



Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide



9861

9871

Cisco is bringing a new standard to desk phones with a portfolio built for working in modern office environments. The Desk Phone 9800 Series was designed with IT and facilities in mind to deliver 4 new phone models. Included on each phone is the newly released PhoneOS software that simplifies the user experience and compliments our video portfolios RoomOS devices to give a seamless experience from desk spaces to meeting rooms. With expanded functionality – the 9800 Series combines secure enterprise calling, meetings, desk reservations, sustainability, emergency alerts and calling all in one device. You don't need to buy a dedicated device for each feature – all the features are built into each phone.

The Desk Phone 9800 Series reduces the complexity of purchasing, deploying, managing, and training. To further simplify, you can use one device for Cisco Unified Communications Manager (CUCM), Webex Calling, Broadworks, or other 3rd party cloud calling platforms. Alongside our extensive portfolio of desk devices, the 9800 series is uniquely positioned in the market to help transform the workplace by bridging the gap between hybrid work, calling, and meetings – and is the most cost-effective solution for workstations at scale.

This guide provides information and guidance to help the network administrator deploy the 9800 Series into a wireless LAN environment.

Revision History

Date	Comments
07/12/24	initial version

Contents

Cisco Desk Phone 9800 Series Overview	7
<i>Models</i>	<i>7</i>
<i>Requirements</i>	<i>7</i>
Site Requirement	7
Call Control	8
Wireless LAN	9
Access Points	9
Antenna System	10
<i>Protocols</i>	<i>10</i>
<i>Wi-Fi</i>	<i>10</i>
5 GHz Specifications	10
2.4 GHz Specifications	12
Regulatory	13
<i>Bluetooth®</i>	<i>13</i>
Bluetooth Profiles	13
Coexistence (802.11b/g/n + Bluetooth)	13
<i>Device Care</i>	<i>14</i>
Wireless LAN Design	15
<i>802.11 Network</i>	<i>15</i>
5 GHz (802.11a/n/ac)	15
Dynamic Frequency Selection (DFS)	15
2.4 GHz (802.11b/g/n)	16
Signal Strength and Coverage	16
Data Rates	17
Rugged Environments	17
Multipath	18
<i>Security</i>	<i>19</i>
Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)	19
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)	20
Protected Extensible Authentication Protocol (PEAP)	20
<i>Quality of Service (QoS)</i>	<i>20</i>
Call Admission Control (CAC)	21
Wired QoS	21
<i>Roaming</i>	<i>21</i>
Fast Secure Roaming (FSR)	22
Interband Roaming	22
<i>Power Management</i>	<i>23</i>
Delivery Traffic Indicator Message (DTIM)	23
<i>Call Capacity</i>	<i>23</i>
<i>Multicast</i>	<i>23</i>
Configuring the Cisco Wireless LAN	24
<i>Cisco AireOS Wireless LAN Controller and Lightweight Access Points</i>	<i>24</i>
802.11 Network Settings	24

Auto RF (RRM)	26
Client Roaming	28
EDCA Parameters	28
DFS (802.11h).....	28
High Throughput (802.11n/ac).....	28
Frame Aggregation.....	29
CleanAir	31
Rx Sop Threshold.....	32
WLAN Settings	32
AP Groups.....	37
Controller Settings.....	39
Call Admission Control (CAC).....	40
RF Profiles	42
FlexConnect Groups.....	44
Multicast Direct.....	45
QoS Profiles	47
Advanced Settings.....	49
Advanced EAP Settings	49
Auto-Immune	50
Rogue Policies.....	51
<i>Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points</i>	51
802.11 Network Settings	52
High Throughput (802.11n/ac).....	53
Parameters.....	54
RRM.....	55
CleanAir	57
WLAN Settings	58
Policy Profiles	60
RF Profiles	63
Flex Profiles	65
Tags.....	66
Controller Settings.....	68
Mobility Settings	69
Call Admission Control (CAC).....	70
Multicast.....	70
Advanced Settings.....	72
Advanced EAP Settings	72
Rx Sop Threshold.....	72
Rogue Policies.....	72
<i>Cisco Mobility Express and Lightweight Access Points</i>	73
Controller Settings.....	73
802.11 Network Settings	74
RF Optimization.....	75
WLAN Settings	77
AP Groups.....	81
RF Profiles	83
Multicast Direct.....	84
<i>Cisco Autonomous Access Points</i>	85
802.11 Network Settings	85
WLAN Settings	88
Wireless Domain Services (WDS).....	92
Call Admission Control (CAC).....	96

QoS Policies	96
Power Management.....	98
<i>Cisco Meraki Access Points</i>	98
Creating the Wireless Network	98
SSID Configuration.....	100
Radio Settings	103
Firewall and Traffic Shaping.....	105
Configure Cisco Call Control	107
<i>Cisco Webex Calling</i>	107
Personal Usage.....	107
Workspace Usage.....	107
Wi-Fi Capability.....	108
<i>Cisco Unified Communications Manager</i>	108
Device Enablement	108
Common Settings	109
QoS Parameters	109
Wireless LAN Profiles	110
Create a Wireless LAN Profile	110
Create a Wireless LAN Profile Group	113
Apply a Wireless LAN Profile Group to a Device Pool.....	114
Apply a Wireless LAN Profile Group to an Individual Phone.....	116
Configure the Cisco Desk Phone 9800 Series	117
<i>Automatic Provisioning</i>	117
<i>Config/Modify Wi-Fi Profile via Phone Web Portal</i>	117
<i>Configure Wi-Fi Settings on the Phone UI</i>	118
Join a Hidden Wireless Network.....	120
Delete a Connected Network.....	120
<i>Certificate Management</i>	121
Manual Installation.....	121
Manufacturing Installed Certificate (MIC)	121
User Installed Certificate.....	121
LSC Certificate	122
Server Certificate.....	124
Certificate Removal.....	124
Simple Certificate Enrollment Protocol (SCEP)	125
Certificate Authority (CA) Configuration.....	126
RADIUS Configuration	132
SCEP RA Configuration	138
Troubleshooting	140
<i>Problem Report Tool</i>	140
<i>Wi-Fi statistics</i>	141
<i>View Streaming Statistics</i>	141
<i>Wi-Fi Signal Indicator</i>	142
<i>View the Information About the Connected Access Point</i>	142
<i>Capture a Screenshot of the Phone Display</i>	143

<i>Capture Packets</i>	143
Additional Documentation	144
<i>Other Documentation for Reference</i>	144

Cisco Desk Phone 9800 Series Overview

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

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 Desk Phone 9800 Series to take advantage of the 802.11a/n data rates available.

Despite the optimizations that Cisco has implemented in the Cisco Desk Phone Series, the use of unlicensed spectrum means that uninterrupted communication cannot 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.

Using unlicensed spectrum, and the inability to guarantee the delivery of messages to a WLAN device, the Cisco Desk Phone 9800 Series is not intended to be used as a medical device and should not be used to make clinical decisions.

Models

The following table shows available phone models with WLAN capability.

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

Part Number	Description	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
DP-9871-K9= DP-9871-L-K9= DP-9871-K9++= DP-9871-K9--=	Cisco Desk Phone 9871	2.400-2.483GHz: 3.22 dBi 5.150-5.250GHz: 3.60 dBi 5.250-5.350GHz: 3.62 dBi 5.470-5.725GHz: 4.23 dBi 5.725-5.850GHz: 4.13 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-144 149,153,157,161,165
DP-9861-K9= DP-9861-L-K9= DP-9861-K9++= DP-9861-K9--=	Cisco Desk Phone 9861	2.400-2.483GHz: 3.06 dBi 5.150-5.250GHz: 3.98 dBi 5.250-5.350GHz: 4.07 dBi 5.470-5.725GHz: 4.11 dBi 5.725-5.850GHz: 3.76 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-144 149,153,157,161,165

Requirements

The Cisco Desk Phone 9800 Series units are IEEE 802.11a/b/g/n/ac collaboration device that provide voice and data communications. The wireless LAN must be validated to ensure it meets the requirements to deploy the Cisco Desk Phone Series.

Site Requirement

Before deploying the Cisco Desk Phone 9800 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 unable in the desired band (5GHz or 2.4GHz). Typically, there is less interference

in the 5GHz band as well as more non-overlapping channels, so 5GHz is the preferred band for operation and even more highly recommended when the Cisco Desk Phone 9800 Series units 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 Desk Phone 9800 Series.

Signal

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

This ensures that the Cisco Desk Phone 9800 Series always has adequate signal and can hold a signal long enough to roam seamlessly where signal-based triggers are utilized vs. packet loss triggers.

Also need to ensure that the upstream signal from the phone 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 phone can hold a signal for at least 5s.

Channel Utilization

Channel Utilization levels should be kept under 40%.

Noise

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

Also need to ensure that the upstream signal from the Cisco Desk Phone 9800 Series meets the access point's signal to noise ratio for the transmitted data rate.

Packet Loss / Delay

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

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

Retries

802.11 retransmissions should be less than 20%.

Multipath

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

Call Control

The Cisco Desk Phone 9800 Series is supported on the following call control platforms.

- Cisco Webex Calling
- Cisco Unified Communications Manager (CUCM) (12.5 or above)
- Webex Dedicated Instance (DI)
- Cisco BroadWorks

Note: Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable Cisco Desk Phone 9800 Series device support.

Device packages for Cisco Desk Phone 9800 Series are available at the following location.

[https://software.cisco.com/download/home/286322286/type/282074299/release/12.5\(1.19210\)](https://software.cisco.com/download/home/286322286/type/282074299/release/12.5(1.19210))

[https://software.cisco.com/download/home/286328117/type/282074299/release/14.0\(1.14056\)](https://software.cisco.com/download/home/286328117/type/282074299/release/14.0(1.14056))

[https://software.cisco.com/download/home/286331940/type/282074299/release/15.0\(1.12004\)](https://software.cisco.com/download/home/286331940/type/282074299/release/15.0(1.12004))

Wireless LAN

The Cisco Desk Phone 9800 Series is supported on the following Cisco Wireless LAN solutions.

- Cisco AireOS Wireless LAN Controller and Cisco Lightweight Access Points
 - Minimum = 8.10.185.0
 - Recommended = 8.10.190.0, 8.10.196.0
- Cisco IOS Wireless LAN Controller and Cisco Lightweight Access Points
 - Minimum = 17.3.5
 - Recommended = 17.9.5, 17.6.6, 17.12.1
- Cisco Mobility Express and Cisco Lightweight Access Points
 - Minimum = 8.10.105.0
 - Recommended = 8.10.105.0, 8.10.130.0, 8.10.142.0, 8.10.196.0
- Cisco Autonomous Access Points
 - Minimum = 15.3(3)JPK2
 - Recommended = 15.3(3)JPK2, 15.3(3)JPK3, 15.3(3)JPK4, 15.3(3)JPK6
- Cisco Meraki Access Points
 - Minimum = MR 27.X, MX 13.33
 - Recommended = MR 30.6, MX 18.211.2

Access Points

See the following table for the Cisco access points that are supported.

Controller Model	AP Models
AireOS	1700, 1810, 1810W, 1815, 1830, 1840, 1850, 2700, 2800, 3700, 3800, 4800, 9105, 9115, 9117, 9120, 9130
IOS XE	1700, 1810, 1810W, 1815, 1830, 1840, 1850, 2700, 2800, 3700, 3800, 4800, 9105, 9115, 9117, 9120, 9130, 9136, 9162, 9164, 9166
Mobility Express	1815 (not 1815t), 1830, 1840, 1850, 2800, 3800, 4800
Autonomous	1700, 2700, 3700
Meraki	9162, 9164, 9166, MR20, MR28, MR30H, MR32, MR33, MR34, MR36, MR36H, MR42, MR44, MR45, MR46, MR52, MR53, MR55, MR56, MR57, MX64W, MX65W, MX67W, MX68W, Z3

Antenna System

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 the 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 wireless LAN protocols include the following:

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

Wi-Fi

Cisco Desk Phone 9800 Series can work with 2.4GHz (HT20) or 5GHz (HT20/HT40/VHT20/VHT40/VHT80) mode. To achieve 802.11n/ac connectivity, it is recommended that the Cisco Desk Phone 9800 Series be within 30 feet of the access point.

5 GHz Specifications

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

	29 Mbps (MCS 3)	1	OFDM-16QAM
	43 Mbps (MCS 4)	1	OFDM-16QAM
	58 Mbps (MCS 5)	1	OFDM-64QAM
	65 Mbps (MCS 6)	1	OFDM-64QAM
	72 Mbps (MCS 7)	1	OFDM-64QAM
5 GHz-802.11n (HT40)	Date Rate	Spatial Streams	Modulation
Max Tx Power=17 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM-BPSK
	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-16QAM
	90 Mbps (MCS 4)	1	OFDM-16QAM
	120 Mbps (MCS 5)	1	OFDM-64QAM
	135 Mbps (MCS 6)	1	OFDM-64QAM
	150 Mbps (MCS 7)	1	OFDM-64QAM
5 GHz-802.11ac (VHT20)	Date Rate	Spatial Streams	Modulation
Max Tx Power=18 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM-BPSK
	14 Mbps (MCS 1)	1	OFDM-QPSK
	21 Mbps (MCS 2)	1	OFDM-QPSK
	29 Mbps (MCS 3)	1	OFDM-16QAM
	43 Mbps (MCS 4)	1	OFDM-16QAM
	58 Mbps (MCS 5)	1	OFDM-64QAM
	65 Mbps (MCS 6)	1	OFDM-64QAM
	72 Mbps (MCS 7)	1	OFDM-64QAM
	87 Mbps (MCS 8)	1	OFDM-256QAM
5 GHz-802.11ac (VHT40)	Date Rate	Spatial Streams	Modulation
Max Tx Power=17 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM-BPSK
	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-16QAM
	90 Mbps (MCS 4)	1	OFDM-16QAM
	120 Mbps (MCS 5)	1	OFDM-64QAM
	135 Mbps (MCS 6)	1	OFDM-64QAM
	150 Mbps (MCS 7)	1	OFDM-64QAM
	180 Mbps (MCS 8)	1	OFDM-256QAM
	200 Mbps (MCS 9)	1	OFDM-256QAM
5 GHz-802.11ac (VHT80)	Date Rate	Spatial Streams	Modulation
Max Tx Power=15 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-16QAM
	195 Mbps (MCS 4)	1	OFDM-16QAM
	260 Mbps (MCS 5)	1	OFDM-64QAM
	293 Mbps (MCS 6)	1	OFDM-64QAM
	325 Mbps (MCS 7)	1	OFDM-64QAM
	390 Mbps (MCS 8)	1	OFDM-256QAM
	433 Mbps (MCS 9)	1	OFDM-256QAM

2.4 GHz Specifications

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

Note: Tx power includes antenna gain.

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 Desk Phone 9800 Series operates best with an access point that has 802.11d enabled, where it can determine the 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 to be 802.11h compliant to utilize those radar frequencies (DFS channels). 802.11h requires 802.11d to be enabled.

The Cisco Desk Phone 9800 Series will passively scan DFS channels first before engaging in active scans for those channels.

If 802.11d is not enabled, then the Cisco Desk Phone 9800 Series will attempt to connect to the access point using reduced transmit power.

Cisco Desk Phone 9800 Series supports county codes which follow WFA definition.

Bluetooth®

The Cisco Desk Phone 9800 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 Desk Phone 9800 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 operates on the 2.4 GHz frequency, similar to 802.11b/g/n and various other devices (e.g., microwave ovens, cordless phones, etc.). Therefore, Bluetooth quality may be affected by potential interference from other devices using this unlicensed frequency.

Bluetooth Profiles

The Cisco Desk Phone 9800 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 + Bluetooth)

If using Coexistence where 802.11b/g/n and Bluetooth are used simultaneously, it is important to consider the following limitations and deployment requirements because they both utilize the 2.4 GHz frequency range.

Capacity

When using Coexistence (802.11b/g/n + Bluetooth), call capacity is reduced due to the utilization of CTS to protect the 802.11g/n and Bluetooth transmissions.

Multicast Audio

Multicast audio from Push to Talk (PTT), Music on Hold (MMOH), and other applications are not supported when using Coexistence.

Voice Quality

Depending on the current data rate configuration, CTS may be sent to protect the Bluetooth transmissions when using Coexistence.

In some environments, 6 Mbps may need to be enabled.

Note: It is recommended to use 802.11a/n/ac when using Bluetooth, not only because both 802.11b/g/n and Bluetooth utilize the 2.4 GHz frequency, but also due to the limitations mentioned above.

Device Care

To clean the Cisco Desk Phone 9800 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 damage the device.

For more information, refer to the Cisco Desk Phone 9800 Series User Guide at <https://cisco.com/go/dp9800help>

Wireless LAN Design

The following network design guidelines must be followed to ensure adequate coverage, call capacity and seamless roaming for the Cisco Desk Phone 9800 Series.

802.11 Network

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

5 GHz (802.11a/n/ac)

5 GHz is the recommended frequency band for operating the Cisco Desk Phone 9800 Series.

Generally, it is recommended for access points to use automatic channel selection instead of manually assigning channels. If there is intermittent interference, it may be necessary to statically assign channels to the access point or access points serving that area.

The Cisco Desk Phone 9800 Series supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) as per 802.11h, required for channels operating at 5.260 - 5.720 GHz, which encompass 16 out of the 25 possible channels.

To ensure seamless roaming in a 802.11a/n/ac environment, it's crucial to have at least 20 percent overlap with adjacent channels. For critical areas, increasing the overlap to 30% or more is recommended to ensure that there can be at least 2 access points available with a signal of -67 dBm or higher. Additionally, the Cisco Desk Phone 9800 Series complies with 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 will pause 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 the access point detects repeated radar events, whether genuine or false alarms, it first determines if the radar signals are affecting a single channel (narrowband) or multiple channels (wideband). Then the access point potentially disables the affected channel or channels in the wireless LAN to mitigate interference.

Having an access point operating on a non-DFS channel can help minimize voice interruptions.

In case of radar activity, it's recommended to have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel remains 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.

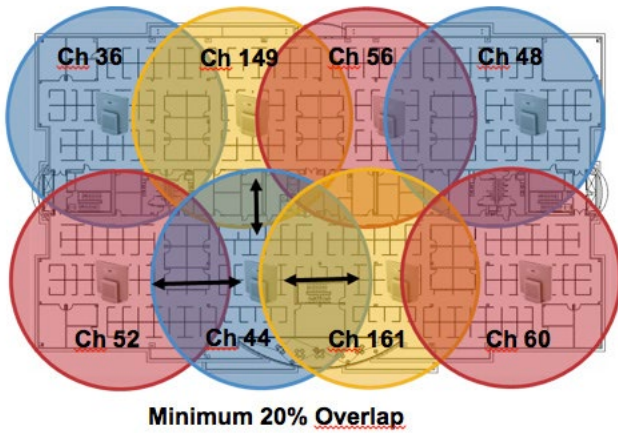
For 5 GHz, 25 channels are available in the Americas, 16 channels in Europe, and 19 channels in Japan.

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.

Below is a sample 5 GHz wireless LAN deployment



2.4 GHz (802.11b/g/n)

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

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

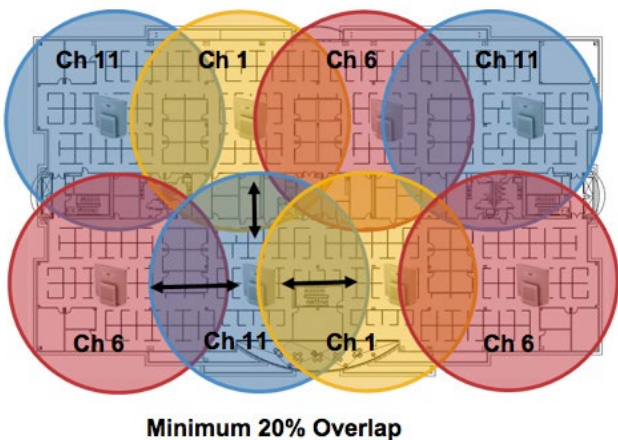
In a 2.4 GHz (802.11b/g/n) environment, only non-overlapping channels must be utilized when deploying VoWLAN. Nonoverlapping channels have 22 MHz of separation and are at least 5 channels apart.

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 Desk Phone 9800 Series in an 802.11b/g/n environment, which allows for seamless roaming.

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

Below is a sample 2.4 GHz wireless LAN deployment.



Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco Desk Phone 9800 Series should always have a signal of -67 dBm or higher when using 5GHz or 2.4 GHz, while the Cisco Desk Phone 9800 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.

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

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

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

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

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

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

Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g/n. Some microwaves are more heavily shielded than others, which reduces the spread of the energy. Microwave emissions can impact channel 11, while some microwaves can affect the entire 2.4 GHz frequency range (channels 1 through 11). To avoid microwave interference, select channel 1 when using access points that are located near microwaves.

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

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

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 Desk Phone 9800 Series is 1x1 with single antenna, therefore they support up to MCS 7 data rates for 802.11n (up to 72 Mbps). For 802.11ac, the Cisco Desk Phone 9800 Series supports up to VHT80 MCS 9 1SS (up to 433 Mbps).

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

For a voice only application, data rates higher than 24 Mbps can optionally be enabled or disabled. 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: that capacity and throughput are reduced when lower rates are enabled.

Rugged Environments

When deploying the Cisco Desk Phone 9800 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 Desk Phone 9800 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 it's 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 Desk Phone 9800 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).

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.

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 delays and travels a longer path to the destination, which creates signal energy loss.

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

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

Below is a list of multipath effects:

Data Corruption

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

Signal Nulling

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

Increased Signal Amplitude

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

Decreased Signal Amplitude

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

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

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

Use of antenna diversity can also help in such environments.

Security

When deploying a wireless LAN, security is essential. The Cisco Desk Phone 9800 Series supports the following wireless security features.

WLAN Authentication

- WPA2 and WPA (802.1x authentication)
- WPA2-PSK and WPA-PSK (Pre-Shared key)
- WPA3-SAE (Simultaneous Authentication of Equals)
- EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol - Generic Token Card/ Microsoft Challenge Handshake Authentication Protocol version 2)
- None

WLAN Encryption

- AES (minimum 128-bit Advanced Encryption Standard)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)

WPA3-Enterprise

- Key derivation and confirmation
Minimum 256-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA256)
- Robust management frame
Minimum 128-bit Broadcast/Multicast Integrity Protocol Cipher-based Message Authentication Code (BIP-CMAC-128)

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

The Cisco Desk Phone 9800 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 Identity Service Engine (ISE).

The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (the Cisco Desk Phone 9800 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 primary key. Both endpoints now have the PAC key, and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must enable on the RADIUS server.

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

The Cisco Desk Phone 9800 Series currently supports automatic provisioning of the PAC only. Therefore, 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 a user account to 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 set up for initial PAC provisioning of the Cisco Desk Phone 9800 Series.

This requires that the staging RADIUS server are set up as a secondary EAP-FAST server and components are replicated from the product primary EAP-FAST server, which include user and group database and EAP-FAST primary key and policy info. Ensure the production primary EAP-FAST RADIUS server is set up to send the EAP-FAST primary keys and policies to the staging secondary EAP-FAST RADIUS server, which will then allow the Cisco Desk Phone 9800 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. Therefore, ensure that **Allow authenticated in-band PAC provisioning** is enabled.

Ensure that the Cisco Desk Phone 9800 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 primary key 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 Desk Phone 9800 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.

Protected Extensible Authentication Protocol (PEAP)

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

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

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

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

Quality of Service (QoS)

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

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

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

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	RTP/RTCP port negotiated with remote peer.
Call Control	CS3 (24)	3	4	TCP/UDP port configured by admin

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

Call Admission Control (CAC)

The Cisco Desk Phone 9800 Series does not support Call Admission Control of voice stream. If TSPEC is enabled for voice the access point, then the priority of voice 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, refer to 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 Desk Phone 9800 Series enables both sets of frequencies, which allows the Cisco Desk Phone 9800 Series to connect to either 5 GHz or 2.4GHz 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, WPA2 and WPA3 introduce additional transient keys and can lengthen roaming time.

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

The Cisco Desk Phone 9800 Series supports 802.11r (FT).

Authentication Roaming Time Table

Authentication	Roaming Time
WPA/WPA2/WPA3 Personal	150 ms
WPA2 Enterprise	300 ms
802.11r (FT)	< 100 ms

The Cisco Desk Phone 9800 Series manages the scanning and roaming events.

The roaming trigger for most roaming events should meet the required RSSI differential based on the current RSSI. This ensures seamless roaming without voice interruptions.

Fast Secure Roaming (FSR)

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

Cisco Centralized Key Management (CCKM) is not supported but requires 802.1x authentication.

802.11r (FT) enables fast secure roaming and limits the off-network time to minimize gaps during calls.

802.1x or PSK without 802.11r (FT) and 802.1x without FT can introduce delay during roaming due to its requirement for full re-authentication. WPA, WPA2 and WPA3 introduce additional transient keys and can lengthen roaming time.

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

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

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

Over the Air

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

Over the Distribution

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

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

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

The Cisco Desk Phone 9800 Series supports 802.11r (FT) with WPA2-PSK, WPA3-SAE or WPA2/WPA3 enterprise.

FSR Type	Authentication	Key Management	Encryption	PMF
802.11r (FT)	PSK	WPA-PSK WPA-PSK-SHA256 FT-PSK	AES	No
802.11r (FT)	WPA3	SAE FT-SAE	AES	Yes
802.11r (FT)	EAP-TLS	WPA-EAP FT-EAP	AES	No
802.11r (FT)	EAP-TLS (WPA3)	WPA-EAP-SHA256 FT-EAP	AES	Yes
802.11r (FT)	EAP-FAST	WPA-EAP FT-EAP	AES	No
802.11r (FT)	EAP-FAST(WPA3)	WPA-EAP-SHA256 FT-EAP	AES	Yes
802.11r (FT)	EAP-PEAP	WPA-EAP FT-EAP	AES	No
802.11r (FT)	EAP-PEAP(WPA3)	WPA-EAP-SHA256 FT-EAP	AES	Yes

Note: If deploying the Cisco Desk Phone 9800 Series into an environment where other Wi-Fi phone models exist but those Wi-Fi phone models do not support 802.11r (FT), then should be able to use that same pre-existing SSID for the Cisco Desk Phone 9800 Series, but is recommended to enable 802.11r (FT) utilizing the Over the Air method on top of the other preexisting key management types (e.g. 802.1x); assuming the other Wi-Fi phone models can interoperate in an 802.11r (FT) enabled network while not utilizing 802.11r (FT).

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

Interband Roaming

The Cisco Desk Phone 9800 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 Desk Phone 9800 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 to perform interband

roaming.

Power Management

The power supply is required to enable the Cisco Desk Phone 9800 Series for wireless LAN mode, as there is no internal battery.

Wireless LAN is automatically disabled temporarily when Ethernet is connected to the Cisco Desk Phone 9800 Series but will be automatically re-enabled once Ethernet is disconnected if Wireless LAN was enabled previously.

The Cisco Desk Phone 9800 Series primarily uses fast sleep 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 Desk Phone 9800 Series uses fast-sleep 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 and 802.11g/n at a data rate of 24 Mbps or higher. To achieve this capacity, there must be minimal wireless LAN background traffic and initial radio frequency (RF) utilization.

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

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 Desk Phone 9800 Series utilizes fast-sleep 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 timely 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 Desk Phone 9800 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 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 AireOS Wireless LAN Controller and Lightweight Access Points, use the following guidelines:

- Enable **802.11r (FT)**
- **CCKM** is Disabled
- Set **Quality of Service (QoS)** to Platinum
- Set the **WMM Policy** to Required
- Ensure **Session Timeout** is enabled and configured correctly
- Ensure **Broadcast Key Interval** is enabled and configured correctly
- Ensure **Aironet IE** is Disabled
- Disable **P2P (Peer to Peer) Blocking Action**
- Ensure **Client Exclusion** is configured correctly
- Disable **DHCP Address Assignment Required**
- Set **Protected Management Frame (PMF)** to Optional or Required for WPA3
- Set **MFP Client Protection** to Optional or Required for WPA3
- 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
- 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 **802.1p tag** to 5 for the Platinum QoS profile

802.11 Network Settings

It is recommended to operate the Cisco Desk Phone 9800 Series only on the 5 GHz band due to the availability of many channels and fewer interferers compared to the 2.4 GHz band.

To use 5 GHz frequency, ensure that the 802.11a/n/ac Network Status is **Enabled**.

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

Maximum Allowed Clients can be configured as necessary.

It's recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates.

However, some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

The screenshot shows the Cisco Wireless LAN Controller configuration interface for 802.11a Global Parameters. The left sidebar contains a navigation menu with options like Access Points, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, and 802.11a/n/ac/ax. The main content area is divided into three sections: General, 802.11a Band Status, and Data Rates. The General section includes settings for Network Status (Enabled), Beacon Period (100), Fragmentation Threshold (2346), DTTPC Support (Enabled), Maximum Allowed Clients (100), RSSI Low Check (Disabled), and RSSI Threshold (-80). The 802.11a Band Status section shows Low, Mid, and High Band all set to Enabled. The Data Rates section shows rates from 6 Mbps to 54 Mbps, with 6 Mbps set to Disabled and others to Supported or Mandatory. Below this are sections for CCX Location Measurement (Mode Enabled, Interval 60) and TWT Configuration (Target Waketime and Broadcast TWT Support both Enabled).

To use 2.4 GHz, ensure that the 802.11b/g/n Network Status and 802.11g are **Enabled**.

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

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

Maximum Allowed Clients can be configured as necessary.

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

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

The screenshot shows the Cisco Wireless LAN Controller configuration interface for 802.11b/g Global Parameters. The left sidebar is identical to the previous screenshot. The main content area is divided into three sections: General, 802.11b/g Band Status, and Data Rates. The General section includes settings for Network Status (Enabled), 802.11g Support (Enabled), Beacon Period (100), Short Preamble (Enabled), Fragmentation Threshold (2346), DTTPC Support (Enabled), Maximum Allowed Clients (100), RSSI Low Check (Disabled), and RSSI Threshold (-80). The 802.11b/g Band Status section shows Mode set to Enabled and Interval set to 60. The Data Rates section shows rates from 1 Mbps to 54 Mbps, with 1 Mbps through 11 Mbps set to Disabled, 12 Mbps set to Mandatory, and 18 Mbps through 54 Mbps set to Supported. Below this are sections for CCX Location Measurement (Mode Enabled, Interval 60) and TWT Configuration (Target Waketime and Broadcast TWT Support both Enabled).

Auto RF (RRM)

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

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

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

The screenshot shows the Cisco Wireless LAN Controller configuration page for Tx Power Control (TPC). The page is titled "802.11a > RRM > Tx Power Control (TPC)". The TPC Version is set to Coverage Optimal Mode (TPCv1). The Tx Power Level Assignment Algorithm is set to Automatic, with a power level assignment method of Automatic, a maximum power level of 17 dBm, and a minimum power level of 11 dBm. The power assignment leader is RTP9-32A-WLC3 (10.81.6.70) and the last power level assignment was 463 seconds ago. The power threshold is -65 dBm and the channel aware feature is disabled. The power neighbor count is 3.

When using 5 GHz, it's recommended to limit the number of channels (e.g. 12 channels only) to avoid any potential delay in access point discovery caused by scanning many channels.

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

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

The screenshot shows the Cisco Wireless LAN Controller configuration page for Dynamic Channel Assignment (DCA). The page is titled "802.11a > RRM > Dynamic Channel Assignment (DCA)". The Dynamic Channel Assignment Algorithm is set to Automatic, with a channel assignment method of Automatic, an interval of 10 minutes, and an anchor time of 0. The channel assignment leader is RTP9-32A-WLC3 (10.81.6.70) and the last auto channel assignment was 556 seconds ago. The DCA channel sensitivity is set to Medium (15 dB) and the channel width is set to 40 MHz. The avoid check for non-DFS channel is disabled. The DCA Channel List shows channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 153, 157, and 161.

When 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 as 20 MHz even when using Cisco 802.11n Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.

The screenshot shows the Cisco Wireless LAN Controller configuration interface for Dynamic Channel Assignment (DCA). The page title is "802.11b > RRM > Dynamic Channel Assignment (DCA)".

Dynamic Channel Assignment Algorithm

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

DCA Channel List

DCA Channels: 1, 6, 11

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

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

This may be necessary if there is an intermittent source of interference in the area.

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

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

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

The screenshot shows the Cisco Wireless LAN Controller configuration interface for "802.11a/n/ac/ax Cisco APs > Configure".

General

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

11n Parameters

- 11n Supported: Yes

CleanAir

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

Antenna Parameters

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

RF Channel Assignment

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

Radar Information

- Channel: Last Heard (Secs)
- No radar detected channels

Tx Power Level Assignment

- Current Tx Power Level: 1
- Assignment Method: Global, Custom

Performance Profile

- View and edit Performance Profile for this AP
-
- Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Client Roaming

The Cisco Desk Phone 9800 Series does not utilize the RF parameters in the Client Roaming section of the Cisco Wireless LAN Controller as scanning and roaming are 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 Access Points.



The screenshot shows the Cisco Wireless LAN Controller configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS (selected), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the configuration tree with 'Wireless' expanded to 'Access Points' > 'Global Configuration'. The main content area is titled 'General' and contains the following settings:

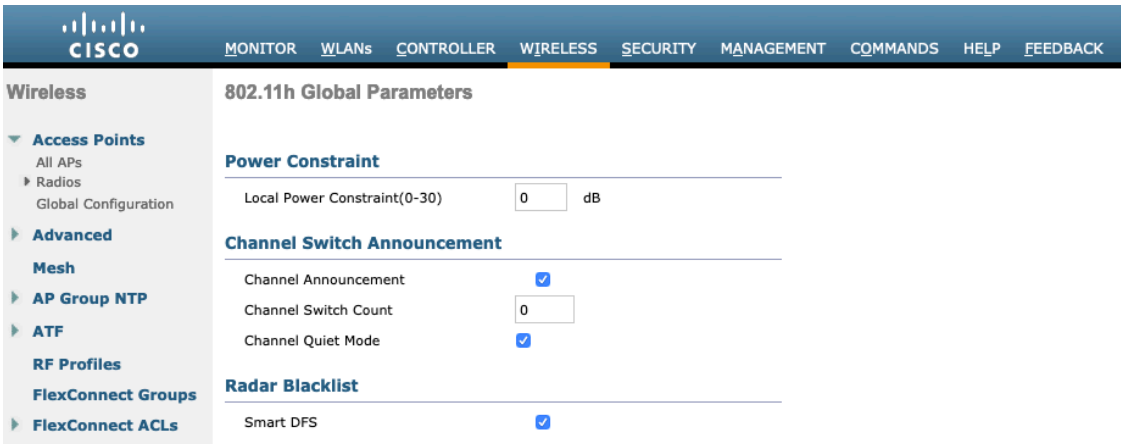
- EDCA Profile: Voice & Video Optimized (dropdown menu)
- Enable Low Latency MAC: (disabled)

A blue note at the bottom of the configuration area states: "Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled."

DFS (802.11h)

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

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



The screenshot shows the Cisco Wireless LAN Controller configuration interface for '802.11h Global Parameters'. The top navigation bar is the same as in the previous screenshot. The left sidebar shows the configuration tree with 'Wireless' expanded to 'Access Points' > 'Global Configuration'. The main content area is titled '802.11h Global Parameters' and contains the following settings:

- Power Constraint**
 - Local Power Constraint(0-30): 0 dB
- Channel Switch Announcement**
 - Channel Announcement: (enabled)
 - Channel Switch Count: 0
 - Channel Quiet Mode: (enabled)
- Radar Blacklist**
 - Smart DFS: (enabled)

High Throughput (802.11n/ac)

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

802.11ac data rates are applicable to 5 GHz only.

Ensure that **WMM** is enabled and WPA2/WPA3(AES) is configured to utilize 802.11n/ac data rates.

The Cisco Desk Phone 9800 Series supports HT MCS 0 – MCS 7 and VHT MCS 0 – MCS 9 1SS data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n/ac clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of those higher data rates.

The screenshot displays the Cisco Wireless LAN Controller configuration interface for 802.11n/ac/ax (5 GHz) Throughput. The left sidebar shows the navigation menu with '802.11a/n/ac/ax' selected. The main content area is divided into several sections:

- General:** 11n Mode, 11ac Mode, and 11ax Mode are all enabled.
- VHT MCS Rates:** SS1, SS2, SS3, SS4, SS5, and SS6 are configured with various sub-streams (0-8, 0-9, 0-7, 0-11) and are all enabled.
- HE MCS Rates:** SS1, SS2, SS3, SS4, SS5, and SS6 are configured with various sub-streams (0-7, 0-9, 0-11) and are all enabled.
- MCS (Data Rate) Settings:** A table showing MCS values from 0 to 31, their corresponding data rates in Mbps, and their support status (all are 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 Desk Phone 9800 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 according to the Cisco Desk Phone 9800 Series requirements.

To configure the 5 GHz settings, enable the 802.11a network first, then re-enable it after the changes are complete.

```

config 802.11a 11nSupport a-msdu tx priority 1 enable
config 802.11a 11nSupport a-msdu tx priority 2 enable
config 802.11a 11nSupport a-msdu tx priority 0 disable
config 802.11a 11nSupport a-msdu tx priority 3 disable
config 802.11a 11nSupport a-msdu tx priority 4 disable

```

```
config 802.11a 11nSupport a-msdu tx priority 5 disable
config 802.11a 11nSupport a-msdu tx priority 6 disable
config 802.11a 11nSupport a-msdu tx priority 7 disable
```

```
config 802.11a 11nSupport a-mpdu tx priority 0 enable
config 802.11a 11nSupport a-mpdu tx priority 3 enable
config 802.11a 11nSupport a-mpdu tx priority 4 enable
config 802.11a 11nSupport a-mpdu tx priority 5 enable
config 802.11a 11nSupport a-mpdu tx priority 1 disable
config 802.11a 11nSupport a-mpdu tx priority 2 disable
config 802.11a 11nSupport a-mpdu tx priority 6 disable
config 802.11a 11nSupport a-mpdu tx priority 7 disable
```

To configure the 2.4 GHz settings, enable the 802.11b/g network first, then re-enable it after the changes are complete.

```
config 802.11b 11nSupport a-msdu tx priority 1 enable
config 802.11b 11nSupport a-msdu tx priority 2 enable
config 802.11b 11nSupport a-msdu tx priority 0 disable
config 802.11b 11nSupport a-msdu tx priority 3 disable
config 802.11b 11nSupport a-msdu tx priority 4 disable
config 802.11b 11nSupport a-msdu tx priority 5 disable
config 802.11b 11nSupport a-msdu tx priority 6 disable
config 802.11b 11nSupport a-msdu tx priority 7 disable
```

```
config 802.11b 11nSupport a-mpdu tx priority 0 enable
config 802.11b 11nSupport a-mpdu tx priority 3 enable
config 802.11b 11nSupport a-mpdu tx priority 4 enable
config 802.11b 11nSupport a-mpdu tx priority 5 enable
config 802.11b 11nSupport a-mpdu tx priority 1 disable
config 802.11b 11nSupport a-mpdu tx priority 2 disable
config 802.11b 11nSupport a-mpdu tx priority 6 disable
config 802.11b 11nSupport a-mpdu tx priority 7 disable
```

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

802.11n Status:

A-MSDU Tx:

```
Priority 0..... Disabled
Priority 1..... Enabled
Priority 2..... Enabled
Priority 3..... Disabled
Priority 4..... Disabled
Priority 5..... Disabled
Priority 6..... Disabled
Priority 7..... Disabled
```

A-MPDU Tx:

```
Priority 0..... Enabled
Priority 1..... Disabled
Priority 2..... Disabled
Priority 3..... Enabled
Priority 4..... Enabled
```

Priority 5..... Enabled
 Priority 6..... Disabled
 Priority 7..... Disabled

CleanAir

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

802.11a > CleanAir

CleanAir/Spectrum Intelligence Parameters

CleanAir Enabled
 Spectrum Intelligence³ Enabled
 Report Interferers¹ Enabled
 Persistent Device Propagation Enabled

Interferences to Ignore

Canopy
 WiMax Fixed
 SI_FHSS

Interferences to Detect

TDD Transmitter
 Jammer
 Continuous Transmitter
 DECT-like Phone
 Video Camera

Trap Configurations

Enable AQI(Air Quality Index) Trap Enabled
 AQI Alarm Threshold (1 to 100)²
 Enable trap for Unclassified Interferences Enabled
 Threshold for Unclassified category trap (1 to 99)
 Enable trap for Classified Interferences Enabled
 Threshold for Classified category trap (1 to 99)
 Enable Interference For Security Alarm Enabled

Do not trap on these types

TDD Transmitter
 Continuous Transmitter
 DECT-like Phone
 Video Camera
 SuperAG

Trap on these types

Jammer
 WiFi Inverted
 WiFi Invalid Channel

Event Driven RRM ([Change Settings](#))

EDRRM	Disabled
Sensitivity Threshold	N/A
Rogue Contribution	N/A
Rogue Duty-Cycle	N/A

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

The screenshot shows the Cisco Wireless configuration interface for a specific AP. The left sidebar contains a navigation menu with categories like Access Points, Advanced, Mesh, AP Group NTP, ATF, RF Profiles, FlexConnect Groups, FlexConnect ACLs, FlexConnect VLAN Templates, Network Lists, 802.11a/n/ac/ax, 802.11b/g/n/ax, Media Stream, Application Visibility And Control, Lync Server, Country, Timers, Netflow, and QoS. The main content area is titled '802.11a/n/ac/ax Cisco APs > Configure' and is divided into several sections:

- General:** AP Name (rtp9-31a-ap1), Admin Status (Enable), Operational Status (UP), Slot # (1).
- 11n Parameters:** 11n Supported (Yes).
- CleanAir:** CleanAir Capable (Yes), CleanAir Admin Status (Enable), Number of Spectrum Expert connections (0). A note states: '* CleanAir enable will take effect only if it is enabled on this band.'
- Antenna Parameters:** Antenna Type (Internal), Antenna (A, B, C, D) with checkboxes for B, C, and D.
- RF Channel Assignment:** Current Channel (48,44), Channel Width (40 MHz), Assignment Method (Global).
- Radar Information:** Channel, Last Heard (Secs), No radar detected channels.
- Tx Power Level Assignment:** Current Tx Power Level (1), Assignment Method (Global).
- Performance Profile:** View and edit Performance Profile for this AP, with a 'Performance Profile' button.

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

Rx Sop Threshold

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

The screenshot shows the Cisco Wireless configuration interface for the 'Rx Sop Threshold' section. The left sidebar is similar to the previous screenshot, with 'Rx Sop Threshold' selected under the 'Advanced' category. The main content area is titled 'Rx Sop Threshold' and contains the following configuration options:

- Rx Sop Threshold 802.11a:** Default (0) [Custom]
- Rx Sop Threshold 802.11b:** Default (0) [Custom]

A note below the configuration options states: 'Rx sop only supported in Local, Flex, Bridge and Flex+Bridge mode Aps.'

WLAN Settings

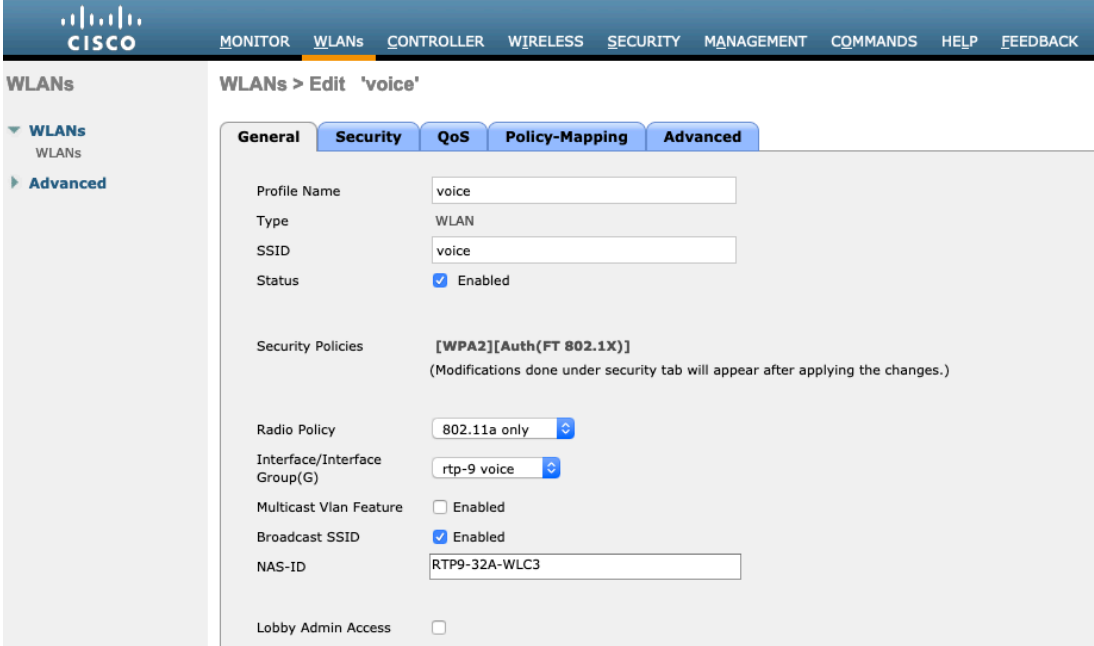
It is recommended to have a separate SSID for the Cisco Desk Phone 9800 Series.

However, you can also use an existing SSID that is configured to support voice capable Cisco Wireless LAN endpoints.

The SSID to be used by the Cisco Desk Phone 9800 Series can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

It is recommended to operate the Cisco Desk Phone 9800 Series on the 5 GHz band only due to availability of many channels and fewer interferers compared to the 2.4 GHz band.

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 when a different security type is utilized.



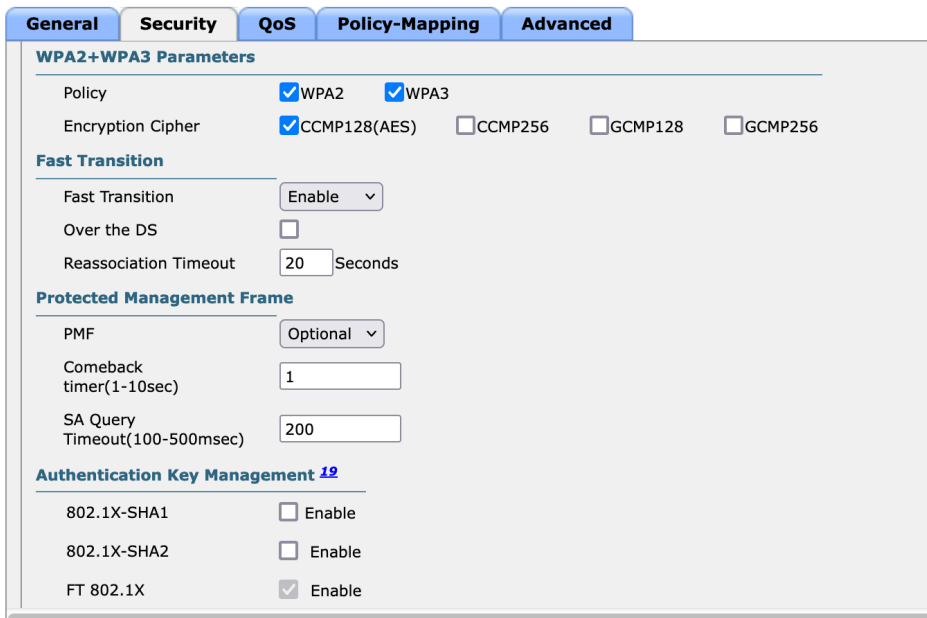
To utilize 802.11r (FT) for fast secure roaming, enable Fast Transition.

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

Protected Management Frame should be set to **Optional** or **Required** for WPA3.

Enable WPA2/WPA3 policy with AES encryption then FT 802.1x, FT PSK or FT SAE for authenticated key management type depending on whether 802.1x or PSK/SAE is to be utilized.

WLANs > Edit 'Wifi_cisco'



WLANs > Edit 'Wifi_cisco'

WPA2+WPA3 Parameters

Policy WPA2 WPA3

Encryption Cipher CCMP128(AES) CCMP256 GCMP128 GCMP256

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout Seconds

Protected Management Frame

PMF

Comeback timer(1-10sec)

SA Query Timeout(100-500msec)

Authentication Key Management ¹⁹

802.1X-SHA1 Enable

802.1X-SHA2 Enable

FT 802.1X Enable

802.11x, PSK, or SAE can be enabled to utilize the same SSID for various types of voice clients. Some clients may not support 802.11r (FT), depending on whether 802.1x, PSK, or SAE is used.

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

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

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

To configure the EAP parameters per SSID, check **Enable** in the EAP Parameters section and enter the desired values.

WLANs > Edit 'voice'

Layer 2 **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Apply Cisco ISE Default Settings Enabled

Server	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 2	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="None"/> <input type="button" value="v"/>
Server 3	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="None"/> <input type="button" value="v"/>
Server 4	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="None"/> <input type="button" value="v"/>
Server 5	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="None"/> <input type="button" value="v"/>
Server 6	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="None"/> <input type="button" value="v"/>

Authorization ACA Server Enabled

Accounting ACA Server Enabled

EAP Parameters

Enable

EAPOL Key Timeout(200 to 5000 millisc)

EAPOL Key Retries(0 to 4)

Identity Request Timeout(1 to 120 sec)

Identity Request Retries(1 to 20)

Request Timeout(1 to 120 sec)

Request Retries(1 to 20)

The WMM policy should be set to **Required** only if the Cisco Desk Phone 9800 Series or other WMM-enabled phones will be using this SSID.

If there are non-WMM clients on the WLAN, it is recommended to put those clients on a separate WLAN.

If non-WMM clients must utilize the same SSID as the Cisco Desk Phone 9800 Series, ensure the WMM policy is set to **Allowed**.

Enabling WMM will enable the 802.11e version of QBSS.

The screenshot shows the Cisco WLAN configuration interface for a 'voice' WLAN. The 'QoS' tab is selected. The configuration includes:

- Quality of Service (QoS): Platinum (voice)
- Application Visibility: Enabled
- AVC Profile: none
- Flex AVC Profile: none
- Netflow Monitor: none
- Fastlane: Disable

Below these settings is the 'Override Per-User Bandwidth Contracts (kbps)' section with a table for DownStream and UpStream rates:

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

A 'Clear' button is located below the table.

The screenshot shows the Cisco WLAN configuration interface for a 'voice' WLAN, continuing from the previous view. The 'Policy-Mapping' tab is selected. The configuration includes:

- Override Per-SSID Bandwidth Contracts (kbps): Section with a table for DownStream and UpStream rates (all values are 0).
- WMM:
 - WMM Policy: Required
 - 7920 AP CAC: Enabled
 - 7920 Client CAC: Enabled
- Media Stream:
 - Multicast Direct: Enabled
- Lync Policy:
 - Audio: Silver

Configure **Enable Session Timeout** as needed. It is recommended to enable the session timeout for 86400 seconds to avoid potential interruptions during audio calls and periodically re-validate client credentials to ensure that the client is using valid credentials.

Disable Aironet Extensions (**Aironet IE**).

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

Configure **Client Exclusion** as needed.

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

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 not preserving DSCP values for priority applications (e.g. voice and call control) to the access point, it is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well as potentially increase the scan defer time.

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

DHCP Address Assignment Required should be disabled.

Management Frame Protection should be set to Optional or Required for WPA3.

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.

Keep the default settings for 802.11k and 802.11v.

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'voice'. The 'Advanced' tab is selected, displaying various configuration options. The 'DTIM Period (in beacon intervals)' section is highlighted, showing settings for 802.11a/n (1 - 255) and 802.11b/g/n (1 - 255), both set to 2. Other visible settings include 'Allow AAA Override' (disabled), 'Coverage Hole Detection' (enabled), 'Enable Session Timeout' (86400), 'Aironet IE' (enabled), 'Diagnostic Channel' (disabled), 'Override Interface ACL' (IPv4: None, IPv6: None), 'Layer2 Acl' (None), 'URL ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (disabled), 'Maximum Allowed Clients' (0), 'Static IP Tunneling' (disabled), 'Wi-Fi Direct Clients Policy' (Disabled), and 'Maximum Allowed Clients Per AP Radio' (200). The 'DHCP' section shows 'DHCP Server' (Override) and 'DHCP Addr. Assignment' (Required). 'Management Frame Protection (MFP)' is set to 'Optional'. 'NAC State' is set to 'None'. 'Load Balancing and Band Select' options are disabled.

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'voice', specifically the 'Advanced' tab. The 'Per AP Radio' section includes 'Clear HotSpot Configuration' (disabled), 'Client user idle timeout(15-100000)' (disabled), 'Client user idle threshold (0-10000000)' (0 Bytes), 'Radius NAI-Realm' (disabled), '11ac MU-MIMO' (checked), 'WGB PRP' (disabled), and 'MBO State' (disabled). The 'Off Channel Scanning Defer' section shows 'Scan Defer Priority' (0-7) with 4, 5, and 6 selected, and 'Scan Defer Time(msecs)' (100). The 'FlexConnect' section has 'FlexConnect Local Switching' (disabled). The 'Passive Client' section has 'Passive Client' (disabled). The 'Voice' section includes 'Media Session Snooping' (disabled), 'Re-anchor Roamed Voice Clients' (disabled), and 'KTS based CAC Policy' (disabled). The 'Radius Client Profiling' section has 'DHCP Profiling' (disabled) and 'HTTP Profiling' (disabled). The 'Local Client Profiling' section has 'DHCP Profiling' (disabled) and 'HTTP Profiling' (disabled). The 'PMIP' section has 'PMIP Mobility Type' (disabled) and 'PMIP NAI Type' (Hexadecimal).

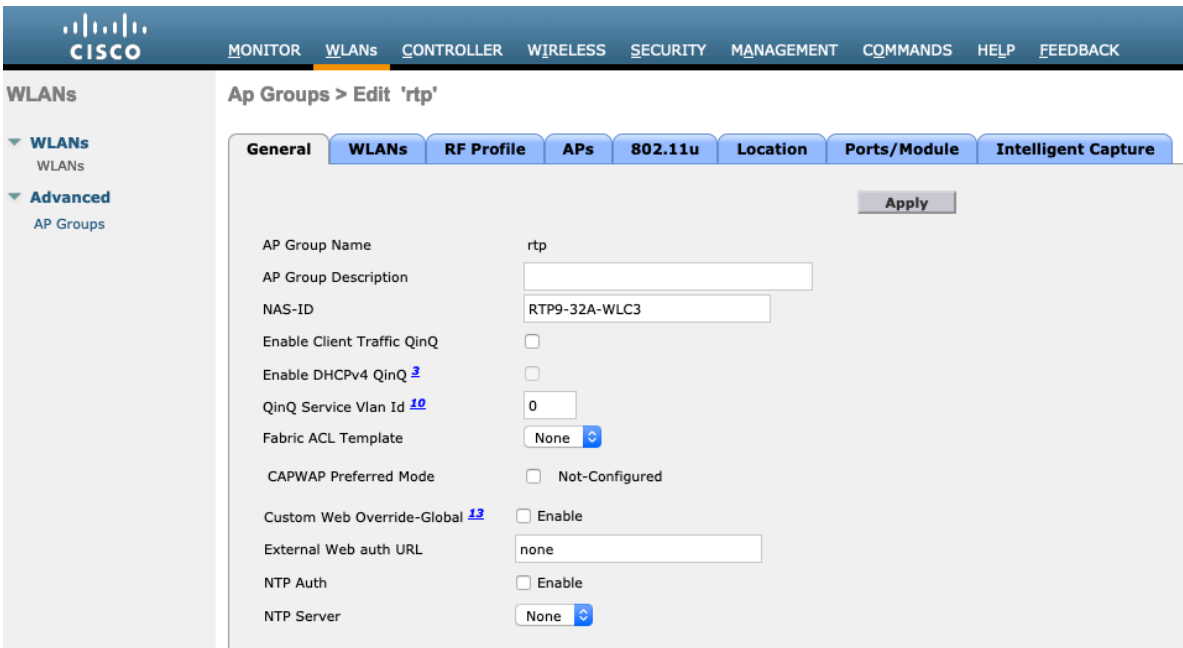
The screenshot shows the Cisco WLC configuration page for a WLAN named 'voice'. The 'Security' and 'Advanced' tabs are active. Under 'Security', 'FlexConnect Local Auth' is disabled, while 'Learn Client IP Address' is enabled. Other security options like 'Vlan based Central Switching', 'Central DHCP Processing', 'Override DNS', 'NAT-PAT', and 'Central Assoc' are also disabled. Under 'Advanced', 'Lync Server' is disabled. The '802.11ax BSS Configuration' section shows 'Down Link MU-MIMO' is enabled. On the right, 'PMIP Profile' is set to 'None', 'PMIP Realm' is empty, and 'Universal AP Admin Support' is disabled. The '11v BSS Transition Support' section has 'BSS Transition' disabled, 'Disassociation Imminent' disabled, 'Disassociation Timer' set to 200, 'Optimized Roaming Disassociation Timer' set to 40, 'BSS Max Idle Service' enabled, and 'Directed Multicast Service' enabled. The 'Tunneling' section has 'Tunnel Profile' set to 'None' and 'EOGRE Vlan Override' disabled. The 'mDNS' section has 'mDNS Snooping' disabled.

This screenshot shows the '802.11ax BSS Configuration' and 'mDNS' sections of the WLAN configuration. In the '802.11ax BSS Configuration' section, 'Down Link MU-MIMO', 'Up Link MU-MIMO', 'Down Link OFDMA', and 'Up Link OFDMA' are all enabled. The 'mDNS' section shows 'mDNS Snooping' is disabled. The 'TrustSec' section has 'Security Group Tag' set to 0. The 'Umbrella' section has 'Umbrella Mode' set to 'Ignore', 'Umbrella Profile' set to 'None', and 'Umbrella DHCP Override' enabled. The 'Fabric Configuration' section has 'Fabric' disabled. The 'Mobility' section has 'Selective Reanchor' disabled. The 'U3 Interface' section has 'U3 Interface' disabled and 'U3 Reporting Interval' set to 30.

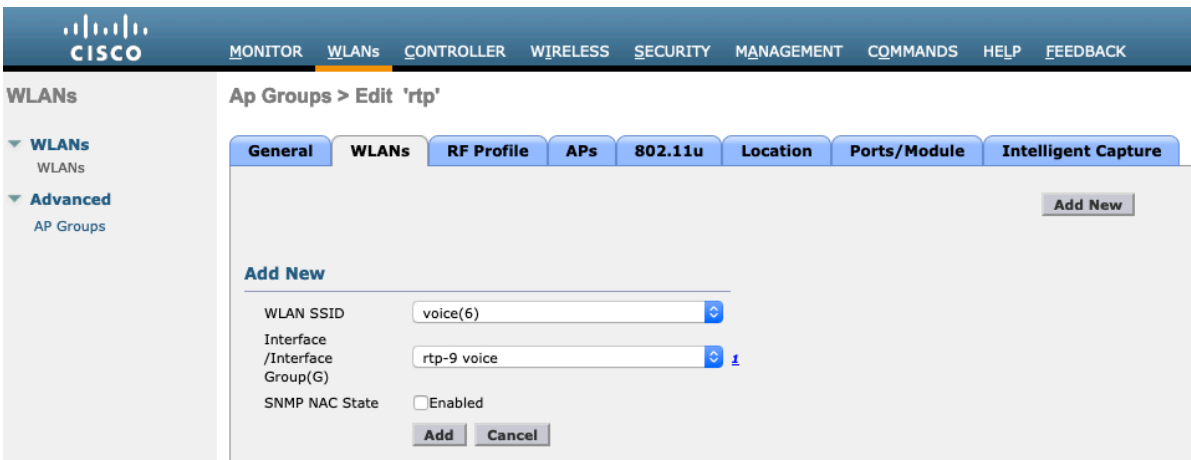
AP Groups

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.

The screenshot shows the 'Add New AP Group' form in the Cisco WLC configuration. The 'AP Group Name' field contains 'rtp'. The 'Description' field is empty. There are 'Add' and 'Cancel' buttons at the bottom of the form.

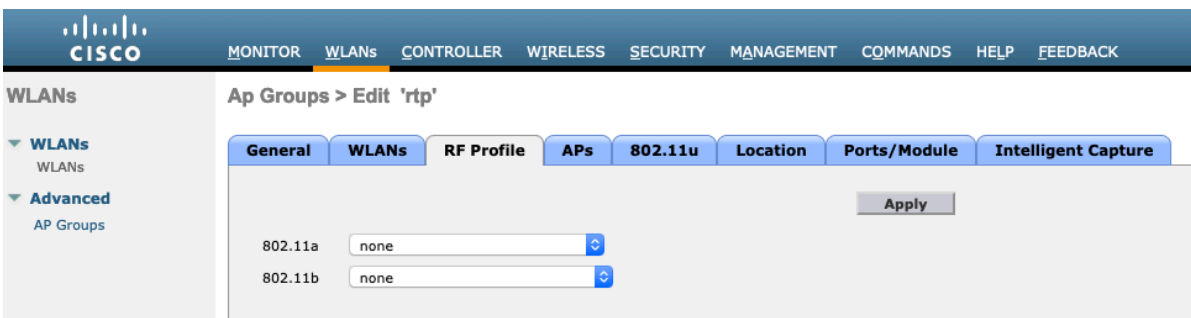


On the **WLANs** tab, select the desired SSIDs and interfaces to map to then select **Add**.



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

If changes are made after access points have joined the AP Group, then those access points will reboot once those changes are made.



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

Those access points will then reboot.

The screenshot shows the Cisco Wireless LAN Controller interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar shows: WLANs, Advanced, AP Groups. The main content area is titled "Ap Groups > Edit 'rtp'". It has tabs for: General, WLANs, RF Profile, APs, 802.11u, Location, Ports/Module, Intelligent Capture. Below the tabs, there are two sections: "APs currently in the Group" and "Add APs to the Group".

AP Name	Ethernet MAC
<input type="checkbox"/> rtp9-31a-ap14	00:81:c4:96:78:28
<input type="checkbox"/> rtp9-32a-ap20	00:81:c4:32:b9:b8
<input type="checkbox"/> rtp9-32a-ap23	00:81:c4:96:74:10

Controller Settings

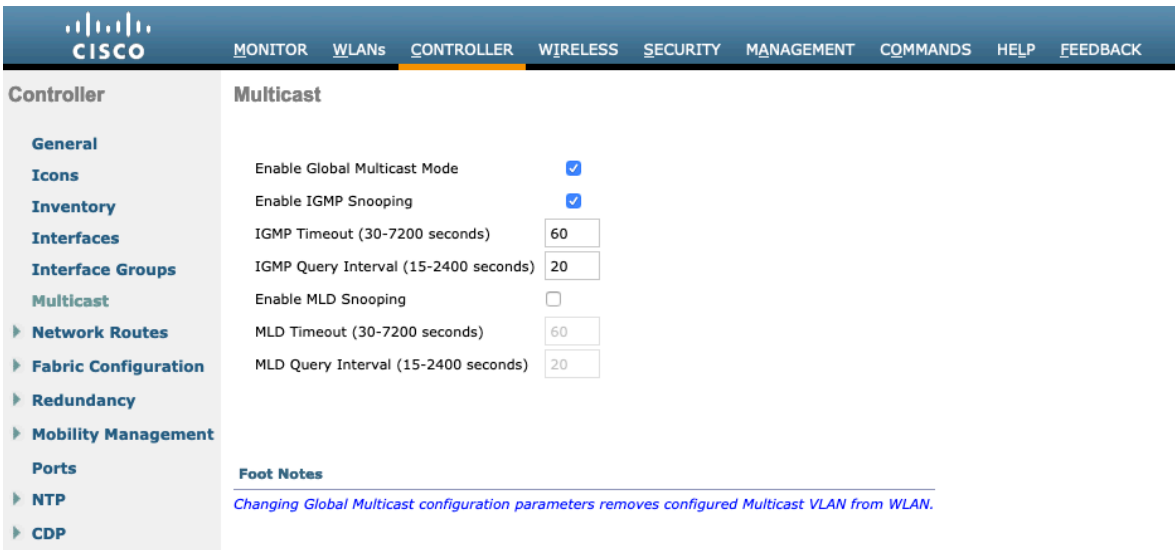
Ensure the Cisco Wireless LAN Controller hostname is configured correctly.
 Enable Link Aggregation (LAG) when utilizing multiple ports on the Cisco Wireless LAN Controller.
 Configure the desired AP multicast mode.

The screenshot shows the Cisco Wireless LAN Controller interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar shows: Controller, General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, Mobility Management, Ports, NTP, CDP, PMIPv6, Tunneling, IPv6, mDNS, Advanced, Lawful Interception. The main content area is titled "General".

Name	RTP9-32A-WLC3
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Multicast 239.1.1.9 Multicast Group Address
AP IPv6 Multicast Mode	Multicast ff1e::239:100:100:21 IPv6 Multicast Group Address
AP Fallback	Enabled
CAPWAP Preferred Mode	ipv4
Fast SSID change	Enabled
Link Local Bridging	Disabled
Default Mobility Domain Name	CTG-VoWLAN2
RF Group Name	RTP9-VoWLAN2
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
ARP Unicast Mode	Disabled
Web Radius Authentication	PAP
Operating Environment	Commercial (10 to 35 C)
Internal Temp Alarm Limits	10 to 38 C
WebAuth Proxy Redirection Mode	Disabled
WebAuth Proxy Redirection Port	0
Captive Network Assistant Bypass	Disabled
Global IPv6 Config	Disabled
Web Color Theme	Default
HA SKU secondary unit	Disabled
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 FlexConnect on this platform. Multicast-Unicast mode does not support IGMP/MLD Snooping. Disable Global Multicast first.
 2. Changes in Web color Theme will get updated after browser Refresh.

To utilize multicast, **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be checked.



Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Fabric Configuration
- Redundancy
- Mobility Management
- Ports
- NTP
- CDP

Multicast

Enable Global Multicast Mode

Enable IGMP Snooping

IGMP Timeout (30-7200 seconds)

IGMP Query Interval (15-2400 seconds)

Enable MLD Snooping

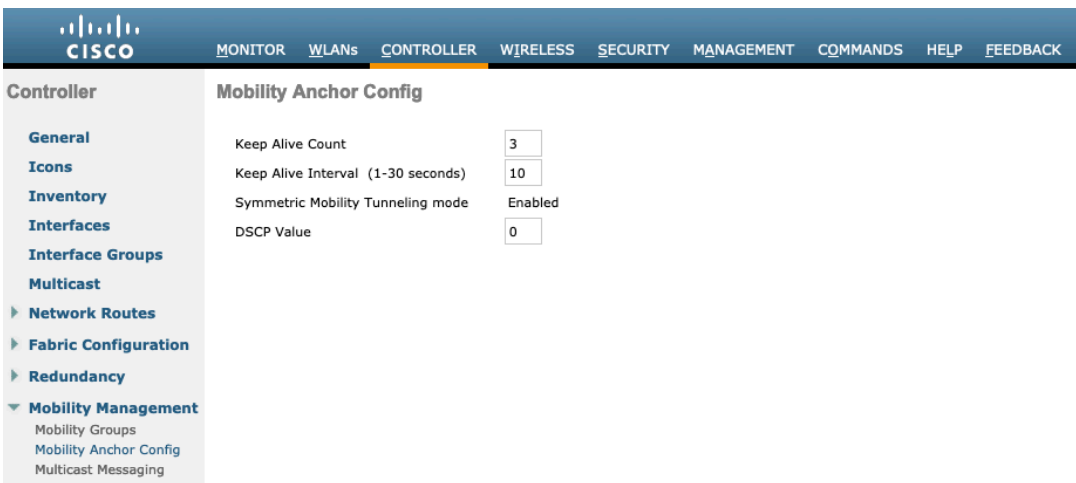
MLD Timeout (30-7200 seconds)

MLD Query Interval (15-2400 seconds)

Foot Notes

Changing Global Multicast configuration parameters removes configured Multicast VLAN from WLAN.

When utilizing layer 3 mobility, **Symmetric Mobility Tunneling** should be **Enabled**.
 In the recent versions, Symmetric Mobility Tunneling is enabled by default and non-configurable.



Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Fabric Configuration
- Redundancy
- Mobility Management
 - Mobility Groups
 - Mobility Anchor Config
 - Multicast Messaging

Mobility Anchor Config

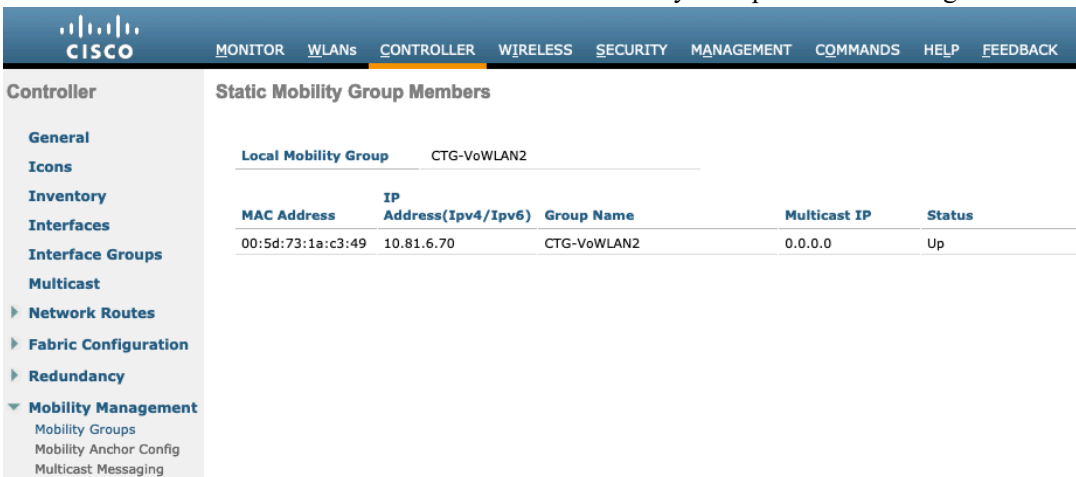
Keep Alive Count

Keep Alive Interval (1-30 seconds)

Symmetric Mobility Tunneling mode Enabled

DSCP Value

When multiple Cisco Wireless LAN Controllers are part of the same mobility group, ensure to add the IP address and MAC address of each Cisco Wireless LAN Controller to the Static Mobility Group Members configuration.



Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Fabric Configuration
- Redundancy
- Mobility Management
 - Mobility Groups
 - Mobility Anchor Config
 - Multicast Messaging

Static Mobility Group Members

Local Mobility Group CTG-VoWLAN2

MAC Address	IP Address (IPv4/IPv6)	Group Name	Multicast IP	Status
00:5d:73:1a:c3:49	10.81.6.70	CTG-VoWLAN2	0.0.0.0	Up

Call Admission Control (CAC)

Admission Control Mandatory for Voice and Video should be disabled.

Voice **Video** **Media**

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method ⁴

Max RF Bandwidth (5-85)(%)

Reserved Roaming Bandwidth (0-25)(%)

Expedited bandwidth

SIP CAC Support ² Enabled

Per-Call SIP Bandwidth ²

SIP Codec

SIP Bandwidth (kbps)

SIP Voice Sample Interval (msecs)

Traffic Stream Metrics

Metrics Collection

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

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

802.11a(5 GHz) > Media

Voice **Video** **Media**

Call Admission Control (CAC)

Admission Control (ACM) Enabled

CAC Method ⁴

Max RF Bandwidth (5-85)(%)

Reserved Roaming Bandwidth (0-25)(%)

SIP CAC Support ² Enabled

Foot Notes

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

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

802.11a(5 GHz) > Media

General

Unicast Video Redirect

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%))

Client Minimum Phy Rate

Maximum Retry Percent (0-100%)

Media Stream - Multicast Direct Parameters

Multicast Direct Enable

Max Streams per Radio

Max Streams per Client

Best Effort QoS Admission Enabled

Foot Notes

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

RF Profiles

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

For the SSID used by the Cisco Desk Phone 9800 Series, it's recommended to apply it 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**.

RF Profile > New

RF Profile Name

Radio Policy

Use default RF Profile Template

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

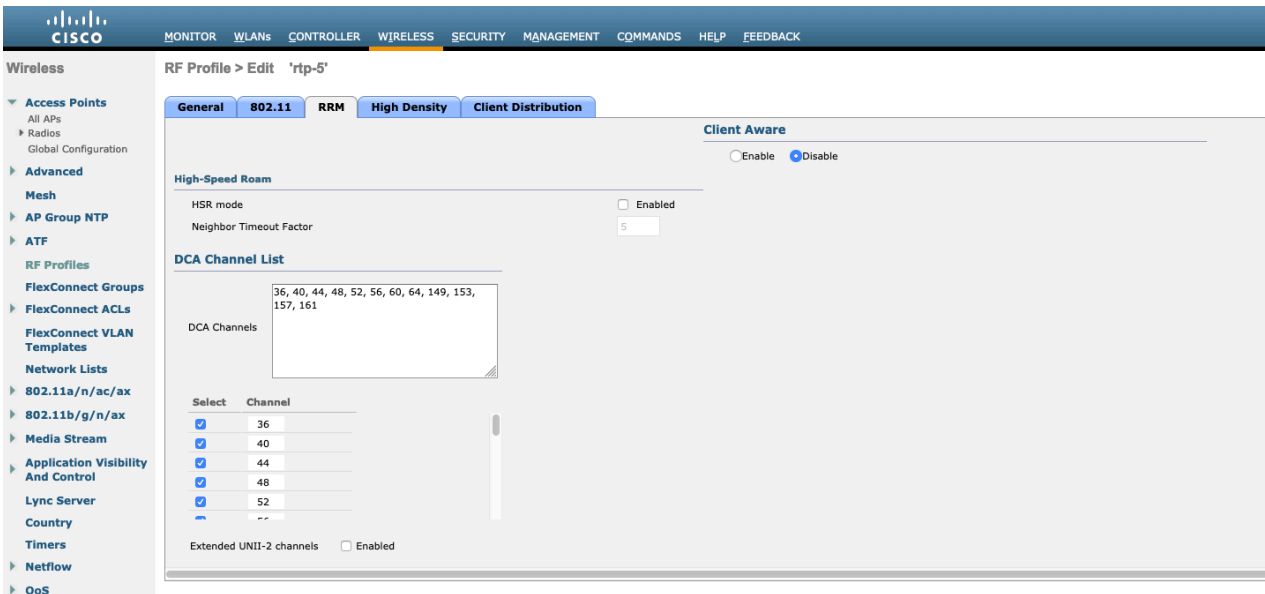
It is recommended to enable 12 Mbps as **Mandatory** and 18 Mbps and higher as **Supported**. However, some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

The screenshot shows the Cisco Wireless configuration interface for an RF Profile named 'rtp-5'. The 'RRM' tab is selected, and the 'Data Rates' and 'MCS Settings' sections are visible. The 'Data Rates' section shows various data rates with their status (e.g., Disabled, Mandatory, Supported). The 'MCS Settings' section shows MCS values from 0 to 16, all of which are checked as 'Supported'.

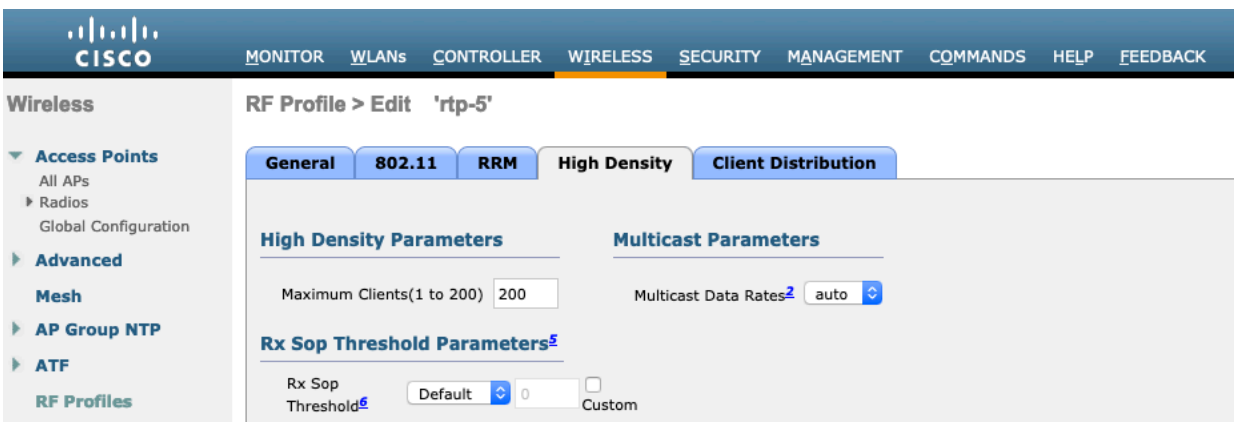
Data Rate	Status	MCS	Status
6 Mbps	Disabled	0	Supported
9 Mbps	Disabled	1	Supported
12 Mbps	Mandatory	2	Supported
18 Mbps	Supported	3	Supported
24 Mbps	Supported	4	Supported
36 Mbps	Supported	5	Supported
48 Mbps	Supported	6	Supported
54 Mbps	Supported	7	Supported
		8	Supported
		9	Supported
		10	Supported
		11	Supported
		12	Supported
		13	Supported
		14	Supported
		15	Supported
		16	Supported

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.

The screenshot shows the Cisco Wireless configuration interface for an RF Profile named 'rtp-5'. The 'RRM' tab is selected, and the 'TPC', 'DCA', 'Coverage Hole Detection', 'Profile Threshold For Traps', 'Client Network Preference', and 'Client Aware' sections are visible. The 'TPC' section shows Maximum Power Level Assignment (30), Minimum Power Level Assignment (-10), Power Threshold v1 (-70), and Power Threshold v2 (-67). The 'DCA' section shows 'Avoid Foreign AP Interference' (Enabled) and 'Channel Width' (40 MHz). The 'Coverage Hole Detection' section shows Data RSSI (-80), Voice RSSI (-80), Coverage Exception (25), and Coverage Level (3). The 'Profile Threshold For Traps' section shows Interference (10), Clients (12), Noise (-70), and Utilization (80). The 'Client Network Preference' section shows 'Automatic' selected. The 'Client Aware' section shows 'Disable' selected.



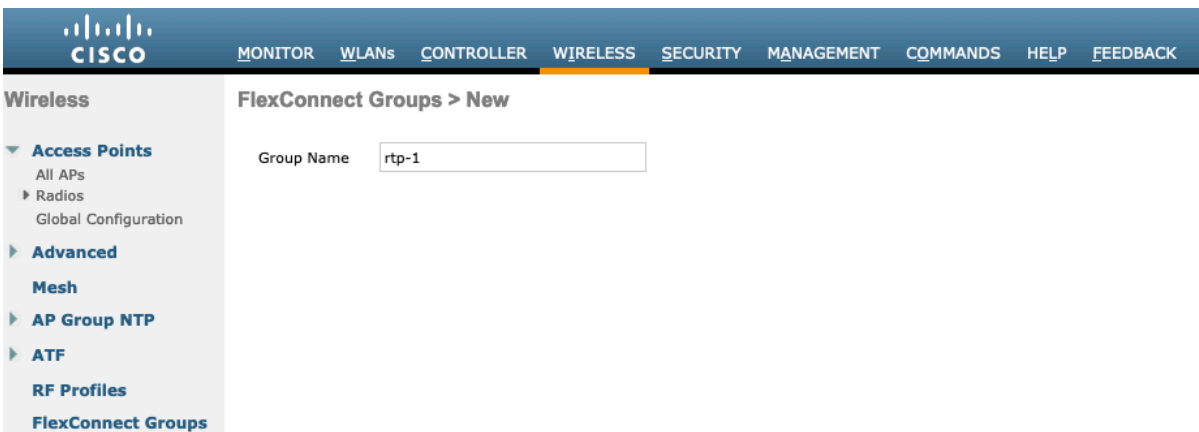
On the **High Density** tab, **Maximum Clients**, **Multicast Data Rates**, and **Rx Sop Threshold** can be configured. It is recommended to use the default value for **Rx Sop Threshold**.



FlexConnect Groups

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

When utilizing 802.11r (FT), seamless roaming can only occur when roaming to access points within the same FlexContext Group.



The screenshot shows the Cisco WLC configuration interface for a FlexConnect Group named 'rtp-1'. The 'General' tab is selected, displaying the following configuration options:

- Group Name:** rtp-1
- VLAN Template Name:** none
- Enable AP Local Authentication:**
- FlexConnect AP:** (Section header)
- HTTP-Proxy:**
 - Ip Address (Ipv4/Ipv6):** [Empty field]
 - Port:** 0
 - Add:** [Add button]
- AAA:**
 - Server Ip Address:** [Empty field]
 - Server Type:** Primary
 - Shared Secret:** [Empty field]
 - Confirm Shared Secret:** [Empty field]
 - Port Number:** 1812
 - Add:** [Add button]

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

The screenshot shows the 'FlexConnect Group AP List' configuration page for group 'rtp-1'. The page displays the group name and a table for listing APs. The table has the following columns: AP MAC Address, AP Name, Status, AP Mode, Type, and Conflict with PnP. There are 0 entries currently listed. An 'Add AP' button is visible above the table.

The screenshot shows the 'Add AP' dialog box for group 'rtp-1'. The dialog box has the following options:

- Select APs from current controller:**
- Ethernet MAC:** [Text input field]
- Add:** [Add button]
- Cancel:** [Cancel button]

Multicast Direct

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

Wireless

MONITOR WLANs CONTROLLER **WIRELESS** SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Media Stream >General

Multicast Direct feature Enabled

Session Message Config

Session announcement State Enabled

Session announcement URL

Session announcement Email

Session announcement Phone

Session announcement Note

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
 - Mesh
 - AP Group NTP
 - ATF
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
 - Network Lists
 - 802.11a/n/ac/ax
 - 802.11b/g/n/ax
- Media Stream
 - General
 - Streams

Wireless

MONITOR WLANs CONTROLLER **WIRELESS** SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Media Streams Entries 1 - 1 of 1

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

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
 - Mesh
 - AP Group NTP
 - ATF
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
 - Network Lists
 - 802.11a/n/ac/ax
 - 802.11b/g/n/ax
- Media Stream
 - General
 - Streams

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

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'voice'. The 'QoS' tab is selected, and the 'Override Per-SSID Bandwidth Contracts (kbps)' section is expanded. The configuration includes:

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

Below this, the 'WMM' section is configured with 'Required' policy, '7920 AP CAC' enabled, and '7920 Client CAC' disabled. The 'Media Stream' section has 'Multicast Direct' enabled. The 'Lync Policy' section has 'Audio' set to 'Silver'.

QoS Profiles

Configure the four QoS profiles (Platinum, Gold, Silver, Bronze), by selecting 802.1p as the protocol type and set the **802.1p** tag for each profile.

- Platinum = 5
- Gold = 4
- Silver = 2
- Bronze = 1

The screenshot shows the 'Edit QoS Profile' page for a profile named 'platinum'. The configuration includes:

- QoS Profile Name:** platinum
- Description:** For Voice Applications
- Per-User Bandwidth Contracts (kbps) *:**

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

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0
- WLAN QoS Parameters:**
 - Maximum Priority: voice
 - Unicast Default Priority: besteffort
 - Multicast Default Priority: besteffort
- Wired QoS Protocol:**
 - Protocol Type: 802.1p
 - 802.1p Tag: 5

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
 - Mesh
 - AP Group NTP
 - ATF
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
 - Network Lists
 - 802.11a/n/ac/ax
 - 802.11b/g/n/ax
 - Media Stream
 - Application Visibility And Control
 - Lync Server
 - Country
 - Timers
 - Netflow
 - QoS
 - Profiles
 - Roles
 - Qos Map

Edit QoS Profile

QoS Profile Name gold

Description For Video Applications

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority video

Unicast Default Priority video

Multicast Default Priority video

Wired QoS Protocol

Protocol Type 802.1p

802.1p Tag 4

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
 - Mesh
 - AP Group NTP
 - ATF
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
 - Network Lists
 - 802.11a/n/ac/ax
 - 802.11b/g/n/ax
 - Media Stream
 - Application Visibility And Control
 - Lync Server
 - Country
 - Timers
 - Netflow
 - QoS
 - Profiles
 - Roles
 - Qos Map

Edit QoS Profile

QoS Profile Name silver

Description For Best Effort

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority besteffort

Unicast Default Priority besteffort

Multicast Default Priority besteffort

Wired QoS Protocol

Protocol Type 802.1p

802.1p Tag 0

Wireless

- Access Points
 - All APs
 - Radios
 - Global Configuration
- Advanced
- Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
- 802.11b/g/n/ax
- Media Stream
- Application Visibility And Control
- Lync Server
- Country
- Timers
- Netflow
- QoS
 - Profiles
 - Roles
 - Qos Map

Edit QoS Profile

QoS Profile Name: bronze

Description: For Background

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority: background

Unicast Default Priority: background

Multicast Default Priority: background

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 1

Advanced Settings

Advanced EAP Settings

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

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

Security

- AAA
 - General
 - RADIUS
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Advanced EAP

Advanced EAP

Identity Request Timeout (in secs): 30

Identity request Max Retries: 2

Dynamic WEP Key Index: 0

Request Timeout (in secs): 30

Request Max Retries: 2

Max-Login Ignore Identity Response: enable

EAPOL-Key Timeout (in milliSeconds): 400

EAPOL-Key Max Retries: 4

EAP-Broadcast Key Interval(in secs): 3600

To view the EAP parameters on the Cisco Wireless LAN Controller via command line, enter the following command.

```
(Cisco Controller) >show advanced eap
EAP-Identity-Request Timeout (seconds)..... 30
EAP-Identity-Request Max Retries..... 2
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 30
EAP-Request Max Retries..... 2
```

EAPOL-Key Timeout (milliseconds)..... 400
EAPOL-Key Max Retries..... 4
EAP-Broadcast Key Interval..... 3600

When 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 with frequent EAP failures, the **EAP-Request Timeout** should be reduced to 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
```

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

When using 802.1x, the default values for **EAPOL-Key Timeout** and **EAPOL-Key Max Retries** should work fine, but it's still recommended to set those values to 400 and 4 respectively.

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

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

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

To change the **EAPOL-Key Max Retries** 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 be enabled optionally for protection against denial of service (DoS) attacks.

However, enabling this feature may introduce interruptions with voice over wireless LAN. Therefore, it is recommended to disable the Auto-Immune feature on the Cisco Wireless LAN Controller.

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

```
(Cisco Controller) >show wps summary
Auto-Immune
  Auto-Immune..... Disabled
Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure..... Enabled
Signature Policy
  Signature Processing..... Enabled
```

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

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

Rogue Policies

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

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu with options: AAA, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies (selected), Web Auth, TrustSec, Local Policies, Umbrella, and Advanced. The main content area is titled "Rogue Policies" and is divided into two sections: "Rogue Detection Security Level" and "Auto Contain".

Rogue Detection Security Level

Radio buttons: Low, High, Critical, Custom

Configuration items:

- Rogue Location Discovery Protocol: (dropdown)
- Expiration Timeout for Rogue AP and Rogue Client entries: Seconds
- Validate rogue clients against AAA: Enabled
- Validate rogue AP against AAA: Enabled
- Polling Interval: Seconds
- Validate rogue clients against MSE: Enabled
- Detect and report Ad-Hoc Networks: Enabled
- Rogue Detection Report Interval (10 to 300 Sec):
- Rogue Detection Minimum RSSI (-70 to -128):
- Rogue Detection Transient Interval (0, 120 to 1800 Sec):
- Rogue Client Threshold (0 to disable, 1 to 256):
- Rogue containment automatic rate selection: Enabled

Auto Contain

Configuration items:

- Auto Containment Level: (dropdown)
- Auto Containment only for Monitor mode APs: Enabled
- Auto Containment on FlexConnect Standalone: Enabled
- Rogue on Wire: Enabled
- Using our SSID: Enabled
- Valid client on Rogue AP: Enabled
- AdHoc Rogue AP: Enabled

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:

- Enable **802.11r (FT)**
- **CCKM** is Disabled.
- Set **Quality of Service (QoS) SSID Policy** to **Platinum**
- Set the **WMM Policy** to **Required**
- Ensure **Session Timeout** is enabled and configured correctly
- Ensure **Broadcast Key Interval** is enabled and configured correctly
- Ensure **Aironet IE** is Disabled
- Disable **P2P (Peer to Peer) Blocking Action**
- Ensure **Client Exclusion Timeout** is configured correctly
- Disable **DHCP Required**
- Set **Protected Management Frame (PMF)** to **Optional** or **Required** for WPA3
- 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 operate the Cisco Desk Phone 9800 Series only on the 5 GHz band due to the availability of many channels and fewer interferers compared to the 2.4 GHz band.

To use 5 GHz, ensure the **5 GHz Network Status** is **Enabled**.

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

It's 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.

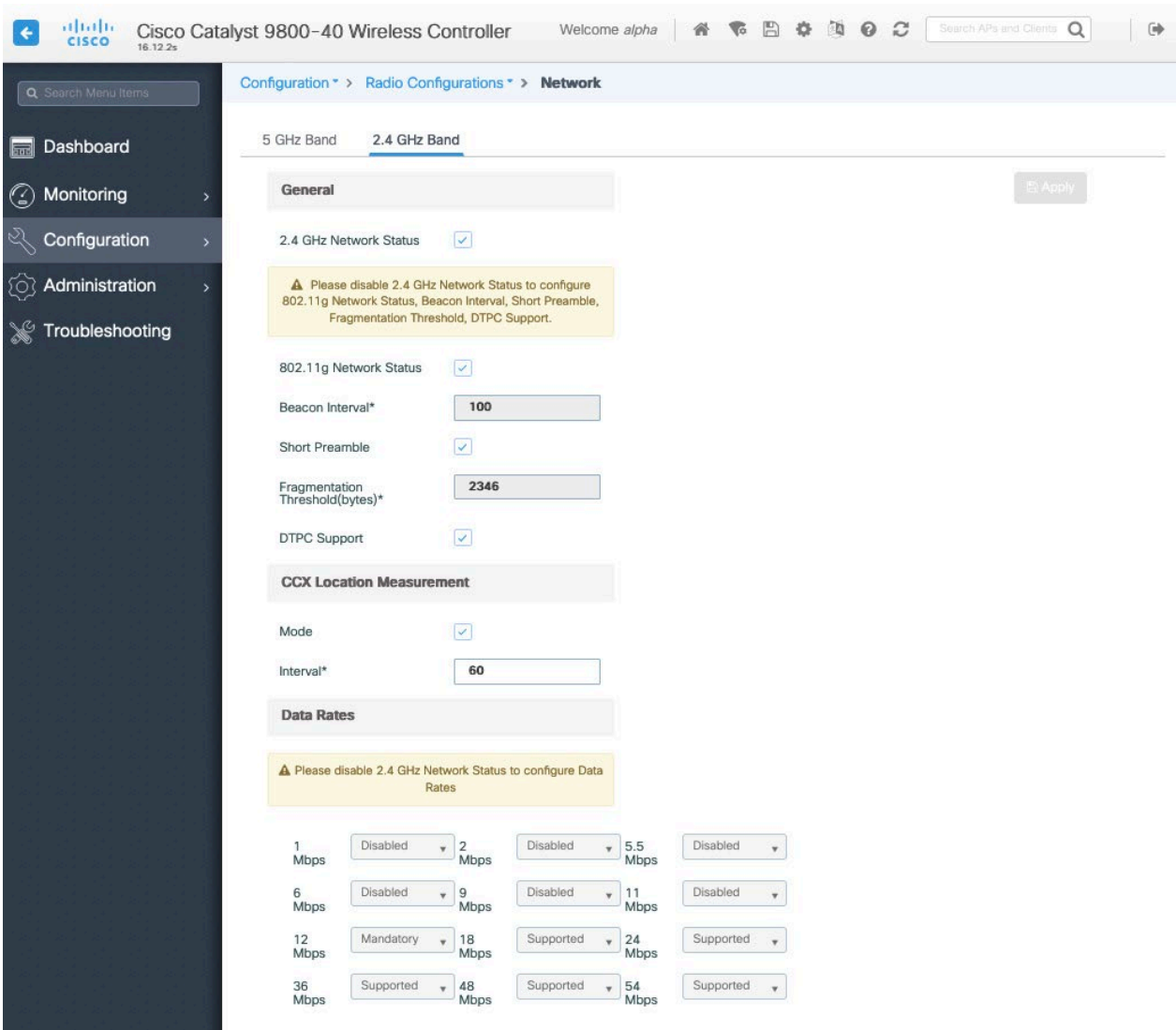
To use 2.4 GHz, ensure the **2.4 GHz Network Status** and **802.11g Network Status** are **Enabled**.

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 there's no legacy clients requiring a long preamble in the wireless LAN. By using the short preamble instead of long preamble, the wireless network performance is improved.

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

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



High Throughput (802.11n/ac)

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

802.11ac data rates are applicable to 5 GHz only.

Ensure that **WMM** is enabled and **WPA2/WPA3(AES)** is configured to utilize 802.11n/ac data rates.

The Cisco Desk Phone 9800 Series supports HT MCS 0 – MCS 7 and VHT MCS 0 – MCS 9 1SS data rates only, but higher MCS rates can be enabled optionally if there are other 802.11n/ac clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of those higher data rates.

Cisco Catalyst 9800-40 Wireless Controller 16.12.2s Welcome alpha

Configuration > Radio Configurations > High Throughput

5 GHz Band 2.4 GHz Band

Apply

11n

Enable 11n Select All

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

11ac

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

Enable 11ac Select All

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

11ax

Enable 11ax Select All

Multiple BSSIDs

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

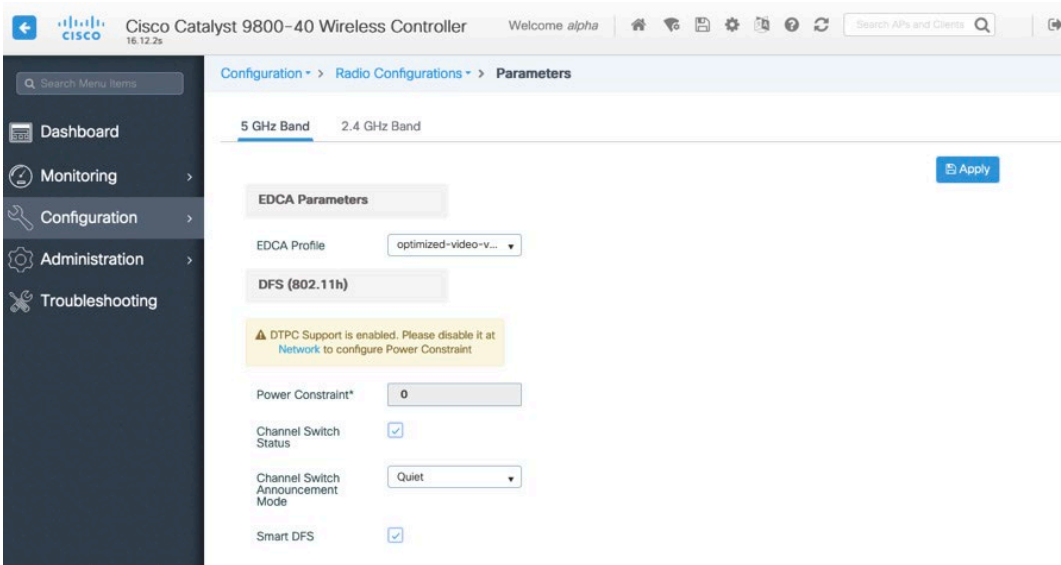
Parameters

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

In the DFS (802.11h) section, **Power Constraint** should be left un-configured or set to 0 dB.

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

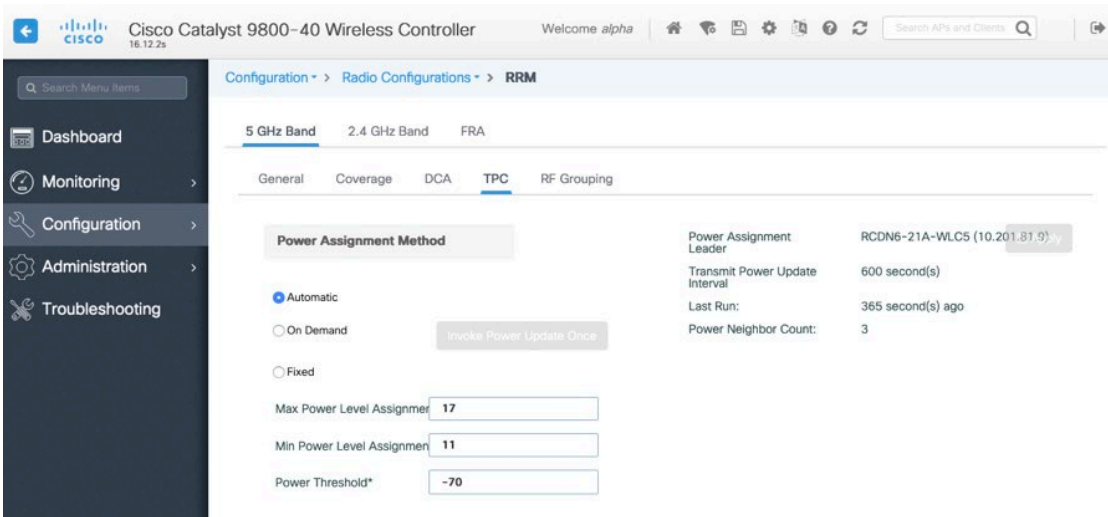
Channel Switch Announcement Mode should be set to **Quiet**.



RRM

It is recommended to enable automatic assignment method to manage the channel and transmit power settings. Configure the access point transmit power level assignment method for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

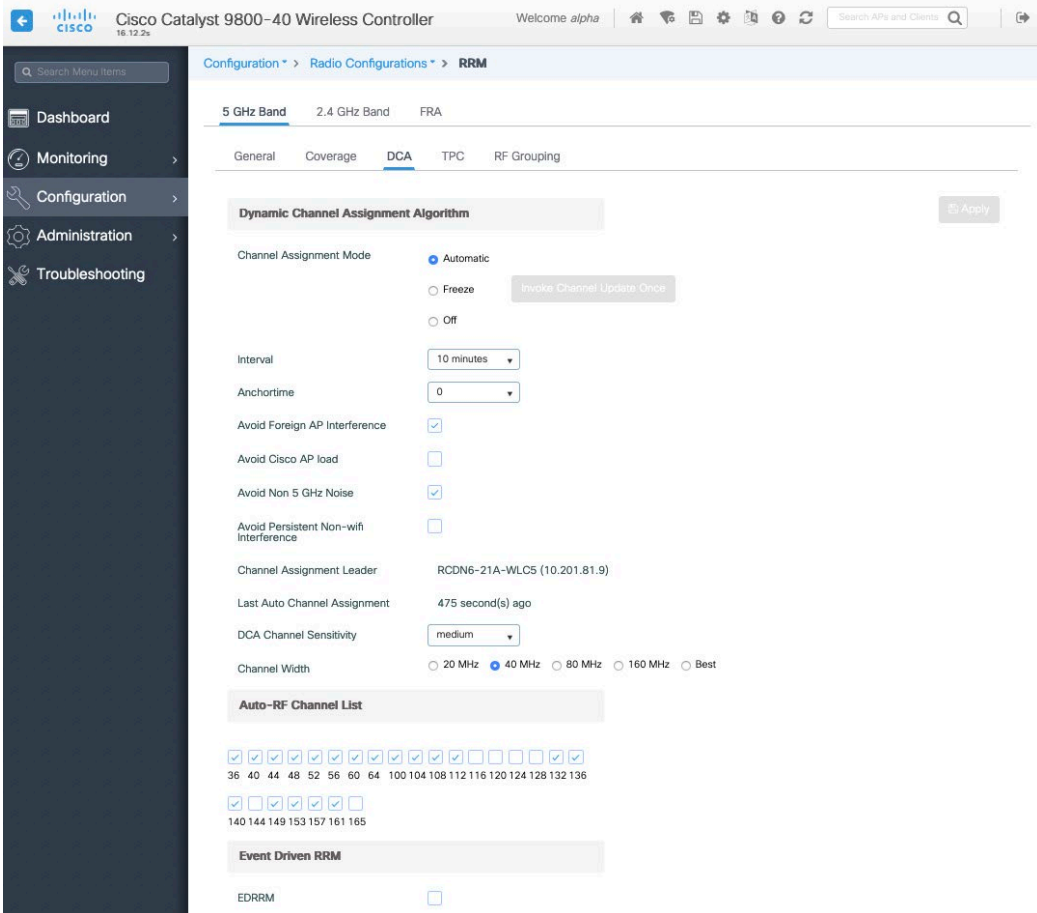
When using automatic power level assignment, a maximum and minimum power level can be specified.



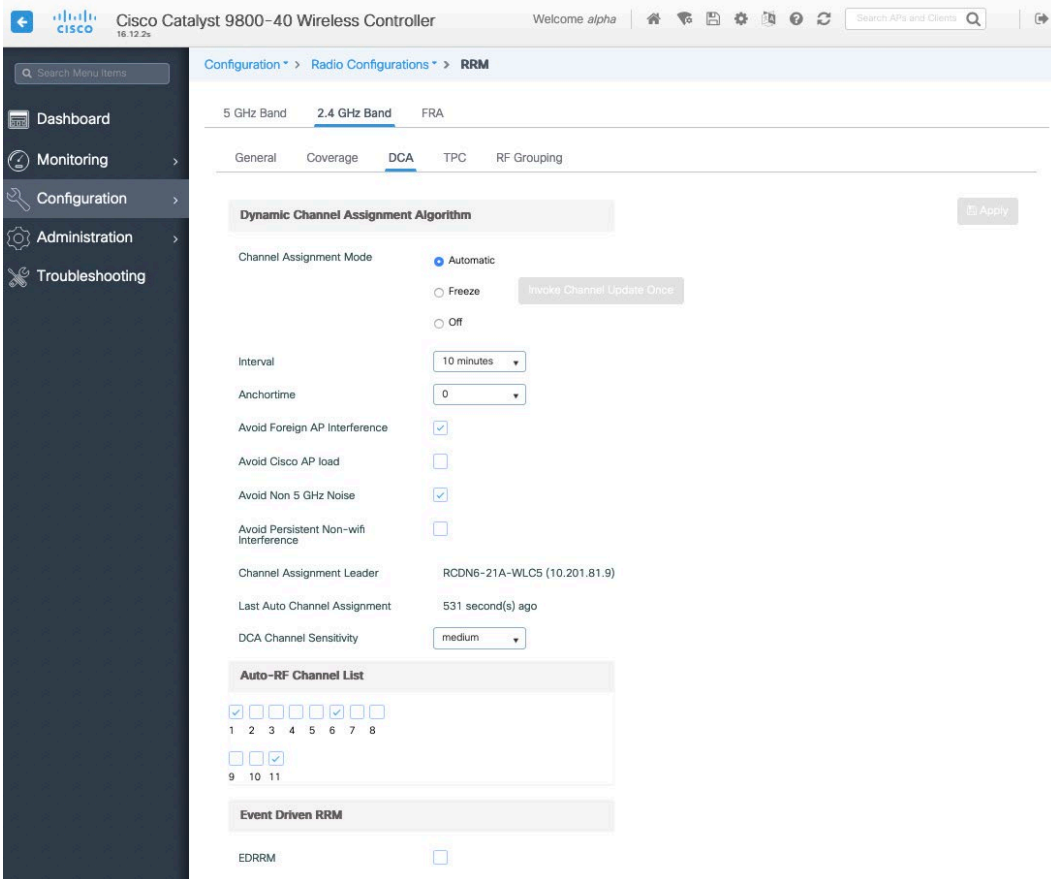
When using 5 GHz, it's recommended to limit the number of channels (e.g. 12 channels only) to avoid any potential delay in access point discovery caused by scanning many channels.

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

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



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

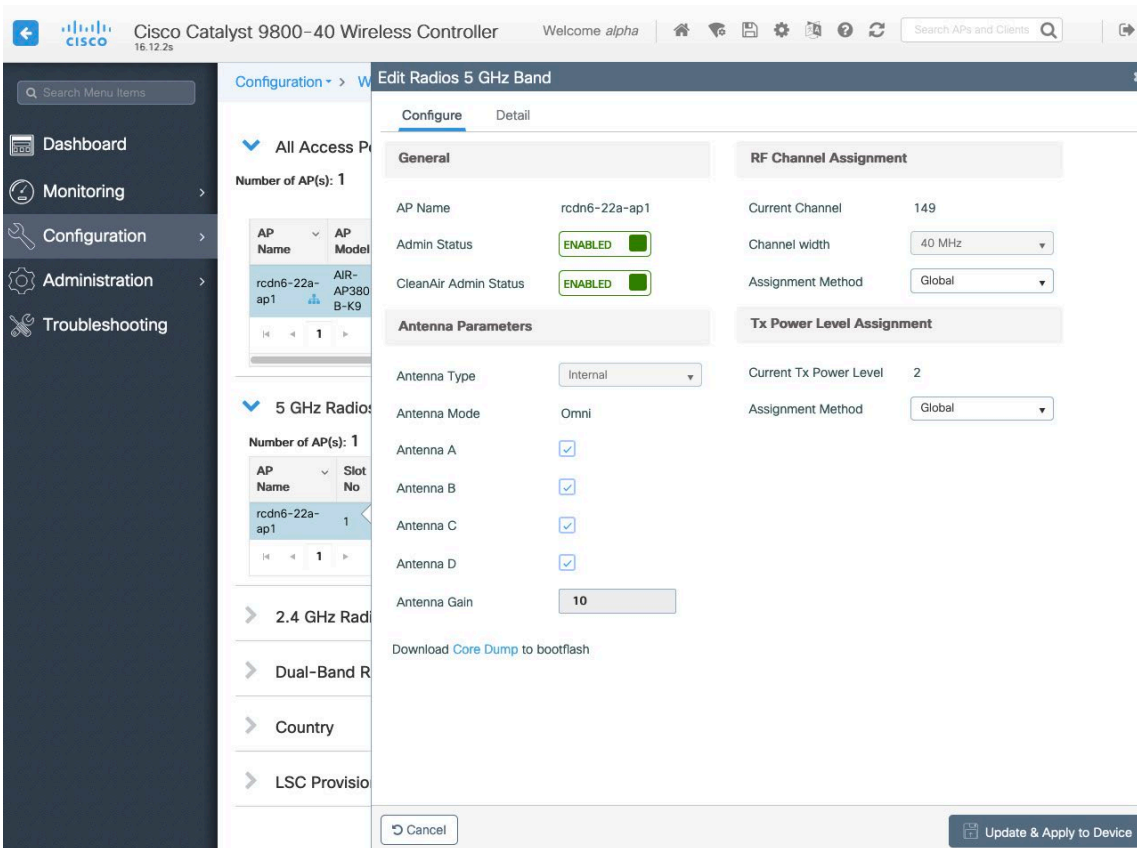


Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized. Other access points can be enabled for automatic assignment method and account for the access points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

This may be necessary if there is an intermittent source of interference in the area.

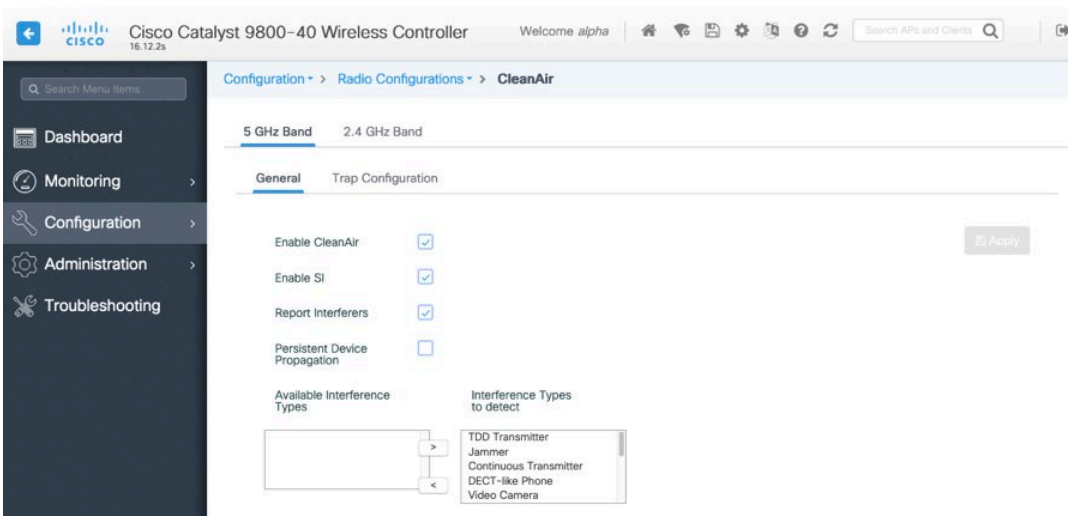
The 5 GHz channel width can be configured as 20 MHz or 40 MHz when using Cisco 802.11n Access Points and as 20 MHz, 40 MHz, or 80 MHz for using Cisco 802.11ac Access Points.

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



CleanAir

The **Enable CleanAir** checkbox should be checked when utilizing Cisco access points with CleanAir technology to detect any existing interferers.



WLAN Settings

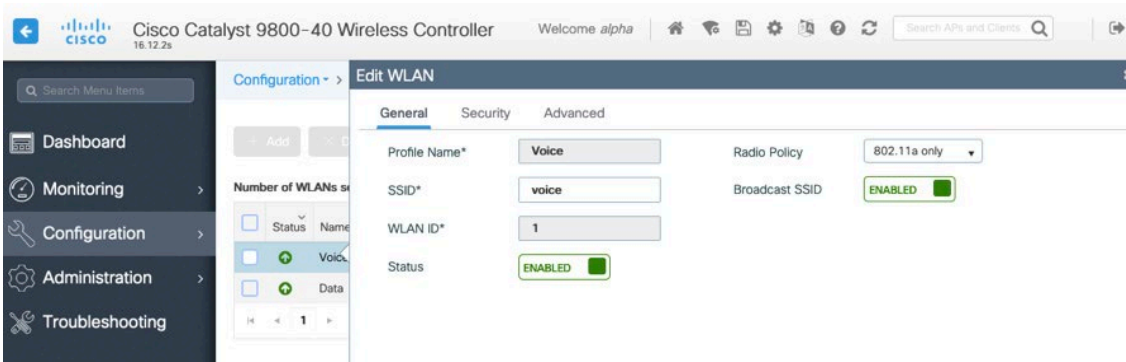
It is recommended to have a separate SSID for the Cisco Desk Phone 9800 Series.

you can also use an existing SSID that is configured to support voice capable Cisco Wireless LAN endpoints.

The SSID to be used by the Cisco Desk Phone Espresso can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

It is recommended to operate the Cisco Desk Phone 9800 Series on the 5 GHz band only due to availability of many channels and fewer interferers compared to the 2.4 GHz band.

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 when a different security type is utilized.

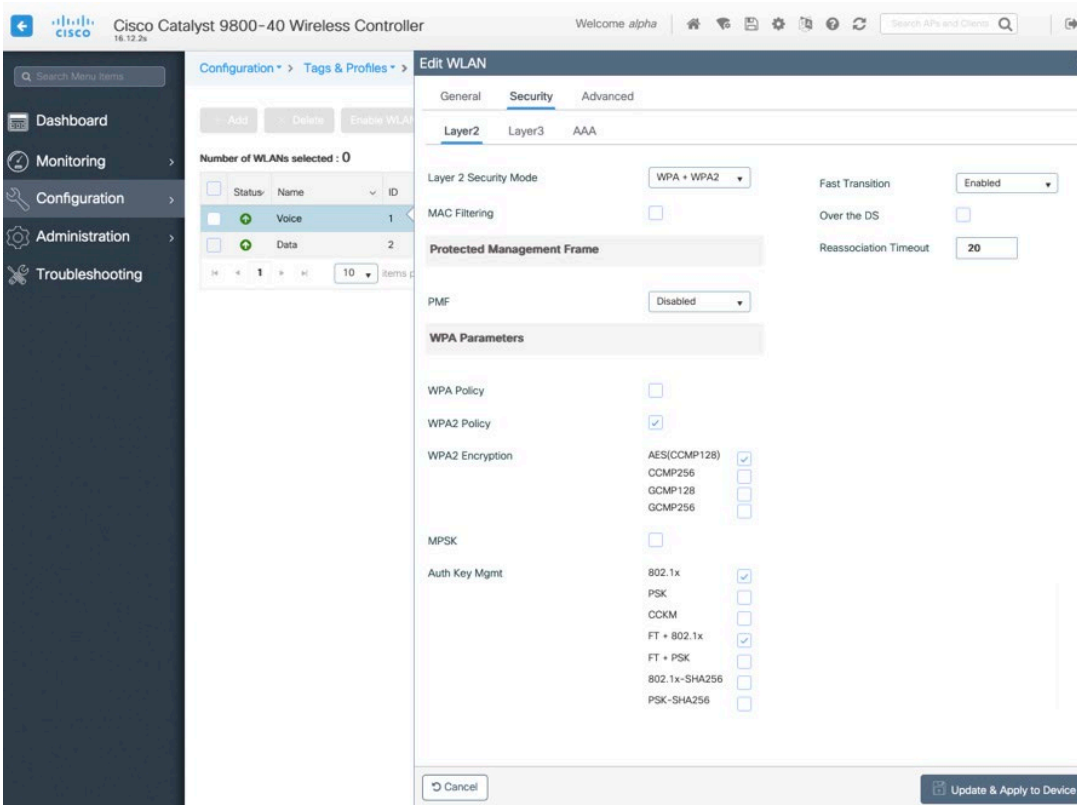


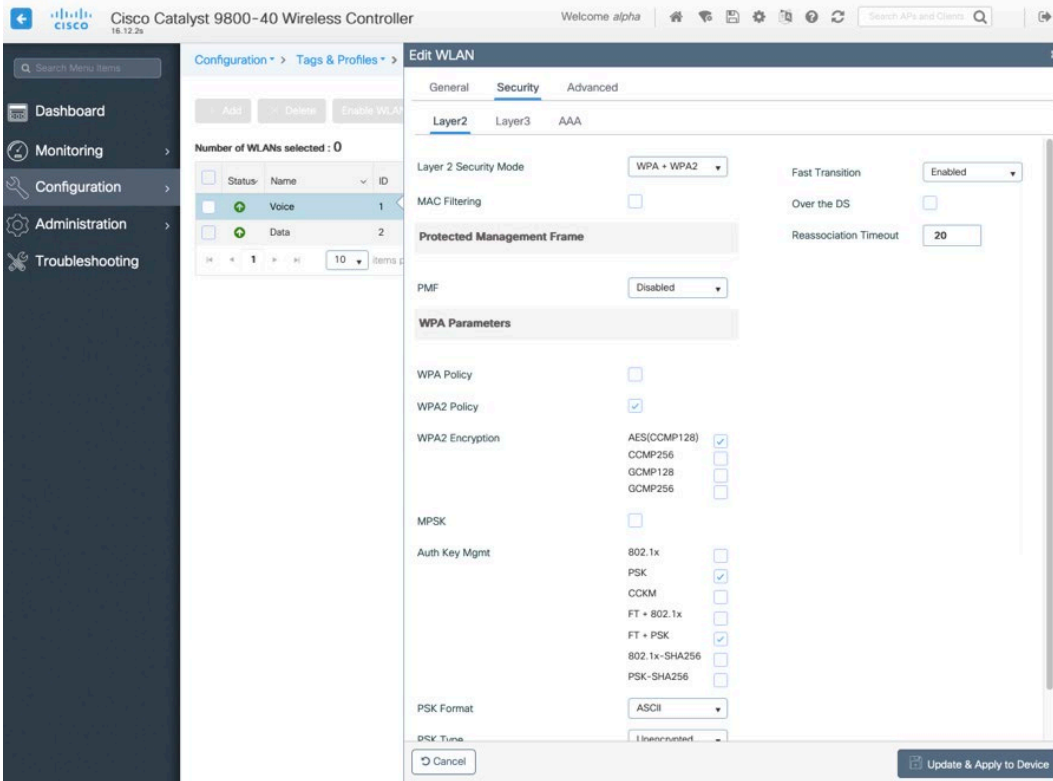
To utilize 802.11r (FT) for fast secure roaming, set **Fast Transition** to **Enabled**.

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

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

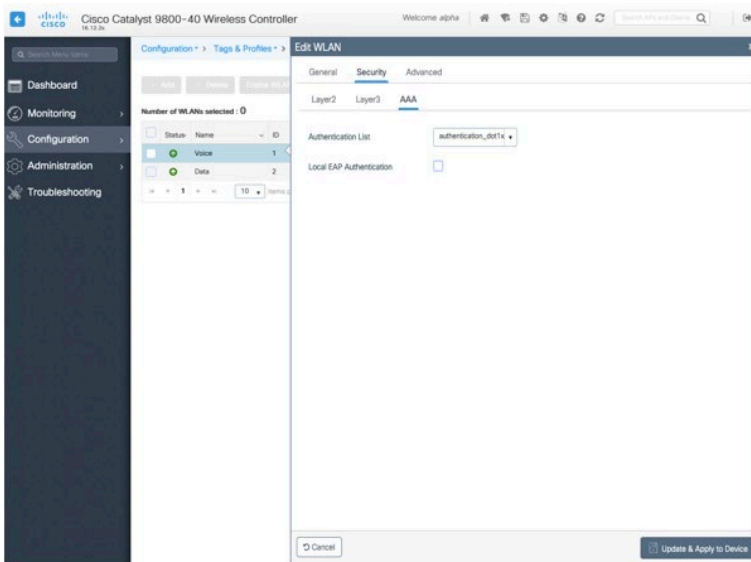
Enable WPA2/WPA3 policy with AES(CCMP128) encryption then 802.1x, PSK or SAE for authenticated key management type depending on whether 802.1x, PSK or SAE is to be utilized.





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

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



Aironet IE should be Disabled.

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

The **WMM Policy** should be set to **Required** only when the Cisco Desk Phone 9800 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 a separate WLAN.

If other non-WMM clients must utilize the same SSID as the Cisco Desk Phone 9800 Series, ensure the WMM policy is set to **Allowed**.

The maximum client connections per WLAN, per AP per WLAN, or 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.

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

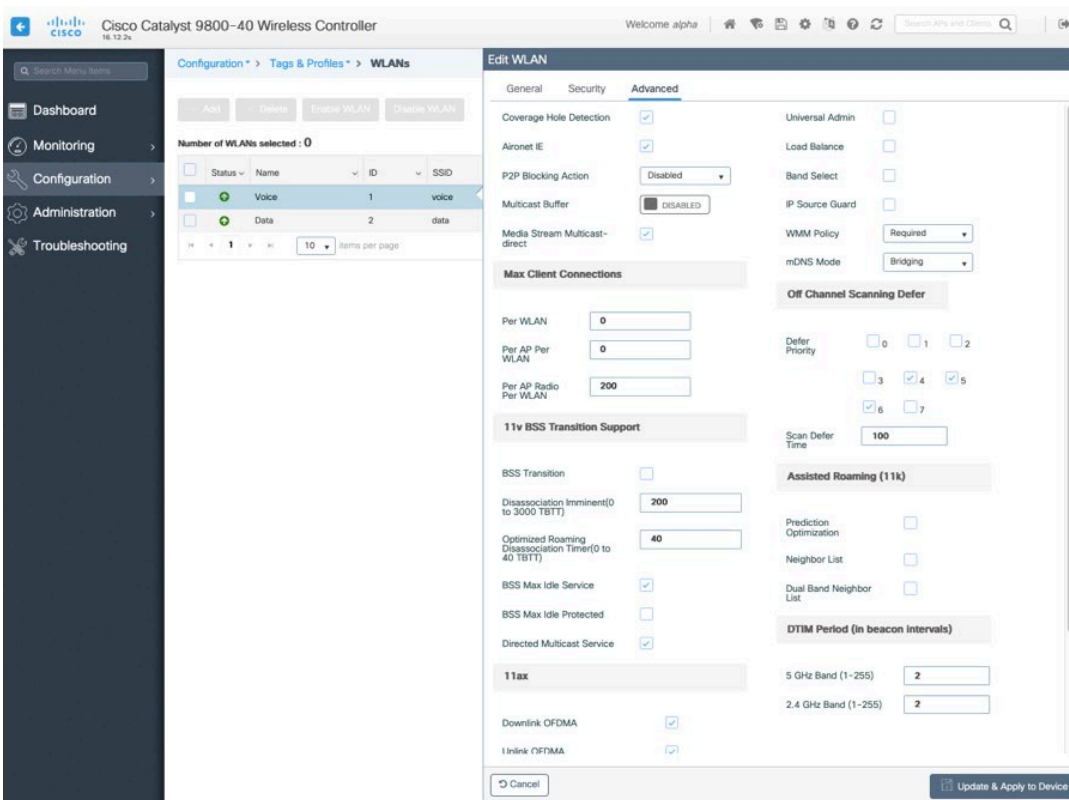
If using best effort applications frequently or not preserving DSCP values for priority applications (e.g. voice and call control) to the access point, it is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well as potentially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

For deployments with frequent EAP failures, 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**.

Keep the default settings for 802.11k and 802.11v.

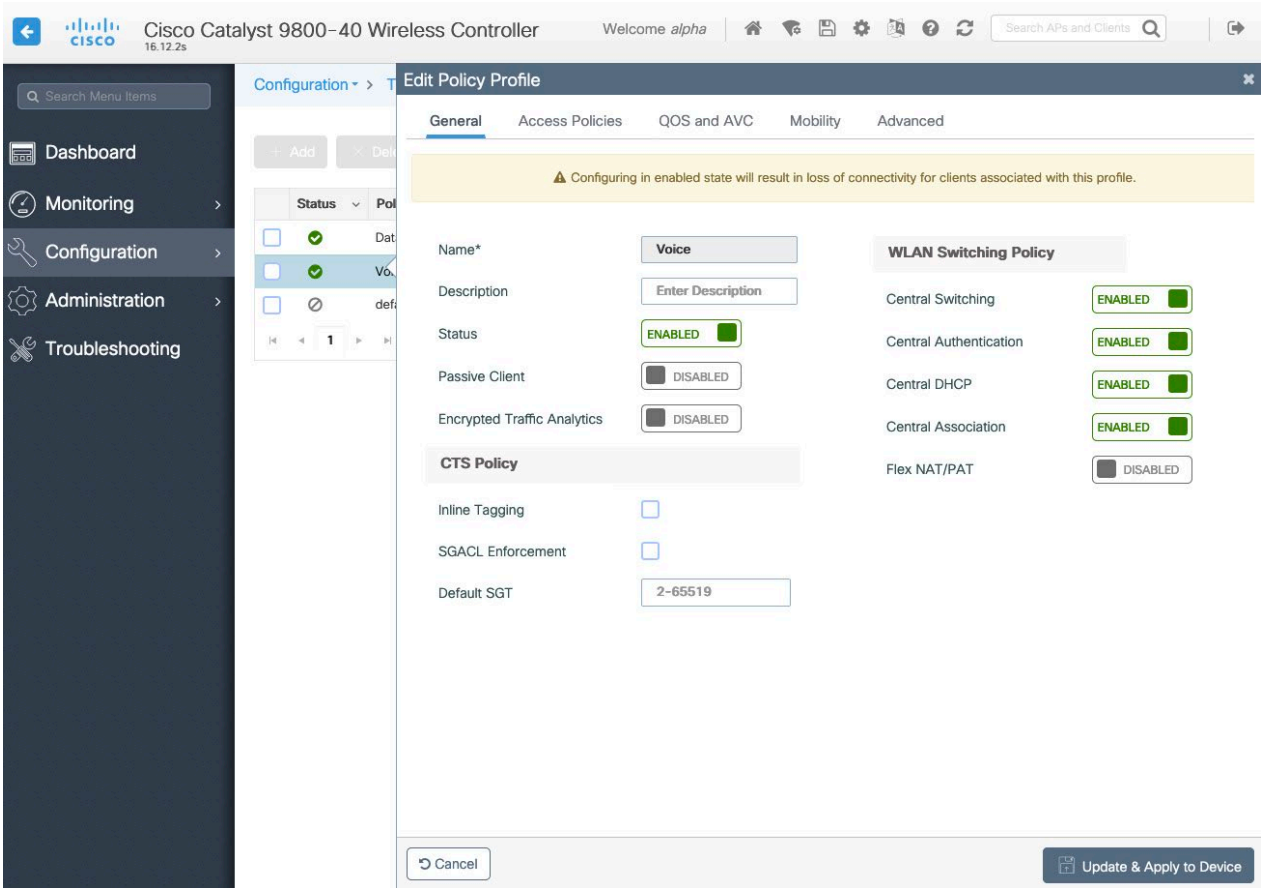


Policy Profiles

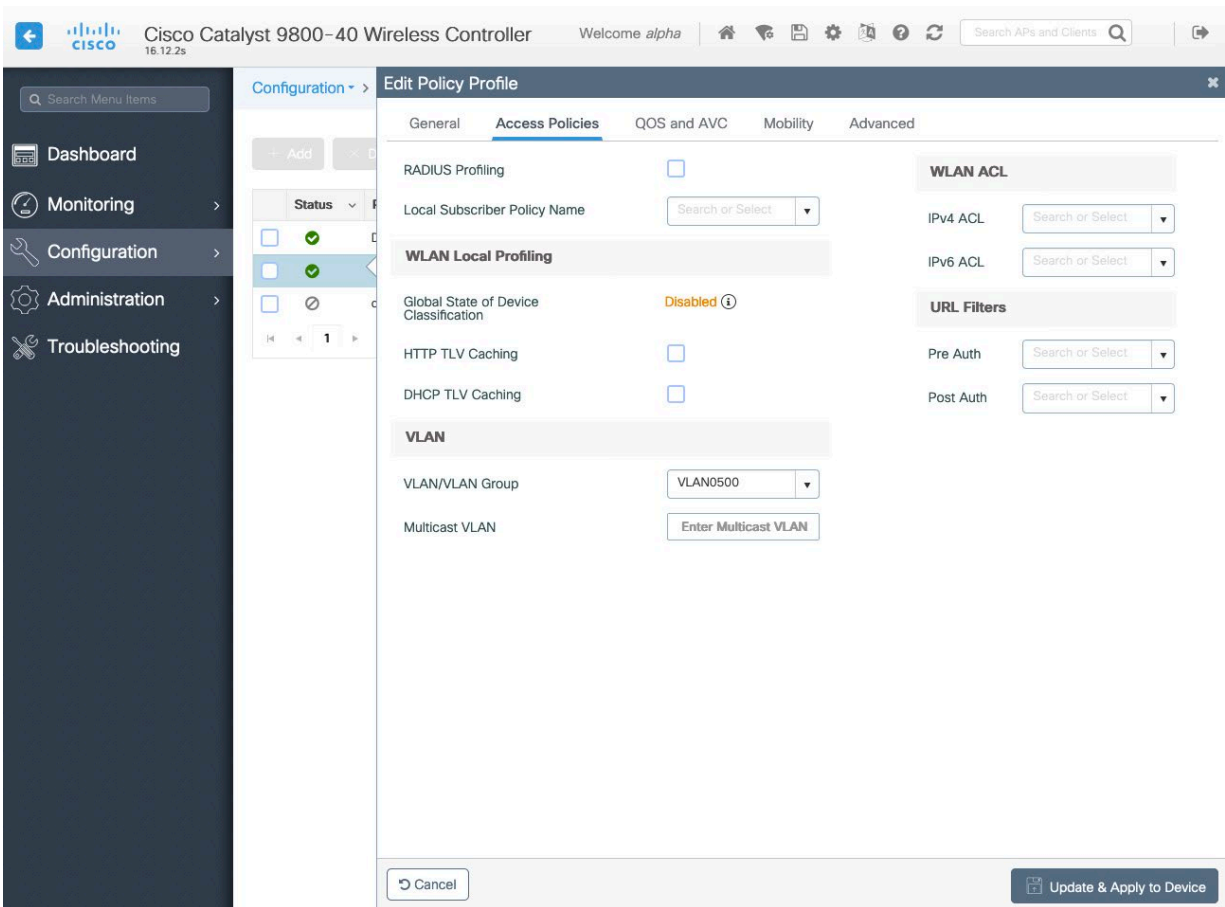
Policy Profiles are used to define additional settings regarding access, QoS, Mobility, and advanced settings.

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

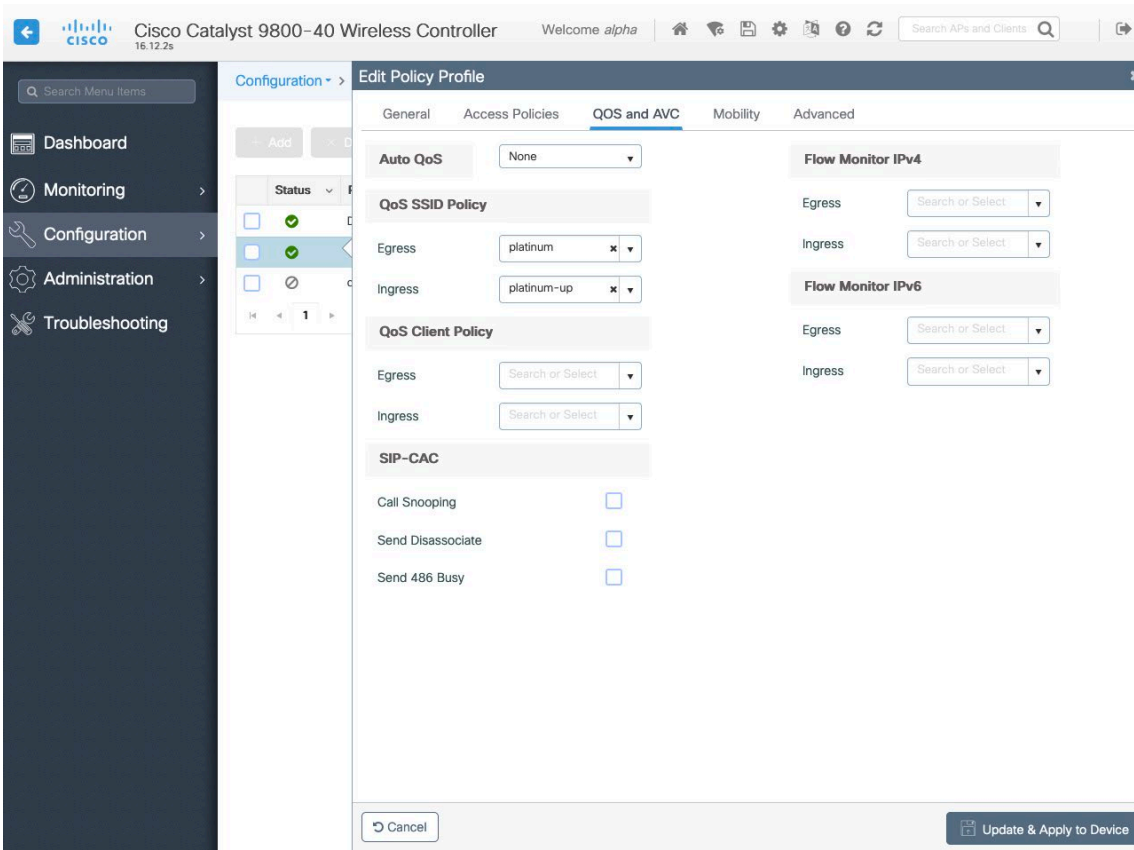
Ensure the **Status** of the policy profile is **Enabled**.



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



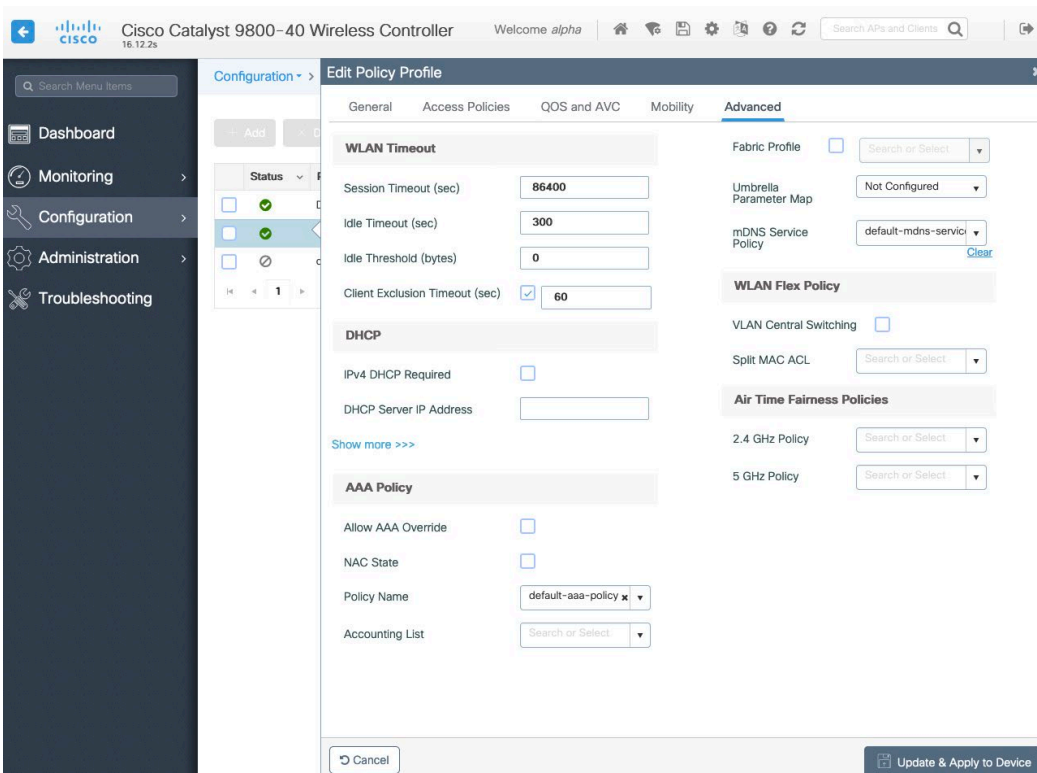
Ensure the QoS SSID Policy is set to **Platinum** for egress and **Platinum-up** for ingress.



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

Configure **Client Exclusion Timeout** as desired.

IPv4 DHCP Required should be disabled.



RF Profiles

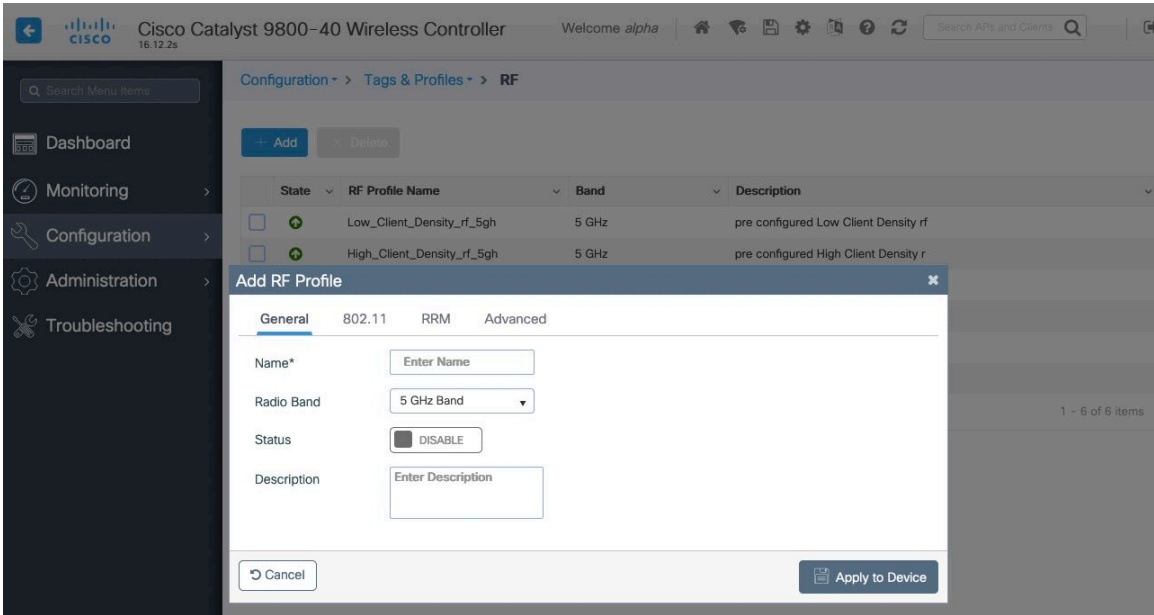
RF Profiles can be created to specify the frequency bands, data rates, RRM settings, and advanced settings that a group of access points should use.

For the SSID used by the Cisco Desk Phone 9800 Series, it's recommended to apply to 5 GHz radios only.

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

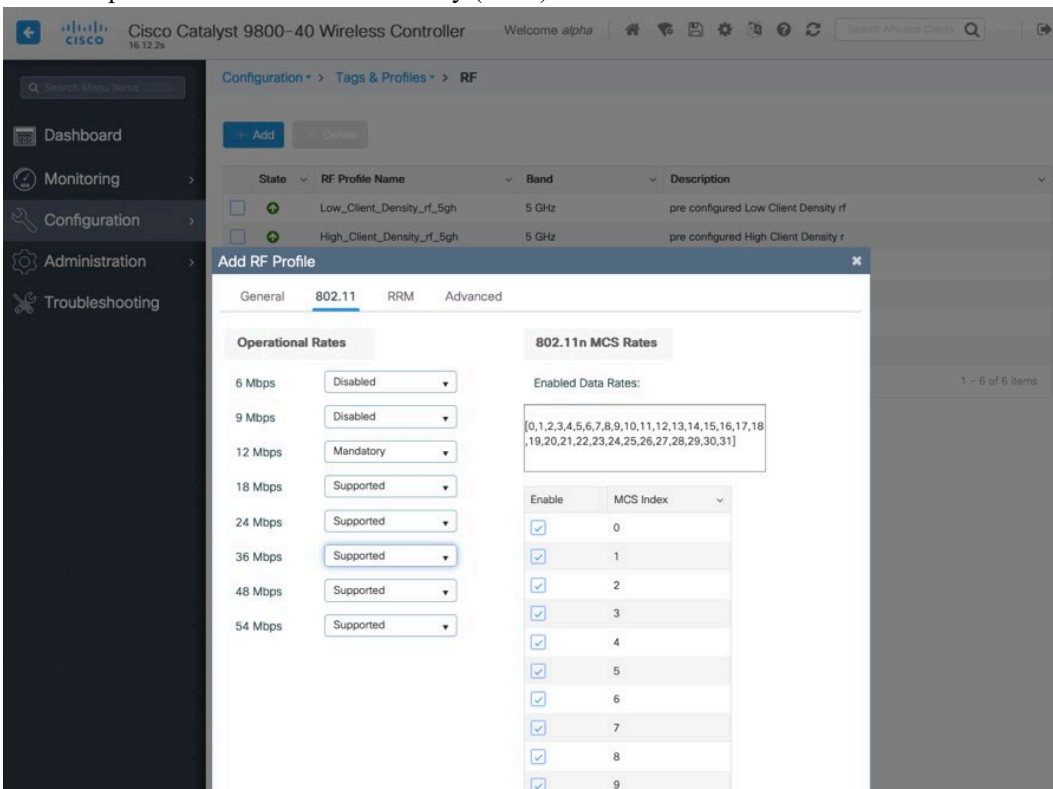
When creating an RF Profile, the **Name** and **Radio Band** must be defined.

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

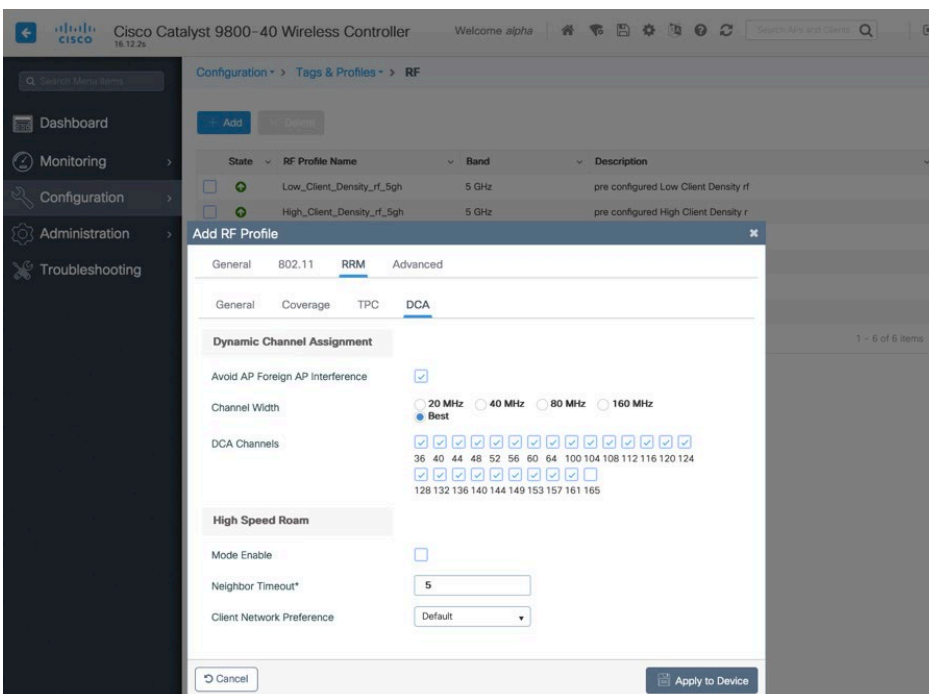
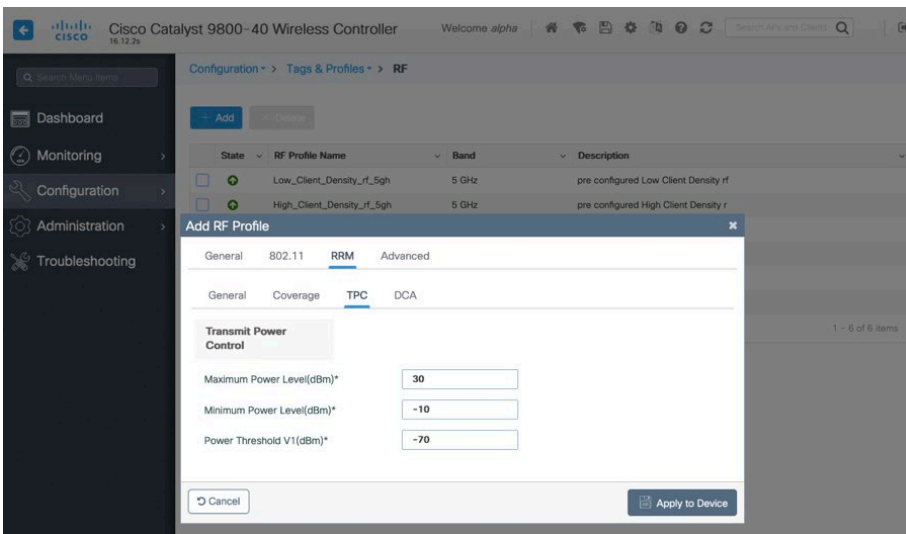
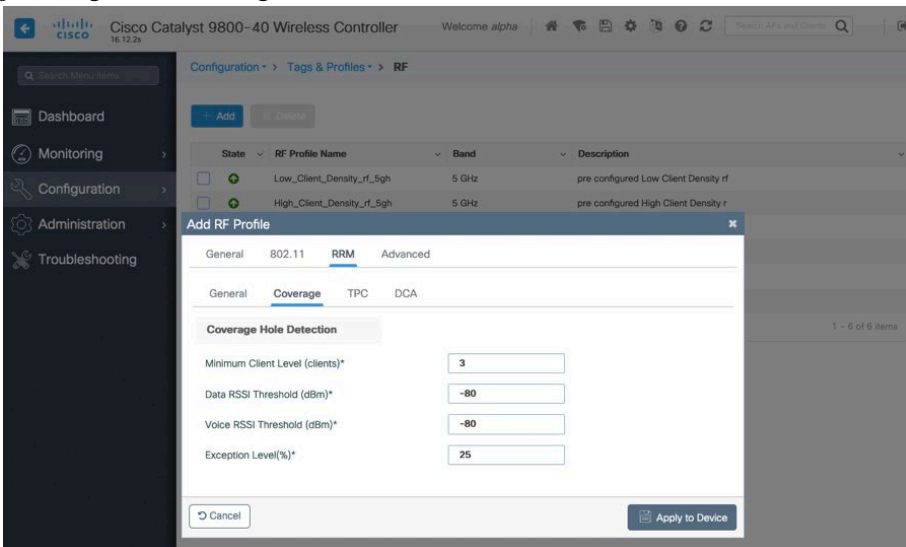


On the **802.11** tab, configure the data rates as necessary.

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

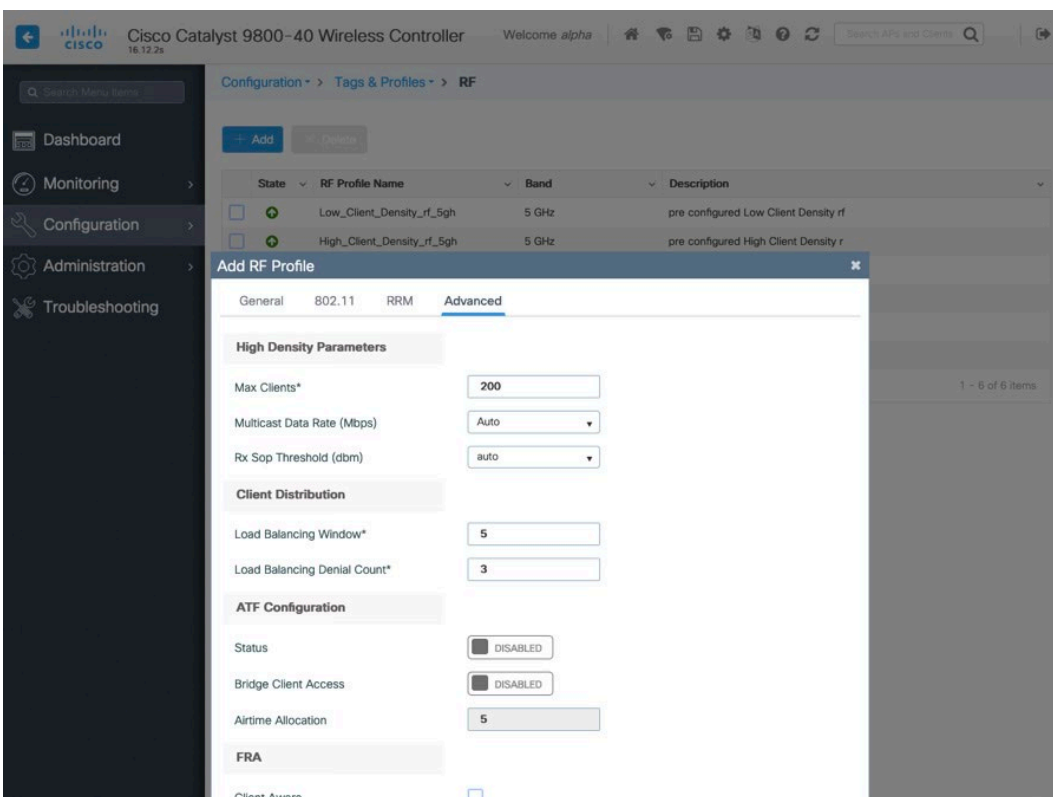


On the **RRM** tab, the **Maximum Power Level** and **Minimum Power Level** settings as well as other **DCA**, **TPC**, and **Coverage** settings can be configured.



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

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



Flex Profiles

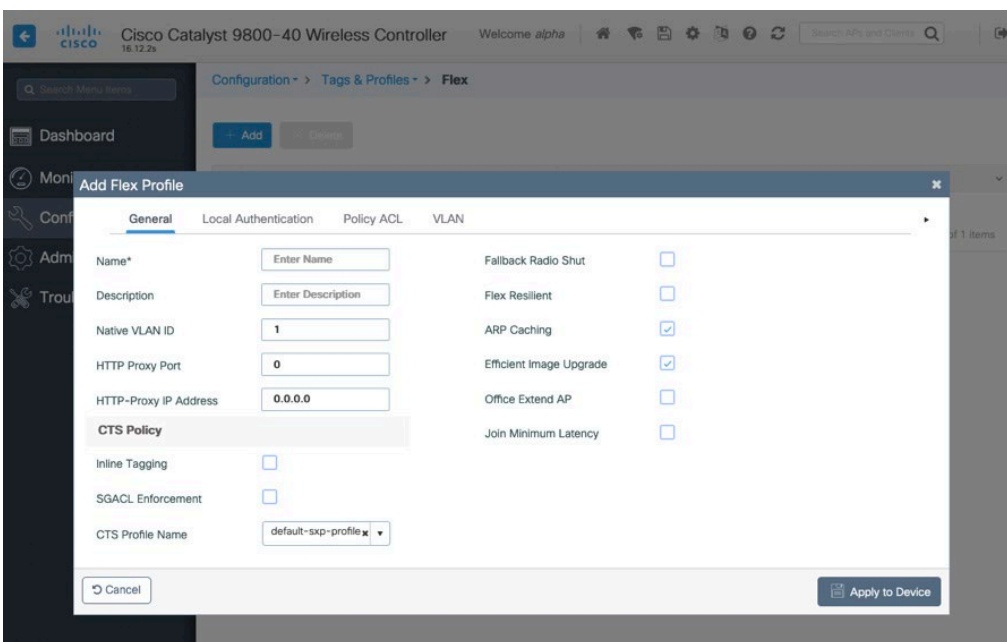
Flex Profiles are used to define the settings the access point should use when in Flexconnect mode.

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

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

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

Enable **Local Authentication** as necessary.



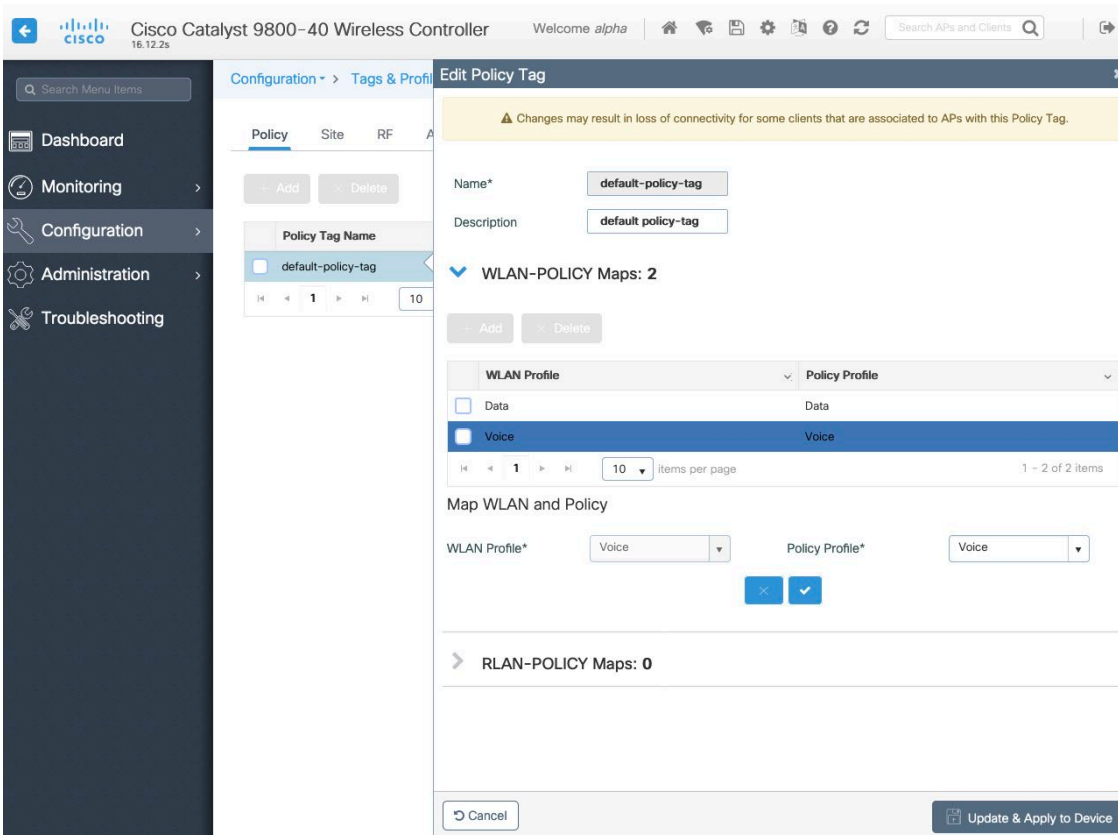
Tags

Policy Tag

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

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

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



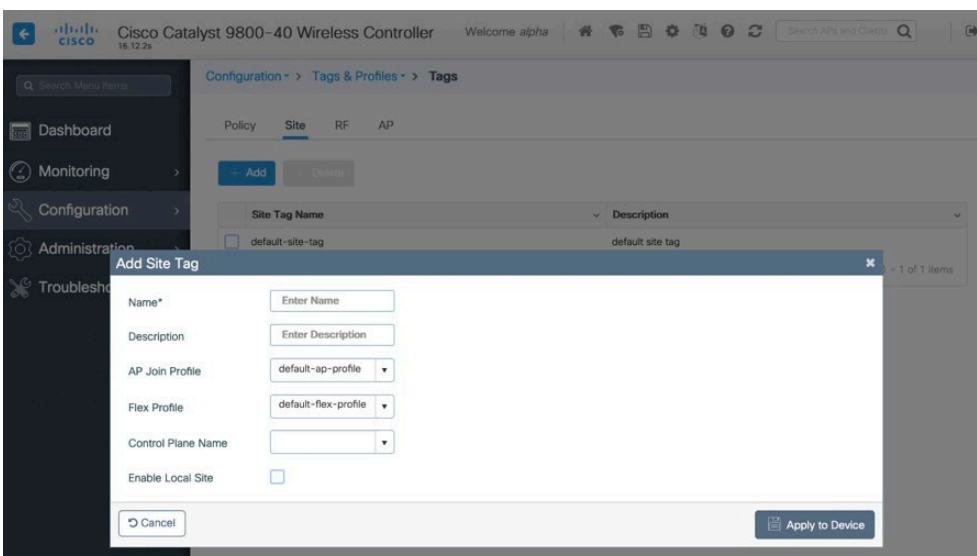
Site Tag

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

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

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

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

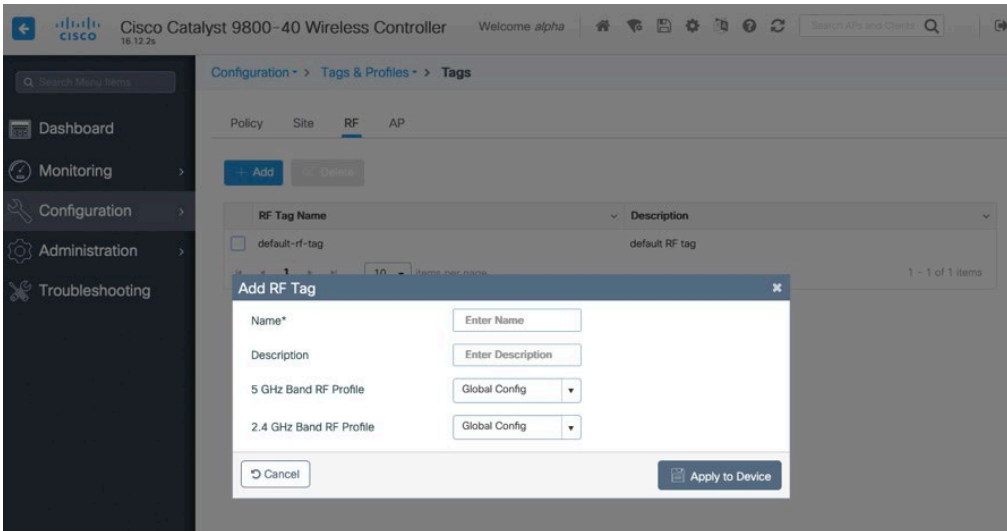


RF Tag

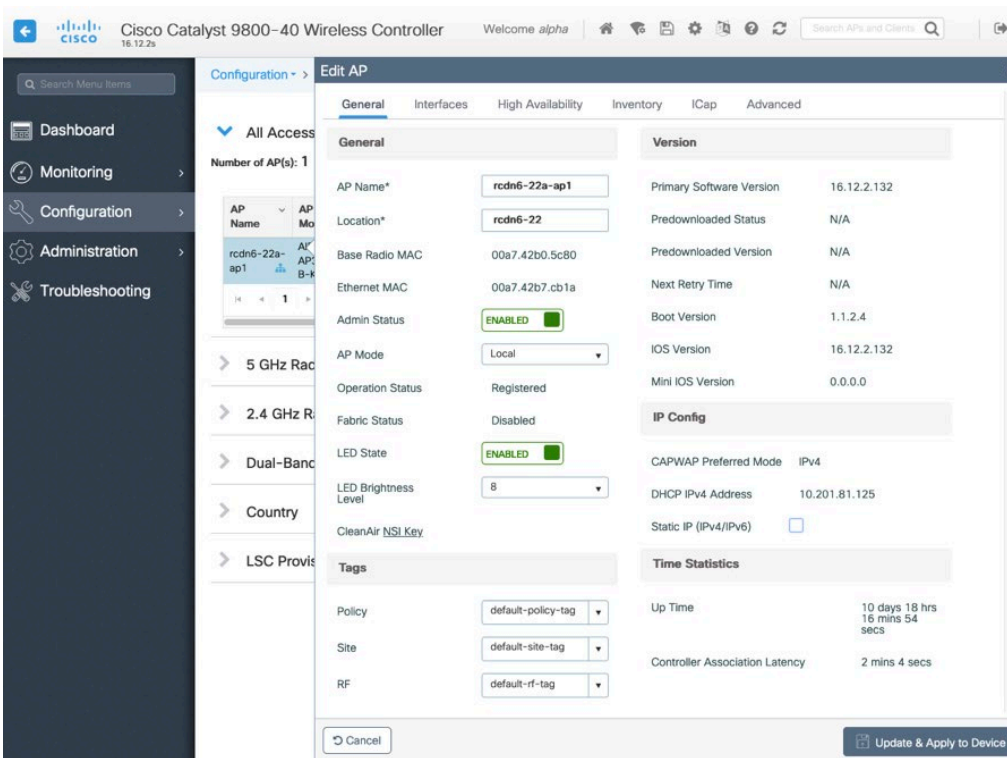
RF Tags define which RF Profiles should be used for 2.4 GHz and 5 GHz.

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

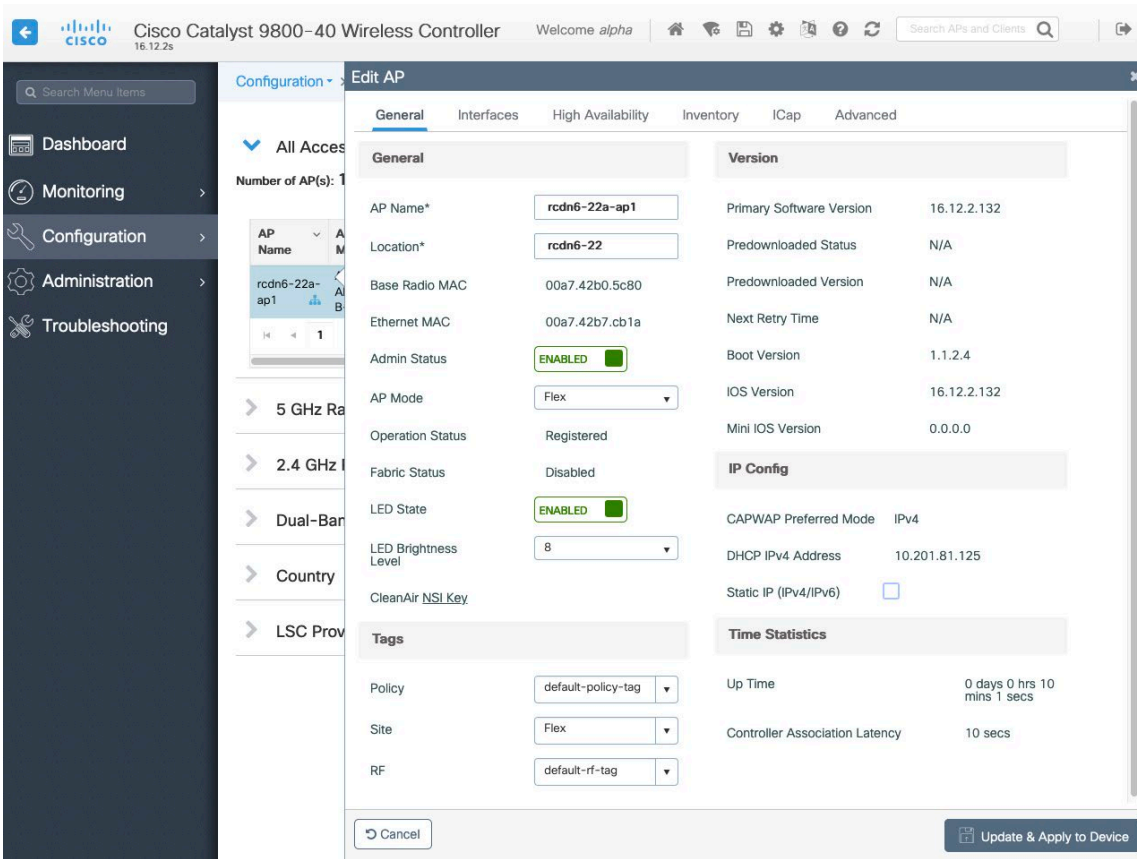
When creating a RF Tag, select the **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be used.



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

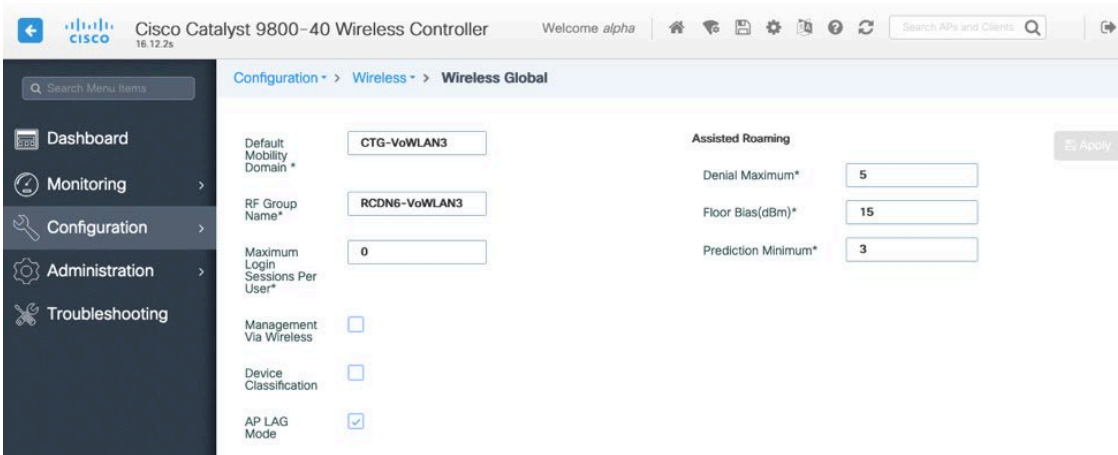


If a Site Tag is applied including a configured Flex Profile, then the **AP Mode** will be changed to **Flex** automatically.



Controller Settings

Ensure the **Default Mobility Domain** is configured correctly.
 Enable **AP LAG Mode**.



Mobility Settings

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

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

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

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

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

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

Below the table, there is a 'Non-Local Mobility Group Multicast Configuration' section.

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

The screenshot shows the 'Wireless' section under 'Interface' configuration. It displays a table of wireless interfaces:

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

Call Admission Control (CAC)

Unicast Video Redirect and Multicast Direct Enable should be Enabled.

The screenshot shows the configuration page for Media Parameters on a Cisco Catalyst 9800-40 Wireless Controller. The breadcrumb navigation is Configuration > Radio Configurations > Media Parameters. The page is divided into two main sections: Media and Voice. The Media section includes a General tab with the following settings: Unicast Video Redirect (checked), Multicast Direct Admission Control (unchecked), Media Stream Admission Control (ACM) (unchecked), Maximum Media Stream RF bandwidth (%) (5), Maximum Media Bandwidth (%) (85), Client Minimum Phy Rate (kbps) (6000), and Maximum Retry Percent (%) (80). Below this is the Media Stream - Multicast Direct Parameters section, where Multicast Direct Enable is checked and Max streams per Radio is set to No Limit. The Voice section includes Call Admission Control (CAC) with Admission Control (ACM) unchecked, and Traffic Stream Metrics with Metrics Collection unchecked, Stream Size* (84000), Max Streams* (2), and Inactivity Timeout checked.

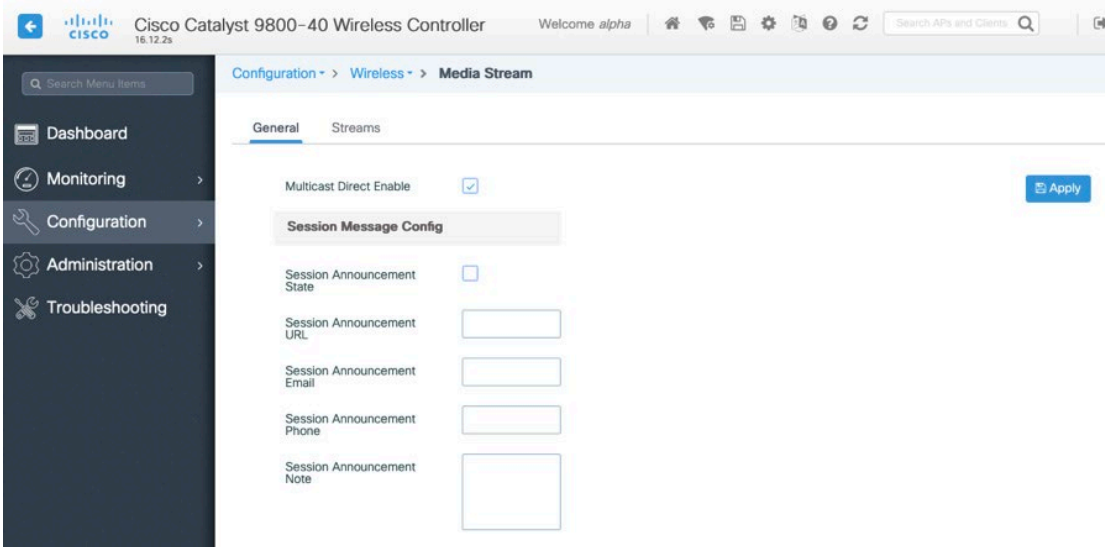
Multicast

To utilize multicast, Global Wireless Multicast Mode and IGMP Snooping should be Enabled.

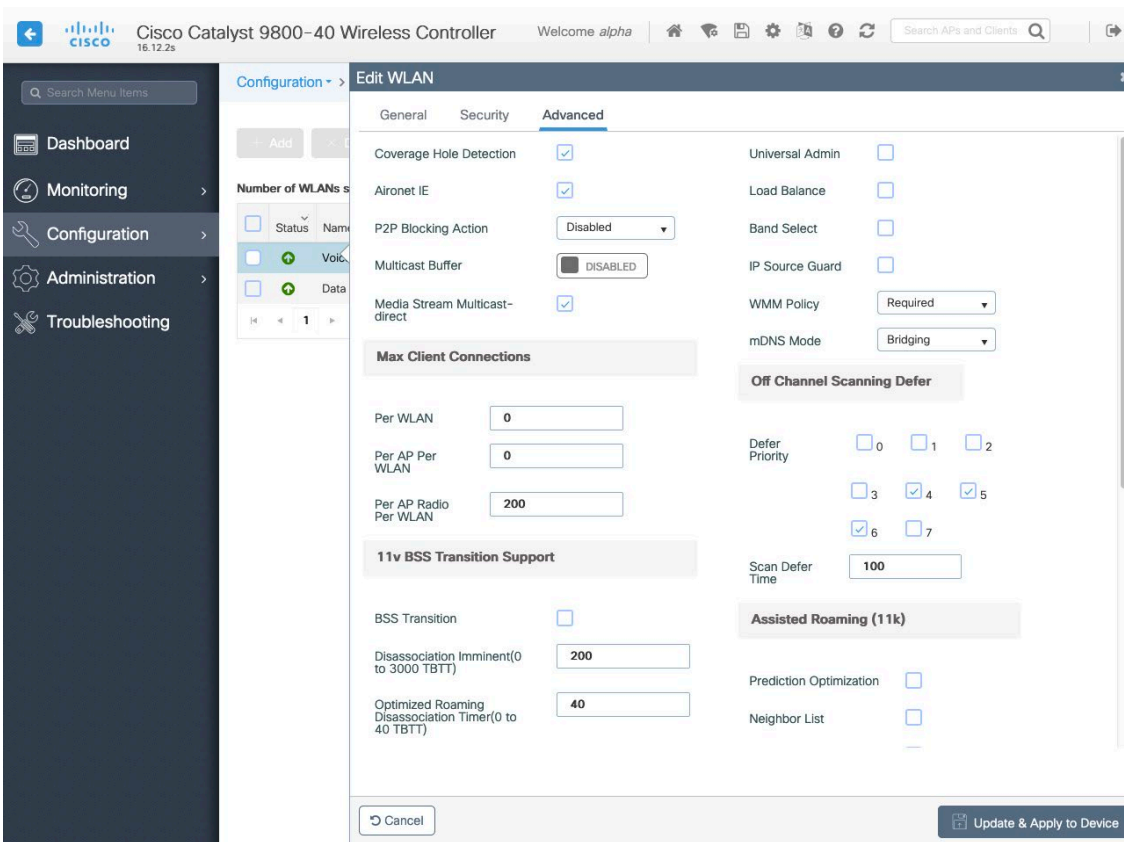
The screenshot shows the configuration page for Multicast on a Cisco Catalyst 9800-40 Wireless Controller. The breadcrumb navigation is Configuration > Services > Multicast. The page is divided into two main sections: Global Wireless Multicast Mode and IGMP Snooping. The Global Wireless Multicast Mode section includes the following settings: Global Wireless Multicast Mode (ENABLED), Wireless mDNS Bridging (DISABLED), Wireless Non-IP Multicast (DISABLED), Wireless Broadcast (DISABLED), AP Capwap Multicast (Unicast), MLD Snooping (DISABLED), IGMP Snooping Querier (DISABLED), IGMP Snooping (ENABLED), and Last Member Querier Interval (milliseconds) (1000). The IGMP Snooping section is divided into Disabled and Enabled states. The Disabled state shows No Vlan available. The Enabled state shows a table of VLANs with their status, VLAN ID, and Name.

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

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



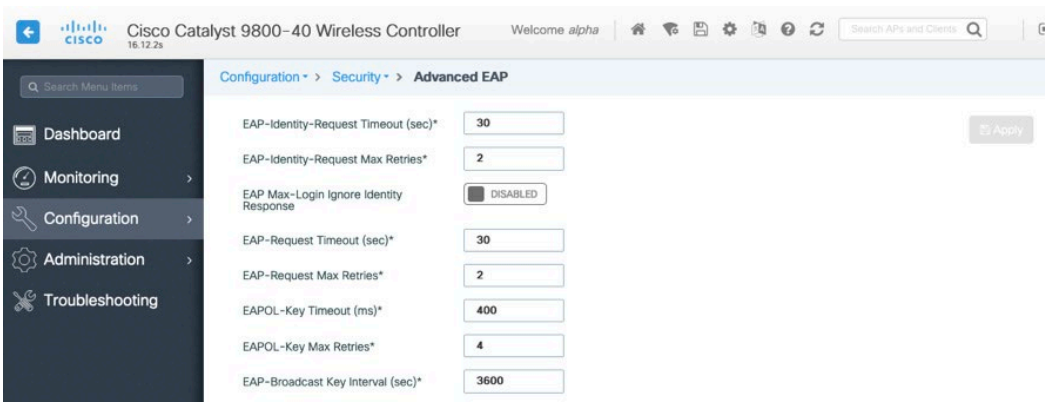
Enable **Multicast Direct** in the WLAN configuration.



Advanced Settings

Advanced EAP Settings

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



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

For deployments with frequent EAP failures, the **EAP-Request Timeout** should be reduced to 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.

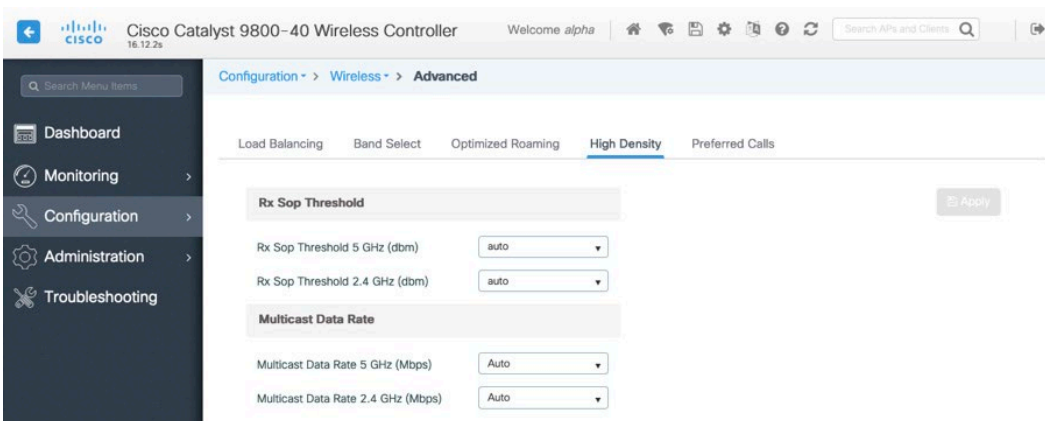
When using 802.1x, the default values for **EAPOL-Key Timeout** and **EAPOL-Key Max Retries** should work fine, but it is still recommended to set those values to 400 and 4 respectively.

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

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

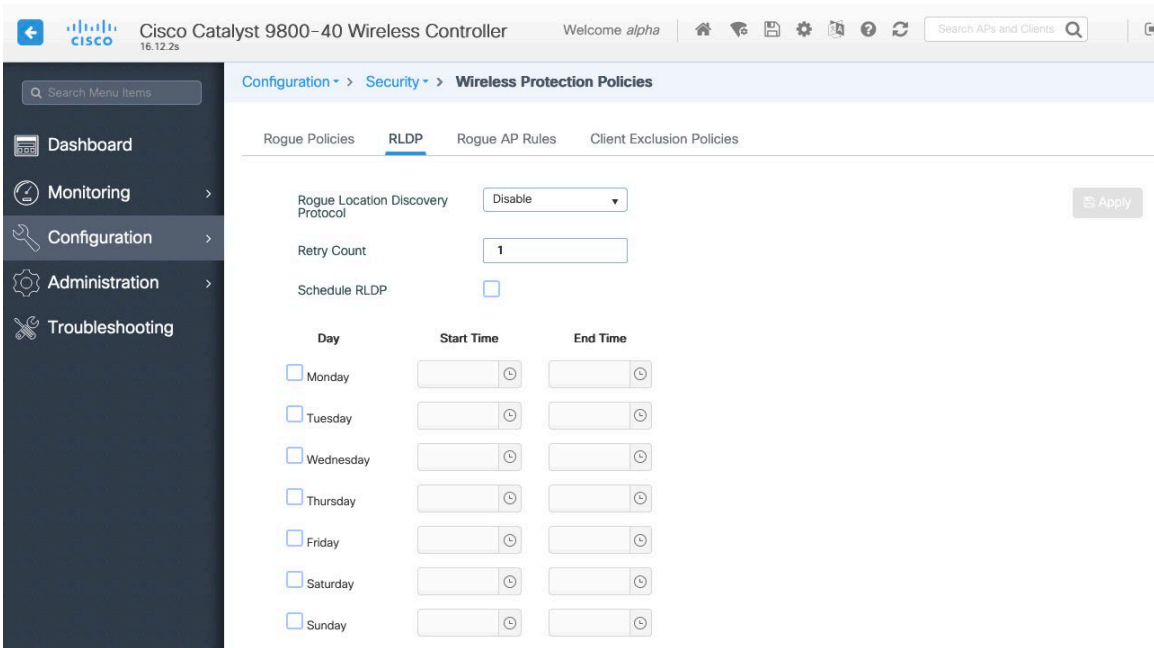
Rx Sop Threshold

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



Rogue Policies

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



Cisco Mobility Express and Lightweight Access Points

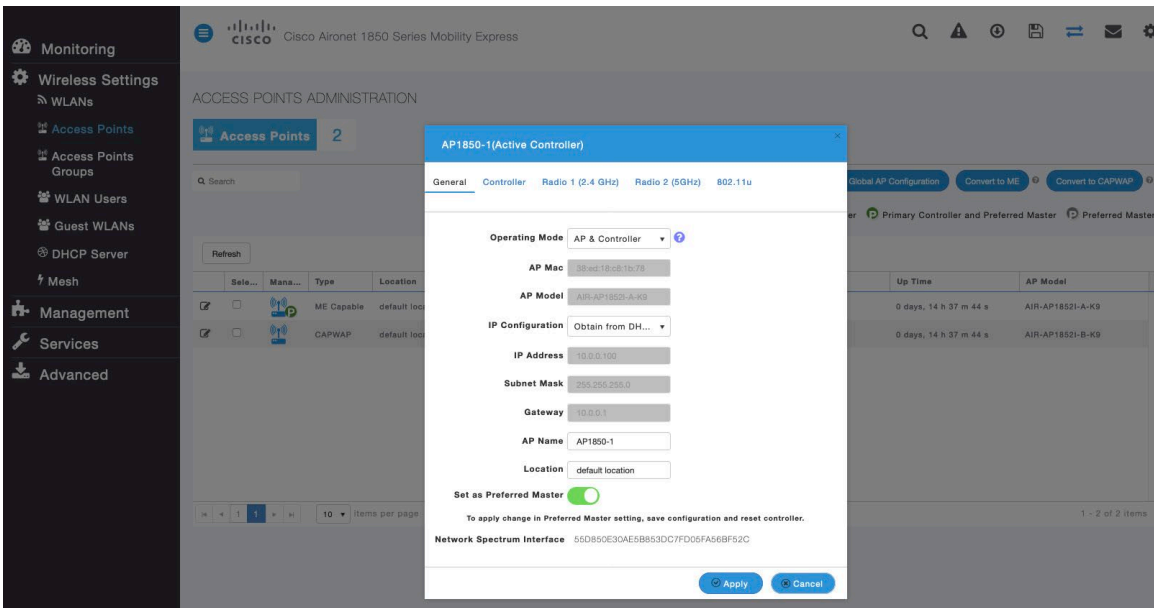
When configuring Cisco Mobility Express and Lightweight Access Points, use the following guidelines:

- Enable **802.11r (FT)**
- Disable **CCKM**
- Set **Quality of Service (QoS)** to **Platinum**
- Ensure **802.11k** is **Disabled**
- Ensure **802.11v** is **Disabled**
- Disable **P2P (Peer to Peer) Blocking Action**
- Set **Client Band Select** to **Disabled**
- Set **Client Load Balancing** to **Disabled**
- Configure the **Data Rates** as necessary
- Configure **RF Optimization** as necessary
- Set **Traffic Type** to Voice and Data
- Enable **CleanAir** if utilizing Cisco access points with CleanAir technology
- Configure **Multicast Direct** as necessary

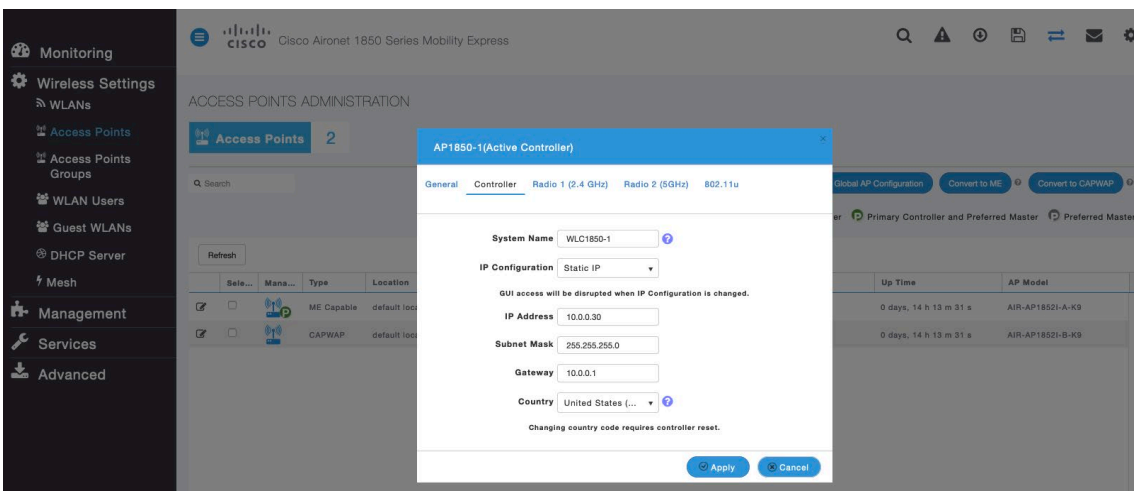
Controller Settings

Configure one or more of the Mobility Express capable access point's **Operating Mode** to include the **Controller** functionality.

Configure the **AP Name** and IP settings as necessary.



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



802.11 Network Settings

It is recommended to operate the Cisco Desk Phone 9800 Series only on the 5 GHz band due to the availability of many channels and fewer interferers compared to the 2.4 GHz band.

To use 5 GHz, ensure the **5.0 GHz Band** is **Enabled**.

It's 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.

To use 2.4 GHz, ensure the **2.4 GHz Band** is **Enabled**.

It's recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps or higher as supported (optional) rates assuming that there will not be any 802.11b only clients connected 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 or higher as supported (optional).

When using 5 GHz, it's recommended to limit the number of channels (e.g. 12 channels only) to avoid any potential delay in access point discovery caused by scanning many channels.

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

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

When 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 to detect any existing interference.

Advanced RF Parameters

- 2.4 GHz Band:
- 5.0 GHz Band:
- Automatic Flexible Radio Assignment:
- 2.4 GHz Optimized Roaming:
- 5 GHz Optimized Roaming:
- Event Driven RRM:
- CleanAir detection:
- 5.0 GHz Channel Width: 40 MHz
- 2.4 GHz Data Rates: (Lower Density to Higher Density)
- 5.0 GHz Data Rates: (Lower Density to Higher Density)
- Select DCA Channels:
 - 2.4 GHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
 - 5.0 GHz: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165

At least one Channel Number should be selected

Apply

RF Optimization

It is recommended to enable **RF Optimization** to manage the channel and transmit power settings. Set **Traffic Type** to **Voice and Data**.

RF OPTIMIZATION

RF Optimization Enabled

- RF Optimization: Enabled
- Client Density: (Low to High)
- Traffic Type: Voice and Data

Apply

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

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

This may be necessary if there is an intermittent source of interference in the area.

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

It is recommended to use channel bonding only when using 5 GHz and utilize the same channel width for all access points.

Monitoring
Wireless Settings
WLANs
Access Points
Access Points Groups
WLAN Users
Guest WLANs
DHCP Server
Mesh
Management
Services
Advanced

ACCESS POINTS ADMINISTRATION

Access Points 2

Global AP Configuration Convert to ME Convert to CAPWAP

Primary Controller Primary Controller and Preferred Master Preferred Master

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

AP1850-1(Active Controller)

General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u

Admin Mode Enabled

Channel Automatic

Channel Width 20 MHz

Transmit Power Automatic

2.4 GHz
802.11b/g/n

Apply Cancel

AP1850-1(Active Controller)

General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u

Admin Mode Enabled

Channel Automatic

Channel Width 20 MHz

Transmit Power Automatic

5GHz
802.11a/n/ac

Apply Cancel

AP1850-2

General Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u

Admin Mode Enabled

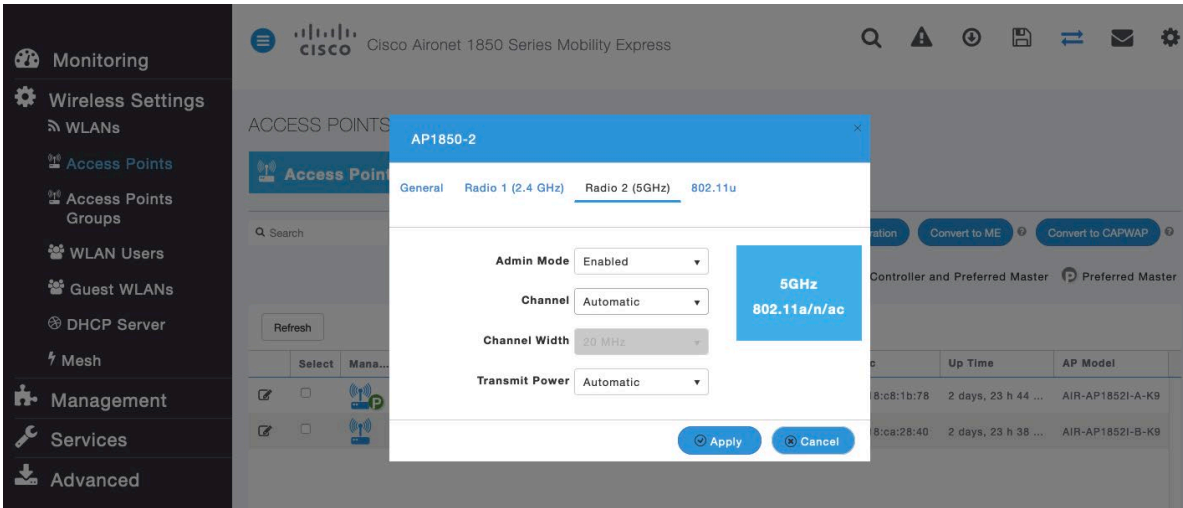
Channel Automatic

Channel Width 20 MHz

Transmit Power Automatic

2.4 GHz
802.11b/g/n

Apply Cancel



WLAN Settings

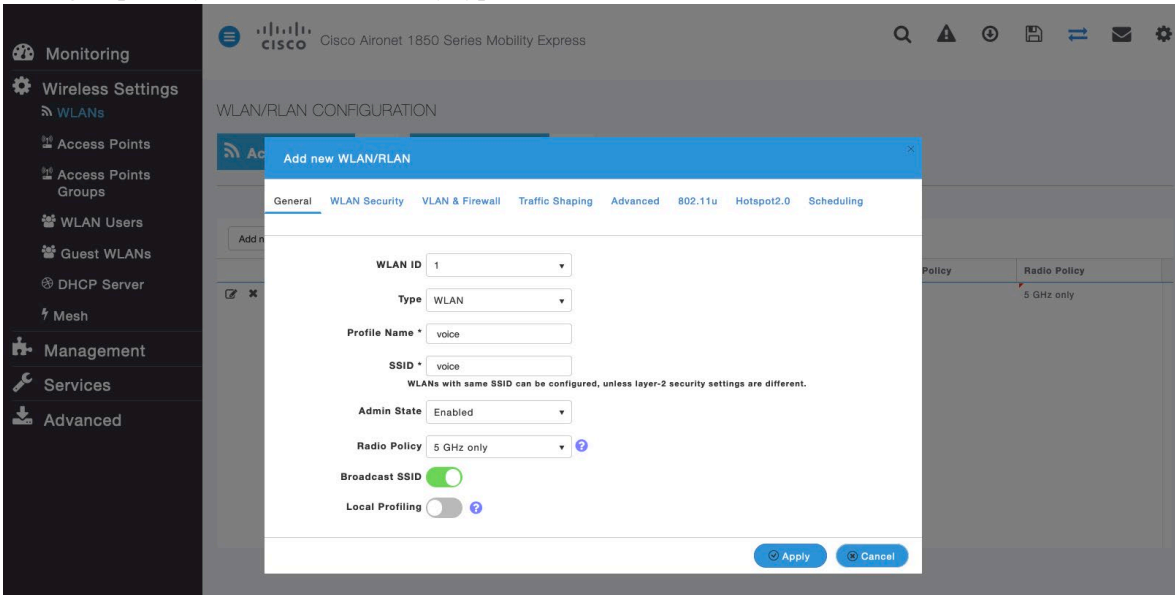
It is recommended to have a separate SSID for the Cisco Desk Phone 9800 Series.

However, you can also use an existing SSID that is configured to support voice capable Cisco Wireless LAN endpoints.

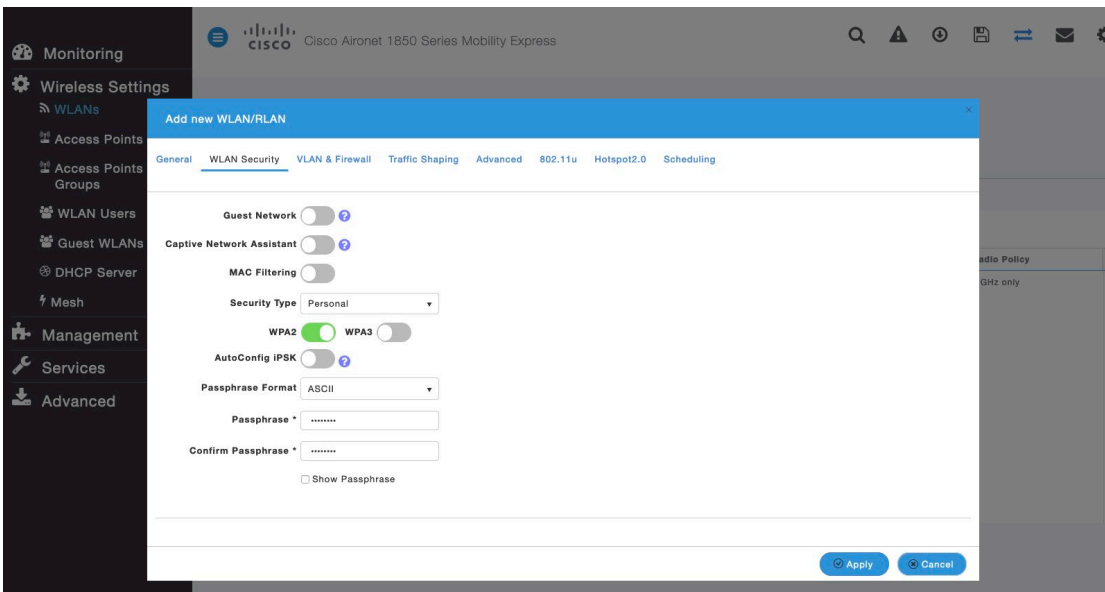
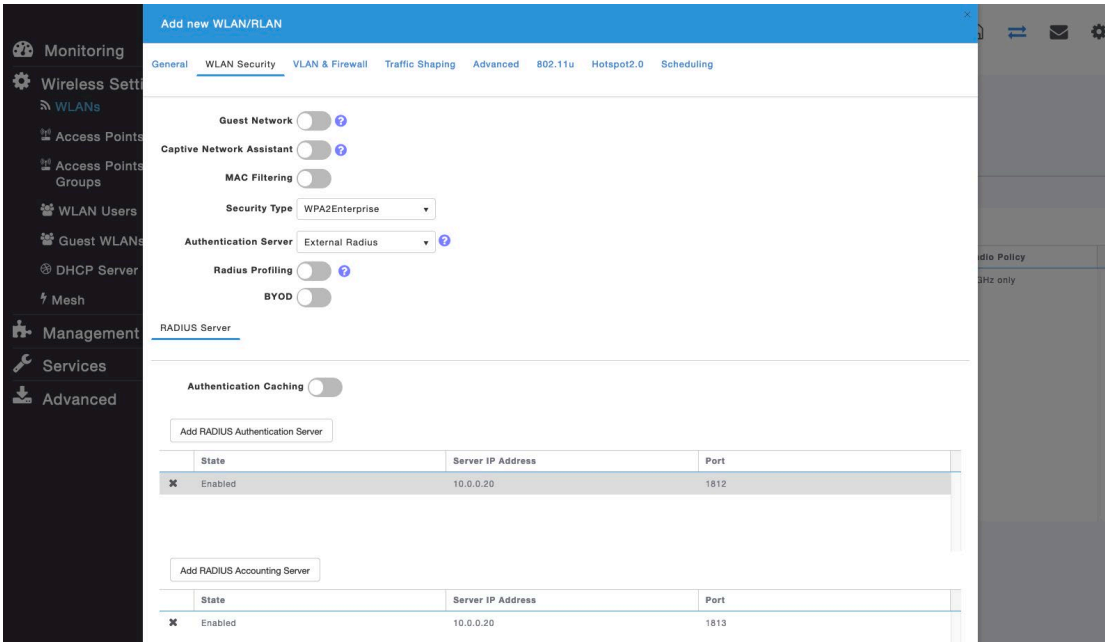
The SSID to be used by the Cisco Desk Phone 9800 Series can be configured to only apply to a certain 802.11 radio type (e.g. 5 GHz only).

It is recommended to operate the Cisco Desk Phone 9800 Series on the 5 GHz band only due to availability of many channels and fewer interferers compared to the 2.4 GHz band.

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

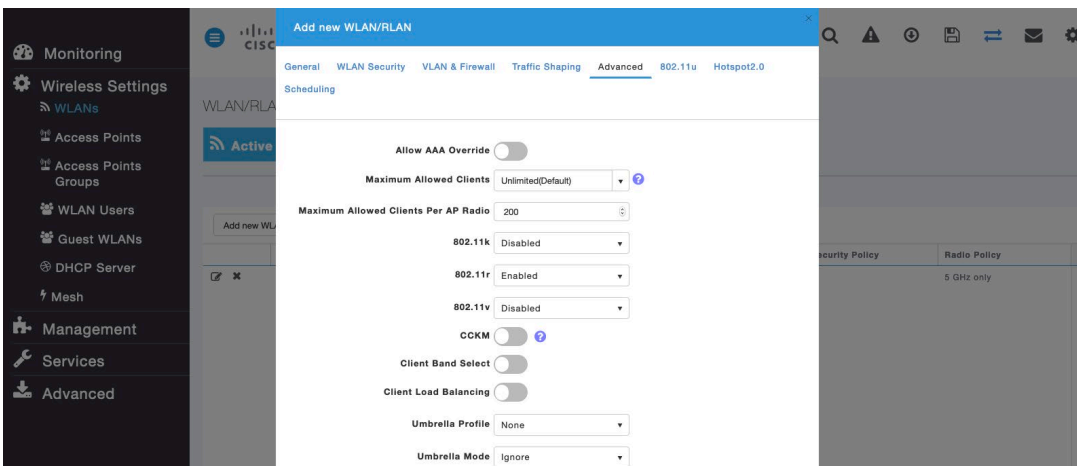


To utilize 802.11r (FT) for fast secure roaming, set **Security Type** to either **WPA2-Enterprise** or **Personal** depending on whether 802.1x or PSK/SAE is to be utilized.



Set 802.11r to **Enable** in the **Advanced** tab of the WLAN configuration. Ensure **Client Band Select** and **Client Load Balancing** are disabled.

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



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

The screenshot shows the 'Add new WLAN/RLAN' configuration page. The 'RADIUS Server' section is active, displaying the following settings:

- Guest Network:
- Captive Network Assistant:
- MAC Filtering:
- Security Type: WPA2Enterprise
- Authentication Server: External Radius
- Radius Profiling:
- BYOD:
- Authentication Caching:

Below the settings, there are two tables for RADIUS servers:

Add RADIUS Authentication Server

State	Server IP Address	Port
Enabled	10.0.0.20	1812

Add RADIUS Accounting Server

State	Server IP Address	Port
Enabled	10.0.0.20	1813

The screenshot shows the 'ADMIN ACCOUNTS' configuration page for a Cisco Aironet 1850 Series Mobility Express. The 'RADIUS' tab is selected, showing the following configuration:

- Authentication Call Station ID Type: AP MAC Address:SSID
- Authentication MAC Delimiter: Hyphen
- Accounting Call Station ID Type: IP Address
- Accounting MAC Delimiter: Hyphen
- Fallback Mode: Passive
- Username: cisco-probe
- Interval: 300 Seconds
- AP Events Accounting:

An 'Apply' button is visible at the bottom of the configuration area.

The screenshot shows the RADIUS server configuration table, which includes the following data:

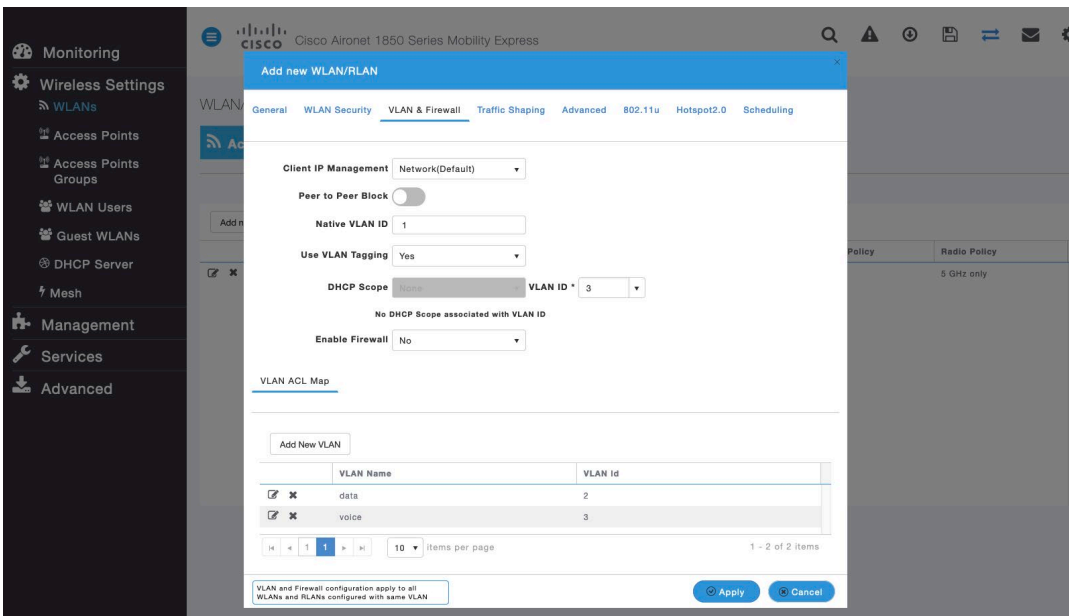
Add RADIUS Authentication Server

Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
✕	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.0.20	*****	1812

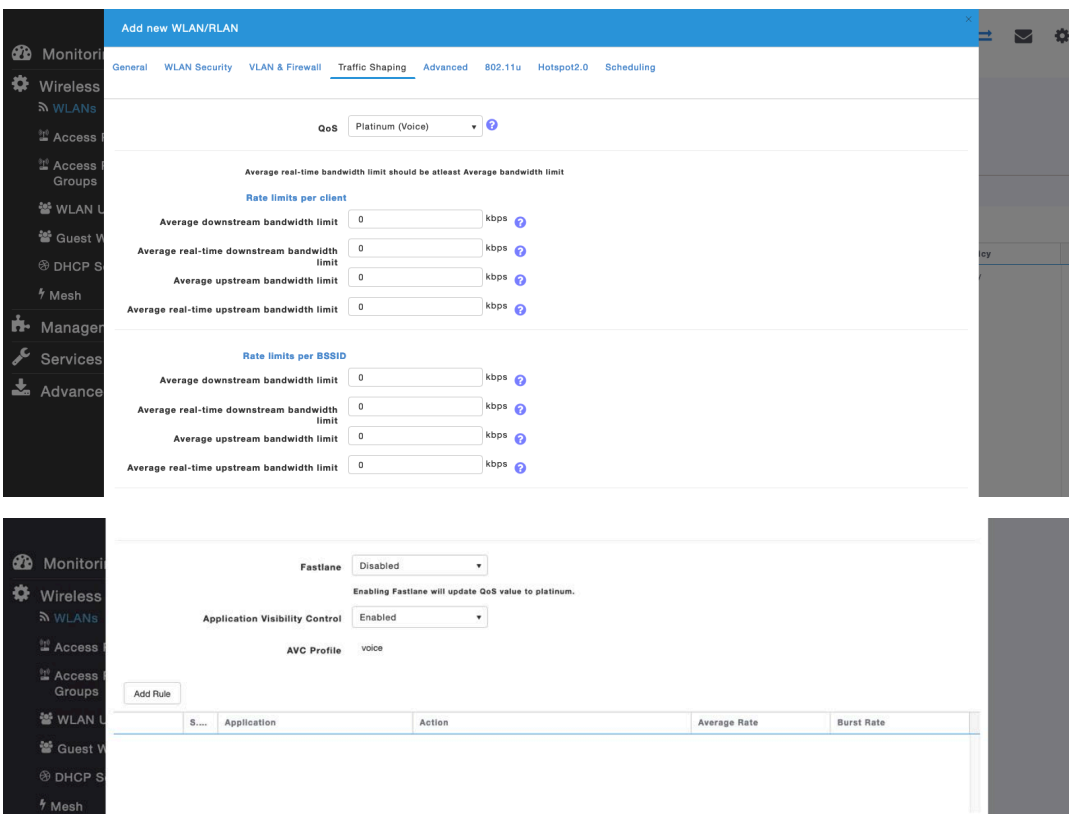
Add RADIUS Accounting Server

Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
✕	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.0.20	*****	1813

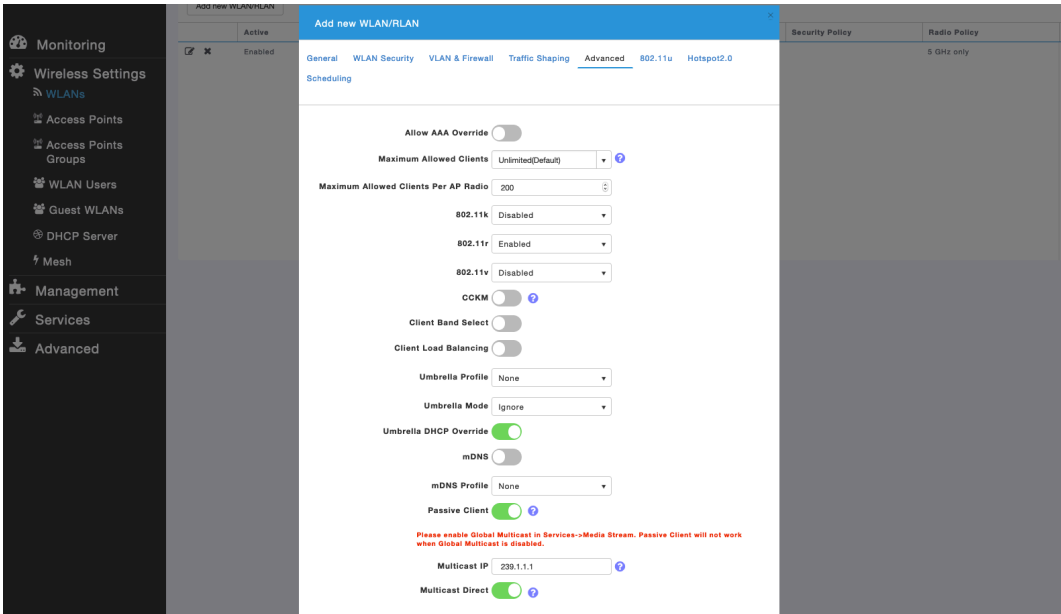
Configure the **Native VLAN ID** and **VLAN ID** for the WLAN as necessary.
 Ensure **Peer to Peer Block** is disabled.



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

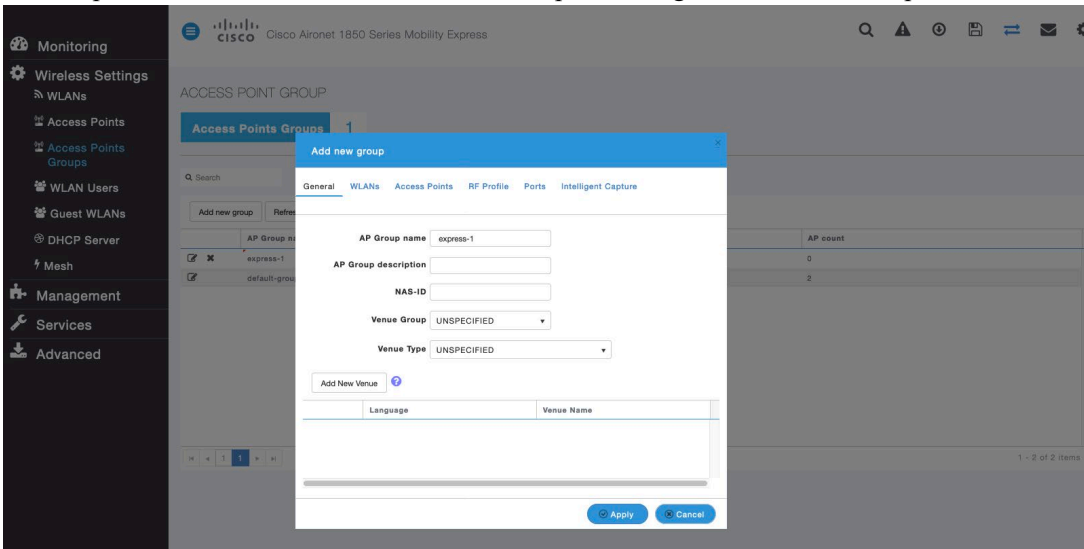


The **Maximum Allowed Clients** and **Maximum Allowed Clients Per AP Radio** can be configured as necessary.

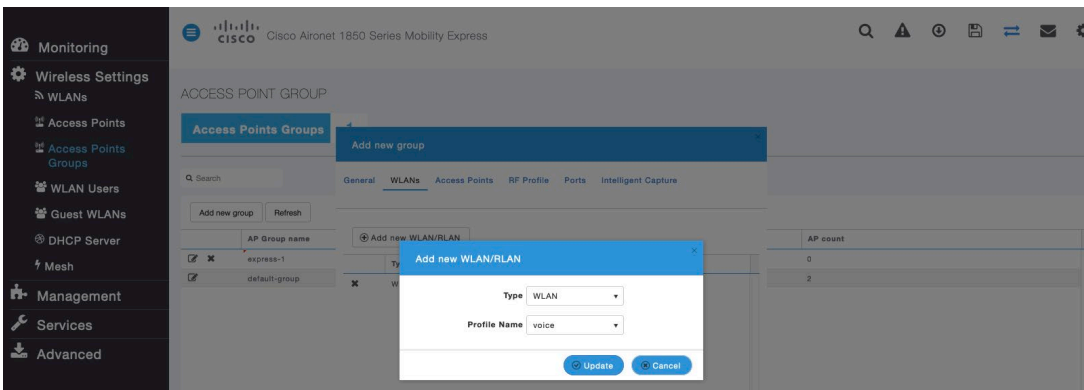


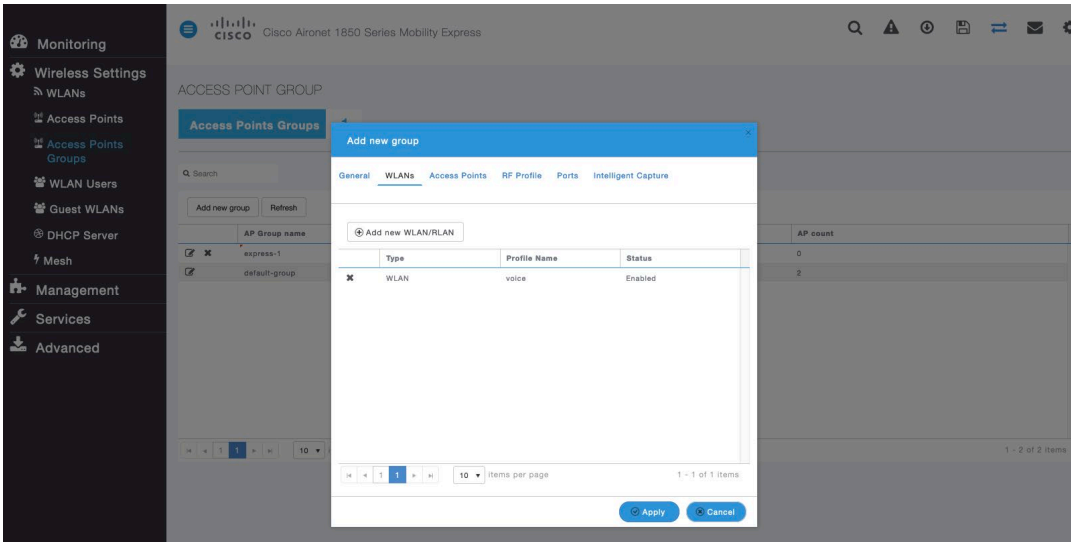
AP Groups

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

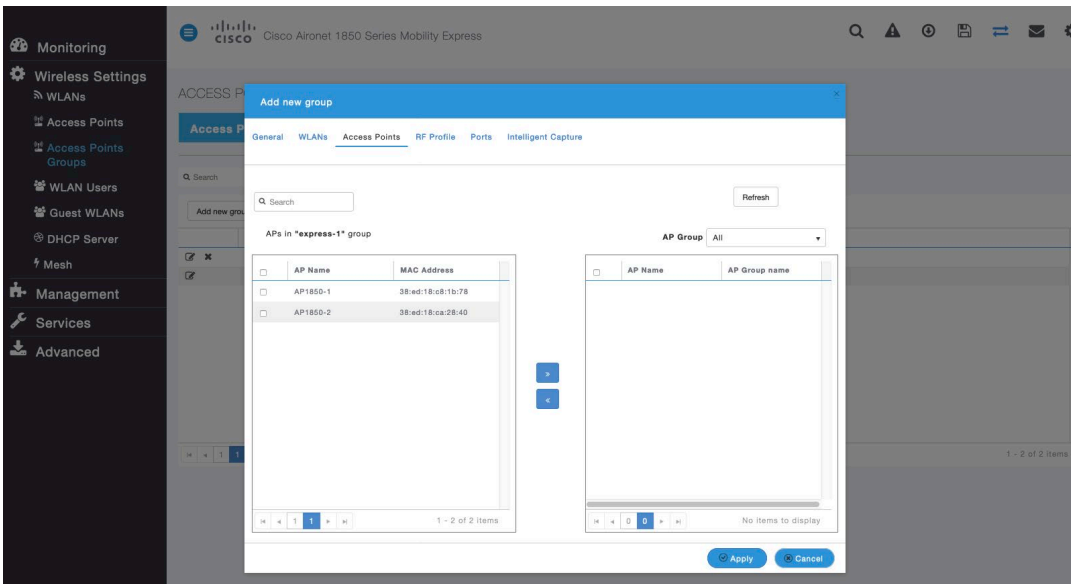


On the **WLANs** tab, select the desired WLANs and interfaces to map to then select **Add**.

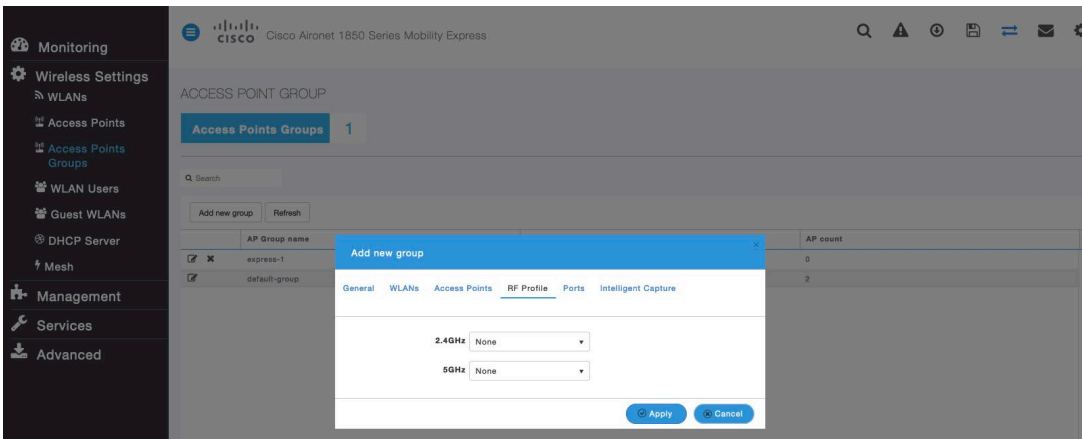




On the **Access Points** tab, select the desired access points then select **Apply**. Those access points will then reboot.



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



RF Profiles

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

For the SSID used by the Cisco Desk Phone 9800 Series, it's recommended to apply it to 5 GHz radios only.

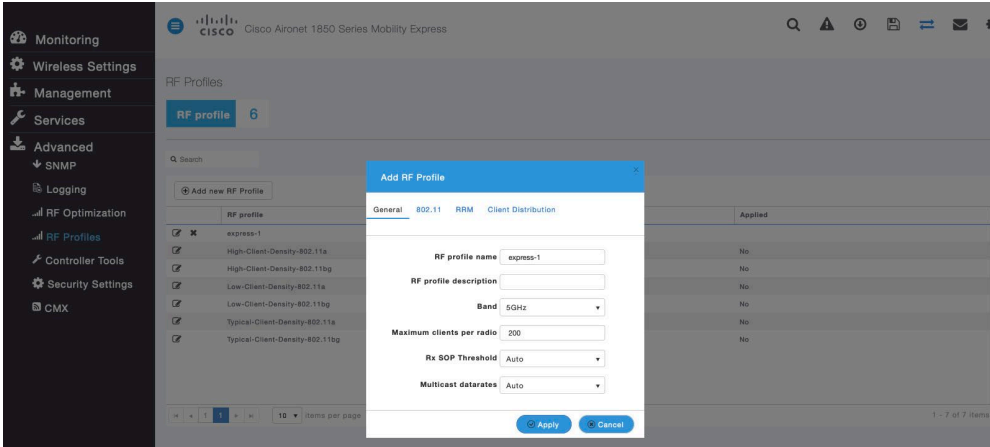
RF Profiles are applied to an AP group once created.

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

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

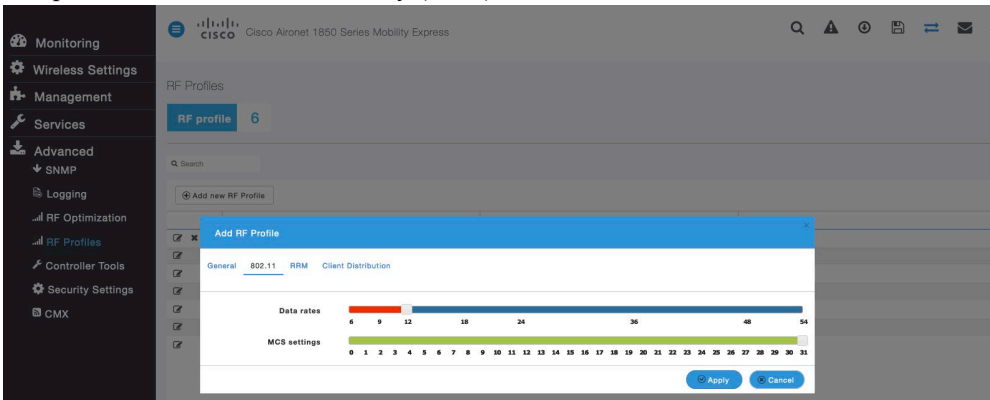
Maximum clients per radio, **Multicast data rates**, and **Rx Sop Threshold** can be configured as necessary.

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

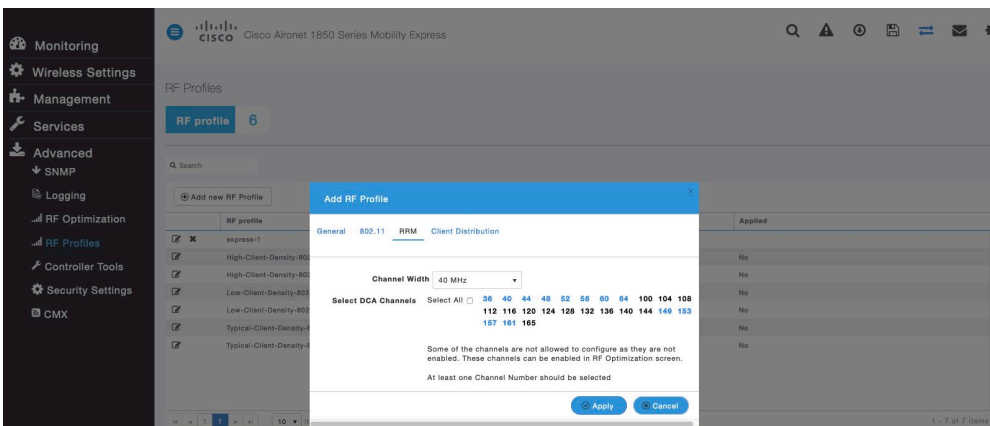


On the 802.11 tab, configure the data rates as necessary.

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

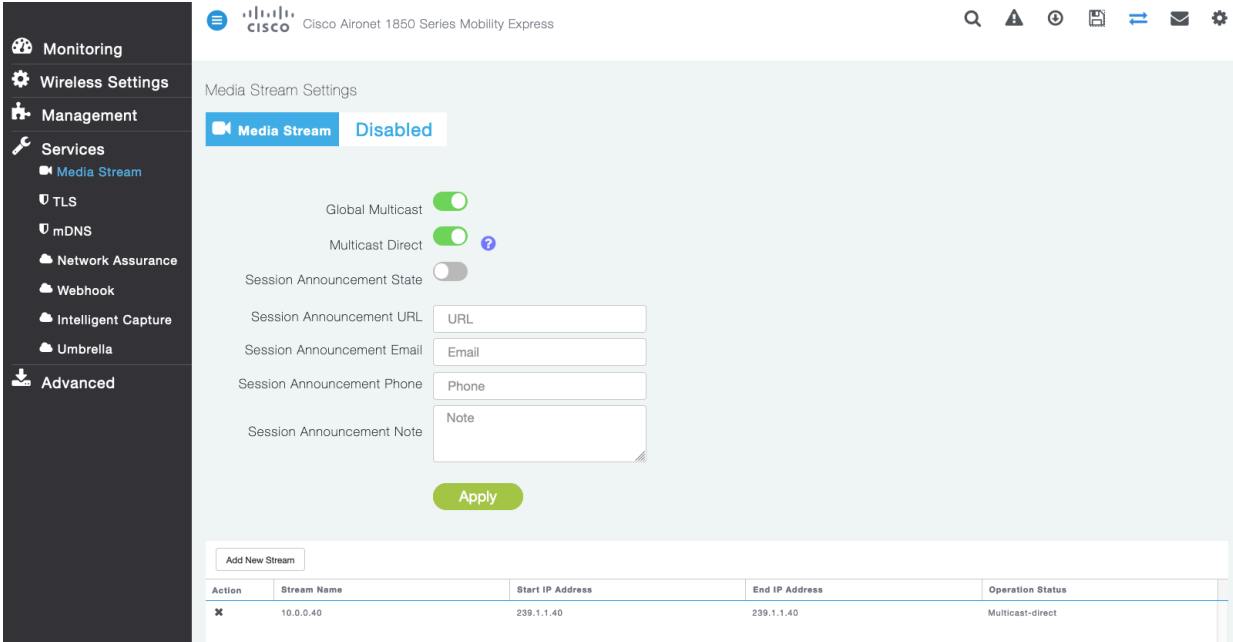


On the **RRM** tab, the **Channel Width** settings and **DCA Channels** can be configured.

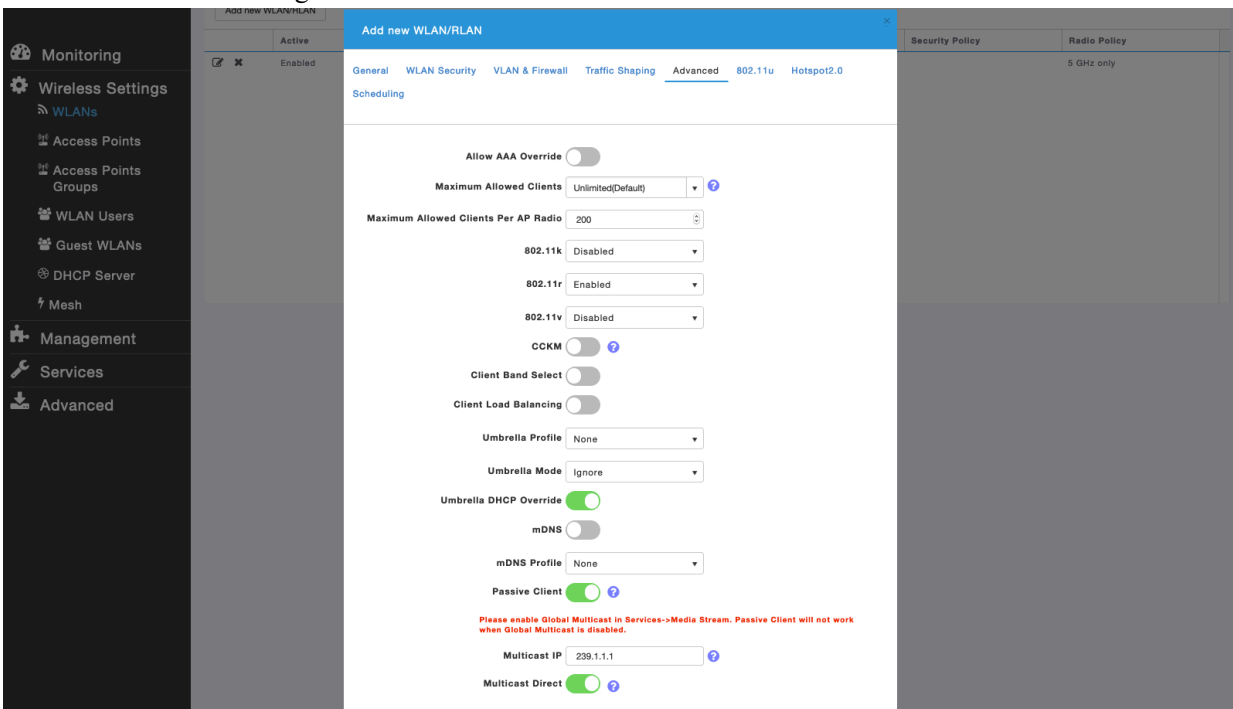


Multicast Direct

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



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



Cisco Autonomous Access Points

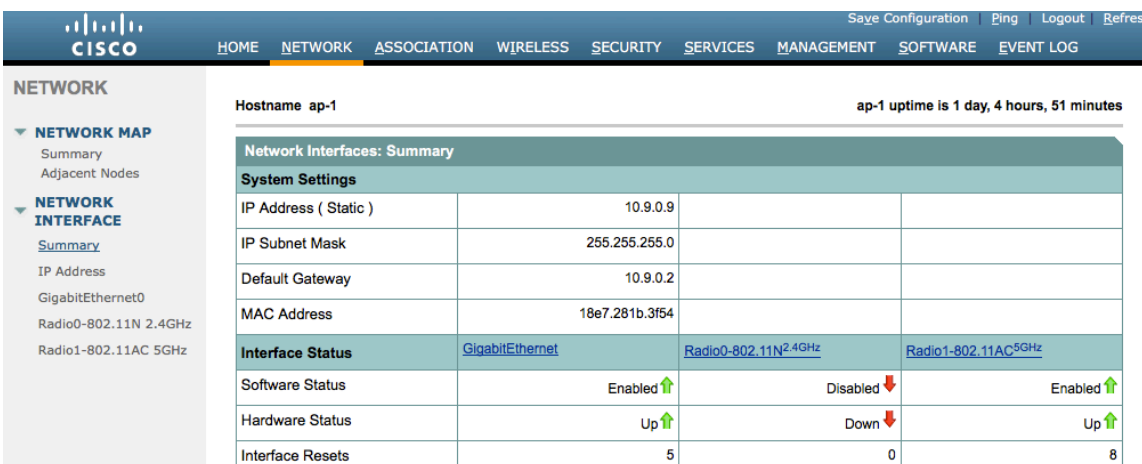
When configuring Cisco Autonomous Access Points, use the following guidelines:

- Enable **802.11r (FT)**
- Disable **CCKM**
- Disable **802.11k**
- Disable **802.11v**
- Configure the **Data Rates** as necessary
- Configure **Quality of Service (QoS)**
- Set the **WMM Policy** to **Required**
- Disable **Aironet Extensions**
- Disable **Public Secure Packet Forwarding (PSPF)**
- Set **IGMP Snooping** to **Enabled**

802.11 Network Settings

It is recommended to operate the Cisco Desk Phone 9800 Series on the 5 GHz band only due to availability of many channels and fewer interferers compared to the 2.4 GHz band.

To use 5 GHz, ensure the 802.11a/n network status is **Enabled**.



The screenshot shows the Cisco configuration interface for Hostname ap-1. The main content area displays the 'Network Interfaces: Summary' section, which includes a table of system settings and interface status for three interfaces: GigabitEthernet, Radio0-802.11N 2.4GHz, and Radio1-802.11AC 5GHz.

Network Interfaces: Summary			
System Settings			
IP Address (Static)	10.9.0.9		
IP Subnet Mask	255.255.255.0		
Default Gateway	10.9.0.2		
MAC Address	18e7.281b.3f54		
Interface Status	GigabitEthernet	Radio0-802.11N 2.4GHz	Radio1-802.11AC 5GHz
Software Status	Enabled ↑	Disabled ↓	Enabled ↑
Hardware Status	Up ↑	Down ↓	Up ↑
Interface Resets	5	0	8

It's recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps or higher as supported (optional) rates. However, some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

When using 5 GHz, it is recommended to enable up to 12 channels only to avoid any potential delay in access point discovery caused by scanning 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).

You 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 Auto RF and workaround the access points that are statically configured.

This may be necessary if there is an intermittent source of interference in the area.

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

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

The screenshot shows the Cisco configuration interface for the Radio1-802.11AC 5GHz interface. The page is titled "Radio1-802.11AC 5GHz Settings" and includes a navigation menu on the left with options like "NETWORK MAP", "NETWORK INTERFACE", "SUMMARY", "IP ADDRESS", "GIGABITETHERNET0", "RADIO0-802.11N 2.4GHZ", and "RADIO1-802.11AC 5GHZ". The main content area is divided into several sections:

- Enable Radio:** Enable Disable
- Current Status (Software/Hardware):** Enabled Up
- Role in Radio Network:** Access Point Access Point (Fallback to Radio Shutdown) Access Point (Fallback to Repeater) Repeater
 Root Bridge Non-Root Bridge Root Bridge with Wireless Clients Non-Root Bridge with Wireless Clients
 Workgroup Bridge Universal Workgroup Bridge Client MAC: (HHHH.HHHH.HHHH) Scanner Spectrum [Spectrum Information](#)
- Max-Client:** enable disable (1-255)
- 11r Configuration:** enable disable over-air over-ds Reassociation-time: (20-1200 ms)
- Data Rates:** Best Range Best Throughput Default
6.0Mb/sec Require Enable Disable
9.0Mb/sec Require Enable Disable
12.0Mb/sec Require Enable Disable
18.0Mb/sec Require Enable Disable
24.0Mb/sec Require Enable Disable
36.0Mb/sec Require Enable Disable
48.0Mb/sec Require Enable Disable
54.0Mb/sec Require Enable Disable
a0.1-2Mb/sec Require Enable Disable
a1.1-2Mb/sec Require Enable Disable
a2.1-2Mb/sec Require Enable Disable
a3.1-2Mb/sec Require Enable Disable
a4.1-2Mb/sec Require Enable Disable
a5.1-2Mb/sec Require Enable Disable
a6.1-2Mb/sec Require Enable Disable
a7.1-2Mb/sec Require Enable Disable
a8.1-2Mb/sec Require Enable Disable
a9.1-4Mb/sec Require Enable Disable
a0.2-2Mb/sec Require Enable Disable
a1.2-2Mb/sec Require Enable Disable
a2.2-2Mb/sec Require Enable Disable
a3.2-2Mb/sec Require Enable Disable
a4.2-2Mb/sec Require Enable Disable
a5.2-2Mb/sec Require Enable Disable
a6.2-2Mb/sec Require Enable Disable
a7.2-2Mb/sec Require Enable Disable
a8.2-2Mb/sec Require Enable Disable
a9.2-4Mb/sec Require Enable Disable
a0.3-2Mb/sec Require Enable Disable
a1.3-2Mb/sec Require Enable Disable
a2.3-2Mb/sec Require Enable Disable
a3.3-2Mb/sec Require Enable Disable
a4.3-2Mb/sec Require Enable Disable
a5.3-2Mb/sec Require Enable Disable
a6.3-2Mb/sec Require Enable Disable
a7.3-2Mb/sec Require Enable Disable

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

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

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

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

DefaultRadio Channel: Channel 36 - 5180 MHz Channel 36 5180 MHz

Dynamic Frequency Selection Bands: Band 1 - 5.150 to 5.250 GHz
Band 2 - 5.250 to 5.350 GHz
Band 3 - 5.470 to 5.725 GHz
Band 4 - 5.725 to 5.825 GHz

Channel Width: Below 40 MHz 20 MHz

World Mode Multi-Domain Operation: Disable Legacy Dot11d

Country Code: Indoor Outdoor

Radio Preamble: Short Long

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

Internal Antenna Configuration: Enable Disable

Antenna Gain(dBi): (-128 - 128)

Gratuitous Probe Response(GPR): Enable Disable

Period(Kusec): (10-255)

Transmission Speed:

Traffic Stream Metrics: Enable Disable

Aironet Extensions: Enable Disable

Ethernet Encapsulation Transform: RFC1042 802.1H

Reliable Multicast to WGB: Disable Enable

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

Beacon Privacy Guest-Mode: Enable Disable

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

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

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

Root Parent Timeout: (0-65535 sec)

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

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

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

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

To use 2.4 GHz, ensure the 802.11b/g/n network status and 802.11g is enabled.

It's recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps or 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 or higher as supported (optional).

WLAN Settings

It is recommended to have a separate SSID for the Cisco Desk Phone 9800 Series.

However, you can also use an existing SSID that is configured to support voice capable Cisco Wireless LAN endpoints.

The SSID to be used by the Cisco Desk Phone 9800 Series can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

Enable **WPA2/WPA3** key management.

Ensure 11r is enabled for fast secure roaming.

The screenshot shows the Cisco WLC configuration interface for a WLAN. The top navigation bar includes links for HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY (selected), SERVICES, MANAGEMENT, SOFTWARE, and EVENT LOG. The left sidebar lists various security and management tools. The main content area is titled "Security: Global SSID Manager" and shows the configuration for a specific SSID named "voice".

SSID Properties:

- Current SSID List:** A list containing "data" and "voice".
- SSID:** voice
- VLAN:** 3 (with a "Define VLANs" link)
- Backup 1:** (empty)
- Backup 2:** (empty)
- Backup 3:** (empty)
- Band-Select:** Band Select
- Universal Admin Mode:** Universal Admin Mode
- Interface:** Radio0-802.11N2.4GHz, Radio1-802.11AC5GHz
- Network ID:** (empty) (0-4096)
- Delete:** (button)

Client Authentication Settings:

Methods Accepted:

- Open Authentication: with EAP
- Web Authentication
- Web Pass
- Shared Authentication: < NO ADDITION >
- Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers:

- Use Defaults [Define Defaults](#)
- Customize
- Priority 1: < NONE >
- Priority 2: < NONE >
- Priority 3: < NONE >

MAC Authentication Servers:

- Use Defaults [Define Defaults](#)
- Customize
- Priority 1: < NONE >
- Priority 2: < NONE >
- Priority 3: < NONE >

Client Authenticated Key Management:

- Key Management:** Mandatory
- CCKM
- Enable WPA
- WPAv2 dot11r

WPA Pre-shared Key: ASCII Hexadecimal
11w Configuration:
11w Association-comeback: (1000-20000)
11w Saquery-retry: (100-500)

IDS Client MFP

Enable Client MFP on this SSID:

AP Authentication

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

Accounting Settings

Enable Accounting

Accounting Server Priorities:
 Use Defaults [Define Defaults](#)
 Customize

Priority 1:
Priority 2:
Priority 3:

Rate Limit Parameters

Limit TCP:

Input: Rate: Burst-Size: (0-500000)
 Output: Rate: Burst-Size: (0-500000)

Limit UDP:

Input: Rate: Burst-Size: (0-500000)
 Output: Rate: Burst-Size: (0-500000)

General Settings

Advertise Extended Capabilites of this SSID

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

Enable IP Redirection on this SSID

IP Address:

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

Association Limit (optional): (1-255)

EAP Client (optional):
 Username: Password:

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

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

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N^{2.4GHz}:

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

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

Radio1-802.11AC^{5GHz}:

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

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

Segment wireless voice and data into separate VLANs.

Ensure that Public Secure Packet Forwarding (PSPF) is not enabled for the voice VLAN, as this would prevent clients from communicating directly when associated with the same access point. Enabling PSPF in this scenario would result in audio communication being disrupted.

Save Configuration | Ping | Logout | Refresh

HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG

Services

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

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

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

VLAN ID: (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N^{2.4GHz}

Radio1-802.11AC^{5GHz}

Management VLAN (If non-native)

VLAN Information

View Information for:

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

Ensure AES is selected for encryption type.

Security

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

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

Security: Encryption Manager

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

Encryption Modes

None

WEP Encryption Optional

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

Cipher AES CCMP

Encryption Keys

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

Global Properties

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

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

[Apply](#) [Cancel](#)

Configure the RADIUS servers for authentication and accounting.

Security

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

SERVER MANAGER GLOBAL PROPERTIES

Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 42 minutes

Security: Server Manager

Backup RADIUS Server

IP Version: IPV4 IPV6

Backup RADIUS Server Name:

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

[Apply](#) [Delete](#) [Cancel](#)

Corporate Servers

Current Server List

RADIUS

	IP Version:	Server Name:	Server:	Shared Secret:
< NEW >	<input checked="" type="radio"/> IPV4 <input type="radio"/> IPV6	10.0.0.20	10.0.0.20 (Hostname or IP Address)	*****
10.0.0.20				
10.9.0.9				

[Delete](#) [Apply](#) [Cancel](#)

Authentication Port (optional): 1812 (0-65535)
Accounting Port (optional): 1813 (0-65535)

Default Server Priorities

EAP Authentication	MAC Authentication	Accounting
Priority 1: 10.0.0.20	Priority 1: < NONE >	Priority 1: 10.0.0.20
Priority 2: < NONE >	Priority 2: < NONE >	Priority 2: < NONE >
Priority 3: < NONE >	Priority 3: < NONE >	Priority 3: < NONE >

Admin Authentication (RADIUS)	Admin Authentication (TACACS+)
Priority 1: < NONE >	Priority 1: < NONE >
Priority 2: < NONE >	Priority 2: < NONE >
Priority 3: < NONE >	Priority 3: < NONE >

[Apply](#) [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 an access point as the primary WDS server and another as the backup WDS server.

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

Wireless Services: WDS/WNM - General Set-Up

WDS - Wireless Domain Services - Global Properties

Use this AP as Wireless Domain Services

Wireless Domain Services Priority: 255 (1-255)

Use Local MAC List for Client Authentication

WNM - Wireless Network Manager - Global Configuration

Configure Wireless Network Manager

Wireless Network Manager Address: DISABLED (IP Address or Hostname)

The Cisco Autonomous Access Points utilizes Inter-Access Point Protocol (IAPP), which is a multicast protocol. Therefore, it is recommended to a dedicated native VLAN for Cisco Autonomous Access Points.

For the native VLAN, it is recommended to not use VLAN 1 to ensure that IAPP packets are exchanged successfully.

Port security should be disabled on switch ports that Cisco Autonomous Access Points are directly connected to.

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

Current VLAN List

VLAN ID: 10 (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

Radio0-802.11N^{2.4GHz}

Radio1-802.11AC^{5GHz}

Management VLAN (If non-native)

VLAN Information

View Information for: VLAN 2

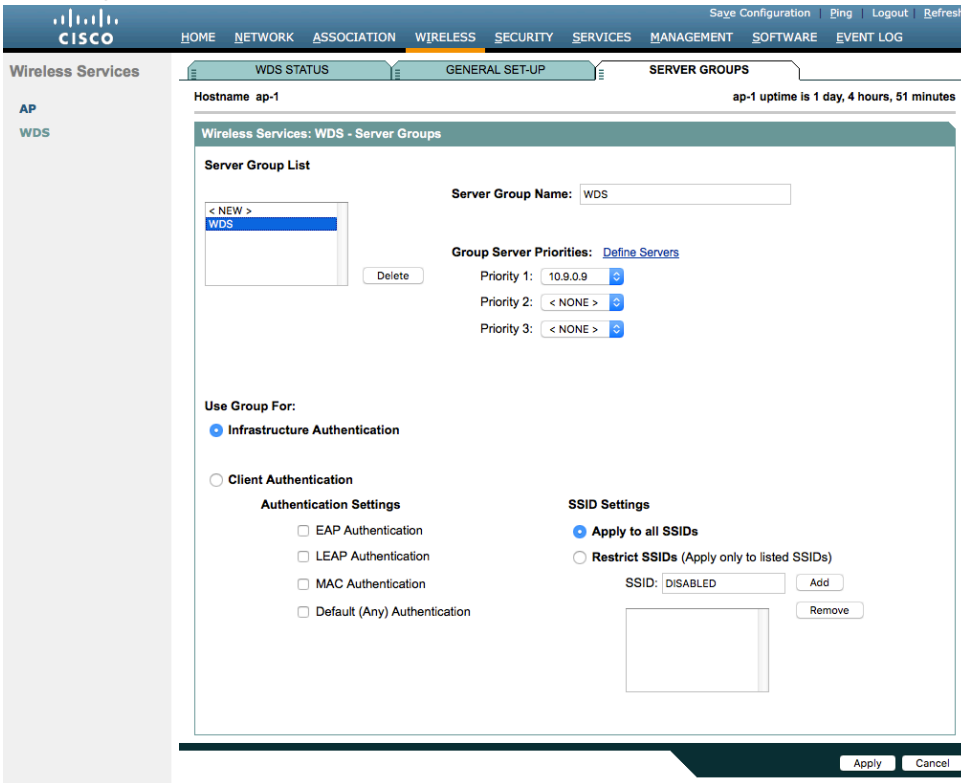
	GigabitEthernet Packets	Radio0-802.11N ^{2.4GHz} Packets	Radio1-802.11AC ^{5GHz} Packets
Received	65884		65884
Transmitted	5462		5462

Server groups for Wireless Domain Services must be defined.

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

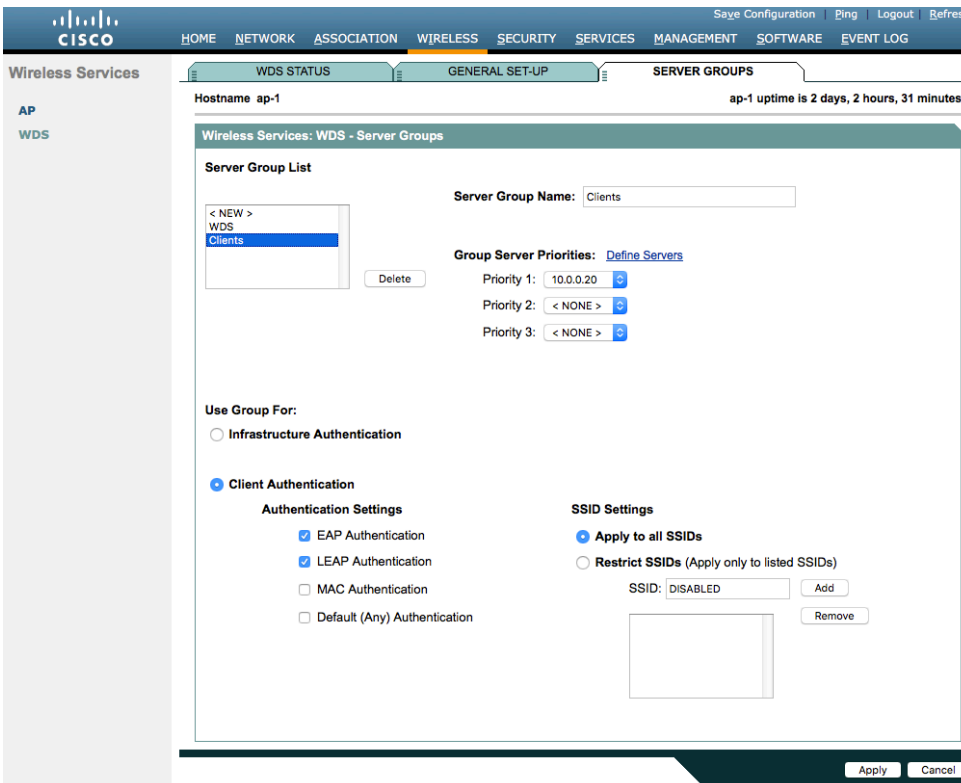
It is recommended to use local RADIUS for infrastructure authentication.

When not using local RADIUS for infrastructure authentication, ensure that all access points with Wireless Domain Services enabled are configured in the RADIUS server.



Then, define the server group to be used for client authentication.

Ensure that all access points with Wireless Domain Services enabled are configured in the RADIUS server.



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

Create a **Network Access Server** entry for the local access point.

Define the user account used to configure access points for authentication to the Wireless Domain Services enabled access point.

Configure local RADIUS on each access point participating in Wireless Domain Services.

The screenshot shows the Cisco configuration interface for a Local RADIUS Server. The interface is divided into several sections:

- Enable Authentication Protocols:** EAP FAST, LEAP, and MAC are all checked.
- Network Access Servers (AAA Clients):** A table with one entry: Network Access Server: 10.9.0.9 (IP Address), Shared Secret:
- Individual Users:** A table with one entry: Username: wds, Password:, Confirm Password:, Group Name: < NONE >, MAC Authentication Only: unchecked.
- User Groups:** A table with one entry: Group Name:, Session Timeout (optional):, Failed Authentications before Lockout (optional):, Lockout (optional): Interval (1-4294967295 sec), VLAN ID (optional):, SSID (optional):

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**.

When using a single WDS server, specify the IP address of the WDS server. Otherwise, enable **Auto Discovery**. Enter the **Username** and **Password** to authenticate to the WDS server.

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

Wireless Services: AP

Participate in SWAN Infrastructure: Enable Disable

WDS Discovery: Auto Discovery Specified Discovery: (IP Address)

Username:

Password:

Confirm Password:

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

Once the access point has been configured to authenticate to the WDS server, you can check WDS Status to view the WDS server state as well as how many access points are registered to the WDS server.

Hostname ap-1 ap-1 uptime is 1 day, 5 hours, 1 minute

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

MAC Address	IPv4 Address	IPv6 Address	Priority	State
18e7.281b.3f54	10.9.0.9	::	255	Administratively StandAlone - ACTIVE

WDS Registration

APs: 1 Mobile Nodes: 0

AP Information

Hostname	MAC Address	IPv4 Address	IPv6 Address	CDP Neighbor	State
ap-1	18e7.281b.3f54	10.9.0.9	::	Switch-2.gil	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID

Wireless Network Manager Information

IP Address	Authentication Status

Call Admission Control (CAC)

Disabled.

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.

The screenshot shows the Cisco configuration interface for QoS Policies on a host named ap-1. The interface is divided into several sections:

- Services: QoS Policies**
 - Create/Edit Policies**
 - Create/Edit Policy:** Voice
 - Policy Name:** Voice
 - Classifications:**
 - DSCP - COS Controlled Load (4)
 - DSCP - COS Video < 100ms Latency (5)
 - DSCP - COS Voice < 10ms Latency (6)
 - Match Classifications:**
 - IP Precedence:** Routine (0)
 - IP DSCP:** Best Effort
 - IP Protocol 119:** No Filters defined. [Define Filters.](#)
 - Filter:** No Filters defined. [Define Filters.](#)
 - Default Classification for Packets on the VLAN:** Best Effort (0)
 - Rate Limiting:**
 - Bits per Sec.:** (8000-2000000000)
 - Burst Rate (Bytes):** (1000-512000000)
 - Conform Action:** Transmit
 - Exceed Action:** Drop
 - Apply Class of Service**
 - Best Effort (0) Add
 - Best Effort (0) Add
 - Best Effort (0) Add
 - Best Effort (0) Add
 - Apply Policies to Interface/ VLANs**

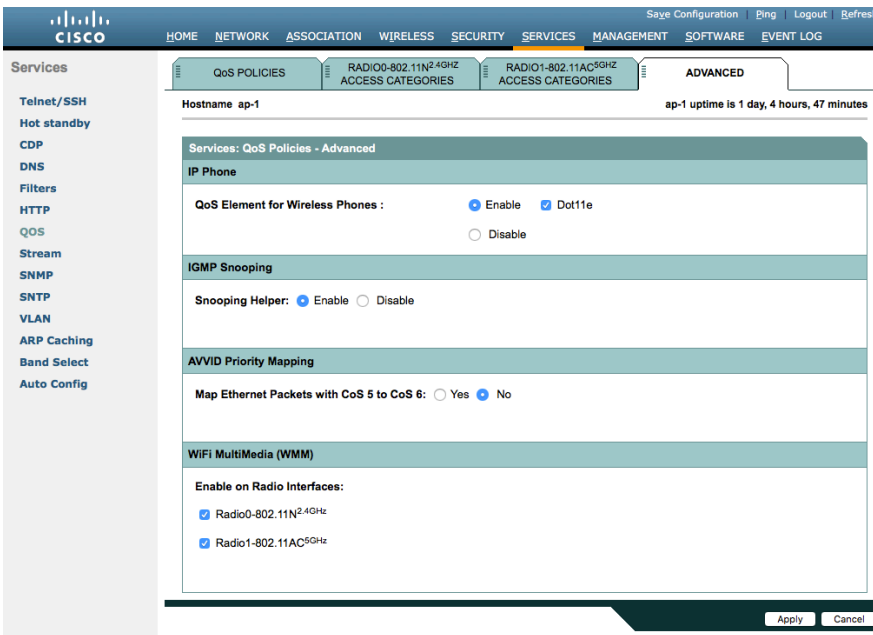
VLAN	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHz}	GigabitEthernet0
VLAN 2	Incoming	Data	Data
	Outgoing	Data	Data
VLAN 3	Incoming	Voice	Voice
	Outgoing	< NONE >	< NONE >
VLAN 10	Incoming	< NONE >	< NONE >
	Outgoing	< NONE >	< NONE >

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

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

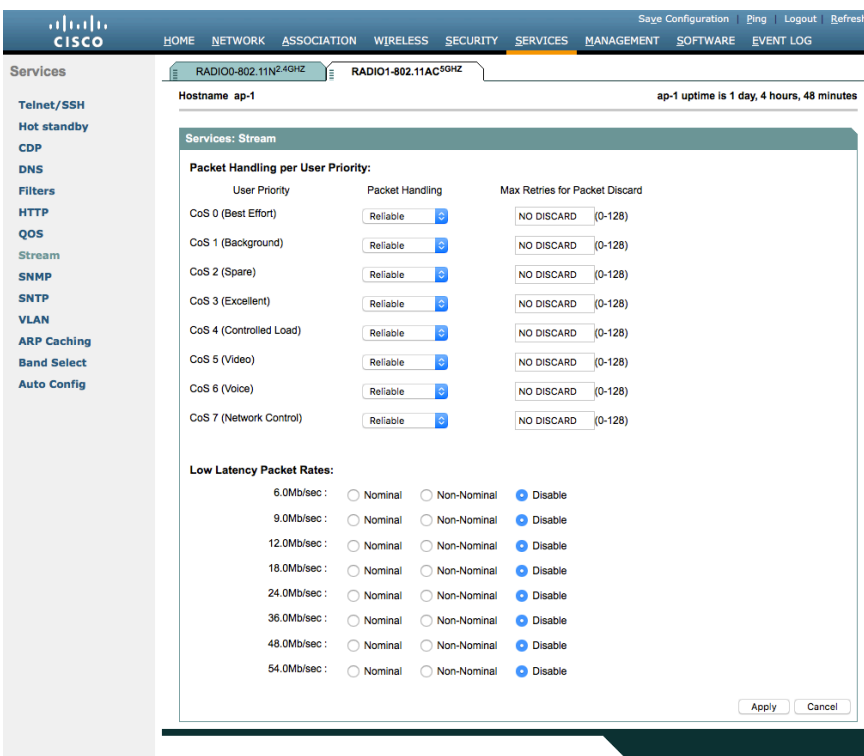
Ensure **IGMP Snooping** is enabled.

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



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

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

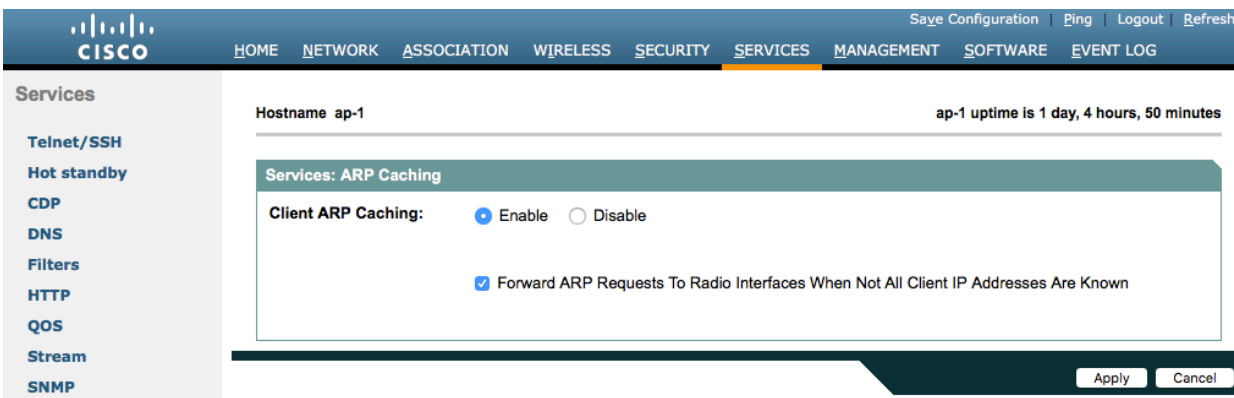


Power Management

Proxy ARP helps 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.



Cisco Meraki Access Points

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

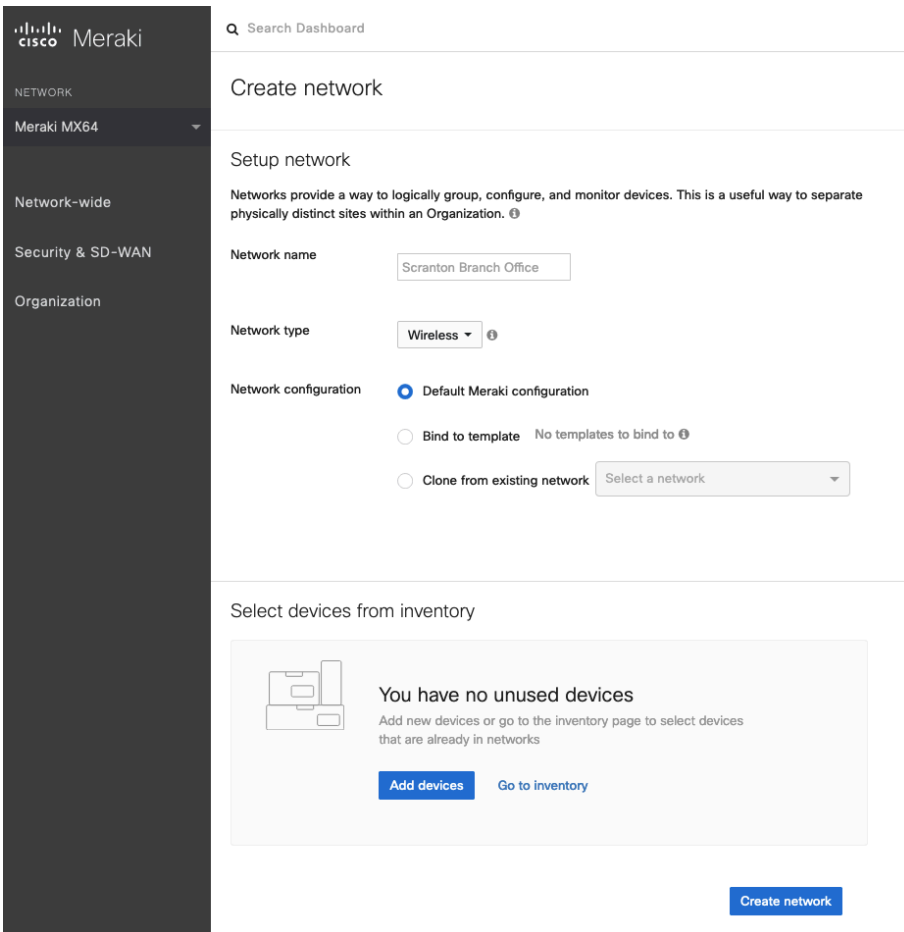
- Enable **802.11r** for **WPA2/WPA3-Enterprise** or **Pre-shared key**
- Set **Splash page** to **None**
- Enable **Bridge mode**
- Enable **VLAN tagging**
- Set **Band selection** to **5 GHz band only**
- Configure the **Data Rates** as necessary
- Configure **Quality of Service (QoS)**

Creating the Wireless Network

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

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

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



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

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

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

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

Claim by serial and/or order number

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

Close

Claim

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

Inventory

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

Add to ... ▾ Unclaim Unused Used Both Search inventory

Existing network

Meraki WLAN ▾

New network

Add to existing

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

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

Add access points

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

Search inventory

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

Add access points

SSID Configuration

To create an 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 Desk Phone 9800 Series. Data clients and other type of clients should utilize a different SSID and VLAN.

However, you can also use an existing SSID that is configured to support voice capable Cisco Wireless LAN.

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

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

Configuration overview

SSIDs Showing 4 of 15 SSIDs. [Show all my SSIDs.](#)

meraki-voice

Enabled

Name [rename](#)

Access control [edit settings](#)

Encryption 802.1X with Meraki RADIUS

Sign-on method None

Bandwidth limit unlimited

Client IP assignment Local LAN

Clients blocked from using LAN no

Wired clients are part of Wi-Fi network no

VLAN tag ⓘ 3

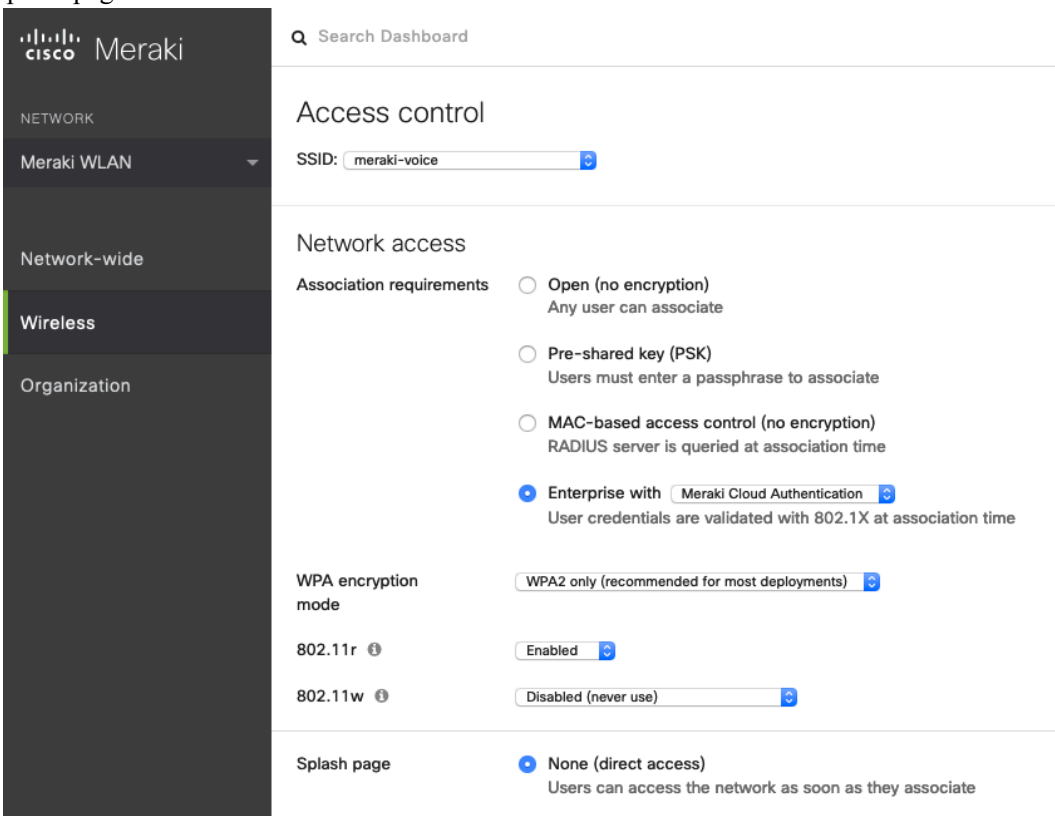
VPN Disabled

Splash page

Splash page enabled no

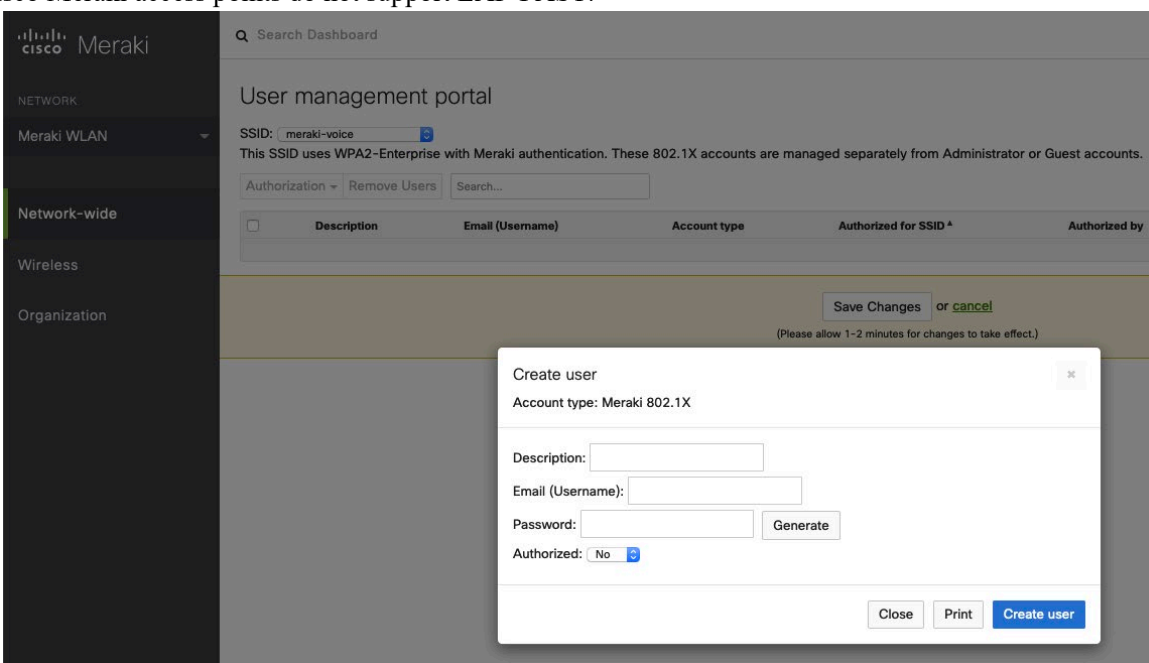
Splash theme n/a

On the **Wireless > Configure > Access control** page, select **WPA2-Enterprise** to enable 802.1x authentication. The Cisco Meraki authentication server or an external RADIUS server can be utilized when selecting **WPA2-Enterprise**. The Cisco Meraki authentication server supports PEAP authentication and requires a valid email address. Other authentication types (e.g. Pre-Shared Key) are available as well. Ensure 802.11r is enabled. Ensure Splash page is set to **None** to enable direct access.



If **WPA2-Enterprise** is enabled where the Cisco Meraki authentication server will be utilized as the RADIUS server, then a user account must be created on the **Network-wide > Configure > Users** page, which the Cisco Desk Phone 9800 Series will be configured to use for 802.1x authentication.

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



On the **Wireless > Configure > Access control** page, it's recommended to enable **Bridge mode**. This configuration allows the Cisco Desk Phone 9800 Series to 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.

For more information about Cisco Meraki MS Switches, refer to the Cisco Meraki MS Switch VoIP Deployment Guide.

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

when utilizing Cisco IOS Switches, use the following switch port configuration for ports that have Cisco Meraki access points connected to enable 802.1q trunking.

```
Interface GigabitEthernet X
switchport trunk encapsulation dot1q
switchport mode trunk
mls qos trust dscp
```

The screenshot shows the Cisco Meraki configuration interface for a wireless network. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled 'Addressing and traffic' and contains several sections:

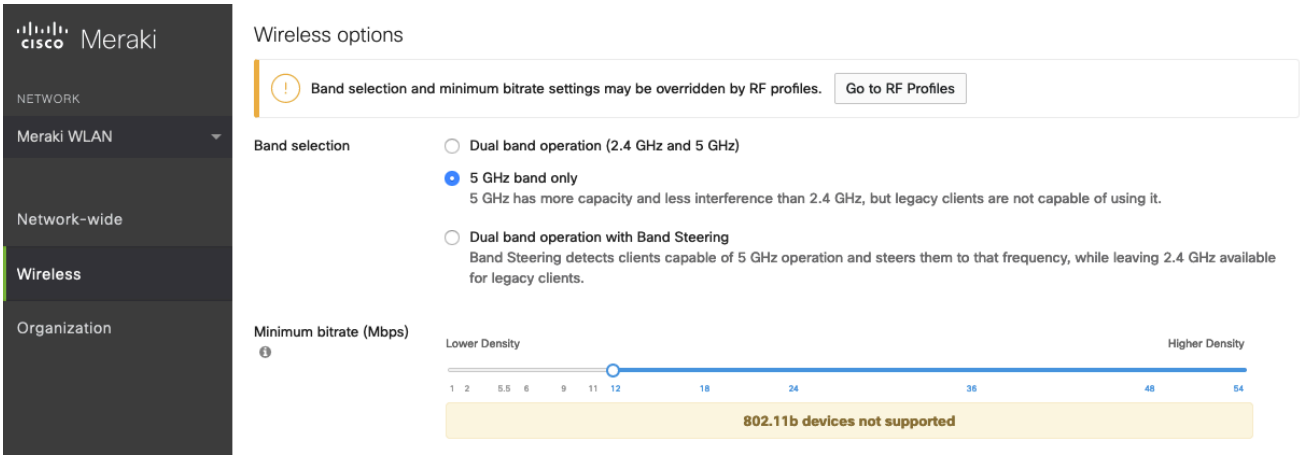
- Client IP assignment:** This section has five radio button options:
 - NAT mode: Use Meraki DHCP. Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.
 - 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.
 - Layer 3 roaming. Clients receive DHCP leases from the LAN or use static IPs, similar to bridge mode. If the client roams to an AP where their original IP subnet is not available, then the client's traffic will be forwarded to an anchor AP on their original subnet. This allows the client to keep the same IP address, even when traversing IP subnet boundaries.
 - Layer 3 roaming with a concentrator. Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.
 - VPN: tunnel data to a concentrator. Meraki devices send traffic over a secure tunnel to an MX concentrator.
- VLAN tagging:** A dropdown menu is set to 'Use VLAN tagging'.
- VLAN ID:** A table with columns 'AP tags', 'VLAN ID', and 'Actions'. The 'All other APs' row has a 'VLAN ID' of 3 and an 'Add VLAN' link.
- Content filtering:** A dropdown menu is set to 'Don't filter content'.
- Bonjour forwarding:** A dropdown menu is set to 'Enable Bonjour Gateway'. Below it, a message states 'There are no Bonjour forwarding rules on this network.' with an 'Add a Bonjour forwarding rule' link.

On the **Wireless > Configure > Access control** page, you can configure the frequency band for the SSID to be used by the Cisco Desk Phone 9800 Series as needed.

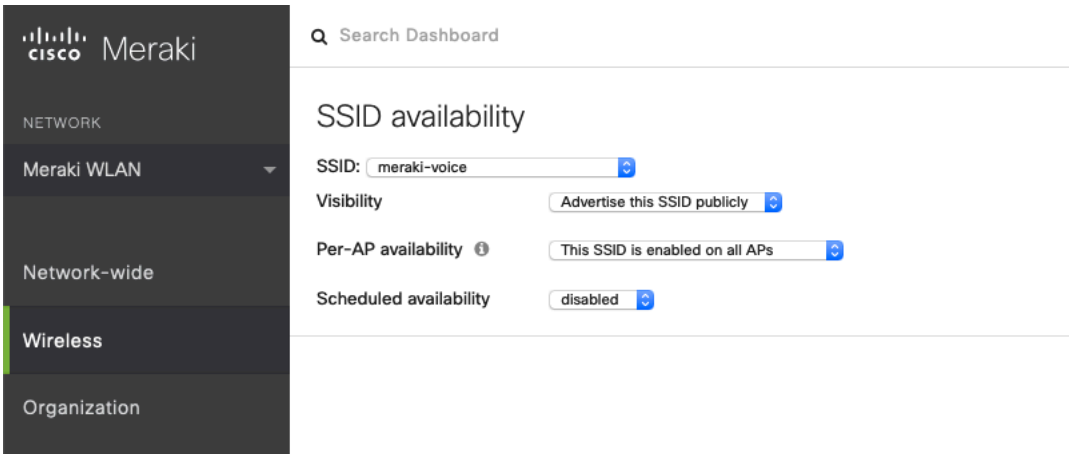
It is recommended to select **5 GHz band only** to operate the Cisco Desk Phone 9800 Series on the 5 GHz band due to availability of many channels and fewer interferers compared to the 2.4 GHz band.

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

Is recommended to disable data rates below 12 Mbps unless a legacy 2.4 GHz client needs to connect to the Wireless LAN. Cisco Meraki access points currently utilize a DTIM period of 1 with a beacon period of 100 ms. These settings are non-configurable.

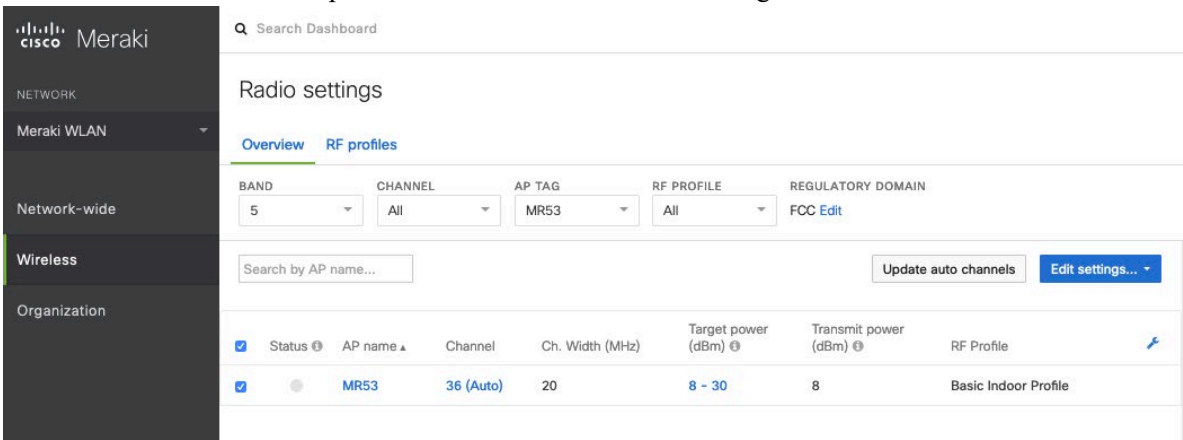


On the **Wireless > Configure > SSID availability** page, the SSID can be broadcasted by setting **Visibility** to **Advertise this SSID publicly**.
 It is recommended to set **Per-AP Availability** to **This SSID is enabled on all APs**.
 A schedule for SSID availability can be configured as needed. However, it is recommended to set **Scheduled Availability** to **Disabled**.

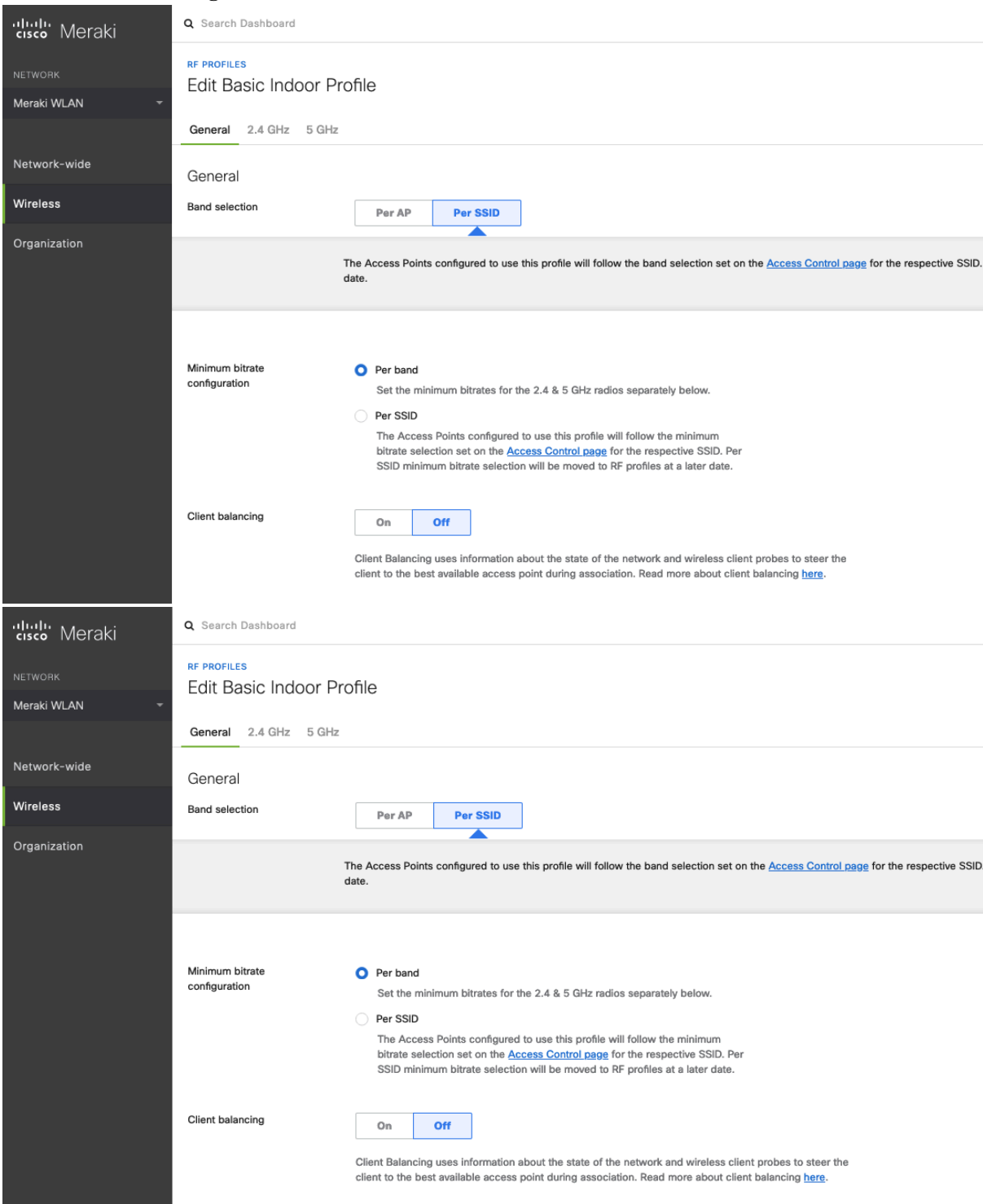


Radio Settings

On the **Wireless > Configure > Radio settings** page, access points can be configured in bulk or individually 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. This configuration may be necessary if there is intermittent interference in the area. While other access points can be enabled for **Auto** and work around the access points that are have static channel assignments.



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



In the RF Profile, the **Channel width** for 5 GHz radios can be set to use 20 MHz, 40 MHz, or 80 MHz channels. 2.4 GHz radios utilize 20 MHz channel width and cannot be configured for any other channel width.

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

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

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

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

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

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

General 2.4 GHz 5 GHz

5 GHz radio settings

Turn off 5GHz radio See band selection above.

Channel width

Manual 5 GHz channel width

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

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

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

Radio transmit power range (dBm) Transmit shorter distance Transmit farther

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

Minimum bitrate Lower Density Higher Density

Change 5 GHz channels used by AutoChannel

Available channels for AutoChannel

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

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

DFS channels

For low to medium density deployments.

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

Firewall and Traffic Shaping

On the **Wireless > Configure > Firewall & traffic shaping** page, firewall and traffic shaping rules can be defined. Ensure a **Layer 3 firewall rule** is configured to allow local LAN access for wireless clients.

To allow traffic shaping rules to be defined select **Shape traffic on this SSID** in the drop-down menu for **Shape traffic**. Once **Shape traffic on this SSID** has been applied, then select **Create a new rule** to define **Traffic shaping rules**.

By default, Cisco Meraki access points currently tag voice frames marked with DSCP EF (46) as WMM UP 5 instead of WMM

UP 6 and call control frames marked with DSCP CS3 (24) as WMM UP 3 instead of WMM UP 4.

The screenshot shows the Cisco Meraki dashboard interface. On the left is a dark sidebar with navigation options: NETWORK, Meraki WLAN, Network-wide, Wireless (highlighted), and Organization. The main content area is titled 'Firewall & traffic shaping' and shows settings for the 'meraki-voice' SSID. It includes sections for 'Block IPs and ports' (Layer 2 LAN isolation and Layer 3 firewall rules), 'Block applications and content categories' (Layer 7 firewall rules), and 'Traffic shaping rules' (Per-client bandwidth limit, Per-SSID bandwidth limit, and Shape traffic).

Firewall & traffic shaping
SSID: meraki-voice

Block IPs and ports
Layer 2 LAN isolation: Disabled (bridge mode only)
Layer 3 firewall rules:

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

[Add a layer 3 firewall rule](#)

Block applications and content categories
Layer 7 firewall rules: There are no rules defined for this SSID.
[Add a layer 7 firewall rule](#)

Traffic shaping rules
Per-client bandwidth limit: unlimited (details) Enable SpeedBurst
Per-SSID bandwidth limit: unlimited (details)
Shape traffic: Shape traffic on this SSID

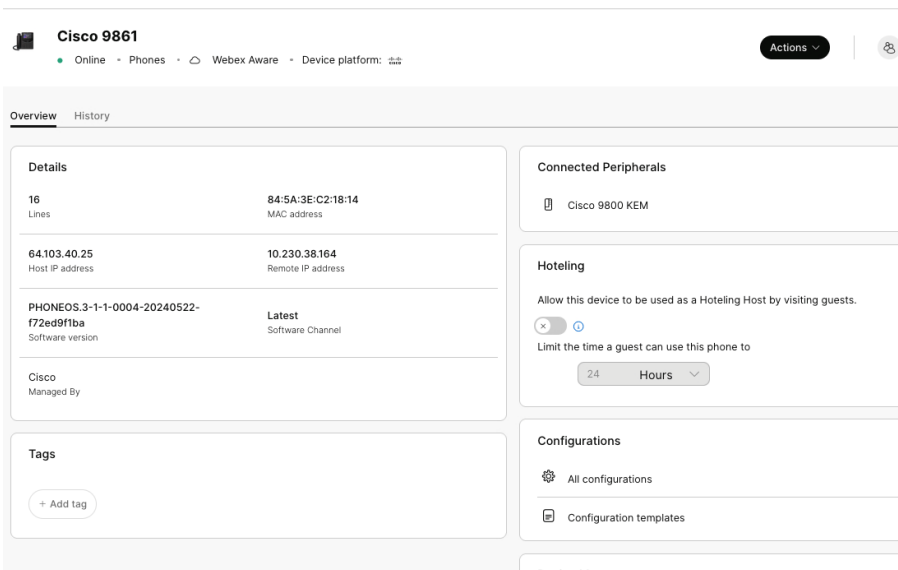
Configure Cisco Call Control

Cisco Webex Calling

You can add Cisco Desk Phone 9800 Series to Cisco Webex Calling and assigned it to a user for personal usage or as a workspace for shared usage.

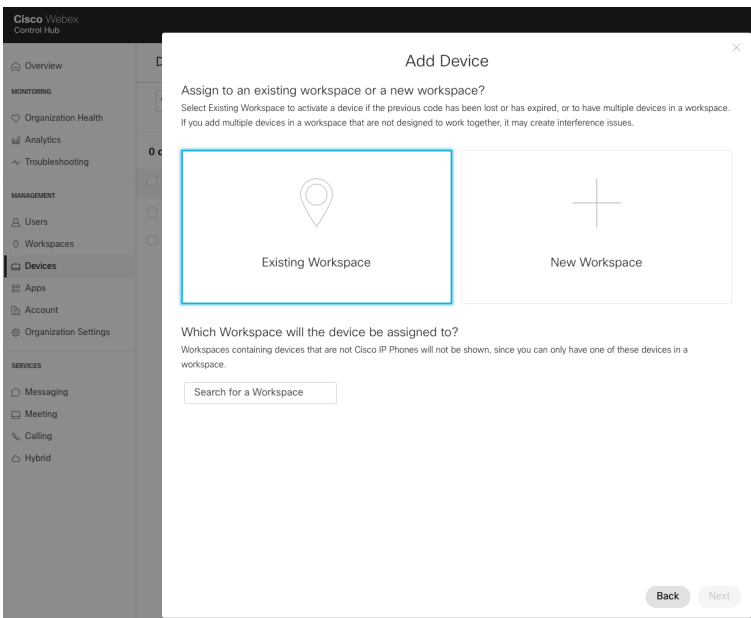
Personal Usage

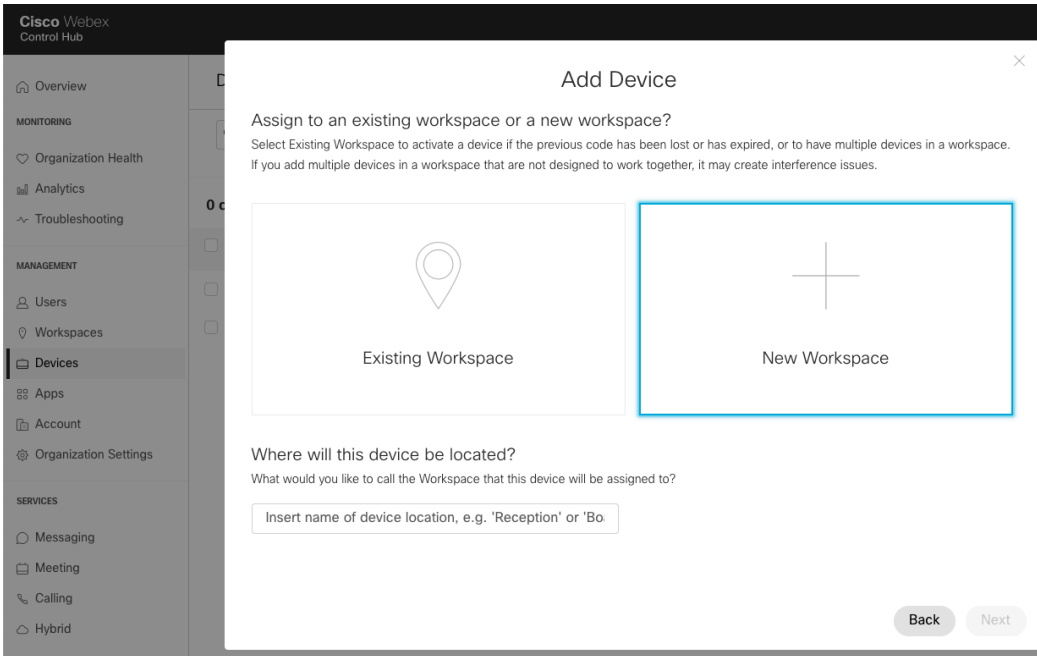
You can assign Cisco Desk Phone 9800 Series to a user and configure the settings in on Control Hub.



Workspace Usage

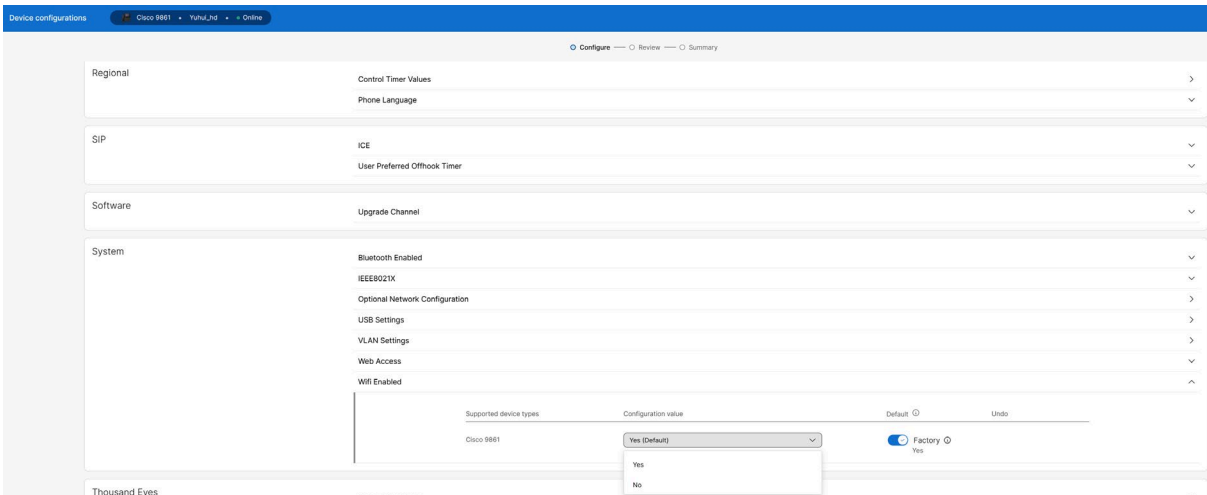
You can configure Cisco Desk Phone 9800 Series as a workspace device on Control Hub.





Wi-Fi Capability

On Cisco Control Hub, ensure that Wi-Fi is enabled to use a Cisco Desk Phone 9800 Series in wireless environment.



Cisco Unified Communications Manager

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

Device Enablement

To enable the Cisco Desk Phone 9800 Series device type in the Cisco Unified Communications Manager, the corresponding device package COP file must be installed via the Cisco Unified Operating System Administration webpage for each Cisco Unified Communications Manager server.

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

Perform the following actions based on the Cisco Unified Communications Manager version.

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 COP file, refer to the Cisco Unified Communication Manager Operation 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 Desk Phone 9800 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 of the Cisco Desk Phone 9800 Series can be found by navigating to **Settings > About this device** on the phone.

Device Information

Device is trusted

MAC Address*

Description

Device Pool* -- Not Selected -- [View Details](#)

Common Device Configuration < None > [View Details](#)

Phone Button Template* -- Not Selected --

Softkey Template < None >

Common Phone Profile* Standard Common Phone Profile [View Details](#)

Common Settings

Some settings such as Wireless LAN can be configured on an enterprise phone through common phone profile or at individual phone level.

Wireless LAN is automatically disabled temporarily when Ethernet is connected to the Cisco Desk Phone 9800 Series and will be automatically re-enabled once Ethernet is disconnected if Wi-Fi is enabled on the phone.

Override common settings can be enabled at either configuration level.

Wi-Fi*

QoS Parameters

The DSCP values for SIP communications, phone configuration, and phone-based services are defined in the Cisco Unified Communications Manager’s Enterprise Parameters.

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

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

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

Wireless LAN Profiles

With Cisco Unified Communications Manager 10.0 release and later, you can provision the Cisco Desk Phone 9800 Series with Wireless LAN Profiles. EAP-TLS support is included.

Create a Wireless LAN Profile

Follow the following steps to provision your phone with a Wireless LAN profile on Cisco Unified Communications Manager.

- Before creating a Wireless LAN Profile and associating it with your phone, the phone should be configured to utilize a security profile with TFTP encryption enabled. This prevents Wireless LAN Profile data from being transmitted in clear text to the phone.

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

Phone Security Profile Information

Product Type: Cisco 9871
Device Protocol: SIP
Name* Cisco 9871 - Standard SIP Secure Profile
Description Cisco 9871 - Standard SIP Secure Profile
Nonce Validity Time* 600
Device Security Mode Encrypted
Transport Type* TLS

Enable Digest Authentication
 TFTP Encrypted Config
 Enable OAuth Authentication

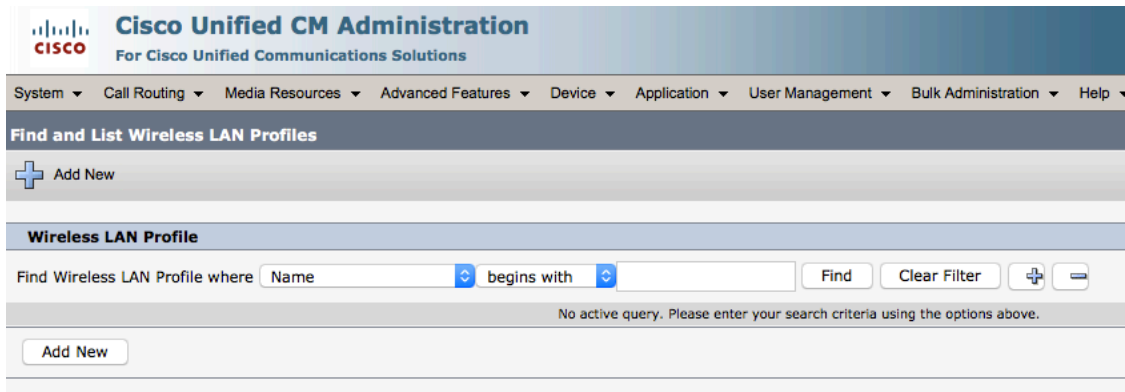
- Once the security profile has been created, it must be applied to the phone to enable TFTP encryption for the phone's configuration files.
- Select the configured security profile from the **Device Security Profile** drop-down menu.

Protocol Specific Information

Packet Capture Mode* None
Packet Capture Duration 0
BLF Presence Group* Standard Presence group
SIP Dial Rules < None >
MTP Preferred Originating Codec* 711ulaw
Device Security Profile* Cisco 9871 - Standard SIP Secure Profile
Rerouting Calling Search Space < None >
SUBSCRIBE Calling Search Space < None >
SIP Profile* Standard SIP Profile [View Details](#)
Digest User < None >

Media Termination Point Required
 Unattended Port
 Require DTMF Reception

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



- Specify the **Name**, **Description**, **Wireless Settings (SSID, Frequency Band, User Modifiable)**, and **Authentication Settings** for the profile.

Below are Wireless LAN Profile defaults:

- **Frequency Band** = Auto
- **User Modifiable** = Allowed
- **Authentication Method** = EAP-FAST

- Enter a **Name** for the Wireless LAN Profile containing up to 50 characters.
- Optionally, enter the **Description** containing up to 63 characters.

- Select **Allowed** in the **User Modifiable** drop-down list.
The user has the capability to change any Wireless LAN settings (e.g. Enable/Disable, SSID, Frequency

Band, Authentication Method, Username and Password, PSK Passphrase, WEP Key) locally on the endpoint.

Note: For Cisco Desk Phone 9800 Series, users are allowed to change the WLAN settings regardless of this parameter.

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

SSID (Network Name)*

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

Frequency Band*

- Select the desired **Authentication Method** option.
 - If **EAP-FAST**, **PEAP-MSCHAPv2**, or **PEAP-GTC** is selected, the option to enter shared credentials (Username and Password) is available.
 - If **Provide Shared Credentials** is not checked, the Username and Password will need to be configured locally on the phone by the admin or user.

- If **Provide Shared Credentials** is checked, then the specified **Username** and **Password** will be utilized for all Cisco Desk Phone 9800 Series that utilize this Wireless LAN Profile.
- Up to 64 characters can be entered for the Username and Password.
- Optionally enter the **Password Description**.

- If **EAP-TLS** is selected, **User Certificate** must be configured to specify the type of user certificate to utilize for EAP-TLS authentication.
- Set **User Certificate** to **MIC** (Manufacturing Installed Certificate), **LSC** (Locally Significant Certificate) or **User Installed**.

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

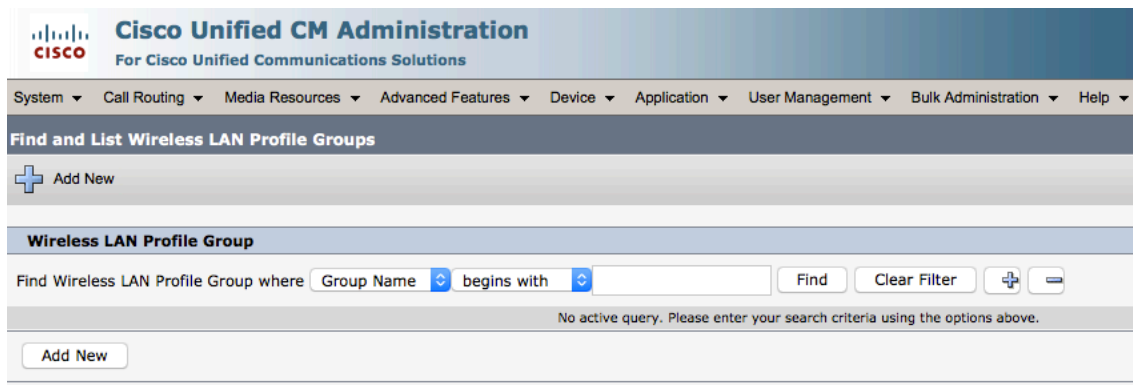
- If **None** is selected, then no authentication is required, and no encryption will be utilized.

Note: Cisco Desk Phone 9800 Series doesn't support WEP or LSC ECC certificate.

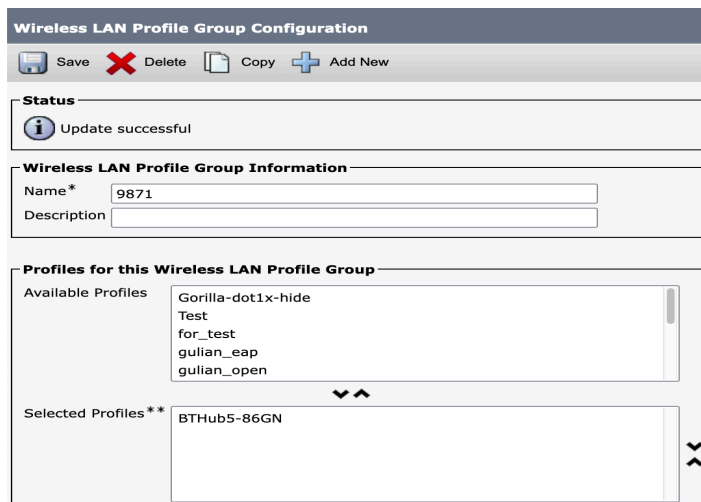
- The Cisco Desk Phone 9800 Series does not support the Network Access Profile option.
- Select **Save** once the Wireless LAN Profile configuration is complete.

Create a Wireless LAN Profile Group

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



3. Specify the Name, Description, and select the Wireless LAN Profile to add.



Note: Only one Wireless LAN Profile should be added to a Wireless LAN Profile Group.

4. Select **Save** once the Wireless LAN Profile Group configuration is complete.

Apply a Wireless LAN Profile Group to a Device Pool

Once the Wireless LAN Profile Group has been created, it can be applied to a Device Pool or an individual phone.

1. To apply a Wireless LAN Profile Group to a device pool, navigate to **System > Device Pool** in the Cisco Unified Communications Manager's Administration interface.
2. If you want to apply the WLAN profile to an existing device pool, do the following actions:
 - a. Find the device pool and open it.

- b. In the Roaming Sensitive Settings section, select your WLAN profile in the Wireless LAN Profile Group list.

Device Pool Settings	
Device Pool Name*	9871
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >
MRA Service Domain	< None >

Roaming Sensitive Settings	
Date/Time Group*	ntp_server
Region*	Default
Media Resource Group List	< None >
Location	< None >
Network Locale	< None >
SRST Reference*	Disable
Connection Monitor Duration***	
Single Button Barge*	Default
Join Across Lines*	Default
Physical Location	< None >
Device Mobility Group	< None >
Wireless LAN Profile Group	9871 View Details

- c. Select **Save**.
 - d. Select **Apply Config**.
3. If you want to apply the WLAN profile to a new device pool, do the following actions:
 - a. Select **Add New** to create a Device.
 - b. Specify the name and the required information.
 - c. In the Roaming Sensitive Settings section, select your WLAN profile in the Wireless LAN Profile Group list.
 - d. Select **Save**.
 - e. Select **Apply Config**.
 - f. Go to **Device > Phone**, and find your phone that you want to add to the device pool.
 - g. In the **Device Information** section, select the device pool that you created in the **Device Pool** drop-down list.

Device Information	
<input checked="" type="checkbox"/> Device is Active	
<input checked="" type="checkbox"/> Device is trusted	
MAC Address*	845A3EC211B6 (SEP845A3EC211B6)
Description	Auto 99899
Current On-Premise Onboarding Method is set to Autoregistration. Activation Code will only apply to onboarding via MRA.	
<input type="checkbox"/> Require Activation Code for Onboarding	
<input type="checkbox"/> Allow Activation Code via MRA	
Activation Code MRA Service Domain	-- Not Selected -- View Details
Device Pool*	9871 View Details
Common Device Configuration	< None > View Details
Phone Button Template*	DocTest ModelID 118 Lines Button Template Find
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile View Details

- h. Select **Save**.
- i. Select **Apply Config**.

Apply a Wireless LAN Profile Group to an Individual Phone

1. Navigate to **Device > Phone** in the Cisco Unified Communications Manager's Administration interface.
2. Find your phone and open the Phone Configuration page.
3. In the **Device Information** section, select your WLAN profile group in the **Wireless LAN Profile Group** drop-down list.
4. Select **Save**.
5. Select **Apply Config**.

Configure the Cisco Desk Phone 9800 Series

Automatic Provisioning

This method is currently available only for phones registered to Cisco Unified Communications Manager. For automatic provisioning of the Wi-Fi Profiles, the Cisco Desk Phone 9800 Series needs to be connected to a network via Ethernet or via Wi-Fi, which has connectivity to the Cisco Unified Communications Manager.

With connectivity to a Cisco Unified Communications Manager 10.0 or later, Wi-Fi profile configuration data can be downloaded and applied to the Cisco Desk Phone 9800 Series.

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

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

Certificates can also be automatically installed upon a network connection.

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

Config/Modify Wi-Fi Profile via Phone Web Portal

Ensure that your Cisco Desk Phone 9800 Series has got a valid IP address either by wired or wireless connection.

Note: The phone web portal is available only for phones registered to Webex Calling or Cisco BroadWorks.

1. Enter the IP address of the phone in your web browser address bar.
For example, <http://10.64.84.147/>
2. Click **Admin Login** and then click **advanced** to access the configurations as an administrator.
3. Go to **Voice > System**.
4. Set **Phone-wifi-on** to **Yes** to turn on Wi-Fi on the phone.
5. Specify the Wi-Fi network name and credentials for the phone to connect to the wireless access point.

The Security Mode can be any of the following depending on the settings on your access point.

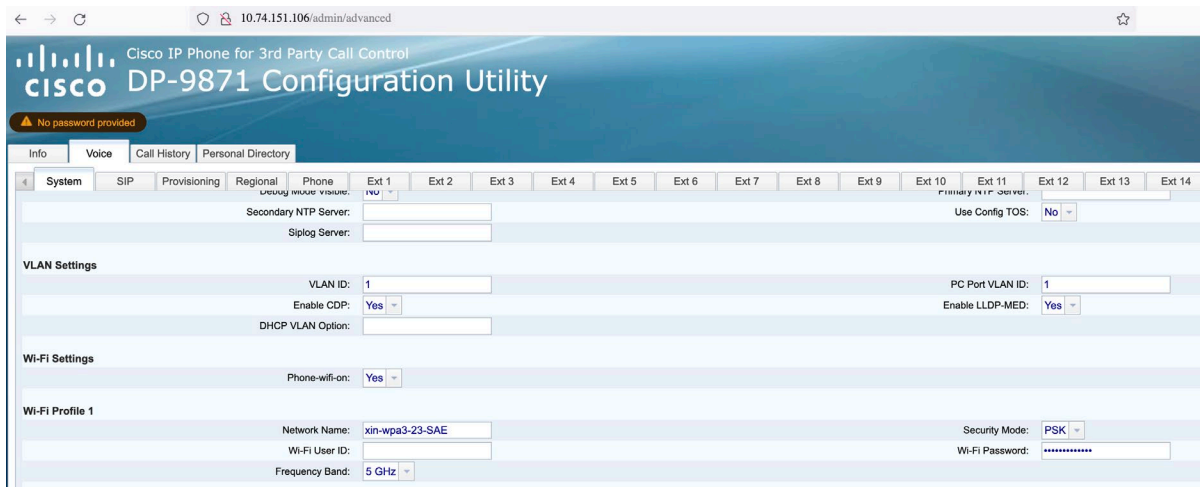
- If **Auto**, **EAP-FAST**, or **PEAP** is selected then **Wi-Fi User ID** and **Wi-Fi Password** are required.
- If **PSK** is selected to utilize Pre-Shared Key authentication, then a **PSK Password** must be entered.

The **PSK Password** must be 8-63 ASCII character string.

- If **WEP** is selected to utilize static WEP (Wired Equivalent Privacy) authentication, then a **WEP Key** must be entered.
- If **None** is selected, then no authentication is required and no encryption will be utilized.
- If **Auto** is selected, the phone could dynamically choose **EAP-FAST** or **EAP-PEAP** as authentication method based on communication with target AP.
- If **EAP-TLS** is selected, currently only **MIC** certificate is supported for phones registered to Webex Calling/ Webex DI/Broadworks.

Select the desired **Frequency Band**:

- **Auto:** Gives preference to 5 GHz channels, but operates on both 5 GHz and 2.4 GHz channels
- **2.4 GHz:** Operates on 2.4 GHz channels only
- **5 GHz:** Operates on 5 GHz channels only



6. Click **Submit All Changes**.


You can go to the **Info > Status** tab to view the network status.



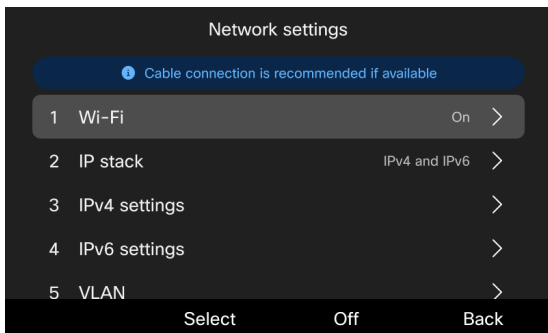
Notes:

- The phone reboots when switching from an access point to another..
- When the phone is connected via Ethernet connection, Wi-Fi is turned off. When the Ethernet cable is unplugged, the phone connects to the wireless network automatically if properly configured.
- The Wi-Fi settings are synchronized to the settings in the phone Settings menu.

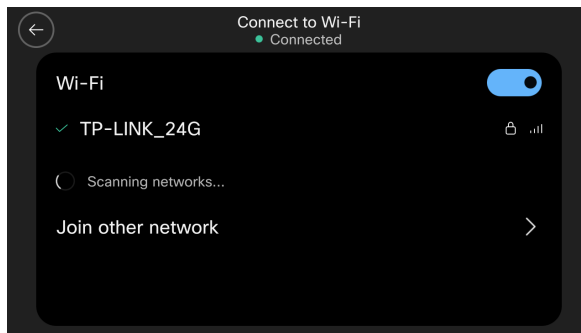
Configure Wi-Fi Settings on the Phone UI

1. Press Settings .
2. If prompted, enter the password to access the Settings menu.
3. Navigate to Network and service > Network settings.

- If Wi-Fi status is Off, turn on Wi-Fi. The phone starts scanning available wireless network.



9861

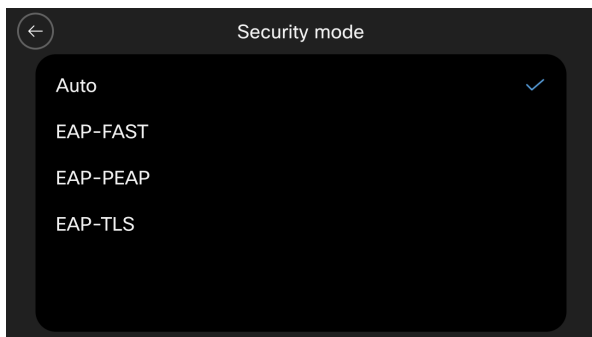


9871

- If you are using a 9861 phone, press **Select** to open the Connect to Wi-Fi screen. If you are on a 9871 phone, go to the next step.
- Select your access point from the available networks and enter your credentials if the network requires authentication.


The security mode and available frequency bands depends on the settings of the access point.

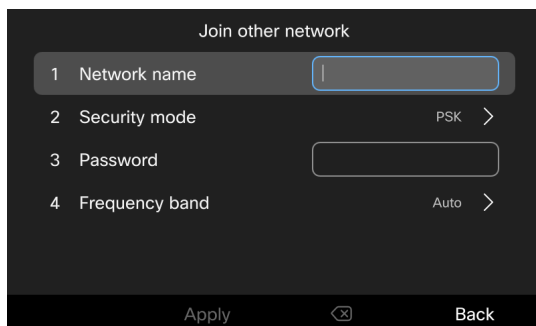
If the network is 802.1x-enabled, the phone will dynamically select Auto for the EAP type, which is determined by the RADIUS server configuration. You can select the inner authentication method.



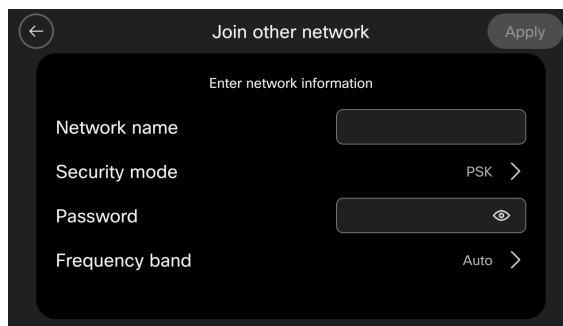
- Select **Apply**.

Join a Hidden Wireless Network

1. Press Settings .
2. If prompted, enter the password to access the Settings menu.
3. Navigate to **Network and service** > **Network settings**.
4. If Wi-Fi status is Off, turn on Wi-Fi.
5. Select **Wi-Fi** and then select **Join other network**.
6. Enter the network name, select the security mode, and enter the credentials.



9861



9871

Ensure that you select the proper security mode based on the settings of the access point.

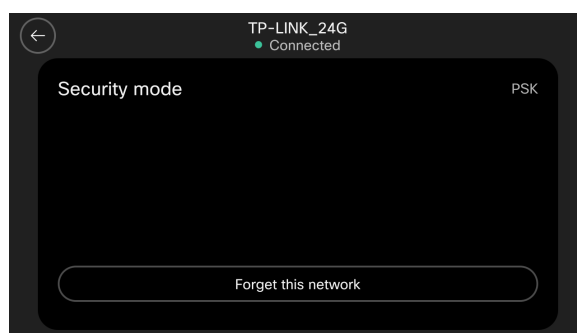
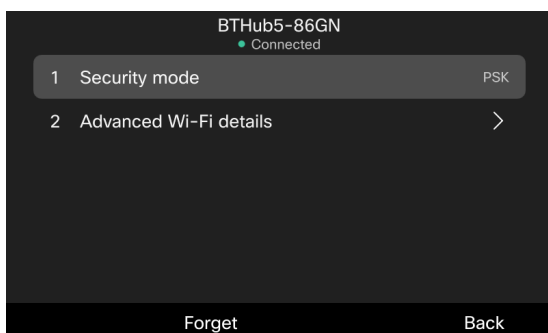
- **None:** Select this option if the wireless network to connect is an open network. No password is needed.
- **PSK:** If your network is secured with Pre-Shared Key or WPA3-SAE, select this option and enter the password. Pre-Shared Key length is 8~63 bytes.
- **Auto/EAP-FAST/EAP-PEAP:** When you select any of these options, user ID and password are required.
- **EAP-TLS:** When you select this option, the user certificate type is required. Currently, only Manufacturing installed certificate (MIC) is supported.
Note: Certificate Management and root CA install is currently available only with Webex Calling/DI/Broadwork.

7. Select **Apply**.

Delete a Connected Network

User can delete the currently connected AP in the Settings menu.

1. In the Network settings screen, select the access point that the phone is connected to.
2. Select **Forget** or **Forget this network** depending on your phone model.



Certificate Management

The Cisco Desk Phone 9800 Series can utilize X.509 digital certificates for EAP-TLS or to enable Server Validation. A User Certificate can be installed either automatically via Simple Certificate Enrollment Protocol (SCEP) or manually via the phone's admin webpage interface (https://<phone_IP_address>:8443).

Only one certificate per certificate type is allowed; 1 User Certificate and 1 Server Certificate (either via SCEP or manual method).

LSC certificate is installed by CUCM CAPF service.

Once a certificate is installed, Server Validation is automatically enabled if configured for EAP-TLS

Microsoft® Certificate Authority (CA) servers are recommended. Other CA server types may not be completely interoperable with the Cisco Desk Phone 9800 Series.

Both DER and Base-64 (PEM) encoding are acceptable for the client and server certificates.

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

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

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

Manual Installation

Ensure that the admin webpage interface is **Enabled**, the username is **admin**, and the **Admin password** is configured by CUCM.



Open manual install page via <https://x.x.x.x:8443>



You can utilize either the internal Manufacturing Installed Certificate (MIC), LSC or a custom User Installed certificate as the User Certificate for EAP-TLS.

Manufacturing Installed Certificate (MIC)

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

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

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



Type	Common name	Issuer name	Valid from	Valid to	
Manufacturing issued	CN=CP-9861-SEP845A3EC22785, O=Cisco, OU=TPM SUDI, serialNumber=PID:DP-9861 SN:FVH281623FV	CN=High Assurance SUDI CA, O=Cisco	05/07/2024 02:44:00	08/09/2099 20:58:26	
Manufacturing CA	CN=High Assurance SUDI CA, O=Cisco	O=Cisco, CN=Cisco Root CA 2099	08/11/2016 20:28:08	08/09/2099 20:58:27	Export
Manufacturing root CA	O=Cisco, CN=Cisco Root CA 2099	O=Cisco, CN=Cisco Root CA 2099	08/09/2016 20:58:28	08/09/2099 20:58:28	Export
User installed	<Not installed>	<Not installed>			Install
Authentication server CA	<Not installed>	<Not installed>			Install

This root CA should be added to Radius server's trust list.

User Installed Certificate

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

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

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

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



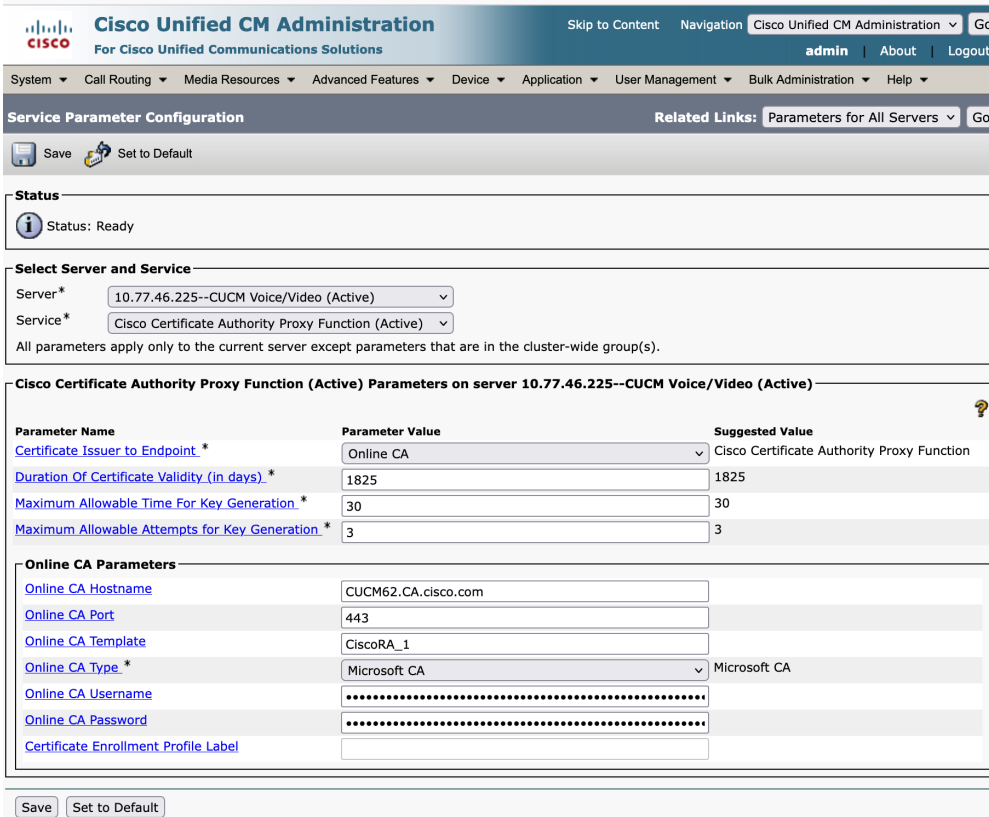
Will need to restart the Cisco Desk Phone 9800 Series after all certificates are installed.



LSC Certificate

Enable CAPF service on CUCM.

1. Login to **Cisco Unified CM Administration**.
2. Enter **System -> Service Parameters**.
3. Select your CUCM server.
4. Select **Cisco Certificate Authority Proxy Function**.
5. Select certificate issuer in **Certificate Issuer to Endpoint**.
6. If **Online CA** is selected, you should configure the external CA in **Online CA Parameters**.
7. If **Cisco Certificate Authority Proxy Function** is selected, the **build-in** CAPF function is used.
8. Click **Save** button.



Service Parameter Configuration

Status: Ready

Select Server and Service

Server*: 10.79.57.147--CUCM Voice/Video (Active)

Service*: Cisco Certificate Authority Proxy Function (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Cisco Certificate Authority Proxy Function (Active) Parameters on server 10.79.57.147--CUCM Voice/Video (Active)

Parameter Name	Parameter Value	Suggested Value
Certificate Issuer to Endpoint *	Cisco Certificate Authority Proxy Function	Cisco Certificate Authority Proxy Function
Duration Of Certificate Validity (in days) *	1825	1825
Maximum Allowable Time For Key Generation *	30	30
Maximum Allowable Attempts for Key Generation *	3	3

Online CA Parameters

Online CA Hostname:

Online CA Port:

Online CA Template: comadministrator

Online CA Type: Microsoft CA

Online CA Username:

Online CA Password:

Certificate Enrollment Profile Label:

Active or restart CAPF server

1. Login **Cisco Unified Serviceability**.
2. Enter **Tools -> Service Activation**.
3. Select your CUCM server.
4. Ensure that **Cisco Certificate Authority Proxy Function** is Activated.
5. Enter Tools -> Control center Feature Service.
6. Choose and restart **Cisco Certificate Authority Proxy Function**.

Install LSC certificate to Cisco Desk Phone 9800 Series

1. Login to **Cisco Unified CM Administration**.
2. Enter **Device -> Phone**, then enter the profile page of your device.
3. Select **Install/Upgrade** in **Certificate Operation**, then **Save** and **Apply**.
4. The phone will install the LSC and reboot.

- Certification Authority Proxy Function (CAPF) Information

Certificate Operation*: Install/Upgrade

Authentication Mode*: By Existing Certificate (precedence to LSC)

Authentication String:

Generate String:

Key Order*: RSA Only

RSA Key Size (Bits)*: 2048

EC Key Size (Bits):

Operation Completes By: 2024 06 29 12 (YYYY:MM:DD:HH)

Certificate Operation Status: Operation Pending

Note: Security Profile Contains Addition CAPF Settings.

Check Phone LSC status via **Settings > Network and services > Security settings**

Security settings

1 Security mode Non secure

2 LSC Installed >

3 Trust list >

4 802.1X Authentication >

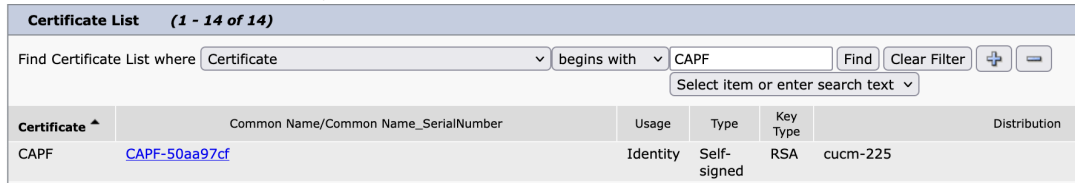
Select Back

Import CAPF CA to ISE.

Export LSC CA cert from CUCM.

If **Online** CAPF is used, user should ask external CA cert from admin. If **build-in** CAPF is used, user can download CA cert from CUCM.

1. Login to **Cisco Unified OS Administration**
2. Enter **Security -> Certificate Management**
3. Download the CAPF Identity certificate



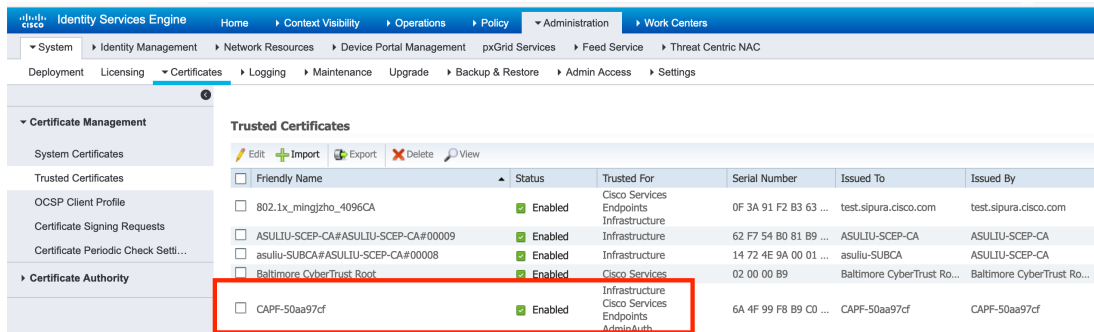
Certificate List (1 - 14 of 14)

Find Certificate List where Certificate begins with CAPF Find Clear Filter

Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution
CAPF	CAPF-50aa97cf	Identity	Self-signed	RSA	cucm-225

Import LSC certificate to trust list.

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



Trusted Certificates

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
802.1x_mingzho_4096CA	Enabled	Cisco Services Endpoints Infrastructure	0F 3A 91 F2 B3 63 ...	test.sapura.cisco.com	test.sapura.cisco.com
ASULIU-SCEP-CA#ASULIU-SCEP-CA#00009	Enabled	Infrastructure	62 F7 54 B0 81 B9 ...	ASULIU-SCEP-CA	ASULIU-SCEP-CA
asuliu-SUBCA#ASULIU-SCEP-CA#00008	Enabled	Infrastructure	14 72 4E 9A 00 01 ...	asuliu-SUBCA	ASULIU-SCEP-CA
Baltimore CyberTrust_Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...
CAPF-50aa97cf	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	6A 4F 99 F8 B9 CD ...	CAPF-50aa97cf	CAPF-50aa97cf

Server Certificate

The root CA certificate that issued the RADIUS server's certificate must be installed for **EAP-TLS** or to enable Server Validation. Service Validation is optional. If user doesn't want it, this step could be dropped.

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



Certificates Cisco IP Phone DP-9861 (SEP845A3EC22785)

Select file (.cer) to upload: Browse... No file selected.

Upload

Will need to restart the Cisco Desk Phone 9800 Series after all certificates are installed.



Certificates Cisco IP Phone DP-9861 (SEP845A3EC21655)

Authentication Server CA certificate has been updated.

Phone will use the new certificate after reboot. You can restart the phone with: **"System/Restart"**

Certificate Removal

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

Cisco		Certificates				Signed in as admin, Sign out	
		Cisco IP Phone DP-9861 (SEP845A3EC21655)					
Device information	Type	Common name	Issuer name	Valid from	Valid to		
Network setup	Manufacturing issued	CN=CP-9861-SEP845A3EC21655, O=Cisco, OU=TPM SUDI, serialNumber=PID:DP-9861 SN:FVH280322J6	CN=High Assurance SUDI CA, O=Cisco	01/29/2024 05:06:35	08/09/2099 20:58:26		
Setup	Manufacturing CA	CN=High Assurance SUDI CA, O=Cisco	O=Cisco, CN=Cisco Root CA 2099	08/11/2016 20:28:08	08/09/2099 20:58:27	Export	
Certificates	Manufacturing root CA	O=Cisco, CN=Cisco Root CA 2099	O=Cisco, CN=Cisco Root CA 2099	08/09/2016 20:58:28	08/09/2099 20:58:28	Export	
Network statistics	User installed	<Not installed>	<Not installed>			Install	
Ethernet information	Authentication server CA	DC=yan, DC=com, CN=yan-YANY2-CRDC-COM-CA	DC=yan, DC=com, CN=yan-YANY2-CRDC-COM-CA	01/27/2021 09:00:25	01/27/2026 09:10:25	Delete	

LSC certificate could be removed on CUCM phone page, then **Save and Apply**.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Order*

RSA Key Size (Bits)*

EC Key Size (Bits)

Operation Completes By (YYYY:MM:DD:HH)

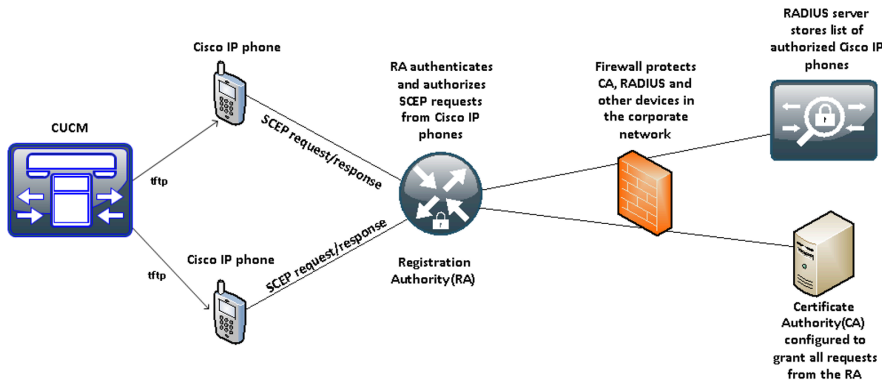
Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

Simple Certificate Enrollment Protocol (SCEP)

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

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



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

For initial certificate enrollment via SCEP, the Cisco Desk Phone 9800 Series needs to be connected to an Ethernet network which has connectivity to the Cisco Unified Communications Manager.

The Cisco Desk Phone 9800 Series utilizes the following parameters defined in Cisco Unified Communications Manager for SCEP requests.

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

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

Removing these parameters will disable SCEP.

WLAN SCEP Server	10.195.19.65	<input checked="" type="checkbox"/>
WLAN Root CA Fingerprint (SHA256 or SHA1)	81512B4316429092925C6891701B374EBD254447	<input checked="" type="checkbox"/>

The Cisco Desk Phone 9800 Series then sends a SCEP enroll request to the SCEP RA including the phone's Manufacturing Installed Certificate (MIC) as the Proof of Identity (POI).

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

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

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

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

The Cisco Desk Phone 9800 Series will periodically check the user and server certificate expiration periods.

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

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

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

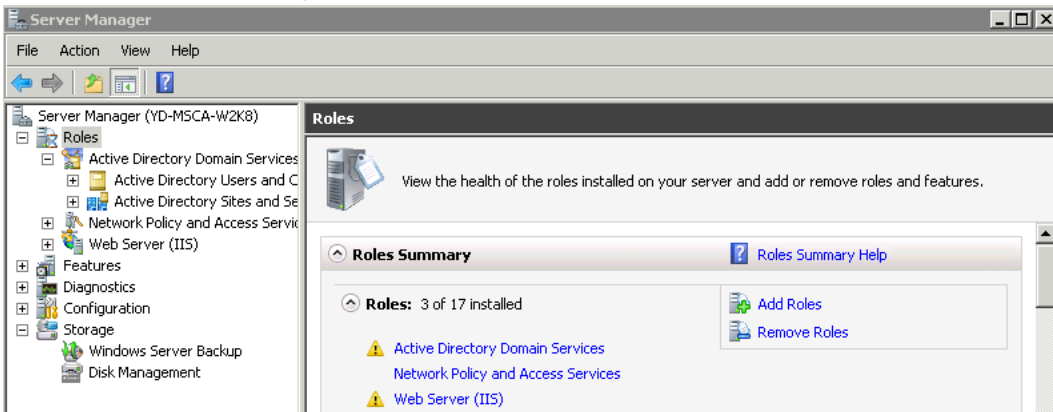
If the **WLAN SCEP Server** or **WLAN Root CA Fingerprint (SHA256 or SHA1)** has been modified, then the Cisco Desk Phone 9800 Series will attempt to update the CA and user certs immediately.

Certificate Authority (CA) Configuration

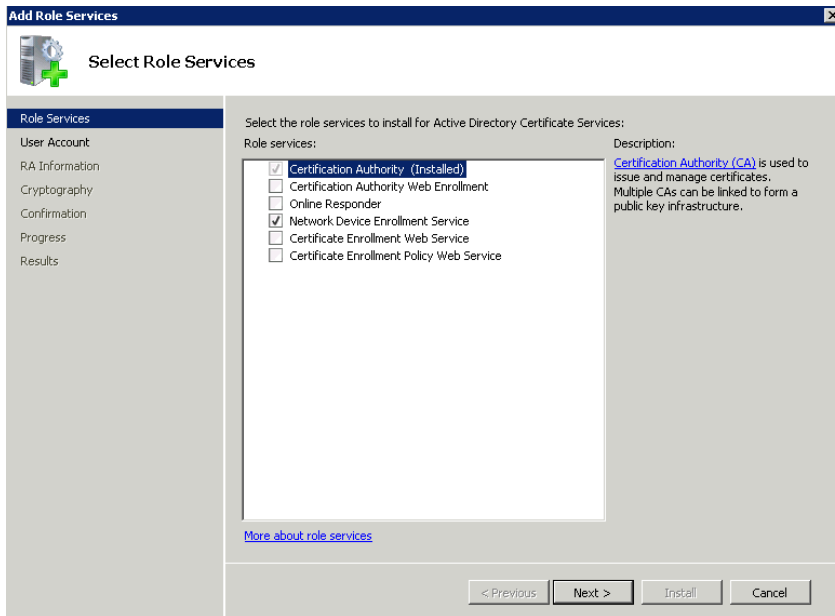
It's recommended to use Microsoft® Certificate Authority (CA) servers.

Use the following guidelines to configure the Microsoft CA.

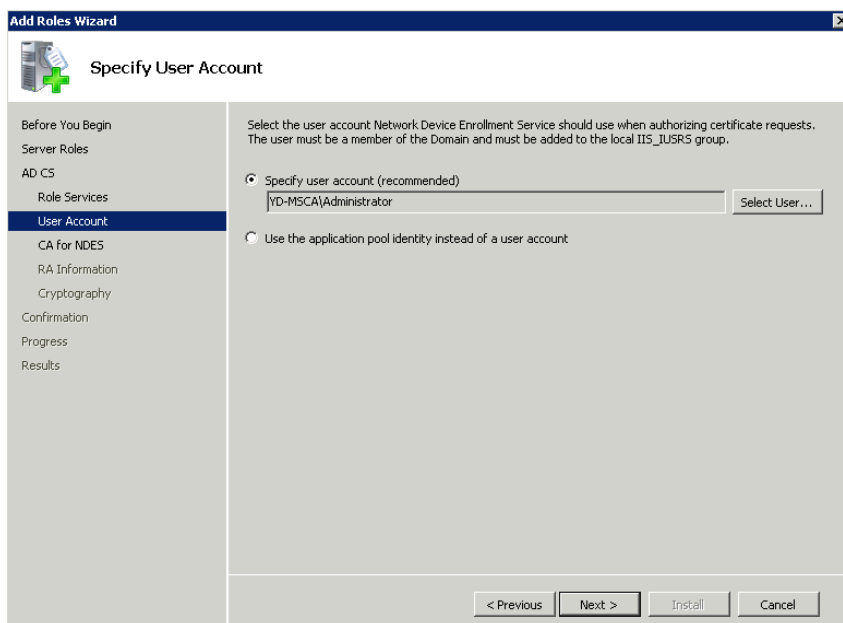
1. Create Certificate Authority and Active Directory Domain Service on Microsoft Windows server.
2. Enable Network Device Enrollment Service.
3. Make **Administrator** a member of **IIS_IUSERS** group by going to **MemberOf** tab of user property screen.
4. Launch **Server Manager**, then click **Add roles**.



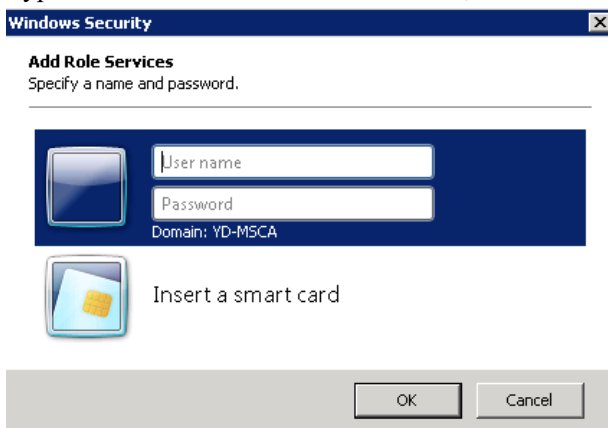
5. On the **Select Server Role** page, select the **Active Directory Certificate Services** role, then click **Next**. The default service selected is the **Certification Authority**, clear the check box, and then go to
6. Add the **Network Device Enrollment Service** role service.
7. In the **Add Roles Wizard**, on the **Select Role Services** page, select the **Network Device Enrollment Service** check box, then click **Next**.



8. The wizard will detect whether all the required dependencies are installed. If any dependencies are missing, you will be prompted with a dialog box explaining what is missing and requesting your permission to install the dependencies. Click **Yes** to continue the installation.
9. Click **User Account** under **Role Services** and then click **Select User...**



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



11. Enter the Registration Authority information.

The screenshot shows the 'Specify Registration Authority Information' step in the 'Add Role Services' wizard. The left sidebar lists 'RA Information' as the current step. The main area contains a text box for 'RA Name' with the value 'YD-MSCA-W2K8-MSCEP-RA' and a dropdown for 'Country/Region' set to 'US (United States)'. Below these are input fields for 'E-mail', 'Company', 'Department', 'City', and 'State/Province'. At the bottom are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

12. Select **Microsoft Strong Cryptographic Provider** for **Signature Key CSP** and **Encryption key CSP**.

13. Select **2048** for **Key character length**.

The screenshot shows the 'Configure Cryptography for Registration Authority' step. The left sidebar highlights 'Cryptography'. The main area has two sections: 'Signature key' and 'Encryption key'. Each section has a dropdown for 'CSP' (both set to 'Microsoft Strong Cryptographic Provider') and a dropdown for 'Key character length' (both set to '2048'). A link for 'More about signature and encryption keys' is at the bottom. Buttons for '< Previous', 'Next >', 'Install', and 'Cancel' are at the bottom.

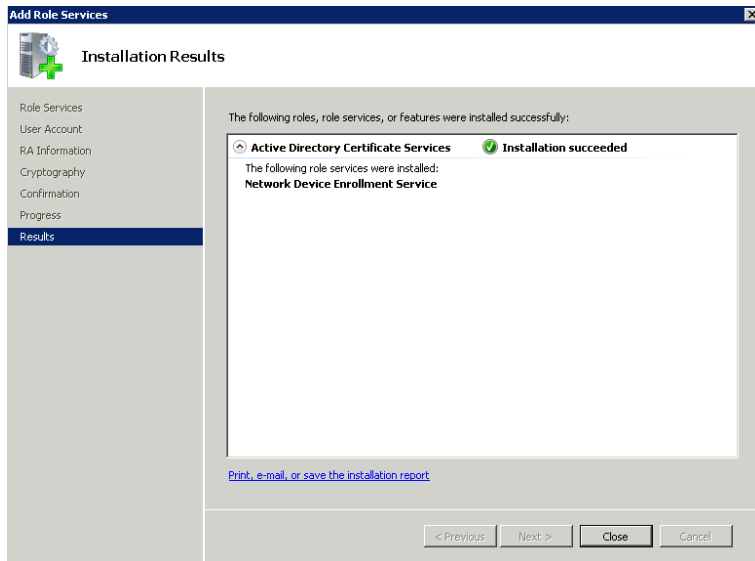
14. Select **Install**.

The screenshot shows the 'Confirm Installation Selections' step. The left sidebar highlights 'Confirmation'. The main area displays a summary of the installation configuration. A message states: 'To install the following roles, role services, or features, click Install. 1 informational message below. This server might need to be restarted after the installation completes.' The configuration details are as follows:

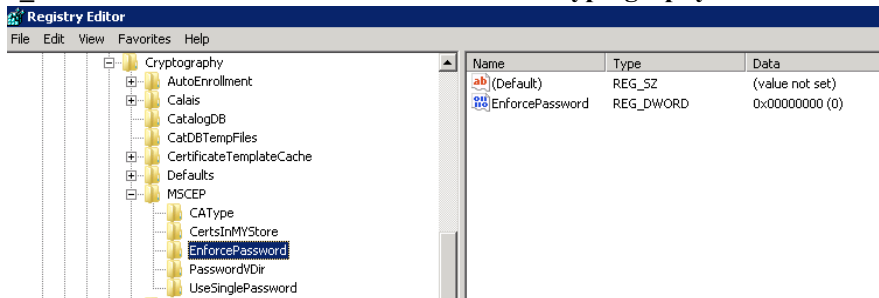
Active Directory Certificate Services	
Network Device Enrollment Service	
Account :	YD-MSCA\Administrator
RA Information:	
Name :	YD-MSCA-W2K8-MSCEP-RA
Country :	US
Email :	<None>
Company :	<None>
Department :	<None>
City :	<None>
State :	<None>
Signature Key CSP :	Microsoft Strong Cryptographic Provider
Signature Key Length :	2048
Exchange Key CSP :	Microsoft Strong Cryptographic Provider
Exchange Key Length :	2048
Challenge Phrase URL :	http://YD-MSCA-W2K8/certsrv/mscep_admin/

Buttons for '< Previous', 'Next >', 'Install', and 'Cancel' are at the bottom.

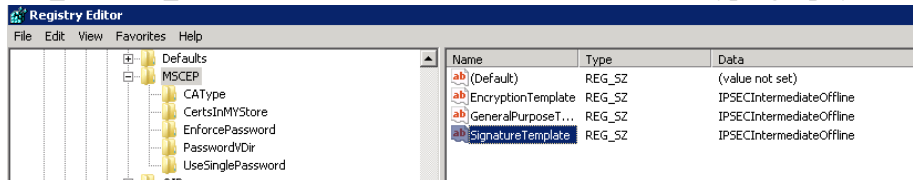
A confirmation page will be displayed if the installation was successful.



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



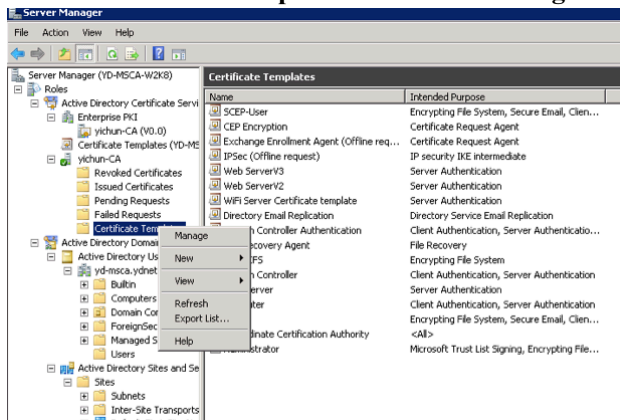
16. Specify certificate templates for SCEP
 SCEP uses the certificate template that is set in the registry for issuing certificates.
(HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP)



Typically the RA will have a longer period (same as that of the CA certificate). The default template used for RA to be enrolled to the SCP server is **IPSECIntermediateOffline** as highlighted above. So make sure a correct template is set to the above registries before enrolling Cisco RA to the SCEP server.

After the Cisco RA is enrolled to the SCEP server, admin needs to change the template in the registry (if the user certificate period needs to be shorter than that of the root CA).

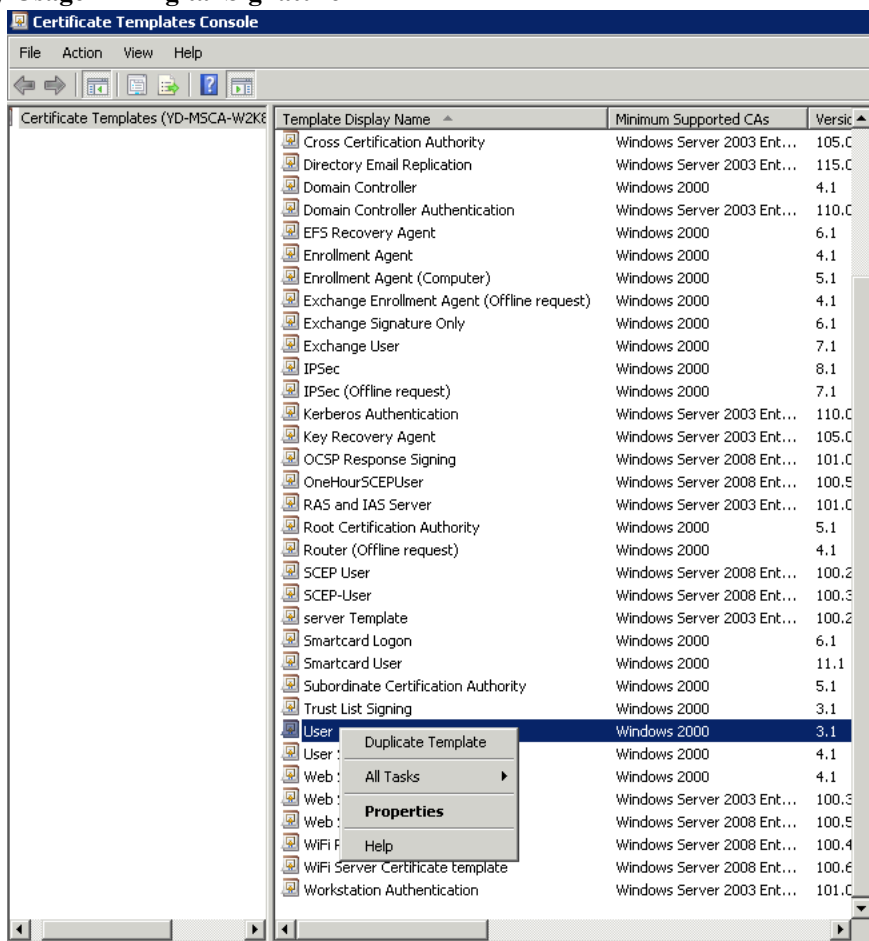
17. Right click **Certificate Templates** then select **Manage**.



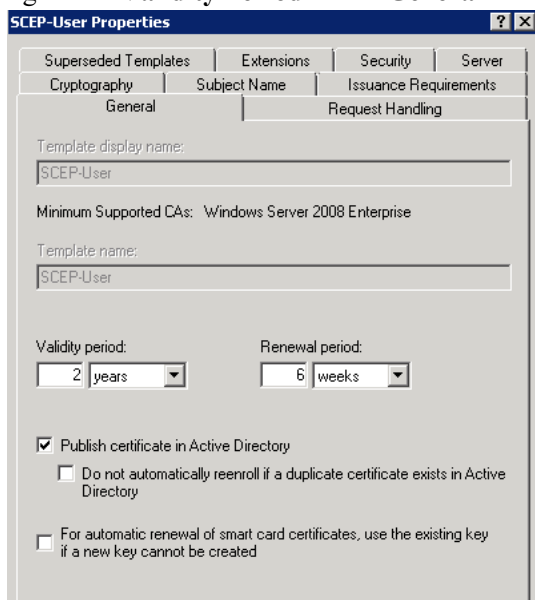
18. Right click **User** template then select **Duplicate Template**.
19. Select **Windows Server 2003 2008 Template**.
20. Under the **General** tab, change template name and validity period.
21. Under the **Extensions** tab, ensure the following:

Client Authentication is set as one of the application policies

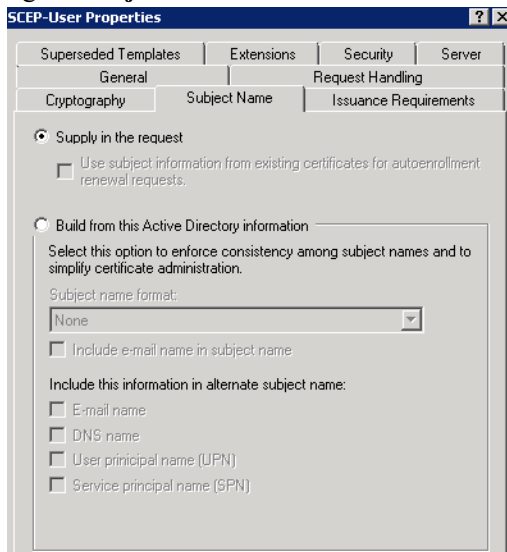
Key Usage has **Digital Signature** attribute



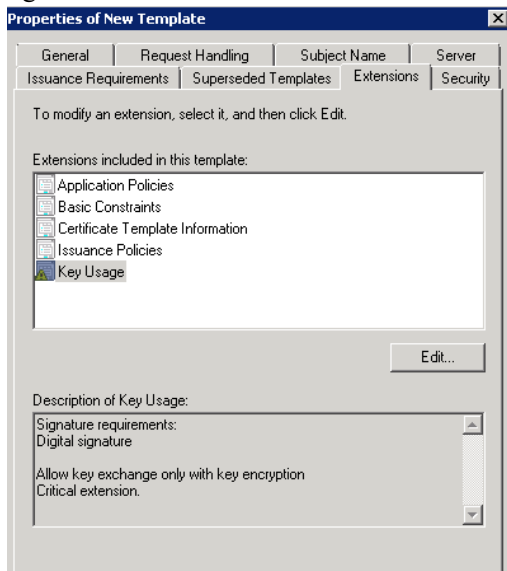
22. Configure the **Validity Period** on the **General** tab as necessary.



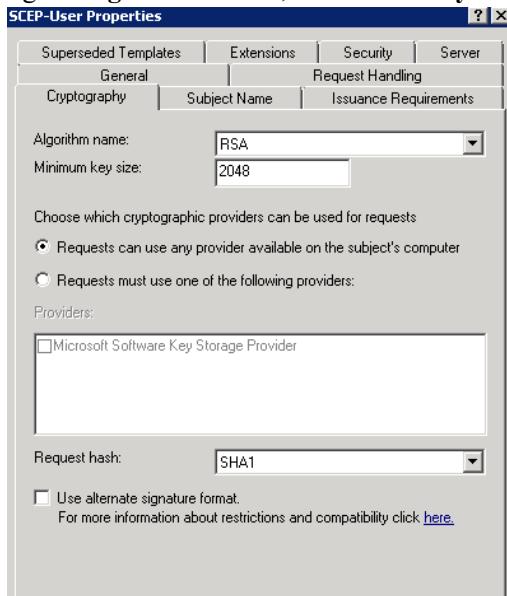
23. Configure **Subject Name** tab as shown below.



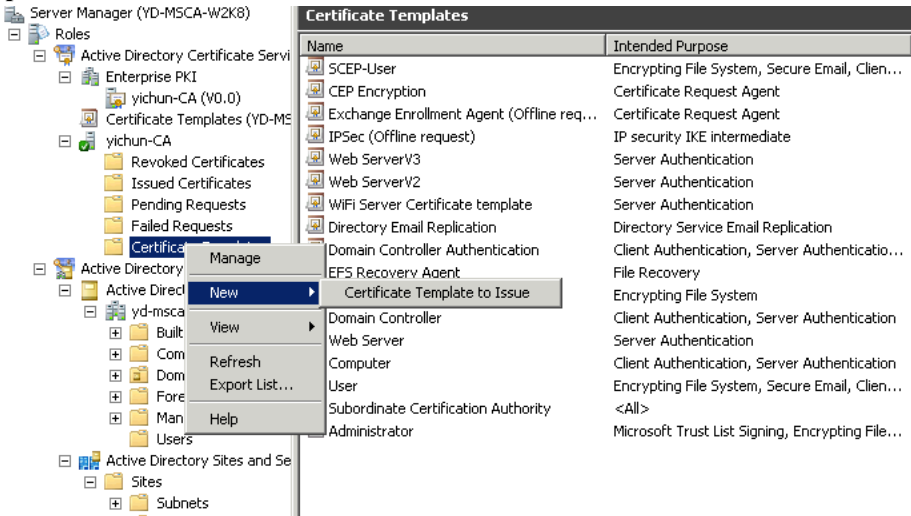
24. Configure **Extensions** tab as shown below.



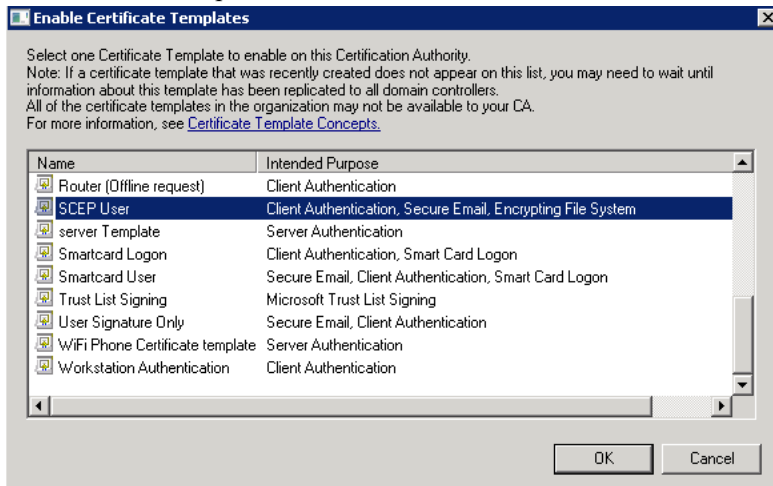
25. Configure **Algorithm Name**, **Minimum Key Size**, and **Request Hash** as necessary on the **Cryptography** tab.



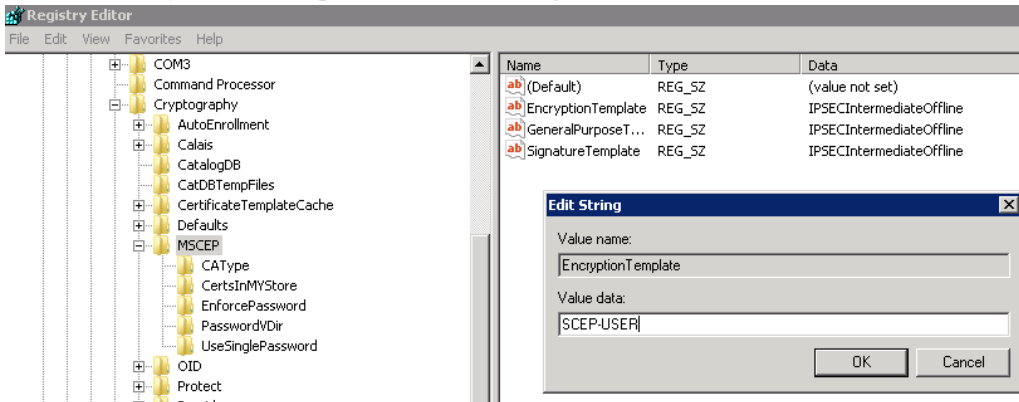
26. Enable the newly created template by right clicking **Certificate Templates** then selecting **New > Certificate Template to Issue**.



27. Select **SCEP User** template.



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

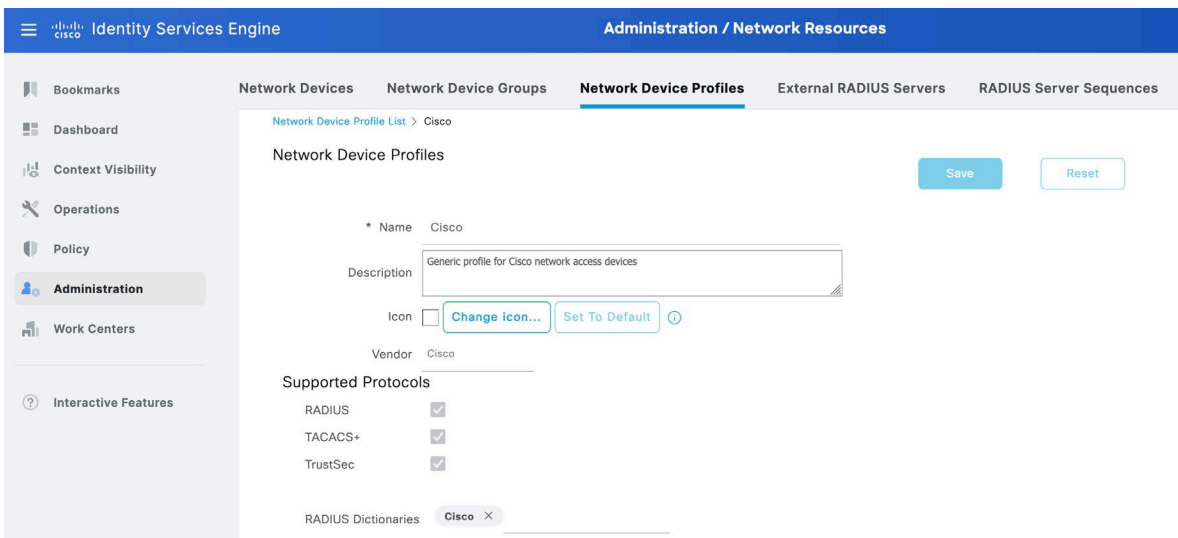
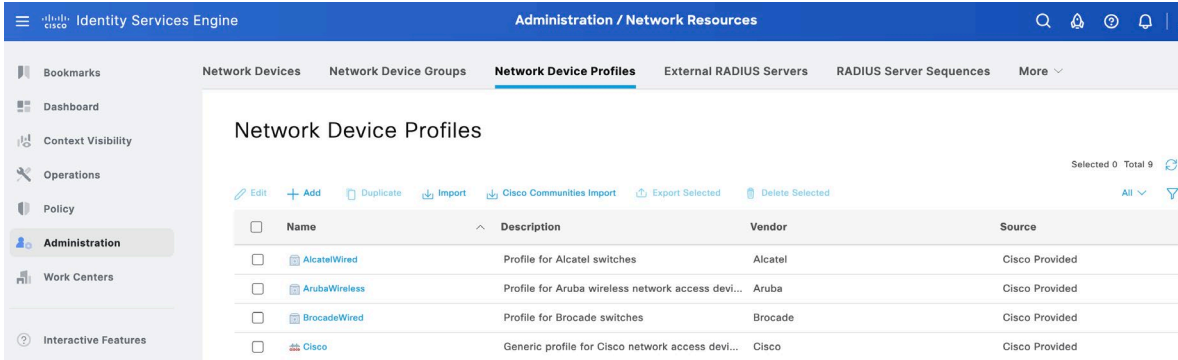


29. Go to **IIS > Application Pools** to restart the SCEP service for the new template to take effect.

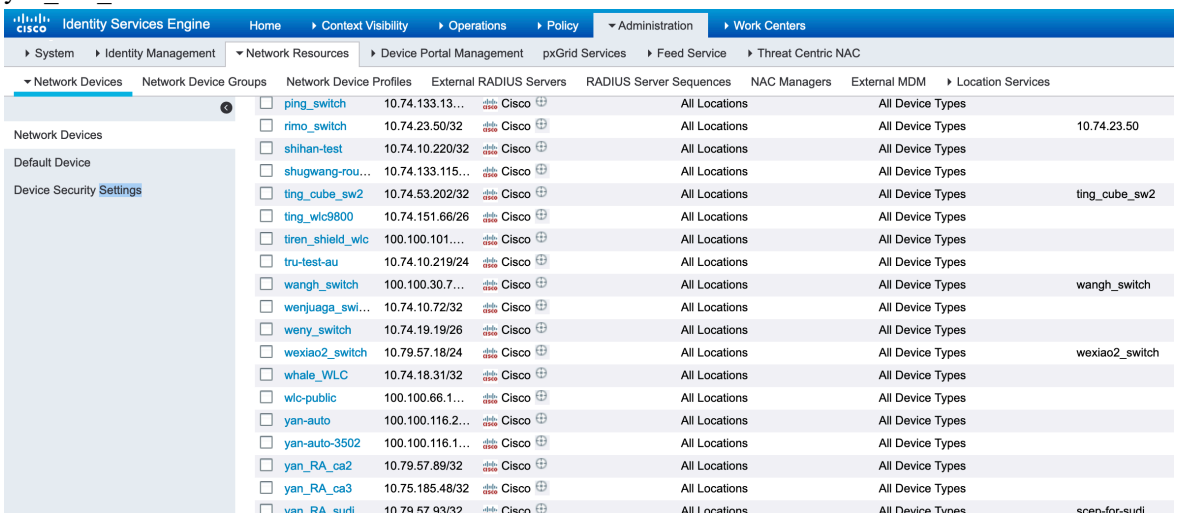
RADIUS Configuration

Use the following guidelines to configure the RADIUS server. ISE server plays a role of SCEP device authentication for enrollment, and it can be used for the PKI integration with Cisco IOS RA for SCEP solution.

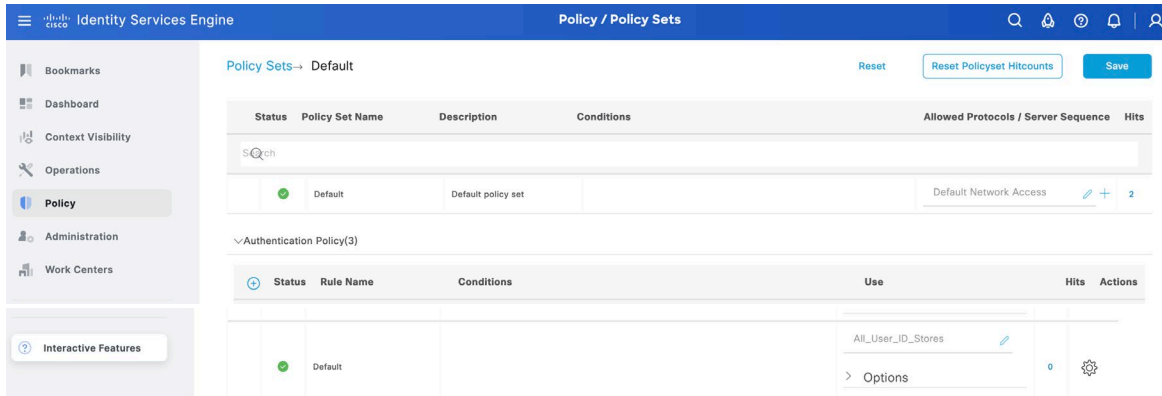
1. Navigate to **Administration > Network Device Profiles**, add a new profile or leveraging existing profile **Cisco**. If create a new profile, remember to configure **Supported Protocols, Authentication/Authorization** and **Permission** properly.



2. Navigate to **Administration > Network Resources > Network Devices** and add a device for Cisco IOS RA like **yan_RA_sudi** as shown bellow

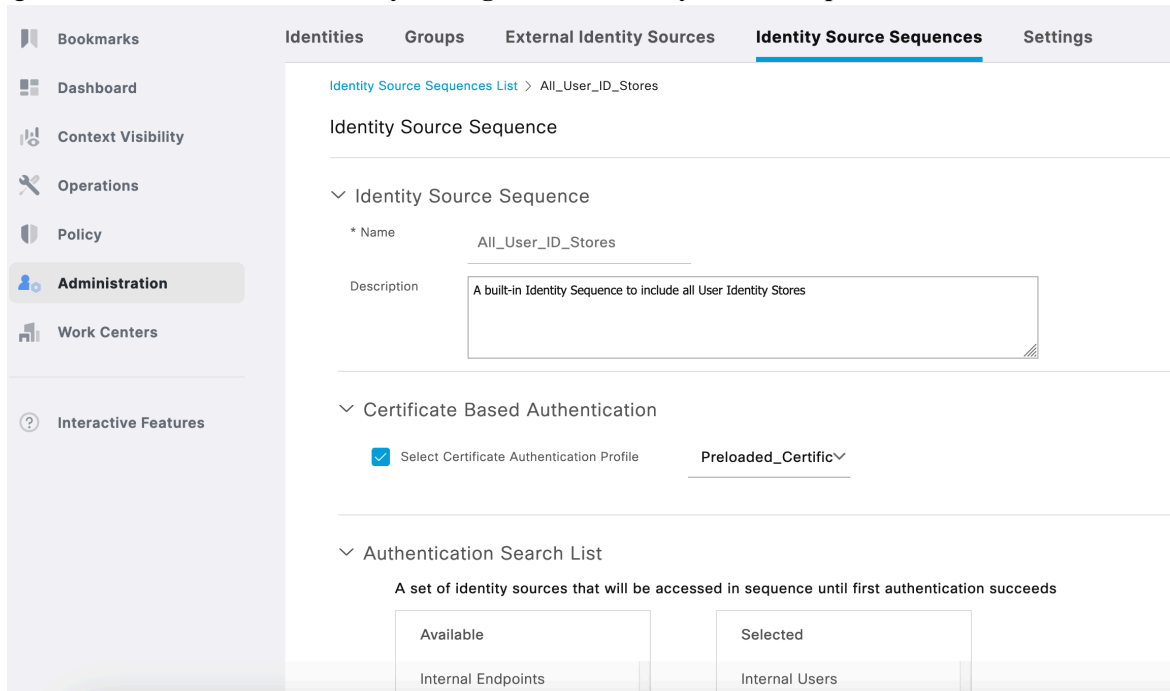


3. Navigate to **Policy > Authentication**, set a **Default** rule to use **Default Network Access** and use **All_Usr_ID_Stores**.



The authentication options can be set to continue for “If authentication failed” or “If user not found” since certificate based authentication has already been done in Cisco IOS RA.

4. Navigate to **Administration > Identity Management > Identity Source Sequence**.



5. Under **Policy > Policy Elements > Results > Authentication > Allowed Protocols**, edit **Default Network Access** as shown below

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

- Process Host Lookup

Authentication Protocols

- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1
- Allow MS-CHAPv2
- Allow EAP-MD5
- Allow EAP-TLS

- Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- Enable Stateless Session Resume

Session ticket time to live: 2 Hours

6. Under **Policy > Policy Elements > Results > Authorization > Authorization Profiles**, add a profile for SCEP (e.g. Phone_SCEP_profile)

Policy Sets Profiling Posture Client Provisioning Policy Elements

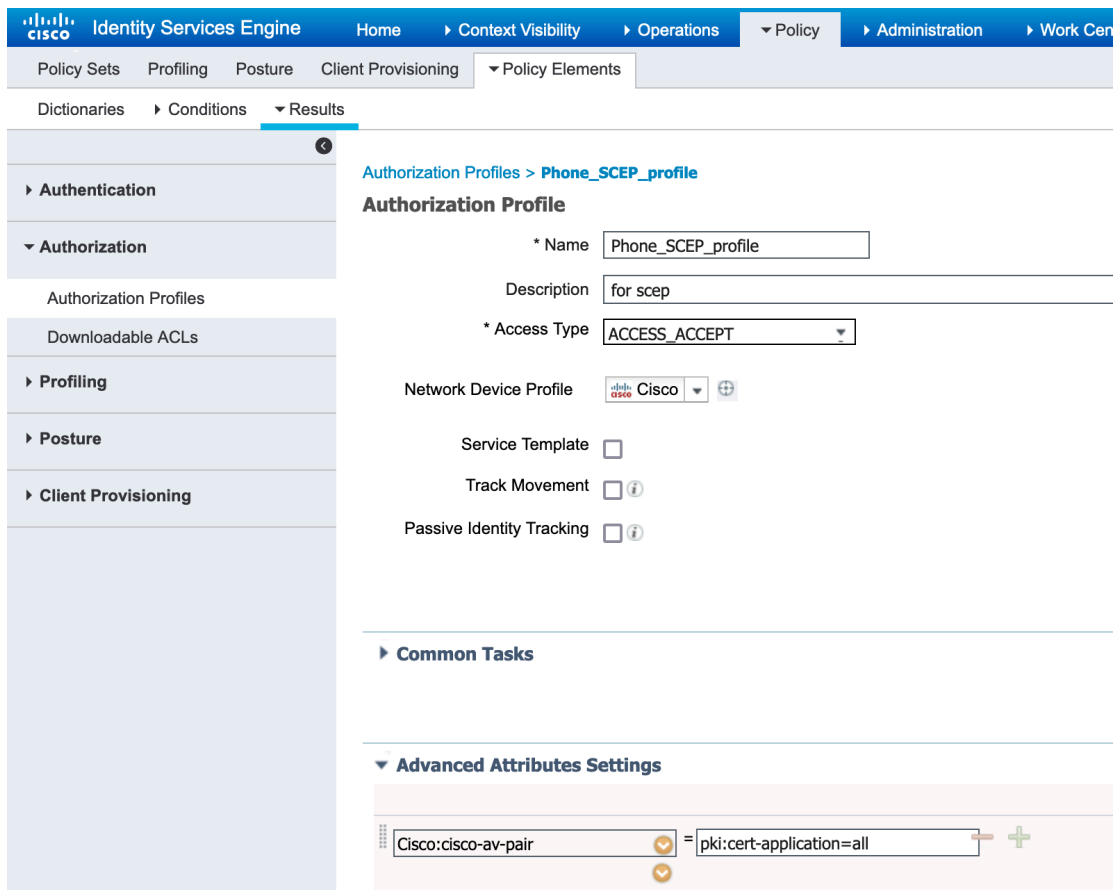
Dictionary Conditions Results

Standard Authorization Profiles

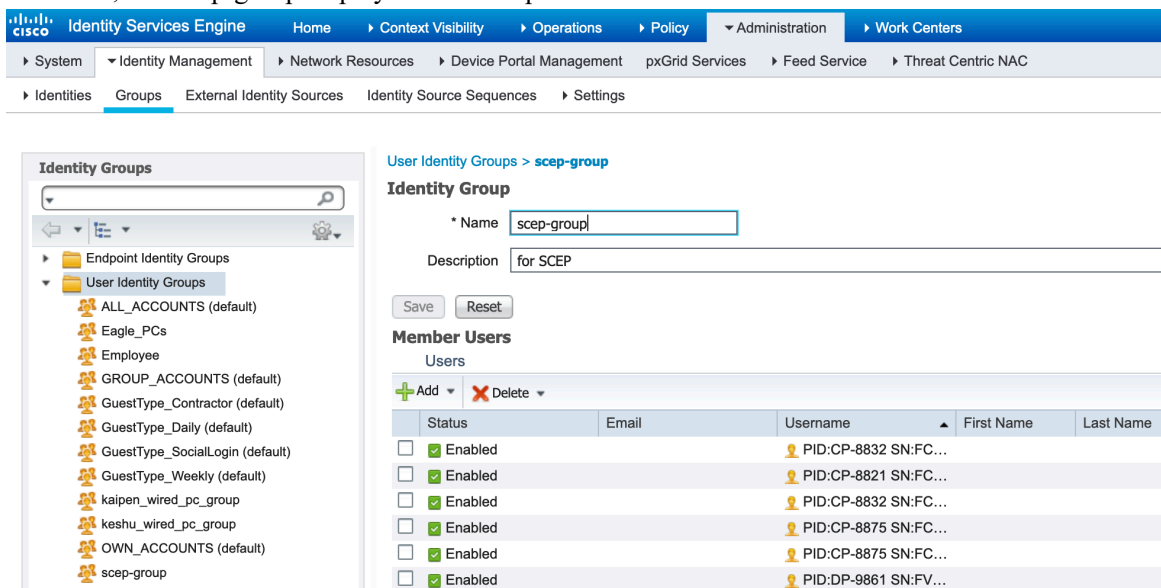
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit Add Duplicate Delete

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices.
<input type="checkbox"/> Cl_bbb_voice_vlan	Cisco	Cl_bbb_voice_vlan
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CW
<input type="checkbox"/> Eagle_PC_VLAN	Cisco	Access PC VLAN 165 of Eagle Team
<input type="checkbox"/> Eagle_Wired_Phone_VVLAN	Cisco	Access VVLAN 604 of Eagle Team
<input type="checkbox"/> FT_pc_vlan_96	Cisco	access vlan 96 for phonenix register
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplicant Prov
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input checked="" type="checkbox"/> Phone_SCEP_profile	Cisco	for scep



7. Navigate to **Administration > Identity Management > Groups > User Identity Groups** and add a user group for SCEP, like scep-group displayed in below picture.



8. Navigate to **Policy > Authorization Policy** and add a SCEP authorization policy by clicking the down arrow beside Edit of an existing policy and selecting **Insert new rule above**.

The screenshot shows the Cisco ISE Policy Sets configuration interface. The 'Authorization Policy' section is expanded to show 'SCEP_Access' with a status of 'Enabled' and a rule name of 'yan_scep'. Below this is the 'Conditions Studio' editor, where a condition is being configured: 'IdentityGroup-Name' is set to 'Equals' and 'User Identity Groups:scep-group'.

- Navigate to **Administration > Identities > Users** and create user accounts for Cisco Desk Phone 9800 Series. The user name has the format of **serialNumber** (e.g. PID:DP-9861 SN:FCH27472020).

The screenshot shows the Cisco ISE Administration > Identities > Users page. The 'Network Access Users' table is visible, showing a list of users with columns for Status, Name, Description, First Name, Last Name, Email Address, and User Identity Group. The users listed include various Cisco Desk Phone 9800 Series models, all with a status of 'Enabled' and assigned to the 'scep-group'.

Status	Name	Description	First Name	Last Name	Email Address	User Identity Group
Enabled	PID:CP-8875 SN:FCH26173BXL					scep-group
Enabled	PID:CP-8875 SN:FCH262831MF					scep-group
Enabled	PID:CP-8875 SN:FCH263038NM					scep-group
Enabled	PID:CP-8875 SN:FCH263038UY					scep-group
Enabled	PID:CP-8875 SN:FCH263332VH	cisco				scep-group
Enabled	PID:CP-8875 SN:FCH26452024					scep-group
Enabled	PID:CP-8875 SN:FCH264520NS					scep-group
Enabled	PID:CP-8875 SN:FCH264520NT	cisco				scep-group
Enabled	PID:DP-9861 SN:FCH27472020	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH280322J6	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623FQ	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623FV	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623U3	cisco				scep-group
Enabled	PID:DP-9861 SN:FVH281623YE	cisco				scep-group
Enabled	PID:DP-9871 SN:FCH2738200Y	cisco				scep-group
Enabled	PID:DP-9871 SN:FCH2746202B	cisco				scep-group
Enabled	PID:DP-9871 SN:FCH27462048	cisco				scep-group
Enabled	PID:DP-9871 SN:FVH28080FNY	cisco				scep-group

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Identities > Groups > External Identity Sources > Identity Source Sequences > Settings > Users.

The main content area is titled "Network Access Users List > PID:DP-9871 SN:FCH2738200Y". It contains the following configuration sections:

- Network Access User:**
 - Name: PID:DP-9871 SN:FCH2738200Y
 - Status: Enabled
 - Email:
- Passwords:**
 - Password Type: Internal Users
 - Login Password: (with "Generate Password" button)
 - Enable Password: (with "Generate Password" button)
- User Information:**
 - First Name:
 - Last Name:
- Account Options:**
 - Description: cisco
 - Change password on next login:

SCEP RA Configuration

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

- Enable HTTP server on the Cisco IOS router.


```
ISR_RA# configure terminal
ISR_RA(config)# ip http server
ISR_RA(config)# exit
```
- Configure a RADIUS server for device authentication.


```
ISR_RA# configure terminal
ISR_RA(config)# radius server MyRadius
ISR_RA(config-radius-server)# address ipv4 10.195.19.63 auth-port 1812 acct-port 1813
ISR_RA(config-radius-server)# key <REMOVED>
ISR_RA(config-radius-server)# exit
ISR_RA(config)# aaa authorization network PhoneList group radius
ISR_RA(config)# exit
```
- Configure a PKI trustpoint for the MIC's CA chain to validate the phone's MIC.


```
ISR_RA# configure terminal
ISR_RA(config)# crypto pki trustpoint MIC_trustpoint
ISR_RA(ca-trustpoint)# authorization list PhoneList
ISR_RA(ca-trustpoint)# authorization username subjectname commonname
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# crypto pki trustpoint MIC_trustpoint
ISR_RA(ca-trustpoint)# enrollment terminal
ISR_RA(ca-trustpoint)# revocation-check none
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# crypto pki authenticate MIC_trustpoint
Enter the base 64 encoded Manufacturing CA certificate. End with a blank line or the word quit on a line by itself.
-----BEGIN CERTIFICATE-----
```

MIIEZTCCA02gAwIBAgIBAjANBgkqhkiG9w0BAQsFADArMQ4wDAYDVQQKEwVDaXNj

```

bzEZMBcGAIUEAxMQQ2lzY28gUm9vdCBDQSBNMjAeFw0xMjExMTIxMzUwNThaFw0z
NzExMTIxMzAwMTdaMDYxDjAMBgNVBAoTBUNpc2NvMSQwIgwYDlVQQDEExtDaXNjbyBN
YW5lZmFjdHVyaW5nIENBIFNIQTlwgEiMA0GCSqSgSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQD0NktCAjJn3kk98hU7wUVp6QIOFrItEce6CpbfYpeLdUeZduAo+S0otzT
LJwS2BlMhZtacu9vUpfmW9w7nQo9zVT3eyPuhF/6/9TEdVBn75zb5CfV+E6ld+fH
nuPiFyBu+HDDJRd373Op+957IdoWyPvD8hHR1HJGFJ3JJKBg0UScL4JCwleu98Xq
/yPLAqBhExa7a2/fqSmZA0vZIG1bBfWZY8ZtSeTxKg3eWynV+xElabHqTDMYwf+2
obs4YB5lINTbYgHyRETP6T8Xr6TiD0h3654OUHcW+1meBu/jctluMKppeSjVtrof
5vt+pbkCg0iQAAsL0qcT3yaNXvAgMBAAGjggGHMIIbgzAObgNVHQ8BAf8EBAMC
AQYwEgYDVR0TAQH/BAgwBgEB/wIBADBcBgNVHSAEVTBTFEGCisGAQQBRCRUBEgAw
QzBBBgggrBgEFBQcCARY1aHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtp
L3BvbGliaWVzL2luZGV4Lmhh0bWwwHQYDVR0OBByEFHrXeZXKu0gruFUU/aPAD7yn
D5YZMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly93d3cuY2lzY28uY29tL3NIY3Vy
aXR5L3BraS9jcmwvY3JyYW0yLmNybDB8BggrBgEFBQcCBAQRwMG4wPgYIKwYBBQUH
MAKGMmh0dHA6Ly93d3cuY2lzY28uY29tL3NIY3VyaXR5L3BraS9jZXJ0cy9jcmNh
bTluY2VyMCAwGCCsGAQUFBzABhiBodHRwczovL3Rvb2xzLmNpc2NvLmNvbS9wa2kv
b2NzcDafBgNVHSMEGDAWgBTJAPkfh/CZr2l0m1lDiluNMMFoDANBgkqhkiG9w0B
AQsFAAOCAQEAc1k2rH6YT4juFxs9q7ObzfcKbNvOyDsaU7av4IHFxmn/JxfnBmUv
YxAI2Hx3xRb0KiG1JGkffQjVAtBboTXynLaQso/jj46ZOubIF8y6Ho3nTAv7Q6VH
kqSCdZCIVu9IzbHV9FFYQzJxjw1QgB0a4ItS4yhdmg13oDNEcb3trQezrQ3/857/
ISqBGVLEbKHOu8H6zOLhxAgZ08ae1oQQQJowki0Ibd+LRLGovtEwLg8yyqiTIGve
7VFL2sRa8Z3rK9tlwKVH2kpFKNAeN3rfKFqr0/weR0cyKpmLMrSBTBZcxQcJCYF4
X6FO/32KQqcxJFIOKGVIUjvAvioQoducw==
-----END CERTIFICATE-----

```

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

Certificate has the following attributes:

Fingerprint MD5: AC14F08F C3780F8F D9EEE6C9 39111280

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

Trustpoint CA certificate accepted.

ISR_RA(config)# exit

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

ISR_RA# configure terminal

ISR_RA(config)# crypto pki trustpoint MSCA

ISR_RA(ca-trustpoint)# enrollment mode ra

ISR_RA(ca-trustpoint)# enrollment url http://10.81.116.249/certsrv/mscep/mscep.dll

ISR_RA(ca-trustpoint)# serial-number

ISR_RA(ca-trustpoint)# fingerprint 81512B4316429092925C6891701B374EBD254447

ISR_RA(ca-trustpoint)# revocation-check none

ISR_RA(ca-trustpoint)# rsakeypair MSCA_Key 2048

ISR_RA(ca-trustpoint)# exit

ISR_RA(config)# crypto pki server MSCA

ISR_RA(cs-server)# grant auto trustpointMIC_trustpoint

ISR_RA(cs-server)# hash sha1

ISR_RA(cs-server)# mode ra transparent

ISR_RA(cs-server)# no shutdown

Troubleshooting

Problem Report Tool

A problem report can be created via the Problem Report Tool in the phone Settings menu. Navigate to **Settings > Issues and diagnostics > Report problem**, enter the information, and press **Submit** to generate an issue report.

The image shows two screenshots from a mobile phone interface. The top screenshot is the 'Report problem' form, which has a dark background. It contains five numbered fields: 1. 'Date of problem (mm/dd)' with a text box containing '06/21'. 2. 'Time of problem (hh:mm + AM/PM)' with a text box containing '7:18 PM'. 3. 'Problem description' with a text box containing 'Failed to place a call' and a right-pointing chevron. 4. 'Last PRT file name'. 5. 'Last uploaded time'. At the bottom of this form are three buttons: 'Submit', 'Select', and 'Back'. The bottom screenshot is the 'Issues and diagnostics' screen, also with a dark background. It has a list of items: 1. 'Issues' with the value 'None' on the right. 2. A box containing 'Problem submitted' with a right-pointing chevron. 3. A box containing 'The PRT file is available at http://10.79.63.52/FS/prt-20240621-192126-845A3EC22785.tar.gz' with a right-pointing chevron. At the bottom of this screen is an 'OK' button.

The date and time and problem description can be defined.

The Customer support upload URL option in either Cisco Unified Communications Manager or Broadwork can be configured per phone to obtain the logs automatically or manually download the logs from the phone's webpage.

The image is a screenshot of a web browser displaying the 'Cisco IP Phone for 3rd Party Call Control DP-9871 Configuration Utility'. The page has a blue header with the Cisco logo and the text 'Cisco IP Phone for 3rd Party Call Control DP-9871 Configuration Utility'. There is a 'No password provided' warning icon. Below the header are several tabs: 'Info', 'Voice', 'Call History', and 'Personal Directory'. Under the 'Info' tab, there are sub-tabs: 'Status', 'Debug Info', 'Download Status', and 'Network Statistics'. The 'Debug Info' sub-tab is active, showing 'Console Logs' and 'ThousandEyes Logs'. The 'Console Logs' section lists 'Debug Message 1' through 'Debug Message 8'. The 'ThousandEyes Logs' section lists 'Agent Message 1' and 'Agent Message 2'. At the bottom, there is a 'Problem Reports' section with a 'Report Problem:' button labeled 'Generate PRT' and a 'Mini Prt File:' link to 'miniprt-20240621-042152-845A3EC2302B.tar.gz'. A 'Prt File:' link to 'prt-20240621-042152-845A3EC2302B.tar.gz' is also visible. An 'Admin Login' link is in the top right corner.

Wi-Fi statistics

Navigate to **Settings > Issues and diagnostics > Diagnostics > Device status > Wireless statistics.**

Wireless statistics	
tx bytes	18259897
rx bytes	22422877
tx packets	00060529
rx packets	00068946
tx packets dropped	00000000
rx packets dropped	00000000
Back	

View Streaming Statistics

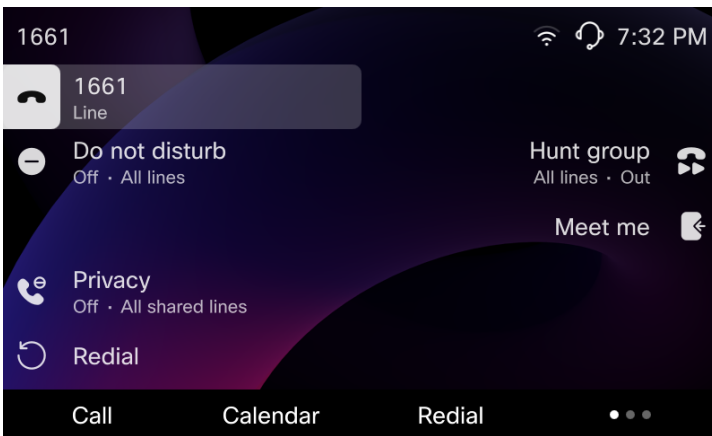
The Cisco Desk Phone 9800 Series provides call statistic information, where codec type, jitter and packet count info, etc. is displayed.

Visit your phone's IP address in a web browser and view the streaming statistics.

Streaming statistics	
Cisco IP Phone DP-9861 (SEP845A3EC229D4)	
Remote address	173.36.143.200/51302
Local address	10.79.63.51/22570
Start time	9:31:25am
Stream status	Active
Host name	SEP845A3EC229D4
Sender packets	237269
Sender octets	12263901
Sender codec	OPUS
Sender reports sent	835
Sender report time sent	10:50:31am
Receiver lost packets	583
Avg jitter	8
Receiver codec	OPUS
Receiver reports sent	0
Receiver report time sent	00:00:00
Receiver packets	236709
Revr octets	40713776
Cumulative conceal ratio	0.0013
Interval conceal ratio	0.0000
Max conceal ratio	0.0594
Conceal seconds	473

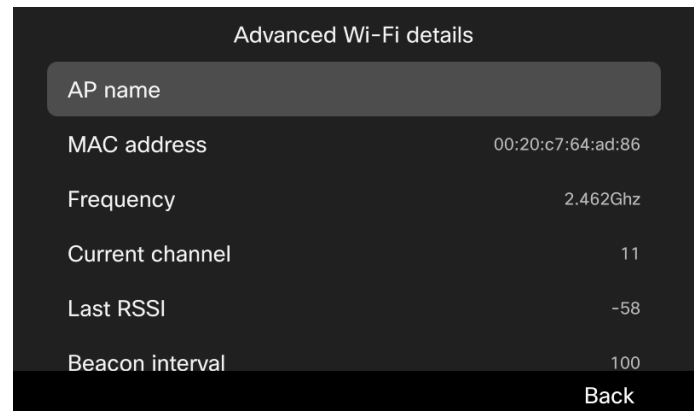
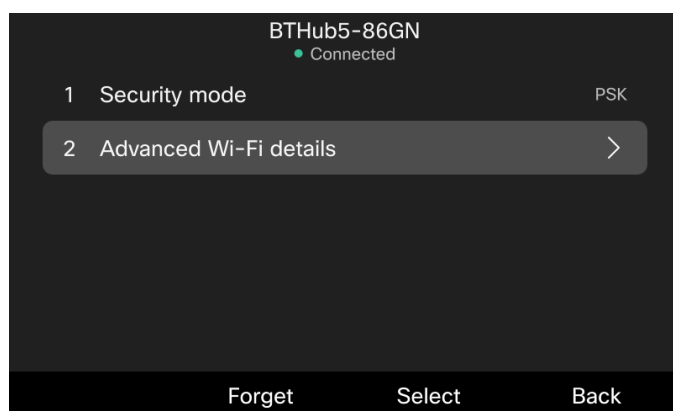
Wi-Fi Signal Indicator

On the Home screen of your phone, Wi-Fi signal is displayed on top-right corner when connected with AP.



View the Information About the Connected Access Point

Navigate to **Settings** > **Network connection** > **Wi-Fi**, select the connected AP, and choose **Advanced Wi-Fi details**.



Note: When user encounters Wi-Fi problem, please check the connected AP status, AP parameters, phone side signal strength and phone Wi-Fi statistics. If the configurations are correct and the desired AP is healthy, toggle Wi-Fi off and on via the

phone menu could help to recover Wi-Fi connection. If this doesn't work, plug-in the wired cable and generate PRT in the phone menu.

Capture a Screenshot of the Phone Display

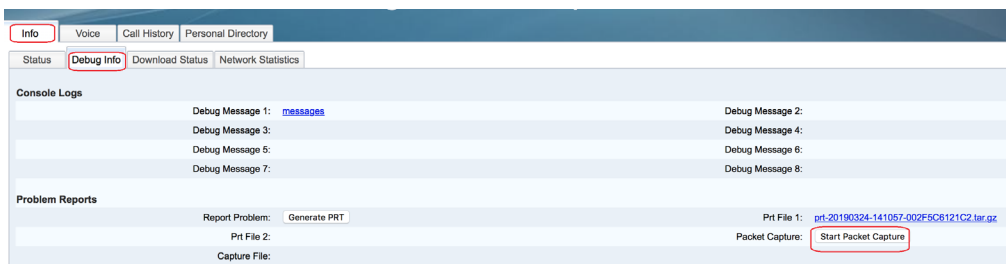
For phones that are registered to Webex Calling or BroadWorks, get the IP address of your phone and visit http://<phone_IP_address>/admin/screendump.bmp in a web browser. For example, <http://192.168.16.43/admin/screendump.bmp>. When prompted, enter the password for the admin.

For phones that are registered to Cisco Unified Communications Manager, get the IP address of your phone and visit http://<phone_IP_address>/CGI/Screenshot. For example, <http://192.168.32.124/CGI/Screenshot>. When prompted, enter the username and password for the account that your phone is associated with in Cisco Unified Communications Manager.

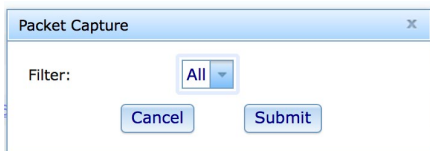
Capture Packets

For phones that are registered to Webex Calling or BroadWorks, you can capture the packets by visiting http://<phone_IP_address>/admin in a web browser.

1. Navigate to **Info > Debug Info** and click **Start Packet Capture**.



2. Click **Submit** in the prompt.



3. When the process completes, click **Stop Packet Capture** to stop capturing.



The captured file is available for downloading.



Additional Documentation

Cisco Desk Phone 9800 Series Datasheet: <https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/ip-phones/desk-phone-9800-series-ds.html>

Cisco Desk Phone 9800 Series User and Administrator Documentation: <https://cisco.com/go/dp9800help>

Other Documentation for Reference

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4-25d-JA/Configuration/guide/cg_12_4_25d_JA.html

<http://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/116167-technote-scep-00.html>

http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/certificates/CertsGuide_cgr1000.html#wp1000815

<http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-product-00.html#anc14>

<https://technet.microsoft.com/en-us/library/cc731183.aspx>

<https://technet.microsoft.com/en-us/library/cc772192.aspx>

<https://technet.microsoft.com/en-us/library/hh831498.aspx>

https://technet.microsoft.com/en-us/library/cc772393%28v=ws.10%29.aspx#BKMK_BS2

<http://social.technet.microsoft.com/wiki/contents/articles/9063-network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx>

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xr-3s/sec-pki-xr-3s-book/sec-cfg-auth-rev-cert.html#GUID-4A2D2A66-F6FB-4FD1-AD40-B7D73531468E

http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfrad.html#wp1001000

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2024 Cisco Systems, All rights reserved.