings  Settings  Susars  Security  CUSTOMIZATION  UI Extensions Editor  Macro Editor  Security  Developer API	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 DSA encrypted private key with or without a passphrase. Optionally the private key file may be supplied separately.         Certificate       Browse         No file selected.         Private key       Browse         No file selected.         (optional)         Passphrase         (optional)	or
SYSTEM MAINTENANCE	Existing Certificates         Certificate       Issuer       802.1X       Audit       HTTPS       HttpClient       HttpProxy       SIP       Pairing       Actions         Self-signed Certificate       TemporaryDefaultCertificate       Image: Certificate       Image: Certificate<	ertificate
Cisco Webex Local Device Controls	Q Find page 💿	2
10.81.12.28 Desk Pro ∩ Home % Call	Security          O Certificates       Image: Sign-in Banner         Services       Custom         Preinstalled	
SETUP © Settings △ Users △ Security	Add     Use the form below to add new certificate authorities.       Certificate     This system supports PEM formatted files (.pem) with one or more CA certificates within the file.       Authority     Browse	
CUSTOMIZATION  Personalization UI Extensions Editor Macro Editor  Cy Developer API	Existing Certificate Authorities       Certificate     Issuer     Details     Actions       No certificates	
SYSTEM MAINTENANCE		

Cisco Webex Local Device Controls		Q Find page	8 0
10.81.12.28         Desk Pro         ∩         Home         ∿         Call         Settups         △         Users	Security          Certificates       Sign-in Banner         Services       Custom         Preinstalled       The Certificate Authoritie         Certificates       The Certificate swith:         • HTTP servers hosti	s listed below are used to validate the certificates of external serv ing content used by the web views, the HttpCLient xAPI, Macros	vers that the video system s, etc.
CUSTOMIZATION  Personalization  UI Extensions Editor	SMTP mail servers Certificate Details Certificate	(on video systems with touch screens)	Details Enabler
➡ Macro Editor % Developer API	AAA Certificate Services	Comodo CA Limited	View
SYSTEM MAINTENANCE	ACCVRAIZ1	ACCV Actalis S.p.A./03358520967	(View)
<ul> <li>Issues and Diagnostics</li> <li>Backup and Recovery</li> </ul>	AffirmTrust Commercial	AffirmTrust	View

## Customization

The Cisco RoomOS Series provides various personalization options as well as other customization options.

Browse to the web interface (<u>https://x.x.x.x</u>) of the Cisco RoomOS Series then select the desired option under **Customization** to view this information.

## **Personalization**

Cisco Webex Local Device Controls				Q Find pa	ge 💿	2
10.81.12.28 Desk Pro	Personalizati	on				
⊖ Home	⊠ Wallpaper and Ha	Branding	Virtual Backgrounds	月 Ringtones □ Cor	ntacts	
SETUP	Halfwake	The device enters halfwal	ke after it has been idle	e for a while.		
<ul><li>중 Settings</li><li>스 Users</li></ul>						
		Default				
Personalization		Upload image Recommend	ed size is 3840×2160 pixel	ls. File format: jpg, png, webp		
UI Extensions Editor  Macro Editor  Volume API		Turn off display after	v			
		Preview on device				
<ul> <li>Software</li> <li>Issues and Diagnostics</li> <li>Backup and Recovery</li> </ul>	Wallpaper	The wallpaper is shown a	s a background on the	home screen.		
		Custom image	light	niç	ght	
Cisco Webex Local Device Controls				Q Find pa	ge 📀	2
10.81.12.28 Desk Pro	Personalizati	on				
⊖ Home	전 Wallpaper and Ha	alfwake G Branding	Virtual Backgrounds	月 Ringtones □ Cor	ntacts	
SETUP	Brand Logo	Halfwake logo Shows brand logo in halfwake				
<ul> <li>Settings</li> <li>Users</li> </ul>		Upload image Recommen	nded size is 272×272 pixels	s. File format: png		
A Security		Home screen logo Show brand logo on home scr	een			
CUSTOMIZATION		Upload image Recommen	nded size is 272×272 pixels	s. File format: png		
UI Extensions Editor Macro Editor						
% Developer API	Custom Text	Custom text displays in the Example: A help desk number	ne bottom left corner o your end users can call for	f the main screen. assistance.		
SYSTEM MAINTENANCE		Feedback? https://cs.co/dt	Apply			
<ul> <li>Issues and Diagnostics</li> <li>Backup and Recovery</li> </ul>						

Cisco Webex Local Device Controls	Q. Find page	0	2
10.81.12.28 Desk Pro	Personalization		
	⊠ Wallpaper and Halfwake		
<ul> <li>S Call</li> <li>SETUP</li> <li>Settings</li> <li>Users</li> <li>Security</li> <li>CUSTOMIZATION</li> <li>Personalization</li> <li>✓ UI Extensions Editor</li> <li>Macro Editor</li> <li>Macro Editor</li> <li>S Developer API</li> <li>SYSTEM MAINTEMAINCE</li> <li>G Software</li> <li>~ Issues and Diagnostics</li> <li>Backup and Recovery</li> </ul>	Virtual Backgrounds       Upload         Yus can upload up to three virtual backgrounds to replace the background of your video during a call.         Image: Comparison of the provided during th		
<b>Cisco</b> Webex Local Device Controls	Q. Find page	0	2
10.81.12.28 Desk Pro	Personalization		
∩ Home S Call	☑ Wallpaper and Halfwake     ☑ Branding     ☑ Virtual Backgrounds     ☐ Ringtones     ☑ Contacts		
SETUP Settings Users Security CUSTOMIZATION Personalization U II Extensions Editor	Ringtones Select Active Ringtone Please note that the ringtone will play on the video system. Sunrise   Ringtone volume  50%		

isco Webex Ical Device Controls			Q Fin	d page 💿
10.81.12.28 Desk Pro	Personalization			
) Home	Wallpaper and Halfwak	Branding Virtual Backgrou	nds 🎜 Ringtones 🔲	Contacts
Call UP Settings	The section below lets you it the Call activity in the device The complete list of contact and then import it into all of	create, edit, and delete local phonebook entries e's user interface. s can be exported. Use this feature either to cre your other devices.	on the system. These entries sh ate a backup of the local phonel	ow up in the "Favorites" panel unde
Security	Search contacts	X C: Add Folder Add Contact		년 Import 다 Ex
STOMIZATION	< Back Favorites		Edit Folder	
Personalization	Name	Number		
UI Extensions Editor Macro Editor		No contacts		
Developer API				
STEM MAINTENANCE				
Software				
Issues and Diagnostics				
Backup and Recovery				

## **System Maintenance**

The Cisco RoomOS Series provides various serviceability options including device logs.

Browse to the web interface (<u>https://x.x.x.x</u>) of the Cisco RoomOS Series then select the desired option under **System Maintenance** to view this information.

#### **Software**

Cisco Webex Local Device Controls		Q Find pag	je Ø	
10.81.12.28 Desk Pro	Software			
G Home	Software Upgrade			
% Call	· Your system is cloud managed, and you cannot manage the software locally.			
SETUP	Go to Cisco Webex Control Hub to change the software channel.			
Settings	•			
요 Users				
🔒 Security				
CUSTOMIZATION				
Personalization				
UI Extensions Editor				
Macro Editor				
Developer API				
SYSTEM MAINTENANCE				
G Software				
✓ Issues and Diagnostics				
Sackup and Recovery				

### **Issues and Diagnostics**



### **Backup and Recovery**

Cisco Webex Local Device Controls				Q Find page (2)
10.81.12.28 Desk Pro	Backup a	nd Recov	/ery	
ි Home	D Backup	$\mathbb C$ Restore	<sup>1</sup> % System Recovery	${}^{\scriptsize }$ Restart and Shutdown
5 Call	Download	This p	age lets you backup a devic	e's configurations. Configurations include xConfigurations, as well as the configurat
ETUP ∄ Settings	Васкир	Select	items to include in your bac	kup. Leave all items checked to generate a complete backup of the device.
2 Users		Brandi	ng	No items installed
Security		Favori	tes	No items installed
USTOMIZATION		UI Exte	ensions	No items installed
9 Personalization		Macro	s	No items installed
<sup>2</sup> UI Extensions Editor		Sign Ir	Banner	✓ Include
Macro Editor Ø Developer API		Config	uration	☑ Include
				The configuration listed below can be modified for a partial backup of the configuration.
Software				Note: Settings such as Network, SIP URI and SystemUnit Name may
<ul> <li>Issues and Diagnostics</li> </ul>				specifically apply to a certain device. Applying a backup with these settings a different device may result in it becoming unreachable on the network. To
Backup and Recovery				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: On Audio Input HDMI 1 VideoAssociation MuteOnInactiveVideo: (

## **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.

_		
	Manage Web Apps Settings	
	Meeting zone	
	Connections	
	Are you sure you want to reset this device	e?
	This will delete all data and settings permanently. You need to configure this device again.	will
	Cancel	et

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.

Cisco Webex Local Device Controls		Q. Find page (2)
10.81.12.28         Desk Pro         G. Home         Call         setup         Settings         A. Users	Software Recovery Swap	A system recovery swap will reinstall the previously installed software image on the device. The previous software image is located on an inactive partition on the device, and by clicking the button below, you will change the active partition and reboot. Performing a software recovery swap is the recommended action if the system has a severe issue, for example if it is unable to start up properly. Please consult with your Cisco technical support representative before performing a system recovery swap. Provide systems logs when opening the support ticket. Active software image: ce11.13.1.5 2f1a43e2808 2024-02-09 Software image on inactive partition: ce11.12.1.6 6c205f3b2e5 2024-01-18
A Security		
CUSTOMIZATION C Personalization C UI Extensions Editor E Macro Editor C Developer API	Factory Reset	Factory Reset       all other troubleshooting measures fail. It is strongly yry reset.         Are you sure you want to perform a factory reset?       e the Backup tab to create a backup bundle of local r to reconfigure the system afterwards.         Cancel       Factory Reset         solution, like Cisco Webex Control Hub, Cisco Unified Communications Manager, Cisco Expressway, or Cisco TelePresence Management Suite.
SYSTEM MAINTENANCE		<ul> <li>Caution: A factory reset cannot be undone.</li> </ul> Further Details <ul> <li>Call logs will be deleted.</li> <li>All local user accounts will be deleted.</li> <li>Customizations, like Macros, UI Extensions, and branding, will be deleted.</li> <li>The alternate software image will be deleted, so that it will no longer be possible to do a software recovery swap afterwards.</li> <li>Release keys and option keys will <i>not</i> be deleted.</li> </ul> Reset to Factory Defaults

## 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 (<u>https://x.x.x.x</u>) of the Cisco RoomOS Series then select **OSD Screenshot** the under **System Maintenance > Issues and Diagnostics > User Interface Screenshots** to capture a screenshot.

Cisco Webex Local Device Controls	Q Find page  (2)	2
10.81.12.28 Desk Pro	Issues and Diagnostics	
☆ Home	~ Issues	
∿ Call	Screenshots Create Screenshot	
seтup ŵ Settings	Taking a screenshot of the touch panel or the on-screen dispay (OSD) can be useful for creating user manuals, reporting bugs to Cisco, and so on.	
<ul><li>△ Users</li><li>合 Security</li></ul>	depending on image resolution and network bandwidth.	
CUSTOMIZATION	Wake System Up	
<ul> <li>Personalization</li> <li>UI Extensions Editor</li> </ul>	Use the buttons below to put the system into awake or halfwake state.	
Macro Editor  Control		
SYSTEM MAINTENANCE		
G Software		
<ul> <li>∽ Issues and Diagnostics</li> <li>⊙ Backup and Recovery</li> </ul>		

# 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/productsmaintenance-guides-list.html

## Cisco RoomOS Series User Guide

 $\frac{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-userguide-list.html$ 

### Cisco RoomOS Series Quick Reference Guide

 $\frac{http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-userguide-list.html}{\label{eq:construct}}$ 

### Cisco RoomOS Series Release Notes

 $\frac{https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html}{\label{eq:collaboration}}$ 

#### 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\_rtowlan-srnd.html

#### Cisco Unified Communications Design Guides

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

#### Cisco AireOS Wireless LAN Controller Documentation

 $\underline{https://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html$ 

### 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: <u>http://www.cisco.com/go/trademarks</u>. 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.