··|···|·· cisco

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide



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
Models	7
Requirements	7
Site Requirement	7
Call Control	8
Wireless LAN	9
Access Points	9
Antenna System	
Protocols	
Wi-Fi	
5 GHz Specifications	10
2.4 GHz Specifications	12
Regulatory	
Bluetooth [®]	
Bluetooth Profiles	13
Coexistence (802.11b/g/n + Bluetooth)	
Device Care	14
Wireless LAN Design	15
802.11 Network	
5 GHz (802.11a/n/ac)	
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	
Security	
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)	
Quality of Service (QoS)	
Call Admission Control (CAC)	21
Wired QoS	
Roaming	
Fast Secure Roaming (FSR)	
Interband Roaming	
Power Management	
Delivery Traffic Indicator Message (DTIM)	23
Call Capacity	
Multicast	23
Configuring the Cisco Wireless LAN	24
Cisco AireOS Wireless LAN Controller and Lightweight Access Points	
802.11 Network Settings	

Auto RF (RRM)	
Client Roaming	
EDCA Parameters	
DFS (802.11h)	
High Throughput (802.11n/ac)	
Frame Aggregation	
CleanAir	31
Rx Son Threshold	32
WI AN Settings	32
AP Groups	37
Controller Settings	39
Call Admission Control (CAC)	40
RF Profiles	42
FlevConnect Groups	
Multicast Direct	
Oos Profiles	
Advanced Settings	
Advanced EAD Settings	ر+ /۱۵
Auto Immune	
Auto-minimute	
Rogue I oncles	
Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points	
802.11 Network Settings	
High Throughput (802.11n/ac)	
Parameters	
RRM	
CleanAir	
WLAN Settings	
Policy Profiles	60
RF Profiles	
Flex Profiles	
Tags	
Controller Settings	
Mobility Settings	
Call Admission Control (CAC)	
Multicast	
Advanced Settings	
Advanced EAP Settings	
Rx Sop Threshold	
Rogue Policies	
Cisco Mohility Fypress and Lightweight Access Points	73
Controller Settings	
802 11 Network Settings	74
BE Ontimization	
WI AN Settings	דר
A D Groups	
DE Drofiles	
Nr 110mcs	
Cisco Autonomous Access Points	
802.11 Network Settings	
WLAN Settings	
Wireless Domain Services (WDS)	
Call Admission Control (CAC)	

QoS Policies	96
Power Management	
Cisco Meraki Access Points	
Creating the Wireless Network	
SSID Configuration	
Radio Settings	
Firewall and Traffic Shaping	
Configure Cisco Call Control	
Cisco Webex Calling	
Personal Usage	
Workspace Usage	
Wi-Fi Capability	
Cisco Unified Communications Manager	
Device Enablement	
Common Settings	
QoS Parameters	
Wireless LAN Profiles	110
Create a Wirless LAN Profile Croup	
Apply a Wireless I AN Profile Group to a Device Pool	
Apply a Wireless LAN Profile Group to an Individual Phone	
Configure the Cisco Desk Phone 9800 Series	
Automatic Provisioning	
Config/Modify Wi-Fi Profile via Phone Web Portal	117
Configure Wi-Fi Settings on the Phone UI	
Join a Hidden Wireless Network	
Delete a Connected Network	
Certificate Management	
Manual Installation	
Manufacturing Installed Certificate (MIC)	
User Installed Certificate	
LSC Certificate	
Server Certificate	
Certificate Removal.	
Simple Certificate Enrollment Protocol (SCEP)	
RADIUS Configuration	
SCEP RA Configuration	
Troubleshooting	
Problem Report Tool	
Wi-Fi statistics	
View Streaming Statistics	
Wi-Fi Signal Indicator	
Wi-Fi Signal Indicator View the Information About the Connected Access Point	

Capture Packets	
Additional Documentation	144
Other Documentation for Reference	

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.

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

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

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, 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.

<u>Signal</u>

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%.

<u>Noise</u>

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

Also need to ensure that the upstream signal from the Cisco 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%.

<u>Multipath</u>

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/286328117/type/282074299/release/14.0(1.14056)

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
 - o 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	6 Mbps	1	OFDM-BPSK
(Depends on region)	9 Mbps	1	OFDM-BPSK
	12 Mbps	1	OFDM-QPSK
	18 Mbps	1	OFDM-QPSK
	24 Mbps	1	OFDM-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	7 Mbps (MCS 0)	1	OFDM-BPSK
(Depends on region)	14 Mbps (MCS 1)	1	OFDM-QPSK
	21 Mbps (MCS 2)	1	OFDM-QPSK

	29 Mbps (MCS 3)	1	OFDM-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	15 Mbps (MCS 0)	1	OFDM-BPSK
(Depends on region)	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-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	7 Mbps (MCS 0)	1	OFDM-BPSK
(Depends on region)	14 Mbps (MCS 1)	1	OFDM-QPSK
	21 Mbps (MCS 2)	1	OFDM-QPSK
	29 Mbps (MCS 3)	1	OFDM-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	15 Mbps (MCS 0)	1	OFDM-BPSK
(Depends on region)	30 Mbps (MCS 1)	1	OFDM-QPSK
	45 Mbps (MCS 2)	1	OFDM-QPSK
	60 Mbps (MCS 3)	1	OFDM-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
1			

2.4 GHz Specifications

2.4 GHz - 802.11b	Data Rate	Spatial Streams	Modulation
Max Tx Power=18 dBm	1 Mbps	1	DSSS-BPSK
(Depends on region)	2 Mbps	1	DSSS-QPSK
	5.5 Mbps	1	DSSS-CCK
	11 Mbps	1	DSSS-CCK
2.4 GHz - 802.11g	Data Rate	Spatial Streams	Modulation
Max Tx Power=18 dBm	6 Mbps	1	OFDM-BPSK
(Depends on region)	9 Mbps	1	OFDM-BPSK
	12 Mbps	1	OFDM-QPSK
	18 Mbps	1	OFDM-QPSK
	24 Mbps	1	OFDM-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	7 Mbps	1	OFDM-BPSK
(Depends on region)	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
		1	1

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 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



Minimum 20% Overlap

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.



Minimum 20% Overlap

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.

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

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.

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

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.

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

• Create a QoS policy on the access point giving priority to voice and call control traffic.

• 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.

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

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

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

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

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 AireOSWireless 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.

ululu cisco	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11a Global Pa	rameters						
Access Points All APs Radios	General				Data Rates**	:		
Global Configuration	802.11a Network Stat	tus 🗹 E	nabled		6 Mbps		Disabled	0
Advanced	Beacon Period (millise	ecs) 1	.00		9 Mbps		Disabled	\$
Mesh	(bytes)	2	346		12 Mbps		Mandatory	0
AP Group NTP	DTPC Support.	🗹 E	nabled		18 Mbps		Supported	0
▶ ATF	Maximum Allowed Cli	ents 100			24 Mbps	(:	Supported	\Diamond
RF Profiles	RSSI Low Check	E	nabled		36 Mbps		Supported	0
ElexConnect Groups	RSSI Threshold (-60 t	to -90 -	80		48 Mbps		Supported	0
FlexConnect ACI s	dBm)				54 Mbps		Supported	
FlexConnect VLAN	802.11a Band Stat	us Enal	bled		CCX Location	Measurem	ent	
Network Lists	Mid Band	Enal	bled		Mode		Enabled	
 802.11a/n/ac/ax 	High Band	Enal	bled		Interval (secor	nds) 6	0	
Network RRM					TWT Configur	ration ***		
RF Grouping					Target Waketir	ne 🗸	Enabled	
TPC DCA					Broadcast TWT	Support 🔽	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).

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTR	OLLER WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>o</u> mmands h	HELP <u>F</u> EEDBACK		
Wireless	802.11b/g Global Parame	eters						
Access Points All APs Radios	General			Data Rates**				
Global Configuration	802.11b/g Network Status	Enabled		1 Mbps	Disab	oled ᅌ		
Advanced	802.11g Support	Enabled		2 Mbps	Disat	oled ᅌ		
Mesh	Beacon Period (millisecs)	100		5.5 Mbps	Disab	Disabled ᅌ		
AP Group NTP	Short Preamble	🗹 Enabled		6 Mbps	Disab	oled ᅌ		
ATF	Fragmentation Threshold (bytes)	2346		9 Mbps	Disab	oled ᅌ		
PE Profiles	DTPC Support.	Enabled		11 Mbps	Disab	oled ᅌ		
FlexConnect Groups	Maximum Allowed Clients	100		12 Mbps	Mand	latory ᅌ		
FlexConnect ACLs	RSSI Low Check	Enabled		18 Mbps	Supp	orted 📀		
ElexConnect VI AN	RSSI Threshold (-60 to -90	-80		24 Mbps	Supp	orted ᅌ		
Templates	dbm)			36 Mbps	Supp	orted ᅌ		
Network Lists	CCX Location Measureme	nt		48 Mbps	Supp	orted ᅌ		
🕨 802.11a/n/ac/ax	Mode	Enabled		54 Mbps	Supp	orted ᅌ		
802.11b/g/n/ax	Interval (seconds)	60		TWT Configu	ration ***			
RRM				Target Waketi	me	Enabled		
RF Grouping TPC				Broadcast TW	T Support	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.



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.

	ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
w	reless	802.11a >	302.11a > RRM > Dynamic Channel Assignment (DCA)								
•	Access Points All APs Radios	Dynamic	Channel	Assignment A	lgorithm			to the Time (
×	Global Configuration Advanced	Channel A	lssignment	Method	 Automatic Freeze 	Interval: Invoke	Channel Update	Once	•		
* *	Mesh AP Group NTP ATF	Avoid For Avoid Cise	eign AP inte co AP load	erference	OFF ✓ Enabled □ Enabled						
	RF Profiles FlexConnect Groups	Avoid non Avoid Per Channel A	i-802.11a n sistent Non Assignment	oise -WiFi Interference Leader	 Enabled Enabled RTP9-32A-WI 	LC3 (10.81.6.7))				
	FlexConnect VLAN Templates Network Lists	Last Auto DCA Chan Channel V	Channel As Inel Sensitiv Vidth	ssignment vity	556 secs ago Medium ᅌ 20 MHz 💿	(15 dB) 40 MHz 080	MHz ()160 MHz ()80+80 MHz ()E	Best		
•	802.11a/n/ac/ax Network RRM RF Grouping	Avoid che	ck for non-	DFS channel	Enabled						
	TPC DCA Coverage General Client Roaming Media EDCA Parameters	DCA Char	nels	36, 40, 44, 157, 161	48, 52, 56, 60	, 64, 100, 153,	lie				

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.

،، ،،، ،، cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Wireless	802.11b >	302.11b > RRM > Dynamic Channel Assignment (DCA)								
 Access Points All APs Radios Global Configuration 	Dynamic (Channel Assignment	Assignment A	Igorithm OAutomatic	Interval:	10 minutes ᅌ	AnchorTime: 0	0		
Advanced				Freeze	Invoke	Channel Update	Once			
Mech				OFF						
AP Group NTP	Avoid For	eign AP inte	erference	🗹 Enabled						
E AF	Avoid Cise	co AP load		Enabled						
P ATF	Avoid non	-802.11b n	oise	Enabled						
RF Profiles	Avoid Per	sistent Non	-WiFi Interference	Enabled						
FlexConnect Groups	Channel A	esignment	Leader	PTP0-32A-WI	C3 (10 81 6 7	0)				
FlexConnect ACLs	Lest Auto	Channel A		75	.05 (10.01.0.7)	0)				
FlexConnect VLAN Templates	DCA Chan	nel Sensiti	vity	75 secs ago Medium ᅌ	(10 dB)					
Network Lists	DCA Chan	nel List								
🕨 802.11a/n/ac/ax	Den chan	iner Else								
802.11b/g/n/ax Network		1, 6	5, 11							
▼ RRM	DCA Chan	nels								
RF Grouping										
DCA					11					
Coverage										

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

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

This may be necessary if there is an intermittent 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.

ດປາດປາດ cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGE	EMENT C <u>O</u> MMANDS HE <u>L</u> P <u>F</u> EEDB	ACK
Wireless	802.11a/n/ac/ax Cisco APs > Co	onfigure		
 Access Points All APs Radios R02 11a/p/ac/ax 	General		RF Channel Assignment	
802.11b/g/n/ax	AP Name	rtp9-31a-ap1	Current Channel	(48,44)
Dual-Band Radios	Admin Status	Enable ᅌ	Channel Width *	40 MHz 💲
Advanced	Operational Status	UP	* Channel width can be configu mode	red only when channel configuration is in custom
Mesh	Slot #	1	Assignment Method	Global
AP Group NTP	11n Parameters			Custom
ATF			Radar Information	
RF Profiles	11n Supported	Yes		
FlexConnect Groups	CleanAir		Channel La:	st Heard(Secs)
FlexConnect ACLs			No radar detected channels	
FlexConnect VLAN Templates	CleanAir Capable CleanAir Admin Status	Yes Enable	Tx Power Level Assignm	nent
Network Lists	* CleanAir enable will take effect only	if it is enabled on this band.	Current Ty Dawer Level	
802.11a/n/ac/ax	Number of Spectrum Expert	0	Assignment Method	
802.11b/g/n/ax	connections		Assignment Pietrou	Custom
Media Stream	Antenna Parameters			0
Application Visibility And Control	Antenna Type	Internal 📀 A 🗹	Performance Profile	
Lync Server	Antenna	В 🗹 С 🗹	View and edit Performance F	Profile for this AP
Country		D 🗹	Performance Profile	
Timers			Note: Changing any of the para	ameters causes the Radio to be temporarily disabled
Netflow			and thus may result in loss of o	connectivity for some clients.
▶ QoS				

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.

	ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
W	ireless									
•	Access Points All APs Radios Global Configuration	General EDCA Prot	file		Voice	& Video Optim	ized ᅌ			
Þ	Advanced	Enable Lo	w Latency	MAC 1						
	Mesh									
Þ	AP Group NTP	Low Jatency	Mac feature	a is not supported	for 1140/1250	/3500 platform	s if more than 3 da	ta rates are enab	led	
Þ	ATF	Low latency	mac reacon		10/ 1140/1250	5500 piacom	s il more chan 5 da	ta rates are enab	neu.	

DFS (802.11h)

Power Constraint should be left un-configured or set to 0 dB. **Channel Announcement** and **Channel Quiet Mode** should be **Enabled**.

۰۱۱۰۰۱۰۰ cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMEN	T C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	802.11h (Global P	arameters						
 Access Points All APs Radios Global Configuration 	Power Co	nstraint ver Constra	int(0-30)	0 di	3				
Advanced	Channel S	witch A	nnouncement						
Mesh AP Group NTP ATF RF Profiles FlexConnect Groups	Channel A Channel S Channel C Radar Bla	Announcem Switch Cour Quiet Mode	ent nt	 ✓ ✓ 					
FlexConnect ACLs	Smart DF	s							

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.

iiliiilii cisco	MONITOR	<u>W</u> LANS <u>C</u> ONTROLI	LER W <u>I</u> RELESS	<u>S</u> ECURITY M <u>A</u> NAGEI	MENT C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Wireless	802.11n/	ac/ax (5 GHz) Thro	oughput					
Access Points	General					MCS	(Data Rate ¹) Settings	5
Global Configuration	11n Mod	e	🗹 Enab	iled ²		0	(7 Mbps)	Supported
Advanced	11ac Mo	de	🗹 Enab	led ³		1	(14 Mbps)	Supported
Mesh	11ax Mo	de	🗹 Enab	led ³		2	(21 Mbps)	Supported
AP Group NTP		Pates				3	(29 Mbps)	Supported
▶ ATF	VIII PICS	Rates				4	(43 Mbps)	Supported
RF Profiles	SS1					5	(58 Mbps)	Supported
FlexConnect Groups	0-8		Enab	led 4		6	(65 Mbps)	Supported
FlexConnect ACLs	0-9		🗸 Enab	led 4		7	(72 Mbps)	Supported
ElexConnect VI AN						8	(14 Mbps)	Supported
Templates	552					9	(29 Mbps)	Supported
Network Lists	0-8		✓ Enab	iled =		10) (43 Mbps)	Supported
💌 802.11a/n/ac/ax	0-9		Enab	iled ⁴		11	(58 Mbps)	Supported
Network	SS3					12	2 (87 Mbps)	Supported
RF Grouping	0-8		Enab	led 4		13	8 (116 Mbps)	Supported
TPC	0-9		🗹 Enab	led 4		14	(130 Mbps)	Supported
Coverage						15	5 (144 Mbps)	Supported
General	554					16	6 (22 Mbps)	Supported
Media	0-8		Enab	iled 4		17	7 (43 Mbps)	Supported
EDCA Parameters	0-9		Enab	iled 4		18	8 (65 Mbps)	Supported
High Throughput	HE MCS F	Rates				19	9 (87 Mbps)	Supported
(802.11n/ac/ax)						20) (130 Mbps)	Supported
802 11b/s/p/av	SS1		SS2			21	(173 Mbps)	Supported
Madia Chasan	0-7	Enabled	0-7	Enabled		22	2 (195 Mbps)	Supported
Media Stream	0-9	Enabled	0-9	Enabled		23	8 (217 Mbps)	Supported
Application Visibility And Control	0-11	Enabled	0-11	Enabled		24	4 (29 Mbps)	Supported
Lync Server	SS3		SS4			25	5 (58 Mbps)	Supported
Country	0-7	Enabled	0-7	Enabled		26	6 (87 Mbps)	Supported
Timers	0-9	✓ Enabled	0-9	Enabled		27	7 (116 Mbps)	Supported
Netflow	0-11	Enabled	0-11	Enabled		28	8 (173 Mbps)	Supported
▶ 0oS	- i - i - i - i - i - i - i - i - i - i	_	,			29	9 (231 Mbps)	Supported
400	SS5		SS6			30	0 (260 Mbps)	Supported
	0-7	Enabled	0-7	Enabled		31	(289 Mbps)	Supported

Frame Aggregation

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

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

It is required to adjust the A-MPDU and A-MSDU settings to the following to optimize the experience with the Cisco 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 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 6 disable config 802.11b 11nSupport a-msdu tx priority 7 disable

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

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

802.11n Status:

A-MSDU Tx:	
Priority 0	Disabled
Priority 1	Enabled
Priority 2	Enabled
Priority 3	Disabled
Priority 4	Disabled
Priority 5	Disabled
Priority 6	Disabled
Priority 7	Disabled
A-MPDU Tx:	
Priority 0	Enabled
Priority 1	Disabled
Priority 2	Disabled
Priority 3	Enabled
Priority 4	Enabled

Priority 5	Enabled
Priority 6	Disabled
Priority 7	Disabled

CleanAir

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



.ı ı.ı ı. cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER	WIRELESS SECURITY MANA	IGEMENT C <u>O</u> MMANDS HELP <u>F</u> E	EDBACK		
Wireless	802.11a/n/ac/ax Cisco APs > C	onfigure				
Access Points All APs Radios	General		RF Channel Assignm	lent		
802.11a/n/ac/ax 802.11b/g/n/ax	AP Name	rtp9-31a-ap1	Current Channel	(48,44)		
Dual-Band Radios	Admin Status	Enable ᅌ	Channel Width *	40 MHz 0		
Global Configuration	Operational Status	UP	* Channel width can be com mode	nfigured only when channel configuration is in custom		
Mesh	Slot #	1	Assignment Method	Global		
AP Group NTP	11n Parameters			Custom		
ATF			Radar Information	Radar Information		
RF Profiles	11n Supported	Yes				
FlexConnect Groups	CleanAir		Channel	Last Heard(Secs)		
FlexConnect ACLs			No radar detected channel	s		
FlexConnect VLAN Templates	CleanAir Capable CleanAir Admin Status	Enable	Tx Power Level Assi	gnment		
Network Lists	* CleanAir enable will take effect only	if it is enabled on this band.				
802.11a/n/ac/ax	Number of Spectrum Expert	0	Current TX Power Level			
802.11b/g/n/ax	connections		Assignment Method	Custam		
Media Stream	Antenna Parameters			Custom		
Application Visibility And Control	Antenna Type	Internal ᅌ A 🗸	Performance Profile			
Lync Server	Antenna	в	View and edit Performan	nce Profile for this AP		
Country		D C	Performance Profile	8		
Timers			Note: Changing any of the	parameters causes the Padio to be temporarily disab		
Netflow			and thus may result in loss	s of connectivity for some clients.		
QoS						

Rx Sop Threshold

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

ululu cisco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	Rx Sop T	hreshold	d						
 Access Points All APs Radios Global Configuration 	Rx Sop T Rx Sop T	hreshold 80 hreshold 80	02.11a Defa	ult ᅌ O	Custom				
 Advanced RF Management Flexible Radio Assignment Load Balancing DTLS Band Select Rx Sop Threshold Optimized Roaming Network Profile 	1 Rxsop o	nly support	ted in Local,Flex,B	ridge and Flex+	-Bridge mode A	ips.			

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.

iliilii cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > New
WLANs WLANs Advanced	Type WLAN Profile Name voice SSID voice ID 6
،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDE
WLANs	WLANs > Edit 'voice'
WLANs WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Profile Name voice
	Type WLAN
	SSID voice
	Status 🗹 Enabled
	Security Policies [WPA2][Auth(FT 802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy 802.11a only
	Interface/Interface rtp-9 voice C
	Multicast Vlan Feature 🛛 Enabled
	Broadcast SSID 🛛 🗹 Enabled
	NAS-ID RTP9-32A-WLC3
	Lobby Admin Access

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.

General Security	QoS Policy-Mapping Advanced
WPA2+WPA3 Parameters	
Policy	✓WPA2 ✓WPA3
Encryption Cipher	CCMP128(AES)
Fast Transition	
Fast Transition	Enable v
Over the DS	
Reassociation Timeout	20 Seconds
Protected Management Fra	ame
PMF	Optional v
Comeback	1
timer(1-10sec)	
timer(1-10sec) SA Query Timeout(100-500msec)	200
timer(1-10sec) SA Query Timeout(100-500msec) Authentication Key Manag	200 ement 19
timer(1-10sec) SA Query Timeout(100-500msec) Authentication Key Manag 802.1X-SHA1	200 ement 19 Enable
timer(1-10sec) SA Query Timeout(100-500msec) Authentication Key Manag 802.1X-SHA1 802.1X-SHA2	200 ement 19 Enable Enable

ieneral Se	ecurity	QoS P	olicy-Map	pping	Adva	nced	
WPA2+WPA3	Parameter	s					
Policy		WPA2	 ₩P/	A3			
Encryption C	Encryption Cipher		28(AES)	□cc	MP256	GCMP128	GCMP256
Fast Transition	n						
Fast Transitio	on	Enable	~				
Over the DS							
Reassociatio	n Timeout	20 Se	conds				
Protected Man	agement F	rame					
PMF		Required	i ~				
Comeback timer(1-10sec)		1					
SA Query Timeout(100-500msec)		200					
Authentication	ı Key Mana	gement <u>19</u>					
802.1X-SHA	1	Enable	3				
802.1X-SHA	12	🗌 Enabl	е				
FT 802.1X		Enabl	e				

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.

cisco	MONITOR WLA	Ns <u>C</u> ONTROLLER	WIRELESS SECURITY	MANAGEMENT	C <u>o</u> mmands he	<u>L</u> P <u>F</u> EEDBACK			
WLANs	WLANs > Edit	'voice'							
WLANs WLANs	General	ecurity QoS	Policy-Mapping Adv	vanced					
Advanced	Layer 2	Layer 3 AAA Se	rvers						
	RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled Authentication Servers EAP Parameters								
		C Enabled	C Enabled		Enable 🗹				
	Server 1	None	None	✓	EAPOL Key T	Timeout(200 to 5000 millised	400		
	Server 2	None	None		EAPOL Key R	tetries(0 to 4)	4		
	Server 3	None	None	©	Identity Requ	uest Timeout(1 to 120 sec)	30		
	Server 4	None	None	\$	Identity Requ	uest Retries(1 to 20)	2		
	Server 5	None	None		Request Timeout(1 to 120 sec)				
	Server 6 None 📀 None				Request Retries(1 to 20) 2				
		Authorization ACA Se	rver Accounting ACA	Server					

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.

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

cisco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> O	NTROLLER W	/ <u>I</u> RELESS S		M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u>	EEDBACK
WLANs	WLANs > Edit 'voice	9"						
WLANs WLANS	General Security	QoS Po	olicy-Mappin	ıg Adv	anced			
Advanced	Quality of Service (QoS) Platinum	(voice)	0				
	Application Visibility	🗹 Enabled	1					
	AVC Profile	none		0				
	Flex AVC Profile	none 🗘						
	Netflow Monitor	none ᅌ						
	Fastlane	Disable	0					
	Override Per-User Ba	andwidth Cor	ntracts (kb	ps) <u>16</u>				
		DownStream	m UpStrea	im				
	Average Data Rate	0	0					
	Burst Data Rate	0	0					
	Average Real-Time Rate	0	0					
	Burst Real-Time Rate	0	0					
	Clear							
CISCO	MONITOR WLANS CONT	ROLLER W <u>I</u> RE	ELESS <u>s</u> ecu	JRITY M <u>A</u>	NAGEMENT C <u>O</u>	MMANDS HEL	P <u>F</u> EEDBA	ACK
WLANs	General Security	QoS Polic	y-Mapping	Advance	ad			
WLANs	Override Per-SSID Ban	dwidth Contr	acts (kbps)	<u>16</u>				
Advanced		DownStream	UpStream					
	Average Data Rate	0	0					
	Burst Data Rate	0	0					
	Average Real-Time Rate	0	0					
	Burst Real-Time Rate	0	0					
	Clear							
	WMM							
	WMM Policy	Required ᅌ						
	7920 AP CAC	Enabled						
	7920 Client CAC	Enabled						
	Media Stream							
	Multicast Direct	Enabled						
	Lync Policy							
	-,,							

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.


cisco	<u>M</u> ONITOR <u>W</u> LAN							
ANs	WLANs > Edit	'voice'						
VLANs WLANS	General Se	ecurity Q	oS Pol	licy-Mapping	Advanced			
dvanced	FlexConnect L	ocal Auth 12	Enable	d			PMIP Profile	None ᅌ
	Learn Client If	P Address 5	✓ Enable	d			PMIP Realm	
	Vlan based Ce	entral					Universal AP Admin Support	
	Switching 13		Enable	d			Universal AP Admin	
	Central DHCP	Processing	Enable	d			11v BSS Transition Support	
	Override DNS		Enable	d			BSS Transition	
	NAT-PAT		Enable	d			Disassociation Imminent	
	Central Assoc		Enable	d			Disassociation Timer(0 to 3000 TBTT)	200
	Lync						Optimized Roaming Disassociation Timer(0 to 40 TB1	T) 40
	Lync Server	L.	Disabled				BSS Max Idle Service	
	11k						Directed Multicast Service	
	Neighbor List			U Er	nabled		Tunneling	New A
	Neighbor List	Dual Band	0-1-1-1-1-1-1		habled		EOGRE Vian Override	None
	Assisted Roam	ning Prediction	Optimizatio	n 🗍 Er	habled		mDNS	
	802.11ax BSS C	onfiguration						
.ı ı.ı ı. cısco	Down Link MU MONITOR	J-MIMO	NTROLLER	☑ Er W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	mDNS Snooping C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	Enabled
.ı ı.ı ı. cısco Ans	Down Link MU MONITOR	J-MIMO <u>(</u> LANs <u>C</u> OP dit 'voice	NTROLLER	☑ Er W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	mDNS Snooping C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	Enabled
	MONITOR W WLANS > EC	J-MIMO VLANS COM dit 'voice Security	NTROLLER y' QoS	VIRELESS	SECURITY	MANAGEMENT	mDNS Snooping C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	Enabled
IIIIII CISCO ANS WLANS WLANS	Down Link MU MONITOR W WLANS > Er General 802.11ax BS	J-MIMO VLANS COI dit 'voice Security SS Configura	NTROLLER y QoS	VIRELESS	<u>SECURITY</u>	MANAGEMENT	mDNS Snooping CQMMANDS HELP FEEDBACK mDNS	Enabled
ULANS WLANS Movanced	Down Link MU MONITOR W WLANS > Er General 802.11ax BS Down Link	J-MIMO <u>V</u> LANS <u>CO</u> dit 'voice Security SS Configura k MU-MIMO	VTROLLER y QoS	WIRELESS Policy-Map	SECURITY	MANAGEMENT	mDNS Snooping COMMANDS HELP FEEDBACK mDNS mDNS Snooping	Enabled
ULANS WLANS Advanced	Down Link MU MONITOR W WLANS > Er General 802.11ax BS Down Link Up Link M	J-MIMO VLANS COT dit 'voice Security SS Configura k MU-MIMO IU-MIMO	NTROLLER 9' QoS	VIRELESS	SECURITY ping Adv. C Enabled C Enabled		mDNS Snooping COMMANDS HELP FEEDBACK mDNS mDNS Snooping TrustSec	Enabled
ULANS WLANS Advanced	Down Link MU MONITOR W WLANS > Er General 802.11ax BS Down Link Up Link M Down Link	J-MIMO <u>V</u> LANS <u>C</u> OT dit 'voice <u>Security</u> <u>SS Configura</u> k MU-MIMO IU-MIMO k OFDMA	NTROLLER 9 ⁵ QoS	VIRELESS	SECURITY ping Adv. ? Enabled ? Enabled ? Enabled		mDNS Snooping COMMANDS HELP FEEDBACK mDNS mDNS Snooping TrustSec Security Group Tag	Enabled
ULANS WLANS WLANS Advanced	Down Link MU MONITOR W WLANS > Er General 802.11ax BS Down Link Up Link M Down Link Up Link O	J-MIMO VLANS COP dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	NTROLLER 9 [°] QoS Ation	VIRELESS	SECURITY ping Adv. ? Enabled ? Enabled ? Enabled ? Enabled ? Enabled		mDNS Snooping COMMANDS HELP FEEDBACK mDNS mDNS Snooping TrustSec Security Group Tag Umbrelia	Enabled
LANS WLANS Advanced	Down Link MU MONITOR W WLANS > Er General 802.11ax BS Down Link Up Link M Up Link O	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	vtRoller 9 ⁵ QoS attion	VIRELESS	SECURITY ping Adv. ? Enabled ? Enabled ? Enabled ? Enabled		mDNS Snooping COMMANDS HELP FEEDBACK mDNS mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode	Enabled
ULANS WLANS WLANS Advanced	Down Link MU MONITOR W WLANS > Er General 802.11ax BS Down Link Up Link M Up Link O	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER ," QoS	VIRELESS	SECURITY ping Adv. ? Enabled ? Enabled ? Enabled ? Enabled		mDNS Snooping COMMANDS HELP FEEDBACK mDNS mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode Umbrella Profile	Enabled
ULANS WLANS WLANS Advanced	Down Link MU MONITOR WLANS > Er General 802.11ax BS Down Link Up Link M Up Link O	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER ," QoS	Er WIRELESS Policy-Map	SECURITY ping Adv. ? Enabled ? Enabled ? Enabled ? Enabled		mDNS Snooping COMMANDS HELP FEEDBACK mDNS mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode Umbrella Profile Umbrella DHCP Override	Enabled
ULANS WLANS WLANS Advanced	Down Link MU MONITOR W WLANS > Er General 802.11ax BS Down Link Up Link M Up Link O	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER y QoS	Er	SECURITY ping Adv. ? Enabled ? Enabled ? Enabled ? Enabled		mDNS Snooping CQMMANDS HELP FEEDBACK mDNS moDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode Umbrella Profile Umbrella DHCP Override Fabric Configuration	Enabled
ULANS WLANS WLANS Advanced	Down Link MU MONITOR WLANS > EC General 802.11ax BS Down Link Up Link M Up Link O	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER y" QoS	VIRELESS Policy-Map	SECURITY ping Adv. 2 Enabled 2 Enabled 2 Enabled 2 Enabled	MANAGEMENT	mDNS Snooping CQMMANDS HELP FEEDBACK mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode Umbrella Profile Umbrella DHCP Override Fabric Configuration Fabric	Enabled
ULANS WLANS Advanced	Down Link MU	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER 9 ⁴ QoS vition	WIRELESS Policy-Map	sECURITY ping Adv 2 Enabled 2 Enabled 2 Enabled 2 Enabled 2 Enabled	MANAGEMENT	mDNS Snooping CQMMANDS HELP FEEDBACK mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode Umbrella Profile Umbrella DHCP Override Fabric Configuration Fabric	Enabled
ULANS WLANS Advanced	Down Link MU	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER 9 ⁴ QoS Ntion	WIRELESS Policy-Map	sECURITY ping Adv. 2 Enabled 2 Enabled 2 Enabled 2 Enabled 2 Enabled	MANAGEMENT	mDNS Snooping CQMMANDS HELP FEEDBACK mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode Umbrella Profile Umbrella DHCP Override Fabric Configuration Fabric Mobility Selective Reanchor	Enabled
ULANS WLANS WLANS Advanced	Down Link MU	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER y ^s QoS ition	WIRELESS Policy-Map	sECURITY ping Adv. 2 Enabled 2 Enabled 2 Enabled 2 Enabled 2 Enabled	MANAGEMENT	mDNS Snooping CQMMANDS HELP FEEDBACK mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Mode Umbrella Profile Umbrella PHCP Override Fabric Configuration Fabric Mobility Selective Reanchor U3 Interface	Enabled
ULANS WLANS Advanced	Down Link MU	LANS CON dit 'voice Security SS Configura k MU-MIMO IU-MIMO k OFDMA	VTROLLER 9 ⁴ QoS Ntion	VIRELESS Policy-Map	sECURITY ping Adv. 2 Enabled 2 Enabled 2 Enabled 2 Enabled 2 Enabled	MANAGEMENT	mDNS Snooping CQMMANDS HELP FEEDBACK mDNS mDNS Snooping mDNS Snooping TrustSec Security Group Tag Umbrella Umbrella Profile Umbrella Profile Umbrella DHCP Override Fabric Configuration Fabric Mobility Selective Reanchor U3 Interface U3 Interface	Enabled

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.

				-	U	1	
ululu cisco		Ns <u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS HE	<u>L</u> P <u>F</u> EEDBACK
WLANs	AP Groups						
WLANs WLANs	Add New AP Gr	oup					
Advanced AP Groups	AP Group Name Description	rtp	1				
		Add Cancel	1				

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LAN	s <u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMEN	r c <u>o</u> mmands	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	Ap Groups > E	lit 'rtp'					
WLANs WLANs	General	ANs RF Profi	le APs	802.11u	Location	Ports/Module	Intelligent Capture
Advanced AP Groups						Apply	
	AP Group Name	ption	rtp				
	NAS-ID	paon	RTP9-32A-W	/LC3			
	Enable Client Tr	affic QinQ OinO 3					
	QinQ Service VI	an Id <u>10</u>	0				
	Fabric ACL Tem	plate	None 📀	figured			
	Custom Web Ov	erride-Global 13	Enable	ingurea			
	External Web a	uth URL	none				
	NTP Auth NTP Server		Enable None				

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

راریاں cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	Ap Group	s > Edit	'rtp'						
WLANs WLANs	General	WLA	Ns RF Profil	e APs	802.11u	Location	Ports/Module	Inte	lligent Capture
Advanced AP Groups	Add New WLAN S Interfa Group((SNMP N	SID e ce 3) AC State	voice(6) rtp-9 voice Enabled Add Cane	sel	• •] <u>1</u>			Add New

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.

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u> EEDBACK
WLANs	Ap Group	os > Edit	'rtp'					
WLANs Advanced	General	WLA	Ns RF Profil	e APs	802.11u	Location	Ports/Module	Intelligent Capture
AP Groups	802.11 802.11	a none	8	.				

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

Those access points will then reboot.

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANs	<u>C</u> ONTROLLER W	IRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMEN	t c <u>o</u> mmands	HELP <u>F</u> E	EEDBACK	
WLANs	Ap Groups > Edit	'rtp'							
WLANs	General WLA	Ns RF Profile	APs	802.11u	Location	Ports/Module	Intellig	jent Capture	
 Advanced AP Groups 	APs currently in th	ne Group		Remove APs	Add APs	to the Group		Ad	d APs
	AP Name	Ethernet M	AC		AP Na	ame	Group Na	me	
	rtp9-31a-ap14	00:81:c4:96	5:78:28						
	rtp9-32a-ap20	00:81:c4:32	2:b9:b8						
	rtp9-32a-ap23	00:81:c4:96	5:74:10						

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.

ıılıılı cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller	General	
General	Name	RTP9-32A-WLC3
Icons	802.3x Flow Control Mode	Disabled 📀
Inventory	LAG Mode on next reboot	Enabled ᅌ
Interfaces	Broadcast Forwarding	Disabled 🗘
Interface Groups	AP Multicast Mode 1	Multicast 📀 239.1.1.9 Multicast Group Address
Multicast	AP IPv6 Multicast Mode ¹	Multicast 🗘 ff1e::239:100:100:21 IPv6 Multicast Group Address
Network Routes	AP Fallback	Enabled 📀
Fabric Configuration	CAPWAP Preferred Mode	ipv4 🔉
Redundancy	Fast SSID change	Enabled 🗘
Mobility Management	Link Local Bridging	Disabled 🗘
Ports	Default Mobility Domain Name	CTG-VoWLAN2
NTP	RF Group Name	RTP9-VoWLAN2
CDP	User Idle Timeout (seconds)	300
MIPv6	ARP Timeout (seconds)	300
Tunneling	ARP Unicast Mode	Disabled 📀
IPv6	Web Radius Authentication	PAP 🗘
mDNS	Operating Environment	Commercial (10 to 35 C)
Advanced	Internal Temp Alarm Limits	10 to 38 C
Lowful Interention	WebAuth Proxy Redirection Mode	Disabled 📀
Lawrul Interception	WebAuth Proxy Redirection Port	0
	Captive Network Assistant Bypass	Disabled 🗘
	Global IPv6 Config	Disabled 🗘
	Web Color Theme ²	Default ᅌ
	HA SKU secondary unit	Disabled ᅌ
	Nas-Id	RTP9-32A-WLC3
	HTTP Profiling Port	80
	DNS Server IP(Ipv4/Ipv6)	171.70.168.183
	HTTP-Proxy Ip Address(Ipv4/Ipv6)	0.0.0.0
	WGB Vlan Client	Disabled ᅌ
	1. Multicast is not supported with FlexC 2.Changes in Web color Theme will get	Connect on this platform. Multicast-Unicast mode does not support IGMP/MLD Snooping. Disable Global Multicast first. t updated after browser Refresh.

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

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

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.



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.

	cisco	<u>M</u> ONITOR	<u>W</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
С	ontroller	Static Mo	bility Gr	oup Members						
	General Icons	Local M	obility Gro	up CTG-VoWL	AN2					
	Inventory Interfaces	MAC Ad	dress	IP Address(Ipv4/I	pv6) Grou	p Name	M	liticast IP	Status	I
	Interface Groups	00:5d:7	3:1a:c3:49	10.81.6.70	CTG-	/oWLAN2	0.0	0.0.0	Up	
Þ	Multicast Network Routes									
*	Fabric Configuration Redundancy									
•	Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging									

Call Admission Control (CAC)

Admission Control Mandatory for Voice and Video should be disabled.

802.11a(5 GHz) > Media

Voice	Video	Media		
Call Ad	mission C	ontrol (C/	AC)	
Admiss	ion Control	(ACM)		Enabled
CAC M	ethod 4			Load Based v
Max R	Bandwidth	(5-85)(%)		85
Reserv	ed Roaming	Bandwidth (0-25)(%)	5
Expedi	ted bandwid	th		
SIP CA	C Support 3	!		Enabled
er-Cal	I SIP Ban	dwidth ²		
SIP Co	dec			G.711 ~
SIP Ba	ndwidth (kbj	os)		64
SIP Vo	ice Sample I	nterval (mse	cs)	20 ~
raffic	Stream M	etrics		



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



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**.

راریاں cısco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLL	ER W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile	e > New							
 Access Points All APs Radios Global Configuration 	RF Profile Radio Poli Use defau	Name cy lt RF Profile	ri E Template	p-5 302.11a 🗘 None		•			
Advanced									
Mesh									
AP Group NTP									
ATF									
RF Profiles									

On the **802.1**1 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.

ululu cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WI	RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile	> Edit	'rtp-5'							
Access Points	General	802.1:	1 RRM	Hig	h Density	Client	Distribution			
 Radios Global Configuration 										
Advanced	Data Rate	est	M	ICS S	ettings					
Mesh	6 Mbps	Disabled	٥	0	🗹 Supp	orted				
AP Group NTP	9 Mbps	Disabled	0	1	🗸 Supp	orted				
▶ ATF	12 Mbps	Mandato	ry ᅌ	2	🗹 Supp	orted				
RF Profiles	18 Mbps	Supporte	ed ᅌ	3	🗸 Supp	orted				
FlexConnect Groups	24 Mbps	Supporte	ed ᅌ	4	🗹 Supp	orted				
FlexConnect ACLs	36 Mbps	Supporte	ed ᅌ	5	🗸 Supp	orted				
FlexConnect VLAN	48 Mbps	Supporte	ed ᅌ	6	🗹 Supp	orted				
Templates	54 Mbps	Supporte	ed ᅌ	7	Supp	orted				
Network Lists				8	🗹 Supp	orted				
802.11a/n/ac/ax				9	🗹 Supp	orted				
802.11b/g/n/ax				10	Supp	orted				
Media Stream				11	🗹 Supp	orted				
Application Visibility				12	🗸 Supp	orted				
And Control				13	🗹 Supp	orted				
Lync Server				14	🗹 Supp	orted				
Country				15	🗹 Supp	orted				
Timers				16	Supp	orted				
Netflow		_	_		• •				_	
QoS										

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.

	cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMM	ANDS HE <u>L</u> P <u>F</u> EEDBACK
٧	Vireless	RF Profile > Edit 'rtp-5'	
	Access Points All APs Radios Global Configuration	General 802.11 RRM High Density Client Distribution	Coverage Hole Detection
1	Advanced	Maximum Davies Laviel Applements (10 to 20 dDm) 20	
	Mesh	Minimum Power Level Assignment (10 to 30 dBm) 30	Veice RCSI (-00 to -60 dBm) -80
ĺ	AP Group NTP	Power Threshold v1(-80 to -50 dBm) -70	Coverage Exception(0 to 100 %) 25
ſ	RE Profiles	Power Threshold v2(-80 to -50 dBm) -67	Coverage Level(1 to 200 Clients) 3
	FlexConnect Groups	DC4	Brofile Throshold For Trans
•	FlexConnect ACLs	Availa Savalar 40 laterfamore	
	FlexConnect VLAN Templates	Avoid Foreign AF interference E Enabled Channel Width 20 MHz 340 MHz 80 MHz 160 MHz 80+80 MHz Best	Interference (0 to 100%) 10 Clients (1 to 200) 12
	Network Lists		Noise (-127 to 0 dBm) -70
•	802.11a/n/ac/ax		Utilization (0 to 100 %) 80
•	802.11b/g/n/ax		Client Network Preference
•	Media Stream		Connectivity Throughput O Automatic
•	Application Visibility And Control		Client Aware
	Lync Server		Enable ODisable
	Country	High-Speed Roam	
	Timers	HSR mode End	abled
•	Netflow		
	QoS		

uluilu cisco	<u>M</u> ONITOR <u>W</u> LAI	Ns <u>C</u> ONTROLI	.er W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP <u>F</u> EEDBA	NCK
Wireless	RF Profile > Ec	dit 'rtp-5'						
All APs	General 8	02.11 RRM	High Densit	y Client D	Distribution			
Radios Global Configuration							Client Aware	o Di
Advanced	High-Speed Roa	im						0010
AP Group NTP	HSR mode					Enabled		
▶ ATF	Neighbor Time	eout Factor				5		
RF Profiles	DCA Channel	List						
FlexConnect Groups FlexConnect ACLs		36, 40, 44, 48 157, 161	, 52, 56, 60, 64, 14	9, 153,				
FlexConnect VLAN Templates	DCA Channels							
Network Lists				li.				
802.11a/n/ac/ax	Select Ch	annel						
Media Stream		36		l.				
Application Visibility And Control		44						
Lync Server		52						
Country Timers	Extended UNII	I-2 channels	Enabled					
▶ QoS								

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**.

ແມ່ນເມ່ນ cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	RF Profile	e > Edit	'rtp-5'						
 Access Points All APs Radios 	General	802.:	L1 RRM	High Density	Client I	Distribution			
Global Configuration Advanced	High De	nsity Pa	ameters	Multid	cast Paramo	eters			
Mesh AP Group NTP	Maximu Rx Son 1	m Clients(1	to 200) 200	Mult	icast Data Rate	es ² auto ᅌ			
ATF RF Profiles	Rx Sop Thresh	olde	Default ᅌ 0	Custom					

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.

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	FlexCon	nect Gro	oups > New						
 Access Points All APs Radios Global Configuration 	Group Na	ime rtp	-1						
Advanced									
Mesh									
AP Group NTP									
ATF									
RF Profiles									
FlexConnect Groups									

 cısco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> ONTRO	DLLER W <u>I</u> RELESS <u>S</u> ECURIT	Y M <u>A</u> NAGEMENT	C <u>o</u> mmands he <u>l</u> f	P <u>F</u> EEDBACK	
Wireless	FlexConnect Groups > E	dit 'rtp-1'				
 Access Points All APs Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates Network Lists 	General Local Authent Group Name VLAN Template Name Enable AP Local Authentication FlexConnect AP HTTP-Proxy Ip Address(Ipv4/Ipv6) Port	tication Image Upgrade rtp-1 none • on2 • Add	ACL Mapping	Central DHCP	WLAN VLAN mapping	WLAN AVC mapping
802.11a/n/ac/ax	AAA					
Media Stream Application Visibility And Control Lvnc Server	Server Ip Address Server Type Shared Secret Confirm Shared Secret	Primary 🗘				
Country	Port Number	1812				
Netflow	Add					
▶ QoS						

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

.ılı.ılı. cısco	MONITOR WLANS	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Wireless	FlexConnect Gro	oup AP List							
 Access Points All APs Radios Global Configuration 	Group Name			rtp-1					
Marked Advanced	FlexConnect APs								
Mesh AP Group NTP ATF	Add AP Entries 0 - 0 of 0			-		4-			
RF Profiles	AP MAC Address	AP Name	St	atus	AP Mo	ae	Туре	3	
FlexConnect Groups									
ululu cisco	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	r c <u>o</u> mmand:	S HELF	P <u>F</u> EEDBACK	
Wireless	FlexConnect Gr	oup AP List							
 Access Points All APs Radios Global Configuration 	Group Name			rtp-1					
Advanced	FlexConnect AP	1							
Mesh AP Group NTP	Add AP								
▶ ATF	Select APs from co	irrent controller							
RF Profiles FlexConnect Groups	Ethernet MAC		Add Car	icel					

Multicast Direct

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

.ı ı.ı ı. cısco	MC	ONITOR	<u>W</u> LANs	<u>C</u> ONTROLI	LER W <u>I</u> RELE	SS <u>S</u> ECURITY	MANAGEMEN	r c <u>o</u> mmands	HELP	<u>F</u> EEDBACK
Wireless	M	edia Str	eam >Ge	eneral						
 Access Points All APs Radios Global Configuration 	54	Multicast D	Direct featu	re	Enabled					
Advanced		Sercion or	nouncemer	nt State	Enabled					
Mesh		Session an	nounceme	nt URL						
AP Group NTP		Session an	nounceme	nt Email						
ATF		Session an	nounceme	nt Phone						
RF Profiles										
FlexConnect Group	ps	Session an	nounceme	nt Note						
FlexConnect ACLs							<u>III.</u>			
FlexConnect VLAN Templates										
Network Lists										
802.11a/n/ac/ax										
802.11b/g/n/ax										
 Media Stream General Streams 										
ululu cisco	<u>M</u> ONITO	R <u>W</u> LANs	<u>C</u> ONTROI	LLER WIRE	LESS <u>s</u> ecurit	Y M <u>A</u> NAGEMENT	C <u>o</u> mmands he	LP <u>F</u> EEDBACK		
Nireless	Media	Streams						Entries 1 - 1 of 1		
Access Points	Stream	Name				Start IP	Address(Ipv4/Ipv6) End IP Address(1	pv4/Ipv6) Operation Status
All APs Radios	10.195.1	19.27				239.1.1.1		239.1.1.1		Multicast Direct
Global Configuration										
Mech										
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.

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	TROLLER W <u>I</u> RELE	SS <u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'voice'						
WLANs Advanced	General Security Override Per-SSID Ba	QoS Policy-I ndwidth Contrac	Mapping Adv ts (kbps) <u>16</u>	vanced			
	Average Data Rate Burst Data Rate Average Real-Time Rate Burst Real-Time Rate Clear	DownStream L 0 0 0 0 0 0	JpStream 0 0 0 0				
	WMM Policy 7920 AP CAC 7920 Client CAC Media Stream Multicast Direct Lync Policy	Required C Enabled Enabled					
	Audio	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

cisco	MONITOR WLANS C	CONTROLLER W	IRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	Edit QoS Profile							
 Access Points All APs Radios Global Configuration 	QoS Profile Name	platinum For Voice Applicat	ions					
Advanced	Per-User Bandwidth	Contracts (kb	ns) *					
Mesh		DownStream	UpStre	am				
AP Group NTP	Average Data Rate	0	0					
RF Profiles	Burst Data Rate	0	0					
FlexConnect Groups	Average Real-Time Rate	e 0	0					
FlexConnect ACLs	Burst Real-Time Rate	0	0					
FlexConnect VLAN Templates	Per-SSID Bandwidth	DownStream	ps) * UpStre	am				
Network Lists	Average Data Rate	0	0					
🕨 802.11a/n/ac/ax	Burst Data Rate	0	0					
802.11b/g/n/ax	Average Real-Time Rate	e 0	0					
Media Stream	Burst Real-Time Rate	0	0					
Application Visibility And Control	WLAN QoS Paramete	ers						
Lync Server	Maximum Priority	voice	٥					
Country	Unicast Default Priority	besteffort	٥					
Timers	Multicast Default Priorit	besteffort	0					
Netflow	Wired QoS Protocol							
QoS Profiles Roles Qos Map	Protocol Type 802.1p Tag	802.1p ᅌ						

		ANI- (CECUDITY		COMMANIDE		FEEDBACK
Wireless	Edit QoS Pro	ofile		WIRELESS	SECORITY	MANAGEMENT	COMMANDS	пс <u>г</u> р	FEEDBACK
Access Points All APs Radios Global Configuration	QoS Profile N	lame	gold For Video App	lications					
Advanced	Description								
Mesh	Per-User Ban	dwidth	Contracts (kbps) *					
AP Group NTP			DownStre	am UpStre	am				
ATF	Average Data	Rate	0	0					
RF Profiles	Burst Data Rat	te	0	0					
FlexConnect Groups	Average Real-1	Time Rat	e 0	0					
FlexConnect ACLs	Burst Real-Tim	ne Rate	0	0					
FlexConnect VLAN Templates	Per-SSID Ban	ndwidth	n Contracts ((kbps) *	am				
Network Lists	Average Data	Rate	0		um				
🕨 802.11a/n/ac/ax	Burst Data Rat	te	0	0					
802.11b/g/n/ax	Average Real-	Time Rat	e 0	0					
Media Stream	Burst Real-Tim	ne Rate	0	0					
Application Visibility And Control	WLAN QoS Pa	aramet	ers						
Lync Server	Maximum Prior	rity	video	٢					
Country	Unicast Defaul	t Priority	video	٥					
Timers	Multicast Defau	ult Priorit	y video	٢					
Netflow	Wired OoS Pr	otocol							
▼ QoS	Protocol Type		802.1p	٥					
Profiles Roles	802.1p Tag		4]					
Qos Map									
lili. cisco	<u>m</u> onitor <u>w</u>	LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
uluulu cisco Wireless	<u>M</u> ONITOR <u>W</u>	LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
· I I I I CISCO Wireless ▼ Access Points	MONITOR W	LANs ofile	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
CISCO Wireless Access Points All APs Addise	MONITOR W Edit QoS Pro QoS Profile N	LANs ofile Name	<u>C</u> ONTROLLER silver	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
CISCO Wireless Access Points All APs Radios Global Configuration	MONITOR W Edit QoS Pro QoS Profile N Description	LANs ofile Name	<u>CONTROLLER</u> silver For Best Effo	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
CISCO Wireless All APs Radios Global Configuration Advanced	MONITOR W Edit QoS Pro QoS Profile N Description	LANs ofile Name	<u>CONTROLLER</u> silver For Best Effo	WIRELESS	SECURITY	MANAGEMENT	C <u>o</u> mmands	HELP	<u>F</u> EEDBACK
CISCO Wireless Access Points All APs Radios Global Configuration Advanced Mesh	MONITOR W Edit QoS Pro QoS Profile M Description Per-User Bar	LANs ofile Name ndwidt	<u>C</u> ONTROLLER silver For Best Effo	WIRELESS rt (kbps) *	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
CISCO Wireless All APs Cobal Configuration Advanced Mesh A D Group NTP	MONITOR W Edit QoS Pro QoS Profile N Description Per-User Bar	LANs ofile Name ndwidt	CONTROLLER silver For Best Effo h Contracts DownStr	w <u>I</u> RELESS rt (kbps) * eam UpStr	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
CISCO Wireless All APs Addios Global Configuration Advanced Mesh AP Group NTP ATF	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data	LANs ofile Name ndwidt	CONTROLLER silver For Best Effo h Contracts DownStr 0	vireless rt (kbps) * eam UpStr	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
CISCO Wireless All APs Adios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra	LANs ofile Name ndwidt	CONTROLLER silver For Best Effo h Contracts DownStr 0 0	WIRELESS rt (kbps) * eam UpStr 0 0		MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Ilinilin CISCO Wireless Access Points All APs Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups	MONITOR M Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real-	LANS ofile Name ndwidt Rate ate -Time Ra	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 0	vireless rt (kbps) * eam UpStrr 0 0 0	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Iliiilii CISCO Wireless Access Points All APs Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect ACLs	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tim	LANS ofile Name ndwidti Rate ate -Time Ra me Rate	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 0 0	vireless rt (kbps) * eam UpStrr 0 0 0 0 0	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Ilinilin CISCO Wireless Access Points All APs Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect VLAN Templates	MONITOR W Edit QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tim	LANS ofile Name ndwidt Rate ate -Time Ra me Rate ndwidt	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Ilinilin CISCO 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	MONITOR W Edit QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Bar	LANS ofile Name ndwidtl Rate -Time Ra me Rate ndwidt	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Ilinitic CISCO 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	MONITOR W Edit QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Bar Average Data	LANS ofile Name Rate te -Time Ra te ndwidt	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	<u>SECURITY</u>	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
 IIIIIII CISCO Wireless Access Points All APs Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect VLAN Templates Network Lists 802.11a/n/ac/ax 802.11b/g/n/ax 	MONITOR W Edit QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tir Per-SSID Bar Average Data Burst Data Ra Average Real-	LANS ofile Name Rate te Time Ra Rate Rate Rate te	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	eam	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
I I I I I I I CISCO 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	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tir Per-SSID Bar Average Data Burst Data Ra Average Real- Burst Real-Tir	LANS ofile Name Adwidt Rate ate -Time Ra me Rate ate -Time Ra me Rate	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 te 0 0 0 th Contracts DownStr 0 0 0 te 0 0 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	eam	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Ilinitic CISCO 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	MONITOR W Edit QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Ban Average Data Burst Data Ra Average Real- Burst Real-Tin Burst Real-Tin	LANS ofile Name Adwidti Rate ate Time Ra Rate ate Time Ra me Rate date	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
 I I I I I I CISCO 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 	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Ban Average Data Burst Data Ra Average Real- Burst Real-Tin WLAN QOS P Maximum Prior	LANS ofile Name Adwidti Rate ate Time Ra me Rate ate Time Ra me Rate data Time Ra	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 te 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	eam	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Ilinilin CISCO 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 Media Stream Application Visibility And Control Lync Server Country	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Bar Average Data Burst Data Ra Average Real- Burst Real-Tin WLAN QOS P Maximum Pric Unicast Defau	LANS ofile Name Rate ate -Time Ra me Rate ate -Time Ra me Rate ate -Time Ra me Rate ate -Time Ra	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 te 0 0 0 te 0 0 0 te 0 0 0 0 0 0 0 0 0 0 0 0 0	rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	eam	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
 I I I I I I CISCO 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 	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Bar Average Data Burst Data Ra Average Real- Burst Data Ra Average Real- Burst Real-Tin WLAN QOS P Maximum Pric Unicast Defau	LANS ofile Name Rate ate -Time Ra me Rate ate -Time Ra me Rate ate -Time Ra me Rate data -Time Ra me Rate ate	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 te 0 0 th Contracts DownStr 0 0 te 0 0 te 0	rt (kbps) * eam UpStr 0 0 0 (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	eam	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
 I I I I I I CISCO Wireless Access Points All APs Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups 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 	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Bar Average Real- Burst Data Ra Average Real- Burst Data Ra Average Real- Burst Real-Tin WLAN QOS P Maximum Pric Unicast Defau Multicast Defau	LANS ofile Name Rate ate -Time Ra me Rate ate -Time Ra me Rate ate -Time Ra use rate ority alt Priority	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 te 0 0 te 0 0 te 0 0 te 0 te 0 0	WIRELESS rt (kbps) * eam UpStr 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ort © ort © ort ©	eam	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
 I I I I I I CISCO 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 	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tin Per-SSID Bar Average Data Burst Data Ra Average Real- Burst Real-Tin WLAN QOS P Maximum Pric Unicast Defau Multicast Defau	LANS ofile Name Rate ate -Time Ra me Rate -Time Ra me Rate -Time Ra me Rate -Time Ra user -Time Ra ste -Time Ra -Time Ra	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 te 0 0 te 0 0 ters besteffo y besteffo ity besteffo I	wireless rt (kbps) * eam UpStr 0 0	eam	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
 I I I I I I I CISCO Wireless Access Points All APs Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups 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 	MONITOR W Edit QoS Profile N QoS Profile N Description Per-User Bar Average Data Burst Data Ra Average Real- Burst Real-Tir Per-SSID Bar Average Real- Burst Real-Tir WLAN QOS P Maximum Pric Unicast Defau Multicast Defau	LANS ofile Name Rate Time Ra Rate Time Ra Rate Time Ra Rate Time Ra Rate Time Ra Rate Time Ra Rate Time Ra Rate Rate Rate Rate Rate Rate Rate Ra	CONTROLLER silver For Best Effo h Contracts DownStr 0 0 0 te 0 0 0 ters besteffo y besteffo ity besteffo 1 802.1p 0	WIRELESS rt (kbps) * eam UpStr 0 0	eam	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK

	ဂျကျက cisco	<u>M</u> ONITOR <u>W</u> L	ANs g		WIREL	ESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEED
W	ireless	Edit QoS Pro	file								
•	Access Points All APs Radios Global Configuration	QoS Profile N	ame	bronze For Backgrour	ıd						
Þ	Advanced	Per-User Ban	dwidtł	Contracts (
	AP Group NTP			DownStre	am Up	Strea	m				
1	ATE	Average Data	Rate	0	0						
ŗ.,		Burst Data Rat	e	0	0						
	RF Profiles	Average Real-1	rime Rat	e 0	0						
	FlexConnect Groups	Burst Real-Tim	e Rate	0	0						
×	FlexConnect ACLs										
	FlexConnect VLAN Templates	Per-SSID Ban	dwidt	h Contracts (DownStre	(kbps) am Ui	* oStrea	m				
	Network Lists	Average Data	Rate	0	0						
Þ	802.11a/n/ac/ax	Burst Data Rat	e	0	0						
Þ	802.11b/g/n/ax	Average Real-1	Time Rat	e 0	0						
Þ	Media Stream	Burst Real-Tim	e Rate	0	0						
Þ	Application Visibility And Control	WLAN QoS Pa	ramet	ers							
	Lync Server	Maximum Prior	rity	backgrou	ınd ᅌ						
	Country	Unicast Default	t Priority	backgrou	ınd ᅌ						
	Timers	Multicast Defau	ult Priori	backgrou	ınd ᅌ						
Þ	Netflow	Wired QoS Pr	otocol								
*	QoS	Protocol Type		802.1p	0						
	Profiles Roles Oos Map	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.

،،ا،،،ا،، cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBAG	ск
Security	Advance	d EAP								
AAA	Identity R	tequest Tim	neout (in secs)						30	
General ▶ RADIUS	Identity r	equest Max	Retries						2	
▶ TACACS+	Dynamic	WEP Key Ir	ndex						0	
LDAP Local Net Users	Request 1	limeout (in	secs)						30	
MAC Filtering	Request M	1ax Retries							2	
 Disabled Clients User Login Policies 	Max-Logi	n Ignore Id	entity Response						enable	٥
AP Policies	EAPOL-Ke	ey Timeout	(in milliSeconds)						400	
Password Policies	EAPOL-Ke	ey Max Retr	ries						4	
Local EAP	EAP-Broa	dcast Key I	interval(in secs)						3600]
Advanced EAP										

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

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

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.

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FE	EDBACK
Security	Rogue Policies	
 AAA General General RADIUS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Pasword Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists General Wireless Protection Policies General Certain Certain Certain Central Certain Central Central	Rogue Detection Security Level Low High Cri Rogue Location Discovery Protocol Disable © Expiration Timeout for Rogue AP and Rogue Client entries 1200 Seconds Validate rogue clients against AAA Enabled Validate rogue clients against MSE Enabled Detect and report Ad-Hoc Networks © Enabled Rogue Detection Report Interval (10 to 300 Sec) 10 Rogue Detection Transient Interval (0, 120 to 1800 Sec) 0 Rogue Client Threshold (0 to disable, 1 to 256) 0 Rogue Client Threshold (0 to disable, 1 to 256) 0 Rogue containment automatic rate selection Enabled	tical 💽 Custom
Regue Rules Friendly Regue Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection Web Auth TrustSec Local Policies Umbrella Advanced	Auto Containment Level 1 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.

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

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).

2 Search Menu Items	Configuration * > Radio Configurations * > Network	
Dashboard	5 GHz Band 2.4 GHz Band	
) Monitoring	General	
Configuration >	2.4 GHz Network Status	
Administration >	Please disable 2.4 GHz Network Status to configure 802.11g Network Status, Beacon Interval, Short Preamble, Fragmentation Threshold, DTPC Support.	
	802.11g Network Status	
	Beacon Interval* 100	
	Short Preamble	
	Fragmentation 2346 Threshold(bytes)*	
	DTPC Support	
inatinatinatinati Sectores di stati	CCX Location Measurement	
	Mode 🗸	
n da da da da ja Tradicial calcado	Interval* 60	
	Data Rates	
	Please disable 2.4 GHz Network Status to configure Data Rates	
	1 Disabled v 2 Disabled v 5.5 Disabled v	
	6 Disabled v 9 Disabled v 11 Disabled v	
trastrastrastrast 1. dz. dz. dz. dz. dz.	12 Mandatory v 18 Supported v 24 Supported v	
inatrainaina 1980 - Statistica	36 Supported v 48 Supported v 54 Supported v	

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 Cat	alyst 9800-40 Wireless	Controller Welcome al	pha 🖌 🏀 🛱 🕅	Image: Search AP	and Clients Q
	Configuration - > Radio Co	onfigurations • > High Throu	ıghput		
Dashboard	5 GHz Band 2.4 GHz	Band			
Monitoring >					
	❤ 11n				
() Administration >	Ena	ble 11n 🔽		Select All	
X Troubleshooting	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate)	MCS/(Data Rate	»)
	_0/(7Mbps)	[]/(14Mbps)	2/(21Mbps)	3/(29Mbps)	
	4/(43Mbps)	58Mbps)	65Mbps)	/(72Mbps)	
	8/(14Mbps)	(29Mbps)	0/(43Mbps)	1/(58Mbps)	
	2/(87Mbps)	3/(116Mbps)	[]4/(130Mbps)	5/(144Mbps	
	6/(22Mbps)	7/(43Mbps)	8/(65Mbps)	9/(87Mbps)	
	20/(130Mbps)	21/(173Mbps)	22/(195Mbps)	23/(217Mbps	li -
	24/(29Mbps)	25/(58Mbps)	26/(87Mbps)	27/(116Mbps	
	28/(173Mbps)	29/(231Mbps)	30/(260Mbps)	31/(289Mbps	
	Enable 13:	ac	Interval	Select All	
		22/1/02	2011/22	20/1/00	
	1/8/(86 7Mbps)	SS/MCS	SS/MCS	SS/MCS	
	3/8/(260.0Mbps)	✓ 1/9/(1/8) ✓ 3/9/(288.9Mbps)	4/8/(346.7Mbps)	4/9/(n/a)	
	✓ 11ax				
	Enable 11	ax 🔽		Select All	
	Multiple	sid			
	SS/MCS	SS/MCS	SS/MCS	SS/MCS	
	[]/7	V 1/9	✓ 1/11	2/7	
	2/9	2/11	3/7	3/9	
	3/11	4/7	4/9	4/11	
	5/7	5/9	5/11	6/7	
	-6 /9	6/11	7/7	7/9	
	3/11	8/7	8/9	8/11	
				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.

Cisco Cata	llyst 9800-40 Wireless Controller Welcome alpha 🛛 🌴 🐑 🖺 🏶 🔞 🥹 🌫 Search Alb and	Cilents Q
Q Search Meriu Items	Configuration - > Radio Configurations - > Parameters	
Dashboard	5 GHz Band 2.4 GHz Band	
) Monitoring	TROA Development	Apply
Configuration >		
Administration >	EDCA Profile optimized-video-v_ •	
C Troubleshooting	JP3 (602.111)	
	DTPC Support is enabled. Please disable it at Network to configure Power Constraint	
	Power Constraint* 0	
	Channel Switch 🔽 Status	
	Channel Switch Announcement Mode	
	Smart DFS	

RRM

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

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

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

Cisco Cata	lyst 9800-40 Wireless Controller	Welcome alpha		C Search APs and Clients Q
Q. Search Menu Items	Configuration - > Radio Configurations - > R	RM		
Dashboard	5 GHz Band 2.4 GHz Band FRA			
Monitoring >	General Coverage DCA TPC	RF Grouping		
🔧 Configuration 🛛 >	Power Assignment Method		Power Assignment Leader	RCDN6-21A-WLC5 (10.201.81.9)
() Administration >			Transmit Power Update Interval	600 second(s)
* Troubleshooting	 Automatic 		Last Run:	365 second(s) ago
	On Demand		Power Neighbor Count:	3
못가 잘 많이 많이?	Fixed			
	Max Power Level Assignmen 17			
	Min Power Level Assignmen 11			
	Power Threshold* -70			

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.

CISCO Cisco Cata	alyst 9800-40 Wireless Contro	Nier vveicome alpha 🕋 🐨 🖻 🗭 🖳 😡 🤅	Search Avs and Clients Q
Q Search Menu Items	Configuration * > Radio Configurati	ons* > RRM	
Dashboard	5 GHz Band 2.4 GHz Band	FRA	
) Monitoring >	General Coverage DC	TPC RF Grouping	
Configuration >	Dynamic Channel Assignmen	Algorithm	
Administration >	-,		
Troubleshooting	Channel Assignment Mode	Automatic	
		O Preeze Invoke Creames Update Onde	
	Anchortime		
	Avoid Foreign AP Interference		
	Avoid Cisco AP load		
	Avoid Non 5 GHz Noise		
	Avoid Persistent Non-wifi Interference		
	Channel Assignment Leader	RCDN6-21A-WLC5 (10.201.81.9)	
	Last Auto Channel Assignment	475 second(s) ago	
	DCA Channel Sensitivity	medium	
	Channel Width	O 20 MHz 0 40 MHz 0 80 MHz 160 MHz Best	
	Auto-RF Channel List		
	Image: Constraint of the state Image:	V V V	
	Ido 144 149 153 157 161 165		
	Event Driven RRM		
	EDRRM		

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

2 Search Menu Items	Configuration * > Radio Configurat	ions* > RRM	
Dashboard	5 GHz Band 2.4 GHz Band	FRA	
) Monitoring >	General Coverage DC	A TPC RF Grouping	
Configuration >	Dynamic Channel Assignmen	t Algorithm	
} Administration →	Channel Assignment Mode	Automatic Freeze Invoke Channel Update Once Off	
	Interval	10 minutes •	
	Avoid Foreign AP Interference		
	Avoid Cisco AP load		
	Avoid Non 5 GHz Noise		
	Avoid Persistent Non-wifi Interference		
	Channel Assignment Leader	RCDN6-21A-WLC5 (10.201.81.9)	
	Last Auto Channel Assignment	531 second(s) ago	
	DCA Channel Sensitivity	medium	
	Auto-RF Channel List		
	9 10 11		
	Event Driven RRM		

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.

Cisco Cata	Configuration - 2 W	ess Controller Edit Radios 5 GHz Ban	Welcome <i>alpha</i> 🖌 🐔 🦷	6 0 0 0 0 C	Search APs and Clients Q	
Q Search Menu Items	✓ All Access Pe	Configure Detail		RF Channel Assignmer	nt	
Monitoring >	Number of AP(s): 1	AP Name	rcdn6-22a-ap1	Current Channel	149	
Configuration >	AP ~ AP Name Model	Admin Status		Channel width	40 MHz v	
() Administration >	rcdn6-22a- ap1 AIR- AP380	CleanAir Admin Status		Assignment Method	Global	
X Troubleshooting	H H 1 ⊨	Antenna Parameters		Tx Power Level Assignment		
	-	Antenna Type	Internal v	Current Tx Power Level	2	
	✓ 5 GHz Radio:	Antenna Mode	Omni	Assignment Method	Global	
	Number of AP(s): 1	Antenna A				
	AP v Slot Name No	Antenna B				
	rcdn6-22a- 1	Antenna C				
	≪ ≺ 1 ≻	Antenna D				
	> 2.4 GHz Radi	Antenna Gain	10			
	> Dual-Band R	Download Core Dump to b	bootflash			
	> Country					
	> LSC Provisio					
		'D Cancel			Update & Apply to Device	

CleanAir

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

Cisco Catal	lyst 9800-40 Wireless C	Controller	Welcome alpha	*		C Search APs and Cile	A A
Q Search Menu Items	Configuration - > Radio Con	figurations - >	CleanAir				
🔜 Dashboard	5 GHz Band 2.4 GHz B	and					
Monitoring >	General Trap Configu	uration					
Configuration >	Enable Cleanáir						
() Administration >	Enable SI						
% Troubleshooting	Report Interferers						
경영동 관광장	Persistent Device Propagation						
	Available Interference Types	Inte to e	erference Types detect				
		> Jam Con < DEC Vide	Transmitter imer tinuous Transmitter T-like Phone to Camera				

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 Esrepsso 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.

	Configuratio	on*> Tag	s & Profiles	• >	General Security Adva	nced		
Dashboard	- Add			WLAP	Layer2 Layer3 AAA			
Monitoring >	Number of W	LANs select	ed : 0					
Configuration >	Status	Name	v	ID	Layer 2 Security Mode	WPA + WPA2 +	Fast Transition	Enabled
Administration >	0	Voice		1 <	MAC Filtering		Over the DS	
roubleshooting	H 4 1	P H	10 .	z tems p	Protected Management Frame		Reassociation Timeout	20
roubloomooung	There are a				PMF	Disabled •		
					WPA Parameters			
					WPA Policy			
					WPA2 Policy			
					WPA2 Encryption	AES(CCMP128)		
						GCMP256		
					MPSK			
					Auth Key Mgmt	802.1x		
						PSK		
						CCKM		
						FT + PSK		
						802.1x-SHA256		
						PSK-SHA256		

	Configuratio	on * > Tags &	Profiles * >	Edit WLAN			
	-			General Security Adva	anced		
Dashboard	- A63			Layer2 Layer3 AAA			
Monitoring >	Number of W	LANs selected :	D		1104 - 11040		
Configuration >	Status-	Name	~ ID	Layer 2 Security Mode	WPA + WPA2 ¥	Fast Transition	Enabled v
	•	Voice	1	MAC Filtering		Over the DS	
Administration >	•	Data	2	Protected Management Frame		Reassociation Timeout	20
Troubleshooting	. H . A . 1	- H - [10 🔹 items p				
				PMF	Disabled +		
				WPA Parameters			
				WPA Policy			
				WPA2 Policy			
				WPA2 Encryption	AES(CCMP128)		
					GCMP128		
					GCMP256		
				MPSK			
				Auth Key Mgmt	802.1x		
					PSK		
					CCKM		
					FT + 802.1x		
					FT + PSK		
					802.1x-SHA256		
					PSK-SHA256		
				PSK Format	ASCII		

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 enabled 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.

Cisco Ca	talyst 9800-40 Wireless Controller		Welcome alpha 🛛 🕷 🤻	8080	2 Search Afra and Chemp Q
Q Search Manu Items	Configuration * > Tags & Profiles * > WLANs	Edit WLAN			3
		General Security	Advanced		
Dashboard	Ast Device English WLAN Disable WLAN	Coverage Hole Detection		Universal Admin	
Monitoring >	Number of WLANs selected : 0	Aironet IE		Load Balance	D
🔍 Configuration 💦 >	Status - Name - ID - SSID	P2P Blocking Action	Disabled	Band Select	
ি Administration	O Voice 1 voice	Multicast Buffer	DISABLED	IP Source Guard	
M Troublesheating	Data 2 diata	Media Stream Multicast-	2	WMM Policy	Required +
3 Iroubleshooting	in a r r r i lo r nems per page			mDNS Mode	Bridging +
		max crient Connections		Off Channel Sca	nning Defer
		Per WLAN 0			
		Per AP Per 0		Defer Priority	0 1 2
		Per AP Radio 200			3 🔽 4 🗹 5
		Per WLAN			6 7
		11v BSS Transition Support	ort	Scan Defer [100
		BSS Transition		Assisted Roami	ng (11k)
		Disassociation Imminent(0 to 3000 TBTT)	200		1.0
		Optimized Rosming	40	Prediction Optimization	
		Disassociation Timer(0 to 40 TBTT)		Neighbor List	
		BSS Max Idle Service		Dual Band Neighbo List	or 🗌
		BSS Max Idle Protected		DTIM Period (in	hearon intervale)
		Directed Multicast Service		Dian Ferror (in	ocacon more analy
		11ax		5 GHz Band (1-25	5) 2
				2.4 GHz Band (1-2	2
		Downlink OFDMA			
		Linink OFDMA	(v)		
		"D Cancel			Update & Apply to Device
	•				

Policy Profiles

Policy Profiles are used to define additional settings regarding access, QoS, Mobility, and advanced settings. Policy Profiles are then mapped to a WLAN Profile via a Policy Tag, which then can be applied to an access point. Ensure the **Status** of the policy profile is **Enabled**.

Cisco Catalyst 9800-40 Win	eless Controller We	elcome alpha 🛛 希 🕏 🖺	🔅 🕅 🛛 📿 Search /	APs and Clients Q
Q Search Menu Items	General Access Policies	s QOS and AVC Mobilit	y Advanced	~
Dashboard + Add × Dek	A Configur	ing in probled state will reput in large	of connectivity for alignta appopiated y	with this profile
Monitoring > Status > Pol	Conigui	ing in enabled state will result in loss	or connectivity for clients associated v	vitri tilis prome.
Configuration >	Name*	Voice	WLAN Switching Policy	1
(○) Administration >	Description	Enter Description	Central Switching	
Troubleshooting	Status	ENABLED	Central Authentication	
	Passive Client	DISABLED	Central DHCP	
	Encrypted Traffic Analytics	DISABLED	Central Association	
	CTS Policy		Flex NAT/PAT	DISABLED
	Inline Tagging			
	SGACL Enforcement	2_65510		
	Default SG1	2-03313		
있는 것은 이상 가장에 있다.				
	Cancel			Update & Apply to Device

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

Cisco Catalyst 9800-40 Wi	reless Controller Welco	me alpha 🛛 🎢 📢 🖺 🕻	0 0	2 Search	APs and Clients Q	•
Q Search Menu Items	Edit Policy Profile					×
	General Access Policies	QOS and AVC Mobility	Advanced			
Dashboard + Add × D	RADIUS Profiling			WLAN ACL		
Monitoring > Status > I	Local Subscriber Policy Name	Search or Select 🔹		IPv4 ACL	Search or Select	•
Configuration >	WLAN Local Profiling			IPv6 ACL	Search or Select	•
(○) Administration → □ ⊘ a	Global State of Device Classification	Disabled (i)		URL Filters		
Troubleshooting	HTTP TLV Caching			Pre Auth	Search or Select	•
	DHCP TLV Caching			Post Auth	Search or Select	•
	VLAN					
	VLAN/VLAN Group	VLAN0500				
	Multicast VLAN	Enter Multicast VLAN				
	'D Cancel				🗄 Update & Apply	/ to Device

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

Q Search Menu Items	Configuration - >	Edit Policy Profile				
		General Acc	ess Policies QOS and A	AVC Mobility	Advanced	
		Auto QoS	None 🔻		Flow Monite	or IPv4
() Monitoring >	Status v F	QoS SSID Policy			Egress	Search or Select
Configuration >		Egress	platinum 🗙 🔻		Ingress	Search or Select
Administration >	□ Ø ¢	Ingress	platinum-up × v		Flow Monite	or IPv6
Troubleshooting	H 4 1 H	QoS Client Policy	1		Egress	Search or Select
n ing ing ing ing ing ing ing ing ing in		Egress	Search or Select		Ingress	Search or Select
		Ingress	Search or Select			
		SIP-CAC				
		Call Spooping				
		Send Disassociate				
i ha ha ha ha he		Send 486 Busy				
lie lie lie lie lie wood lie on lie sy						

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.

Q Search Menu Items	Configuration • >	Edit Policy Profile			
		General Access Policies	QOS and AVC Mobil	ity Advanced	
B Dashboard		WLAN Timeout		Fabric Profile	Search or Select
) Monitoring >	Status v	Session Timeout (sec)	86400	Umbrella Parameter Man	Not Configured
Configuration >		ldle Timeout (sec)	300	mDNS Service	default-mdns-servici
Administration >		c Idle Threshold (bytes)	0	Policy	Clear
Sector Troubleshooting	H 4 1 +	Client Exclusion Timeout (sec)	60	WLAN Flex Policy	r I
, ,		DHCP		VLAN Central Switch	ning
e - Mar Mer - Mar Mer - Mar a se tan se tan se tan se tan		IDud DHCD Required		Split MAC ACL	Search or Select
전 동안에 동안이 동안이 동안이 동안 19 - 전화 도인화 도인화 도인화		DHCP Server IP Address		Air Time Fairness	Policies
		Show more and		2.4 GHz Policy	Search or Select
		Show more FFF		5 GHz Policy	Search or Select
e star star star star star		AAA Policy		,,	
		Allow AAA Override			
		NAC State			
		Policy Name	default-aaa-policy x v		
n stán selen stán selen selen 1. svýt svýt svýt svýt se		Accounting List	Search or Select		

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

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.

		Cisco Catal 6.12.2s	yst 9800-40	Wireless Controller	۷	Velcome <i>alpha</i>	*	• • • • •	C	Q
	2, Search Menu Item		Configuration +	Tags & Profiles - > RF						
bac	Dashboard		+ Add							
C) Monitoring	>	State v	RF Profile Name	~	Band	×	Description		~
2	Configuratio	n >	•	Low_Client_Density_rf_5gh		5 GHz		pre configured Low Client D	lensity rf	
			•	High_Client_Density_rf_5gh		5 GHz		pre configured High Client	Density r	
Ś	Administratio	on >	Add RF Profile						×	
X	7 Troubleshoo	ting	General	302.11 RRM Advan	ced					
			Name*	Enter Name						
			Radio Band	5 GHz Band	•					1 - 6 of 6 items
			Status	DISABLE						
			Description	Enter Description	a a					
			ື Cancel					Apply to	Device	

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.

Cisco Catalyst 98	800-40 Wireless Controller	Welcome alpha	🌾 🖺 🕸 🔞 🕢 💭 Standt Affand Cherth Q
Q. Search Meria Itoms	uration * > Tags & Profiles * > RF		
Dashboard	dd X Defeta		
Monitoring >	State v RF Profile Name	v Band	 Description
	C Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf
	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r
Administration > Add R	F Profile		×
% Troubleshooting	neral 802.11 RRM Advanced	d	
Оре	erational Rates	802.11n MCS Rat	les
6 Mt	Disabled •	Enabled Data Rates:	1 - 6 of 6 itoms -
9 Mt	Disabled 🔻	[0,1,2,3,4,5,6,7,8,9,10,1	11,12,13,14,15,16,17,18
12 M	Mandatory v	,19,20,21,22,23,24,25,2	26,27,28,29,30,31]
18 M	Ibps Supported v	Enable MCS I	Index v
24 N	Supported +	o	
36 N	Ibps Supported v	✓ 1	
48 N	fbps Supported v	2	
54 N	tops Supported +	3	
		4	
		5	
		6	
		7	
		8	
		9	

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

Cisco Catalyst 9800-40 Wireless Cont	troller Welcome alpha 🖌 🕷 🖺 🏟 🕲 🕫 🕄 Touch fin and Cares 🔍 🗌 Թ
Q. Sebrch Menu Imma	r+> RF
Dashboard	
Monitoring State RF Profile Name	v Band v Description v
Configuration	rf_Sgh S GHz pre configured Low Client Density rf
Administration Add RF Profile	rf_Sgh 5 GHz pre configured High Client Density r
Ceneral 802.11 RRM	Advanced
General Coverage TPG	C DCA
Coverage Hole Detection	1 - 6 of 6 items
Minimum Client Level (clients)*	3
Data RSSI Threshold (dBm)*	-80
Voice RSSI Threshold (dBm)*	-80
Exception Level (A)	
D Cancel	🗎 Apply to Device
Cisco Catalyst 9800-40 Wireless Cont	troller
Q. Search Manulterra	• > RF
Dashboard + Add	
Monitoring State RF Profile Name	✓ Band ✓ Description ✓
Configuration	rf_5gh 5 GHz pre configured Low Client Density rf
Administration Add RF Profile	rf_5gh 5 GHz pre configured High Client Density r X
General 802.11 RRM	Advanced
General Coverage TPC	C DCA
Transmit Power Control	1 - 6 of 6 items
Maximum Power Level(dBm)*	30
Minimum Power Level(dBm)*	-10
Power Threshold V1(dBm)*	-70
Cancel	🔛 Analysis Departure
CISCO Catalyst 9800-40 Wireless Co	
Q. Satich Menu Items	(3*) RF
Dashboard	
Monitoring State RF Profile Name	V Band V Description
Configuration	y_rf_5gh 5 GHz pre configured Low Client Density rf hy_rf_5gh 5 GHz pre configured High Client Density r
Administration > Add RF Profile	×
Ceneral 802.11 RRM	Advanced
General Coverage T	
Dynamic Channel Assignment	nt 3 - 6 of 6 items
Avoid AP Foreign AP Interference	
Channel Width	
DUA Channels	26 4 4 48 52 6 0 64 100 104 108 112 116 120 124 v v v v v v v v v
High Speed Boam	128 132 136 140 144 149 153 157 161 165
Mode Enable	
Neighbor Timeout*	5
Client Network Preference	Default
"D Cancel	Apply to Device

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

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

Cisco Cata	lyst 9800-40 Wireless Contro	oller Welcome alpha	5 0 Ø Ø Ø Ø Ø	APs and Clerite Q
Q Search Menu Items	Configuration • > Tags & Profiles •	> RF		
Dashboard	+ Add A Delete			
Monitoring >	State v RF Profile Name	 ✓ Band 	 Description 	~
	Low_Client_Density_rf_	5gh 5 GHz	pre configured Low Client Density rf	
	High_Client_Density_rf_	5gh 5 GHz	pre configured High Client Density r	
205 Administration >	Add RF Profile		*	
💥 Troubleshooting	General 802.11 RRM	Advanced		
	High Density Parameters			
	Max Cliante*	200		
	Multicast Data Rate (Mbps)	Auto		
	Rx Sop Threshold (dbm)	auto		
	Client Distribution			
·	Load Balancing Window*	5		
	Load Balancing Denial Count*	3		
	ATE Configuration			
et al esta de la companya de la comp	···· comgutation			
	Status	DISABLED		
	Bridge Client Access	DISABLED		
	Airtime Allocation	5		
	FRA			
	Client Aware			

Flex Profiles

Flex Profiles are used to define the settings the access point should use when in Flexconnect mode. Flex Profiles are then mapped to a Site Tag, which then can be applied to an access point. Configure the **Native VLAN ID** for the access point to use as well as the allowed VLANs.

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

Enable Local Authentication as necessary.

	Kinu Itema	guration • > Tags & Profiles •	> Flex		
ashb	oard	Add X Delets			
loni	Add Flex Profile				×
onf	General Local A	Authentication Policy ACL	VLAN		•
dmi	Name*	Enter Name	Fallback Radio Shut		
roul	Description	Enter Description	Flex Resilient		
	Native VLAN ID	1	ARP Caching		
	HTTP Proxy Port	0	Efficient Image Upgrade		
	HTTP-Proxy IP Address	0.0.0	Office Extend AP		
	CTS Policy		Join Minimum Latency		
	Inline Tagging				
	SGACL Enforcement				
	CTS Profile Name	default-sxp-profile x			

Tags

Policy Tag

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

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

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

Cisco Catalyst 9800-40	Wireless Controller Well	come alpha 🛛 🗥 🕏 🖺	🗘 🖄 🛛 📿 Search	APs and Clients Q
Q Search Menu Items	> Tags & Profil Edit Policy Tag			×
Dashboard Policy S	Site RF A	s may result in loss of connectivity for	some clients that are associated	to APs with this Policy Tag.
Monitoring > + Add	× Delete Name*	default-policy-tag		
Configuration >	ag Name	default policy-tag		
Administration → default-p	oolicy-tag 🗸 🗸 WLAN-PO	LICY Maps: 2		
₩ 4 1	▶ ₩ 10 - Add × I			
	WLAN Profile		v Policy Profile	~
	Data		Data	
	Voice		Voice	
le de de de di	∺ ∢ 1 >	► 10 v items per page		1 - 2 of 2 items
for the for the for the	Map WLAN and	Policy		
	WLAN Profile*	Voice 💌	Policy Profile*	Voice
			× .	
	RLAN-POI	ICY Maps: 0		
	'S Cancel			Update & Apply to Device

Site Tag

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

Site Tags are then applied to an access point to specify which AP Join Profile and Flex Profile parameters should be used. When creating a Site Tag, click **Add**, select the **AP Join Profile** to be used.

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

Cisco Catalyst	9800-40 Wireless Controller Web	come alpha 🛛 🐐 😮 📴 🗘 😧 📿 Search Afra and G	enta Q
Q: Search Menu Items	nfiguration - > Tags & Profiles - > Tags		
Dashboard	Policy Site RF AP		
Monitoring →	+ Add × Deleter		
\sim Configuration \rightarrow	Site Tag Name	< Description	~
Administration	default-site-tag	default site tag	- 1 of 1 items
% Troublesho	Enter Name		
Description	Enter Description		
AP Join Profile	default-ap-profile 🔹		
Flex Profile	default-flex-profile		
Control Plane Nam	B .		
Enable Local Site			
"D Cancel		Apply to Device	

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

<u>RF Tag</u>

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

RF Tags are then applied to an access point to specify which RF Profile parameters should be used. When creating a RF Tag, select the **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be used.

	Configuration - > Tags & Profile:	s-> Tags		
Dashboard	Policy Site RF AP			
Monitoring	> + Add SC Delete			
Configuration	RF Tag Name		V Description	
Administration	> default-rf-tag		default RF tag	
Troubleshooting	Add RF Tag	dems ner name.	×	
	Name*	Enter Name		
	Description	Enter Description		
	5 GHz Band RF Profile	Global Config 🔹		
	2.4 GHz Band RF Profile	Global Config 🔹		

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

Search Menu Items	onfiguration - >	Edit AP			
		General Interfaces	High Availability In	wentory ICap Advanced	
Dashboard	 All Access 	General		Version	
Monitoring >	umber of AP(s): 1	AP Name*	rcdn6-22a-ap1	Primary Software Version	16.12.2.132
Configuration	AP v AP Name Mo	Location*	rcdn6-22	Predownloaded Status	N/A
Administration >	rcdn6-22a- Al'	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
Troubleshooting	B-K	Ethernet MAC	00a7.42b7.cb1a	Next Retry Time	N/A
		Admin Status		Boot Version	1.1.2.4
	5 GHz Bac	AP Mode	Local 🗸	IOS Version	16.12.2.132
-	e driz rud	Operation Status	Registered	Mini IOS Version	0.0.0.0
	> 2.4 GHz R	Fabric Status	Disabled	IP Config	
	> Dual-Banc	LED State		CAPWAP Preferred Mode IPv	4
	0	LED Brightness Level	8 💌	DHCP IPv4 Address 10.	201.81.125
	Country	CleanAir <u>NSI Key</u>		Static IP (IPv4/IPv6)	
	LSC Provis	Tags		Time Statistics	
		Policy	default-policy-tag 👻	Up Time	10 days 18 hrs 16 mins 54
		Site	default-site-tag	Controller Association Latency	2 mins 4 secs
		RF	default-rf-tag 👻	contractor in advoction Eateries	2

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

	Configuration				
		General Interface	es High Availability I	nventory ICap Advanced	
ashboard	 All Acces 	General		Version	
lonitoring >	Number of AP(s): I	AP Name*	rcdn6-22a-ap1	Primary Software Version	16.12.2.132
onfiguration >	AP v A Name M	Location*	rcdn6-22	Predownloaded Status	N/A
dministration >	rcdn6-22a- A	Base Radio MAC	00a7.42b0.5c80	Predownloaded Version	N/A
roubleshooting	B	Ethernet MAC	00a7.42b7.cb1a	Next Retry Time	N/A
		Admin Status		Boot Version	1.1.2.4
	5 GHz Pa	AP Mode	Flex v	IOS Version	16.12.2.132
		Operation Status	Registered	Mini IOS Version	0.0.0.0
	> 2.4 GHz I	Fabric Status	Disabled	IP Config	
	> Dual-Bar	LED State		CAPWAP Preferred Mode IP	v4
	N	LED Brightness Level	8 🗸	DHCP IPv4 Address 10	0.201.81.125
	Country	CleanAir NSI Key		Static IP (IPv4/IPv6)	
	> LSC Prov	Tags		Time Statistics	
		Policy	default-policy-tag v	Up Time	0 days 0 hrs 10 mins 1 secs
		Site	Flex	Controller Association Latency	10 secs
		RF	default-rf-tag 🔻		

Controller Settings

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

Cisco Cat	talyst 9800-40	Wireless Controller	Welcome alpha	6 8 0 8	Search APs and Clien	Q
Q Search Menu Itams	Configuration -	> Wireless - > Wireless G	Blobal			
Dashboard	Default Mobility	CTG-VoWLAN3	As	ssisted Roaming		
Monitoring >	Domain *		1	Denial Maximum*	5	
Configuration >	RF Group Name*	RCDN6-VoWLAN3		Floor Blas(dBm)*	15	
Administration >	Maximum Login Sessions Per User*	0		Prediction Minimum*	3	
💥 Troubleshooting	Management Via Wireless					
	Device Classification					
	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.

Dashboard	Global Configuration Peer Config				
Monitoring		uration			
wonitoning	Mobility Group Name*	CTG-VoWLAN3			🖹 Appl
Configuration >	Multicast IPv4 Address	0.0.0.0			
	Multicast IPv6 Address	:			
	Keep Alive Interval (sec)*	10			
Troubleshooting	Mobility Keep Allve Count*	3			
	Mobility DSCP Value*	48	7		
날 옷 옷 옷 옷	Mohilty MAC Address*	706d 153d b50b			
Search Menu Items	Configuration - > Wireless - > Mobility Global Configuration Peer Configuration	1			
	 Mobility Peer Configuration 				
Nonitoring	and a set a stranger set.				
Nonitoring >	+ Add > Delese				
Nonitoring > Configuration > Administration >	+ Add > Delete MAC Address > IP Address	v Public IP v Grou	Ip Name v Multicast IPv4	 Status 	PMTU ~
Aonitoring > Configuration > Administration >	Add Prime MAC Address V IP Address 706d.153d.b50b 10.201.81.9	V Public IP V Grow N/A CTG	P Name v Multicast IPv4 -VoWLAN3 0.0.0	 ✓ Status ✓ N/A 	PMTU ~ N/A
Monitoring >					

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

Cisco Cisco C	Catalyst 9800-40 Wireless Controller	Welcome alpha	* * 8	• 14 0	C Search APs and (Cherris Q
Q Search Menu Items	Configuration - > Interface - > Wireless					
Dashboard	- Add S Delete					
	> Interface Name v Interface Type v	Trustpoint Name v	VLAN ID v	IP Address v	IP Netmask v	MAC Address v
🔧 Configuration	Vlan310 Management H 4 1 P H 10 r items per page		310	10.201.81.9	255.255.255.240	70:6d:15:3d:b5:0b
O Administration	>					
💥 Troubleshooting						

Call Admission Control (CAC)

Unicast Video Redirect and Multicast Direct Enable should be Enabled.

Q Search Menu Items		Configuration * > Radio Configurations *	> Media Parameters			
Dashboard	-	5 GHz Band 5 GHz Band 2.4 GHz	Band			
Monitoring	>	A 6 GHz Network is operational. Configuring	Media Parameters will result in los	s of connectivity of clients.		
Configuration	>	Media			Voice	
O Administration	>	General			Call Admission Control (CAC)	
C Licensing		Unicast Video Redirect			Admission Control (ACM)	
X Troubleshooting		Multicast Direct Admission Control			Traffic Stream Metrics	
		Media Stream Admission Control (ACM)			Metrics Collection	
		Maximum Media Stream RF bandwidth (%)*	5		Stream Size*	84000
		Maximum Media Bandwidth (%)*	85		Max Streams*	2
		Client Minimum Phy Rate (kbps)	6000 🔻		Inactivity Timeout	
		Maximum Retry Percent (%)*	80			
		Media Stream - Multicast Direct Parar	meters			
		Multicast Direct Enable				
		Max streams per Radio	No Limit 🔻			

Multicast

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

	Configuration * > Service	es · > Multicast							
Dashboard	Global Wireless	ABLED						🖹 Ap	ply
) Monitoring >	Multicast Mode]	IGMP S	Snooping					
Configuration >	Wireless mDNS Bridging	DISABLED	Disableo	1		Enabled	Q Se	arch	
) Administration >	IP Multicast	DISABLED	Status	VLAN ID	Name	Status	VLAN ID	Name	-
C Troubleshooting	Wireless Broadcast	DISABLED				O	1	default	÷
	AP Capwap Ur	nicast 🔹				O	310	VLAN0310	÷
	Multicast					0	400	VLAN0400	÷
	MLD Snooping	DISABLED		No Vlan avai	lable	O	500	VLAN0500	÷
	IGMP Snooping Querier	DISABLED							
	IGMP Snooping	ABLED							
	Last Member Querier Interval (milliseconds)	000						Disable	All

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

Cisco Cat	talyst 9800-40 Wireless Controller Welcome alpha 🖌 🏘 📽 🖺 🏟 🔞 🧭 🏵 Search APs and Cleres Q	۲
Q Search Menu Items	Configuration - > Wireless - > Media Stream	
📷 Dashboard	General Streams	
Monitoring >	Multicast Direct Enable	pply
\sim Configuration \rightarrow	Session Message Config	
 ⊘ Administration → ➤ Troubleshooting 	Session Announcement	
	Session Announcement URL	
	Session Announcement Email	
	Session Announcement Phone	
	Session Announcement Note	

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

Cisco Catal	lyst 9800-40 Wi	reless Controller Welc	come alpha 🛛 🐔 🥵 🖺		Search APs and Clients Q
Q Search Menu Items	Configuration - > E	dit WLAN			×
Dashboard	+ Add × I	General Security Adv	anced	Universal Admin	1
Monitoring >	Number of WLANs s	Aironet IE	2	Load Balance	5
Representation >	Statuš Name	P2P Blocking Action	Disabled 🔻	Band Select	
() Administration >	Voić	Multicast Buffer	DISABLED	IP Source Guard	
₩ Troubleshooting	H ≪ 1 ►	Media Stream Multicast- direct	3	WMM Policy	Required
		Max Client Connections		mDNS Mode	Bridging v
				Off Channel Scanning	3 Defer
		Per WLAN 0 Per AP Per 0 WLAN		Defer 0 Priority	1 2
		Per AP Radio 200 Per WLAN		3	✓ 4 ✓ 5 □ 7
		11v BSS Transition Support		Scan Defer 100 Time	
i na shi na shi na shi na shi na shi Nga na shekara na shi na shi na shi		BSS Transition) (Assisted Roaming (1	1k)
		Disassociation Imminent(0 to 3000 TBTT)	200	Prediction Optimization	
		Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40	Neighbor List	
					-
		"D Cancel			Update & Apply to Device

Advanced Settings

Advanced EAP Settings

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

	Configuration - > Security - > Advan	ced EAP			
Dashboard	EAP-Identity-Request Timeout (sec)*	30			
	EAP-Identity-Request Max Retries*	2			
Monitoring >	EAP Max-Login Ignore Identity	DISABLED			
Configuration >	Response				
	EAP-Request Timeout (sec)*	30			
	EAP-Request Max Retries*	2			
X Troubleshooting	EAPOL-Key Timeout (ms)*	400			
	EAPOL-Key Max Retries*	4			
	EAP-Broadcast Key Interval (sec)*	3600			

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.

Cisco Cata	alyst 9800-40 Wireless Controller	Welcome alpha	* * 8 * 8 *	Search APs and Clients Q
Q Search Menu Items	Configuration • > Wireless • > Advance	ced		
Dashboard	Load Balancing Band Select C	Optimized Roaming High	Density Preferred Calls	
Monitoring >				
	Rx Sop Threshold			
() Administration >	Rx Sop Threshold 5 GHz (dbm)	auto 🔻		
X Troubleshooting	Rx Sop Threshold 2.4 GHz (dbm)	auto 🔹		
	Multicast Data Rate			
	Multicast Data Rate 5 GHz (Mbps)	Auto		
	Multicast Data Rate 2.4 GHz (Mbps)	Auto		

Rogue Policies

It is recommended to use the default value (Disable) for Rogue Location Discovery Protocol.
Cisco Cata	alyst 9800-40 Wireless Cont	roller	Welcome alpha	N	8 4 3	0 C S	arch APs and Clients	Q 🕩
Q Search Menu Items	Configuration • > Security • > V	Vireless Pro	tection Policies					
ashboard	Rogue Policies RLDP R	logue AP Rule	es Client Exclusio	on Policies				
Monitoring	Rogue Location Discovery Protocol	Disable	•					
Configuration >	Retry Count	1						
() Administration >	Schedule RLDP							
X Troubleshooting	Day Star	t Time	End Time					
	Monday	Ŀ	9					
	Tuesday	G	9					
	Wednesday	C	9					
	Thursday	C	©					
	Friday	G	9					
이 가는 것은 것은 것은 것은 것이다. 이 나무 가족을 다른 것을 가족을 다.	Saturday	C	9					
	Sunday	G	9					

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.

Monitoring	CISCO Cisco Alronet 1880 Series Mobility Express	Q & ⊕ ≕ ⊠ \$
 Wireless Settings WLANs WLANs Access Points Access Points Access Points WLAN Users Guest WLANs DHCP Server Management Services Advanced 	ACCESS POINTS ADMINISTRATION Access Points Access Points AP1850-1(Active Controller) General Controller Retreach AP Mode AP Access to default tes P Address Configuration Obtain from DH P Address Controller Controller Configuration Obtain from DH P Address Controller Controller Configuration Obtain from DH Configuration Obtain from DH	Clobal AP Configuration Convert to MB Convert to CAPWW Image: Convert to CAPWW er Primary Controller and Preferred Master Preferred Master Up Time AP Model 0 days, 14 h 37 m 44 a AIR-AP18521-A-K9 0 days, 14 h 37 m 44 a AIR-AP18521-B-K9
	он в Preferre Master setting, save configuration and reset controller. То apply change in Preferred Master setting, save configuration and reset controller. Network Spectrum Interface SciDbSoESOAE588S3DC/PD05FA588F52C С Аррју С Салсе	1 - 2 of 2 items

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

🕫 Monitoring	Cisco Aircnet 1850 Series Mobility Express		۹	A @	Ð	8 7	M	\$
Wireless Settings	ACCESS POINTS ADMINISTRATION							
2 Access Points	Access Points 2							
Access Points Groups	P Search General Controller Barlio 1/2 4 GMrt	adio 2 (5GHz) 802 110	Global AP Configuratio	Convert	to ME	0 Convert	to GAPWA	00
管 WLAN Users								
管 Guest WLANs	System Name WI 01850-1	0	er 🖸 Primary Con	troller and Pre	ferred N	laster 🗇 P	Preferred I	laster
DHCP Server	Refresh							
∮ Mesh	Sele Mana Type Location GUI access will be disrupted wh	• IP Configuration is changed.	Up Time		A	P Model		
ሱ Management	C D ME Capable default loc: IP Address 10.0.30		0 days, 14	4 h 13 m 31 s	A	IR-AP1852I-A	-K9	
Services	CAPWAP default locs Subnet Mask 255.255.0		0 days, 14	4 h 13 m 31 s	A	IR-AP1852I-B	-K9	
📥 Advanced	Gateway 10.0.0.1							
	Country United States							
	Changing country code r	quires controller reset.						
		Apply Scancel						

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.

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

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

🍄 Monitoring	Advanced RF Parameters	
Wireless Settings	2.4 GHz Band	
Management	5.0 GHz Band	
Somilago	Automatic Flexible Radio Assignment	
	2.4 GHz Optimized Roaming	
Advanced	5 GHz Optimized Roaming	
◆ SNMP	Event Driven RRM	
🗟 Logging	CleanAir detection	
RF Optimization	5.0 GHz Channel Width	40 MHz •
RF Profiles الس		
& Controller Tools	2.4. CHz Date Bates	Lower Density Higher Densit
🌣 Security Settings	2.4 GHZ Data hates	1 2 55 6 9 11 12 18 24 36 48 1
🗟 СМХ		802.11b devices not supported
		Lower Density Higher Densi
	5.0 GHz Data Rates	6 9 12 18 24 36 48
		Some legacy devices not supported
	Select DCA Channels	2.4 GHz □ 1 2 3 4 5 <u>6</u> 7 8 9 1 11
		5.0 GHz 36 40 44 48 52 56 60 64 100 1
		149 153 157 161 165
		At least one Channel Number should be selected
	Арріу	

RF Optimization

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

æ	Monitoring	Cisco Aironet 1850 S		Q	A	٩	B	₽	\geq	¢		
\$	Wireless Settings											
ġ.	Management	RE OPTIMIZATION										
æ	Services	Il RF Optimization Enable	d									
*	Advanced ↓ SNMP											
	🗟 Logging	RF Optimization	Enabled	•	0							
	I RF Optimization	Client Density	Low Typical	High	0							
	Il RF Profiles	Traffic Type	Voice and Data	•	8							
	& Controller Tools											
	Security Settings		Apply									
	CMX											

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	Cisco Aironet 1850 Series Mobility Express	Q	A	٩	Ð	#		\$
Wireless Settings	ACCESS POINTS AP1850-2	×						
🖆 Access Points	Access Point							
Access Points Groups	General Radio 1 (2.4 GHz) Radio 2 (5GHz) 802.11u	ration		puert to MI	.	Convert to C	ADWAR	9
📽 WLAN Users	Admin Mode Enabled					Somer to Co	AT TAA	
📽 Guest WLANs	Channel Automatic	Cont	troller an	d Preferre	ed Master	Prefe	rred Ma	ster
OHCP Server	Refresh 802.11a/n/ad							
۶ Mesh	Channel Width 20 MHz	c		Up Time		AP Mode	1,	
ሱ Management	Transmit Power Automatic •	8:08	l:1b:78	2 days, 2	3 h 44	AIR-AP18	1521-A-K	9
Services	C C Cancel	8:ca	:28:40	2 days, 2	3 h 38	AIR-AP18	1521-B-K	Ð
📥 Advanced								

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.

🙆 Monitoring	Cisco Aironet 1850 Series Mobility Express	Q	A	٩		#	٥
Wireless Setti	ngs WLAN/RLAN CONFIGURATION						
Access Points							
Access Points Groups	General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling						
 WLAN OSERS Image: Barrier Stress Image: Barrier Stress Image: Barrier Stress 	Addin WLAN ID 1 +		Policy		Radio P	Policy	
∮ Mesh	Type WLAN •				5 GHZ 0	anty	
Hanagement	Profile Name * voice						
Services	SSID * voice WLANs with same SSID can be configured, unless layer-2 security settings are different.						
📥 Advanced	Admin State Enabled •						
	Radio Policy 5 GHz only V						
	Broadcast SSID						
	Local Profiling 🕖 🥹						
	S Apply Can	cel					

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.

		Add new WLAN/RLAN		2	
-	Monitoring				
•	Wireless Setti	General WLAN Security VLAN & Firewall Traffic Sha	ping Advanced 802.11u Hotspot2.0 Schedi	uling	
	N WLANs				
	Maccess Points	Cantive Network Assistant			
	Access Points	MAC Filtering			
	WI AN LIGAR	Security Type WPA2Enterprise T			
	· Guest WI ANs	Authentication Server External Badius	0		
	DHCP Server	Radius Profiling 2			dio Policy
	⁵ Mesh	BYOD			3Hz only
÷.	Management	RADIUS Server			
عر	Services				-
+	Advanced	Authentication Caching			
	Advanced				
		Add RADIUS Authentication Server		-	
		State Enabled	Server IP Address	Port 1812	
		Add RADIUS Accounting Server			
		State	Server IP Address	Port	
		X Enabled	10.0.0.20	1813	
		Cisco Aironet 1850 Se	ries Mobility Express	Q 🛦 🙂	🌣 🗷 💳 🖨
02.0	Monitoring				
**	Wireless Settir	gs			
	Access Points	Add new WLAN/RLAN			
	Access Points	General WLAN Security VLAN & Firewall Traffic Sh	aping Advanced 802.11u Hotspot2.0 Sched	duling	
	Groups				-
	WLAN Users	Guest Network 🔵 💡			
	Guest WLANs	Captive Network Assistant			adio Policy
	DHCP Server	MAC Filtering			GHz only
	7 Mesh	Security Type Personal 🔻			
H-	Management	WPA2 WPA3			
de.	Services	Passphrase Format ASCII -			
*	Advanced	Pasenbrase *			
		Confirm Pasenbrase *			
		Show Passohrase			
				O Apply (S Cancel	

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.

			Add new WLAN/RLAN		×	Q	A	٢	8	† 2	•
Mor 🏙	onitoring	CISC	General WLAN Security VLAN & Firewall	Traffic Shaping Advanced	802.11u Hotspot2.0						
🗱 Wire	reless Settings /LANs	WLAN/RLA	Scheduling								
⁰ <u>1</u> ⁰ Ac	ccess Points	Active	Allow AAA Questide								
≌ Ac Gr	ccess Points roups		Maximum Allowed Clients	Unlimited(Default) • ?		:					
않 w	VLAN Users		Maximum Allowed Clients Per AP Radio	200 ©							
楷 Gi	Guest WLANs	Add new WL	802.11k	Disabled 🔻							
⊕ DF	HCP Server	@ ×	802.11r	Enabled v		ecurity F	Policy		5 GHz onl	licy	
⁵ Me	esh		802.11v	Disabled •							
🖬 Mar	inagement		CCKM								
🖋 Ser	rvices		Client Band Select								
📥 Adv	vanced		Client Load Balancing								
			Umbrella Profile	None 🔻							
			Umbrella Mode	Ignore 🔻							

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

		Add new WLAN/RLAN						×	⇒	•
æ	Monitoring	General WLAN Security	VLAN & Firewall Traf	fic Shaping Advanced	802.11u	Hotspot2.0	Scheduling			
\$	Wireless Setti									
	≫ WLANs	Guest Networ	k 🕜 🕜							
	Access Points	Captive Network Assistan								
	Access Points Groups	MAC Filterin	a 💭							
	WLAN Users	Security Type	e WPA2Enterprise	•						
	📽 Guest WLANs	Authentication Serve	r External Radius	• 0						
	DHCP Server	Radius Profiling	9 🕜 🕜					id a	io Policy	
	4 Mesh	BYO								
÷.	Management	RADIUS Server								
J.C	Services									
+	Adversed	Authentication Cach	ing O							
	Advanced									
		Add RADIUS Authenticatio	in Server							
		State		Server IP Addr	985		Port			
		X Enabled		10.0.0.20			1812			
		Add RADIUS Accounting S	Server							
		State		Server IP Addr	855		Port			
		X Enabled		10.0.0.20			1813			

			Cisco Aironet 1850 Ser	ies Mobility Express				Q	A	٩	B	≓	\sim	Φ
æ	Monitoring													
۵	Wireless Settings	ADMIN ACCOL	JNTS											
ġ.	Management • Access	🐸 Users	1											
	😁 Admin Accounts													
	0 Time	Management	User Priority Order	Local Admin Accou	nts TACACS+	RADIUS Aut	h Cached Users							
	✤ Software Update													
æ	Services	Authentication	n Call Station ID Type	AP MAC Address:S	SID .									
*	Advanced	Authenti	ication MAC Delimiter	Hyphen	•									
		Accounting	g Call Station ID Type	IP Address	•									
		Acco	ounting MAC Delimiter	Hyphen	•									
			Fallback Mode	Passive										
			Username	cisco-probe										
			Interval	300	© Secon	ds								
		β	AP Events Accounting											
				Apply										
æ	Monitoring	Add RAD	DIUS Authentication Server	ø										
\$	Wireless Settings	Action	Server Index	Network User	Management	State	Server IP Address	Sha	red Key		Por	t		
ġ.	Management • Access	₿ ¥	1				10.0.0.20	•••••			181	2		
	😤 Admin Accounts													
	0 Time		a											
	✤ Software Update	Add RAD	DIUS Accounting Server											
se.	Services	Action	Server Index	Network User	Management	State	Server IP Address	Sha	red Key		Por	t		_
Ł	Advanced	C ×	1				10.0.20				181	3		

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

æ	Monitoring	Cisco Alronet 1850 Series Mobility Express	٩	A	٩	Ð	₽	\$
\$	Wireless Settings >> WLANs	Add new WLAN/RLAN VLAN General WLAN Security VLAN & Firewall Traffic Shaping Advanced 802.11u Hotspot2.0 Scheduling						
	텔 Access Points Groups 쯀 WLAN Users	Client IP Management Network(Default) Peer to Peer Block Addn Native VLAN ID 1						
	Y Guest WLANS 중 DHCP Server 카 Mesh	Use VLAN Tagging Yes		Policy		Radio 5 GHz	Policy only	
њ. К	Management Services	No DHCP Scope associated with VLAN ID Enable Firewall No v						
Ł	Advanced	VLAN AGL Map Add New VLAN VLAN Name VLAN Id						
			-					
		Image: State Sta						
		H I	ems					

Ensure Platinum (Voice) is selected for QoS.

		Add new WLAN/RLAN						× 🚽	•
- 629 	Monitori	General WLAN Security VLAN & Firewall Tra	ffic Shaping Advan	ced 802.11u Hotspo	2.0 Scheduling				
**	Wireless ≫ WLANs							_	
	🖆 Access F	QoS	Platinum (Voice)	v 😧					
	Access F	Average real-time bandwi	dth limit should be atlea	st Average bandwidth limit					
		Rate limits per client							
		Average downstream bandwidth limit	0	kbps 🕜					
	Guest W	Average real-time downstream bandwidth	0	kbps 🕜				icy	
	« DHCF 3	Average upstream bandwidth limit	0	kbps 🕜				1	
	7 Mesh	Average real-time upstream bandwidth limit	0	kbps 💡					
n •	Manager							_	
J.C.	Services	Rate limits per BSSID							
Ł	Advance	Average downstream bandwidth limit	0	kbps 🕜					
		Average real-time downstream bandwidth limit	0	kbps 🕜					
		Average upstream bandwidth limit	0	kbps 🕜					
		Average real-time upstream bandwidth limit	0	kbps 🕜					
B	Monitori	Fastlane	Disabled						
•	Wireless		Enabling Fastlane will u	pdate QoS value to platinum					
		Application Visibility Control	Enabled	•					
	🖞 Access I	AVC Profile	voice						
	Access I Groups	Add Rule							
_	양 WLAN L	S Application	Action			Average Rate	Burst Rate	1	
	📽 Guest W								
	[⊗] DHCP S								
	4 Mesh								

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

		Add new	WLAN/HLAN			×		
	an		Active	Add new WLAN/RLAN		s	ecurity Policy	Radio Policy
	Monitoring Wireless Settings WLANs	⊮ ×	Enabled	General WLAN Security VLAN & Firewal Scheduling	II Traffic Shaping Advanced 802.11u Hotspot2.0			5 GHz only
	堂 Access Points 앱 Access Points Groups			Allow AAA Override Maximum Allowed Clients				
	ở WLAN Users			Maximum Allowed Clients Per AP Radio	200 ③			
	[●] Guest WLANs [●] DHCP Server			802.11k 802.11r	Disabled •			
	∱ Mesh			802.11v				
	Services			Client Band Select				
ľ	Advanced			Client Load Balancing Umbrella Profile	None T			
				Umbrella Mode Umbrella DHCP Override	Ignore v			
				mDNS				
				mDNS Profile Passive Client	None 🔻			
				Please enable Globa when Global Multica Multicast IP	al Multicast in Services->Media Stream. Passive Client will not work ast is disabled.			
				Multicast Direct	•			

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.

æ	Monitoring	Cisco Aironet 1850 Series Mobility Express	Q	A	٩	Ð	1	M	٥
\$	Wireless Settings ର _{WLANs}	ACCESS POINT GROUP							
	🖆 Access Points	Access Points Groups							
		Add new group							
	📽 WLAN Users	Q Search General WLANs Access Points RF Profile Ports Intelligent Capture							
	📽 Guest WLANs	Add new group Refre							
		AP Group ni AP Group name express-1 AP count							
	4 Mesh	AP Group description							
÷.	Management	2 Cef autr-grou NAS-ID							
Je.	Services	Venue Group UNSPECIFIED +							
*	Advanced	Venue Type UNSPECIFIED +							
		Add New Verue							
		Language Venue Name							
		WEB I NO							
		Apply Cancel							

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

🖚 Monitoring	clsco Aironet 1850 Series Mobility Express		Q	A	٩	6	1	M	\$
🗱 Wireless Settings জ WLANs	ACCESS POINT GROUP								
📱 Access Points	Access Points Groups								
Maccess Points Groups	Add new group								
^쓥 WLAN Users	Q. Search General WLANs Access Points RF Profile Ports Intelligent Capture								
醟 Guest WLANs	Add new group Refresh								
OHCP Server	AP Group name Add new WLAN/RLAN	AP count							
⁵ Mesh	Add new WLAN/RLAN	0							
ሱ Management	UE default:group ¥ ₩ Type WLAN ▼	2							
🖋 Services	Profile Name voice 🔻								
🕹 Advanced	🕑 Updata 🖉 Cancel								

🍪 Monitoring	Cisco Aironet 1860 Series Mobility Express			Q	A	٩	6	11	٥
 Wireless Settings WLANs WLANs Access Points Access Points Groups WLAN Users Guest WLANs DHCP Server Mesh 	ACCESS POINT GROUP Access Points Group Add new group General WLANs Access Points RP Profile Ports Intelligent Capture Add new WLAN/RLAN @ A Group name @ Add new WLAN/RLAN @ x express.1 @ default-group X WLAN voice Enabled		AP count 0						
Advanced	(м к 1 1 + и) 10 v) и к 1 1 + и) 10 v Items per page 1 - 1 of 1 Items (САрру) (С Салсе)	s							

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

🖚 Monitoring	Cisco Aironet 1850 Beries Mobility Express	Q	A	٩	6	11	\$
 Wireless Settings WULANS WLANS WACSS Points WLAN Users WULAN Users WULAN Users WOLAN S O DHCP Server Mosh Management 	Add new group Access P General WLANs Access Points RF Profile Ports Intelligent Capture General WLANs Access Points RF Profile Ports Intelligent Capture General WLANs Access Points RF Profile Ports Intelligent Capture General WLANs Access Points RF Profile Ports Intelligent Capture General WLANs Access Points RF Profile Ports Intelligent Capture General WLANs Access Points RF Profile Ports Intelligent Capture General WLANs Access Points RF Profile Ports Intelligent Capture Add new group AP Group All AP Inne AP Group All AP Inne AP Group name AP Group name						
 ✓ Services ▲ Advanced 							

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

🕸 Monitoring	G Cisco Aironet 1860 Series Mobility Express	Q	A	٩	6	#	M	0
♥Wireless Settings N WLANs 텍 Access Points 텍 Access Points	ACCESS POINT GROUP Access Points Groups 1							
Groups 쑴 WLAN Users 쑴 Guest WLANs	Q. Search Add new group: Refeat							
ঞ্জ DHCP Server * Mesh	AP Group name AP Group name Add new group							
 Management Services 	General WLANs Access Points RF Profile Ports Intelligent Capture							
🕹 Advanced	2.44Hz None • SGHz None • Catcol							

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.

æ			Cisco Aironet 1850 Serie	s Mobility Express				Q	A	٩	B	1	0
Ф	Wireless Settings												
÷.	Management	RF Profile:											
Je.	Services	RF prof	ile 6										
*	Advanced SNMP	Q Search		Add RF Profile									
		⊕ Add ne	w RF Profile										
			RF profile	General 802.11 RRM Cli	ent Distribution		Applied						
		⊗ ×	express-1			_							
	& Controllar Tools	C	High-Client-Density-802.11a	RF profile name	express-1		No						
		C.	High-Client-Density-802.11bg				No						
	Security Settings	œ	Low-Glient-Density-802.11a	RF profile description			No						
	CMX	C2	Low-Client-Density-802.11bg	Band	5GHz ¥		No						
		8	Typical-Client-Density-802.11a	Maximum clients per radio	200		No						
		8	Typical-Client-Density-802.11bg				No						
				Rx SOP Threshold	Auto 🔻								
				Multicast datarates	Auto 🔻								
			1 + н 10 v items per page		Apply Cancel								

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

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

🍄 Monitoring	Cisco Aronet 1850 Series Mobility Express Q	\$
Wireless Settings		
📩 Management	RF Profiles	
	RF profile 6	
Advanced	. Q Seech	
🗟 Logging	Add new RF Profile	
I RF Optimization	x x x x x x x x x x x x x x x x x x x	
all RF Profiles	Add RF Profile	
Controller Tools	General 802.11 RRM Client Distribution	
Security Settings	3	
CMX	Office Data rates 6 9 12 18 24 36 48 54	
	MCS settings	
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	
	@ Apply @ Cancel	

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

Wireless Settings RF Profiles		
Imagement RF profile Services RF profile Advanced 9.5uch		
Services RF profile 6 Advanced + SNMP 9, Sector 9		
Advanced V SNMP		
Logging OAdd new RF Profile Add INF Profile		
ARF Optimization Applied Applied		
al RF Profiles G * express-1 General 802.11 HHM Client Distribution		
Controller Tools		
High-Client-Dansity-802 Channel Width 40 MHz + No		
Select All 36 40 44 48 52 58 60 64 100 104 108 No		
CMX CMX 112 116 120 124 128 132 136 140 144 140 153 No 157 161 165		
Uf Typical-Glient-Density-i		
Topical-Clean Descript Some of the channels are not alreaded to configure as they are not excluded in the channels are not alreaded. These channels are not alreaded in the channels are not alreaded in the channel kundler should be selected		

Multicast Direct

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

			Cisco Aironet 1850 Se	Q	A	٩	₽	\searrow	Ф			
æ	Monitoring											
\$	Wireless Settings	Media St	ream Settings									
ġ.	Management											
ø	Services ➡ Media Stream	Let Med										
	₽ tls		Global Multicast									
	♥ mDNS		Multicast Direct									
	Network Assurance		Mattoust Direct									
	📥 Webhook	Ses	ssion Announcement State									
	Intelligent Capture	Se	ession Announcement URL	URL								
	🗅 Umbrella	Ses	ssion Announcement Email	Email								
*	Advanced	Sess	sion Announcement Phone	Phone								
		Se	ssion Announcement Note	Note	ĥ							
				Apply								
		Add New	Stream									
		Add New		0	C 1-1							
		×	10.0.0.40		239.1.1.40	 239.1.1.40		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.

		- 100 1101	THE CONDAIN					
æ	Manitania a		Active	Add new WLAN/RLAN			Security Policy	Radio Policy
\$	Monitoring Wireless Settings	8 x	Enabled	General WLAN Security VLAN & Firewa Scheduling	II Traffic Shaping Advanced	802.11u Hotspot2.0		5 GHz only
	1 Access Points			Allow AAA Override				
	Access Points Groups			Maximum Allowed Clients	Unlimited(Default) •			
	📽 WLAN Users			Maximum Allowed Clients Per AP Radio	200 ©			
	📽 Guest WLANs			802.11k	Disabled •			
	OHCP Server			802.11r	Enabled •			
	⁵ Mesh			802.11v	Disabled •			
ġ.	Management			сскм				
J.C.	Services			Client Band Select				
Ł	Advanced			Client Load Balancing				
				Umbrella Profile	None 🔻			
				Umbrella Mode	Ignore 🔻			
				Umbrella DHCP Override				
				mDNS				
				mDNS Profile	None •			
				Passive Client				
				Please enable Globa when Global Multic	al Multicast in Services->Media Stream ast is disabled.	a. Passive Client will not work		
				Multicast IP	239.1.1.1			
				Multicast Direct	0			

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.

ululu cisco	<u>H</u> OME	<u>N</u> ETWORK	<u>A</u> SSOCIATIO	ON W <u>I</u> RELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e C <u>M</u> ANAGEMENT	onfiguration	Ping Logout	<u>R</u> efres
	Host	name ap-1					ap-1	uptime is 1 day	, 4 hours, 51 mi	nutes
Summary	Net	twork Interfac	es: Summary							
Adjacent Nodes	Sys	tem Settings								
NETWORK INTERFACE	IP A	Address (Statio	;)		10.9.0.9					
Summary	IP S	Subnet Mask			255.255.255.0					
IP Address GigabitEthernet0	Def	ault Gateway			10.9.0.2					
Radio0-802.11N 2.4GHz	MA	C Address			18e7.281b.3f54					
Radio1-802.11AC 5GHz	Inte	erface Status		GigabitEthernet		Radio0-802.1	1N ^{2.4GHz}	Radio1-802.1	1AC ^{5GHz}	
	Soft	tware Status			Enabled		Disabled	k in the second s	Enable	ed î
	Han	dware Status			Up 🏦		Down	F	ι	Jp 🏫
	Inte	rface Resets			5		(D		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.

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

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.

ululu cisco	HOME NETWORK ASSOCIATION V		Save Configuration Ping Logout Refree MANAGEMENT SOFTWARE EVENT LOG
NETWORK	= RADIO1-802,11AC ^{5GHZ} = DETAIL		
NETWORK	STATUS	ED STATUS	
NETWORK MAP Summary	Hostname ap-1		ap-1 uptime is 1 day, 4 hours, 56 minutes
Adjacent Nodes	Network Interfaces: Radio1-802 11AC	5GHz Settings	
NETWORK INTERFACE		ooungo	
Summary	Enable Radio:	 Enable 	◯ Disable
IP Address	Current Status (Software/Hardware):	Enabled 🔒	Up 🕇
Radio0-802.11N 2.4GHz	Role in Radio Network:	 Access Point 	
Radio1-802.11AC 5GHz		Access Point (Fallback to Radio S Access Point (Fallback to Repeate	Shutdown) er)
		Repeater	
		Root Bridge	
		Non-Root Bridge	
		Non-Root Bridge with Wireless Cl	lients
		Workaroup Bridge	
		Universal Workgroup Bridge Cli	ient MAC: (HHHH.HHHH.HHHH)
		Scanner	
	Max-Client:	enable odisable (1-258	5)
	11r Configuration:	oenable disable	
		over-air Oover-ds Reassociat	tion-time: (20-1200 ms)
	Data Rates:	Best Range Best Throughput	Default
	9.0Mb/sec		
	12.0Mb/sec		Enable Disable
	18.0Mb/sec	Require	Enable Disable
	24.0Mb/sec	Require	Enable Disable
	36.0Mb/sec	c Require	Enable Disable
	48.0Mb/sec		Enable Disable Disable
	a0 1-2Mb/set		
	a1.1-2Mb/set	C Require	Enable Disable
	a2.1-2Mb/se	c Require	Enable Disable
	a3.1-2Mb/se	c Require	Enable
	a4.1-2Mb/se	c Require	Enable Disable
	a5.1-2Mb/se		Enable Disable Disable
	a7.1-2Mb/set		Enable Disable
	a8.1-2Mb/set	c Require	• Enable Disable
	a9.1-4Mb/set	c Require	• Enable Obisable
	a0.2-2Mb/sec	c Require	• Enable Disable
	a1.2-2Mb/se		Cenable Disable Disable
	a3.2-2Mb/set		Enable Disable
	a4.2-2Mb/se	c Require	Chable Disable
	a5.2-2Mb/se	c Require	Enable Disable
	a6.2-2Mb/se	c Require	• Enable Disable
	a7.2-2Mb/se	C Require	Cashie Cashie Cashie
	a8.2-2Mb/sei a9.2-4Mb/sei		
	a0.3-2Mb/set	c Require	Chable Disable
	a1.3-2Mb/se	c Require	• Enable Disable
	a2.3-2Mb/set	c Require	• Enable Disable
	a3.3-2Mb/set	C Require	Enable Disable
	a4.3-2Mb/set		Enable Disable Disable
	a6.3-2Mb/set		Chable Disable
	a7.3-2Mb/se	c Require	Enable Disable

a9.3-2	2Mb/sec (Require	Enable	Olisable				
MCS Rates: 0 1 2 3	3 4 5	6 7 8 9 10	11 12 13 14 15 16 17	18 19 20 21 22 23				
Enable 🔿 💿 🔘	00	0000	0000000	$\mathbf{O} \mathbf{O} \mathbf{O} \mathbf{O} \mathbf{O} \mathbf{O}$				
Disable 💿 🔘 🔘		00000						
Transmitter Power (dBm):	(15 12 9 6	⊖3 O Max	Power Translation Ta				
Client Power (dBm):				<u>(mW/dBm)</u>				
chent Power (dbhi).								
DefaultRadio Channel:		Channel 36 - 5180 MH:	2 Channel 36 5180) MHz				
Dynamic Frequency Selection	Bands: E	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 5.950 GHz						
Channel Width:		Below 40 MHz ᅌ 20	MHz					
World Mode Multi-Domain Operation:	(Disable	◯ Legacy	 Dot11d 				
Country Code:		🖸 🗹 Indoor 🗸	Outdoor					
Radio Preamble		Short						
Antenna:	(a-antenna a	b-antenna Oabc-antenna	 abcd-antenna 				
Internal Antenna Configuration	n: (• Enable Oisable						
	A	Antenna Gain(dBi):	0 (-128 - 128)					
Gratuitous Probe Response(G	PR): (Enable	 Disable 					
	F	Period(Kusec): DIS/	ABLED (10-255)					
	т	ransmission Speed	: none ᅌ					
Traffic Stream Metrics:	(Enable	 Disable 					
Aironet Extensions:	•	Enable	O Disable					
Ethernet Encapsulation Transf	form:	RFC1042	○ 802.1H					
Reliable Multicast to WGB:		Disable	C Enable					
Public Secure Packet Forward	ling: P	SPF must be set per V	LAN. See VLAN page					
Beacon Privacy Guest-Mode:	(Enable	 Disable 					
Beacon Period:	100	(20-4000 Kusec)	Data Beacon Rate (DTIM):	2 (1-100)				
Max. Data Retries:	64	(1-128)	RTS Max. Retries:	64 (1-128)				
Fragmentation Threshold:	2346	(256-2346)	RTS Threshold:	2347 (0-2347)				
Root Parent Timeout:		0	(0-65535 sec)					
Root Parent MAC 1 (optional):			(НННН.НННН.НННН)					
Root Parent MAC 2 (optional):			(НННН.НННН.НННН)					
Root Parent MAC 3 (optional):			(НННН.НННН.НННН)					
Root Parent MAC 4 (optional):			(НННН.НННН.НННН)					

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.

ululu cisco	<u>H</u> OME	<u>N</u> ETWORK	ASSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configuration	Ping Logout EVENT LOG	<u>R</u> efresh
Security	Hostna	ame ap-1					ap-	1 uptime is 1 day	v, 4 hours, 33 mir	nutes
Admin Access										_
Encryption Manager	Secu	rity: Global S	SSID Manager							
SSID Manager	SSID	Properties								
Dot11u Manager	Curr	ent SSID List	t							
Server Manager	< NE	- W			SSID:		voice			
AP Authentication	data voice	e			VLAN:		3	Define VLA	Ns	
Intrusion Detection							Backup 1:			
Local RADIUS Server							Backup 2:			
Advance Security							Backup 3:			
					Band-Select	:	Band Se	lect		
					Universal Ad	Imin Mode:	Universa	Admin Mode		
					Interface:		☐ Radio0-8 Radio1-8	02.11N ^{2.4GHz} 02.11AC ^{5GHz}		
	N	etwork ID:	(0-40	96)						
	De	elete								
	Clien	t Authenticat	ion Settings							
		Methods A	ccepted:							
		🗹 Op	en Authentication:	with	EAP		0			
		□ We	b Authentication	□ W	Web Pass					
		Sh:	ared Authentication	n: < NC	ADDITION>		0			
		🗹 Ne	twork EAP:	< NC	ADDITION >	0				
		Server Pric	orities:							
		EAP A	uthentication Ser	vers		N	AC Authentication	on Servers		
		💿 Us	e Defaults Define	Defaults			 Use Defaults 	Define Defaults		
		🔿 C u	stomize			(Customize			
		Pr	riority 1: < NONE	> ᅌ			Priority 1: <	NONE > 🗘		
		Pr	riority 2: < NONE	> ᅌ			Priority 2: <	NONE > ᅌ		
		Pr	riority 3: < NONE	> 🗘	Priority 3: < NONE > 0					
	Clien	t Authenticat	ed Key Managem	ent						
		Key Manag	jement:	Manda	atory ᅌ	_ (CKM 🗹 Enal	ble WPA WP	Av2 dot11r ᅌ	

	-			ASCII O Hexadecim
11w Configuration	1:	Disable ᅌ		
11w Association-o	comeback:	1000	(1000-2000	00)
11w Saquery-retry	' :	100	(100-500)	
IDS Client MFP				
Enable Client	MFP on this SS	ID: Optional	\$	
AP Authentication				
Credentials:		< NONE >	\$	Define Credentials
Authentication Methe	ods Profile:	< NONE >	٥	Define Authentication Methods Profiles
Accounting Settings				
Enable Accou	nting		Account	ing Server Priorities:
			o Use	Defaults Define Defaults
			⊖ Cust	omize
			Prio	rity 1: < NONE > ᅌ
			Prior	rity 2: < NONE > 📀
			Prio	rity 3: < NONE > ᅌ
			Prior	rity 3: < NONE > 😒
Rate Limit Parameters			Prior	rity 3: < NONE > 0
Rate Limit Parameters Limit TCP:			Prio	rity 3: < NONE > 0
Rate Limit Parameters Limit TCP:	Rate:	Burst-Siz	Prio	rity 3: <a>NONE > (0-500000)
Rate Limit Parameters Limit TCP: Input: Output:	Rate: Rate:	Burst-Siz Burst-Siz	Prior	rity 3: <a> NONE > (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP:	Rate: Rate:	Burst-Siz	Prior e:	rity 3: <a>NONE > (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input:	Rate: Rate: Rate:	Burst-Siz Burst-Siz Burst-Siz	Prior e: e:	rity 3: <a>NONE > (0-500000) (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output:	Rate: Rate: Rate: Rate:	Burst-Siz Burst-Siz Burst-Siz Burst-Siz	Prior e:	rity 3: <a>NONE > (0-500000) (0-500000) (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: Output: General Settings	Rate: Rate: Rate: Rate:	Burst-Siz Burst-Siz Burst-Siz Burst-Siz	Prior e:	rity 3: <a>NONE > (0-500000) (0-500000) (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Limit UDP: Input: Output: General Settings Advertise Exten	Rate: Rate: Rate: Rate: ded Capabilite:	Burst-Siz Burst-Siz Burst-Siz Burst-Siz Burst-Siz	Prior	rity 3: <a> NONE > (0-500000) (0-500000) (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Input: Output: Output: Coutput: General Settings Advertise Exten	Rate: Rate: Rate: Rate: ded Capabilite:	Burst-Size Burst-Size Burst-Size Burst-Size s of this SSID	Prior e: e: e: e: e: oning Servi	rity 3: <pre> < NONE > </pre> (0-500000) (0-500000) (0-500000) (0-500000) (0-500000)
Rate Limit Parameters Limit TCP: Input: Output: Input: Output: Output: General Settings Advertise Exten	Rate: Rate: Rate: Rate: ded Capabilite: Advertise W	Burst-Size Burst-Size Burst-Siz Burst-Siz s of this SSID fireless Provisic is SSID as a Se	Prior	rity 3: <pre> < NONE > </pre> (0-500000) (0-500000) (0-500000) (0-500000) (0-500000) ces (WPS) Support roadcast SSID
Rate Limit Parameters Limit TCP: Input: Output: Input: Output: Output: Contput: Cont	Rate: Rate: Rate: Rate: Rate: ded Capabilite: Advertise W Advertise th ection on this S	Burst-Size Burst-Size Burst-Size Burst-Size Burst-Size s of this SSID fireless Provisio is SSID as a Se	Prior	rity 3: <a>NONE > (0-500000) (0-500000) (0-500000) (0-500000) (0-500000) ces (WPS) Support roadcast SSID

IP Filte	(optional): < NONE > ODefine Filte	<u>9r</u>	
Association Limit	ptional): (1-255)		
EAP Client (option): Jsername:	Password:	
Multiple BSSID Beacon	ettings		
Multiple BSSID Be	con		
	Set SSID as Guest Mode		
	Set DataBeacon Rate (DTIM): DISABLE	D (1-100)	
			Apply Cancel
Guest Mode/Infrastructu	e SSID Settings		
Radio0-802.11N ^{2.4GHz} :			
Set Beacon Mode:	Single BSSID Set Single Guest N	Node SSID: < NONE > 🗘	
Set Infrastructure SSID:	Multiple BSSID NONE > O Force Infrastructure E	Devices to associate only to this SSID	
Radio1-802.11AC ^{5GHz} :			
Set Beacon Mode:	Single BSSID Set Single Guest Me	ode SSID: < NONE > ᅌ	
Set Infrastructure SSID:	Multiple BSSID NONE > O Torce Infrastructure De	evices to associate only to this SSID	
			Apply Cancel

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.

sco	<u>H</u> OME <u>N</u>	ETWORK	ASSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	<u>M</u> ANAGEMENT	<u>S</u> OFTWARE <u>E</u> V	ent log	
	Hostnam	e ap-1					а	p-1 uptime is 1 day, 4	hours, 48 m	
SH	_	-								
dby	Service	es: VLAN								
	Global	VLAN Pro	perties							
	Curro	nt Nativo \								
	Curren	It Native v	CAN: VLAN 10							
	Assign	ed VLANs								
	Currer	nt VLAN Li	st	Create V	LAN		Define SSI	<u>)s</u>		
	< NEW	>								
	VLAN 2	2 3		VLA	N ID:		3	(1-4094)		
	VLAN 1	10					•	(1.100.1)		
			Delete	VLA	N Name (opt	ional):				
ning			Delete	0	Native VL	AN				
ect		Enable Public Secure Packet Forwarding								
rig		□ Radio0-802.11N ^{2.4GHz}								
					Z Radio1-80	2.11AC ^{5GHz}				
		Management VI AN //f non-native)								
					managem		ion-native)			
								Арр	ly Cance	
	VLAN I	nformation	n							
	View In	formation	for: VLAN 2 ᅌ							
			GigabitEtherne	et Packets	Radio0	-802.11N ^{2.4GHz}	Packets	Radio1-802.11AC	GHz Packets	
	Receive	d		65884					6	

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



Configure the RADIUS servers for authentication and accounting.

սիսիս			Sa <u>v</u> e C	onfiguration <u>P</u> ing Logout <u>R</u> efres							
CISCO	HOME NETWORK ASSOCIA	TION WIRELESS SECURITY	<u>SERVICES</u> <u>M</u> ANAGEMENT	SOFTWARE EVENT LOG							
Security	SERVER MANAGER	GLOBAL PROPERTIES									
Admin Assoss	Hostname ap-1		ap-1	uptime is 1 day, 4 hours, 42 minutes							
Encryption Manager	Security: Server Manager										
SSID Manager	Backup RADIUS Server										
Dot11u Manager											
Server Manager	IP Version:	○IPV4 ○IPV6									
AP Authentication	Backup RADIUS Server Nam	ie:									
Intrusion Detection	Backup RADIUS Server:		(Hostname or IP Address)							
Local RADIUS Server	Shared Secret:										
Advance Security				Apply Delete Cancel							
	Corporate Servers										
	Current Server List										
	RADIUS										
		IP Version:	OIPV4 OIPV6								
	< NEW >	Server Name:	10.0.0.20								
	10.9.0.9	Server:	10.0.0.20	(Hostname or IP Address)							
		Shared Secret:									
	Delete	Authentication Port (optional):	1812 (0-65535)								
		Accounting Port (ontional):	1813 (0-65535)								
		Accounting Fort (optional).	(0-05555)	Apply Cancel							
	Default Server Priorities										
	EAP Authentication	MAC Authenticat	tion A	ccounting							
	Priority 1: 10.0.0.20 ᅌ	Priority 1: < NON	NE > 📀 P	riority 1: 10.0.0.20 ᅌ							
	Priority 2: < NONE > 🗘	Priority 2: < NON	NE > 🗘 P	riority 2: < NONE > ᅌ							
	Priority 3: < NONE > ᅌ	Priority 3: < NOM	NE > 📀 P	riority 3: < NONE > ᅌ							
	Admin Authentication (RADI	US) Admin Authentic	ation (TACACS+)								
	Priority 1: < NONE > ᅌ	Priority 1: < NON	VE > 📀								
	Priority 2: < NONE > ᅌ	Priority 2: < NOM	NE > 😒								
	Priority 3: < NONE > ᅌ	Priority 3: < NOM	NE > 📀								
				Apply Cancel							

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

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).



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.

uluilu cisco	<u>H</u> OME <u>N</u> ETWORK	ASSOCIATION WIR	eless <u>s</u> ecurity	<u>S</u> ERVICES	Sa <u>v</u> e (<u>M</u> ANAGEMENT	Configuration Ping Lo	ogout <u>R</u> efresh LOG				
Services	Hostname ap-1				at	p-1 uptime is 1 day, 4 hour	rs, 48 minutes				
Telnet/SSH											
Hot standby	Services: VLAN										
CDP	Global VLAN Pro	perties									
DNS	Current Notice)										
Filters	Current Native	CAN: VEAN TO									
НТТР	Assigned VLANs										
QOS	Current VLAN L	st	Create VLAN		Define SSID	S					
Stream	< NEW >										
SNMP	VLAN 2				10						
SNTP	VLAN 10		VLAN ID:		10	(1-4094)					
VLAN			VLAN Name (op	tional):							
ARP Caching		Delete	Native VL	AN							
Band Select			Enable Pr	ublic Secure Pa	acket Forwarding	9					
Auto Config			Radio0-8	02.11N ^{2.4GHz}							
			Radio1-8	11 AC5GHz							
		Management VLAN (If non-native)									
						Apply	Cancel				
	VLAN Information	n									
	View Information	View Information for: VLAN 2 0									
		GigabitEthernet Pack	et Packets Radio0-802.11N ^{2.4GHz} Packets			Radio1-802.11AC ^{5GHz} Packets					
	Received		65884				65884				
	Transmitted		5462				5462				
							Refresh				

Server groups for Wireless Domain Services must be defined.

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

Is recommended to use local RADIUS for infrastructure authentication.

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

cisco	HOME NETWORK ASSOCIATION WIRELESS SECUR	Save Configuration Ping Logout Refresh TY <u>S</u> ERVICES MANAGEMENT <u>S</u> OFTWARE <u>E</u> VENT LOG										
Wireless Services	US STATUS	P SERVER GROUPS										
AP	Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 51 minutes											
WDS	Wireless Services: WDS - Server Groups											
	Server Group List											
	Server Group Name: WDS WDS											
	Group Server Priorities: Define Servers											
	Delete Priority 1: 10.9.0.9											
	Priority 2:	Priority 2: < NONE > ©										
	Pnority 3:	< NONE > 📀										
	Use Group For: Infrastructure Authentication 											
	Client Authentication											
	Authentication Settings	SSID Settings										
		Restrict SSIDs (Apply only to listed SSIDs)										
	MAC Authentication	SSID: DISABLED Add										
	Default (Any) Authentication	Remove										
		Apply Cancel										

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.

،، ،،، ،، cısco	<u>H</u> OME	NETWORK	ASSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configuration	Ping Logout	<u>R</u> efresh	
Wireless Services		WDS STA	TUS	GENEI	RAL SET-UP		SERVER GROUP	s			
AP	Hostna	ame ap-1					ap	1 uptime is 2 d	ays, 2 hours, 31	minutes	
WDS	Wireless Services: WDS - Server Groups										
	Serv	er Group Lis	t								
	< NE WDS Clier	Group For:	Delet	Grou	er Group Nan p Server Price Priority 1: 1 Priority 2: Priority 3:	rities: Define 0.0.0.20 © NONE > © NONE > ©	Servers				
	0	Client Auther	tication Settings			SSID Settings					
			EAP Authenticat	ion	Apply to all SSIDs						
		e	LEAP Authentica	ation		O Restric	t SSIDs (Apply only	to listed SSID	5)		
			MAC Authentica	tion		S	SID: DISABLED	Ad	d		
		C	Default (Any) Au	thentication				Re	move		
									Apply	Cancel	

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.

iiliiilii cisco	HOME <u>N</u> ETWORK <u>A</u> SSOCI	ATION W <u>I</u> RELESS	SECURITY	<u>S</u> ERVICES	Sa <u>v</u> e (<u>M</u> ANAGEMENT	Configuration	Ping Logout	<u>R</u> efresh			
Security	STATISTICS	E GENERA	L SET-UP	Y	EAP-FAST SET-UP						
	Hostname ap-1				ap-1	uptime is 1 day	y, 4 hours, 43 mir	nutes			
Encryption Manager	Security: Local RADIUS Se	rver - General Set-Up									
SSID Manager	Local Radius Server Auther	ntication Settings									
Dot11u Manager	Enable Authentication Pro	tocols: 🔽 EA	P FAST								
Server Manager			AP								
Intrusion Detection											
Local RADIUS Server		•				Α	pply Cancel				
Advance Security											
	Network Access Servers (AAA Clients)										
	Current Network Access S										
	< NEW > 10.9.0.9		Network Acces	s Server:	10.9.0.9		(IP Address)				
		\$	Shared Secret:		••••••						
	Delete										
	Delete						anka Connad				
						A	pply Cancel				
	Individual Users										
	Current Users										
	< NEW >	Username:	wds								
	was	Password:		•••••		🔿 Text 💿 NT	l Hash				
		Confirm Pas	sword:								
	Delete	Group Name	e:	< NONE >	0						
				MAC Au	thentication Only						
						A	pply Cancel				
								_			
	User Groups										
	Current User Groups										
	< NEW >	Group Name:									
		Session Timeout (o	optional):			(1-4294967295 s	ec)			
	Delete	Foiled Authenti	one hofers I -	akout (ant)-	anal):	(1.4204067005	`				
	Delete	Paried Authenticati	ons before Lo	ckout (optio	() l=6='t-	(1-4294907295	,				
		Lockout (optional).									
					 Interval 	(1-42	294967295 sec)				
		VLAN ID (optional)	:								
		SSID (optional):					Add				
							Delete				
						_ A	pply Cancel				

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.

،، ،،، ،، cısco	<u>H</u> OME	<u>N</u> ETWORK	ASSOCIATION	WIRELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e (5 <u>M</u> ANAGEMENT	Configuration	Ping Logou	t <u>R</u> efresh
Wireless Services	Host	name ap-1					ar	o-1 uptime is 1 d	lay, 4 hours, 50) minutes
WDS	Wir	eless Service	s: AP							
WDS	Pa	rticipate in S	WAN Infrastructure	ə: (Enable 🔵 D	lisable				
			WDS Disco	very:	Auto Discove	ry				
					Specified Dis	covery: 10.	9.0.9	(IP Address)		
			Username:	w	ds					
			Password:	•	•••••					
			Confirm Pa	ssword:						
			Authenticat Methods Pr	tion rofile:	< NONE >	<u></u>	Define Authentication	Methods Profiles		
									Apply	Cancel

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.

ıılıılı cısco	HOME <u>N</u> ETWORK	ASSOCIATION	W <u>I</u> RELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	Sa <u>v</u> e <u>M</u> ANAGEMENT	Configur	ration <u>P</u> ing WARE <u>E</u> VI	Logout <u>R</u> efresh ENT LOG
Wireless Services		TATUS	GENER	AL SET-UP		SERVER GROU	PS		E haven d minute
AP	Hostname ap-1						ap-1 up	otime is 1 day	, 5 nours, 1 minute
WDS	Wireless Services: WDS - Wireless Domain Services - Status								
	WDS Informatio	n							
	MAC Address	IPv4 Addr	ess	IPv6 Addre	955	Priority		State	
	18e7.281b.3f54	10.9.0.9		:: 255		255	Administrativ		ively StandAlone
WDS Registration									
	APs: 1		Mobile Nodes: 0						
	AP Information								
	Hostname	MAC Add	MAC Address		955	IPv6 Address		CDP Neighbor	State
	ap-1	18e7.281b	.3f54	10.9.0.9		:: Switch-2.gil REGI		REGISTERED	
	Mobile Node Inf	ormation							
	MAC Address	IP Address	State			SSID	VLAN I	D BSS	ID
	Wireless Network Manager Information								
	IP Address	Authentication Status							
									Refresh

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.

uluili. cisco	Home Network Ass	OCIATION WIRELESS SECU	Sa <u>v</u> e Co RITY <u>S</u> ERVICES <u>M</u> ANAGEMENT	onfiguration <u>P</u> ing Logout <u>R</u> efresh <u>S</u> OFTWARE <u>E</u> VENT LOG
Services		RADIO0-802.11N ^{2.4GHZ} ACCESS CATEGORIES	RADIO1-802.11AC ^{5GHZ} ACCESS CATEGORIES	ADVANCED
Telnet/SSH	Hostname ap-1		ap-1	uptime is 1 day, 4 hours, 44 minutes
Hot standby				
CDP	Services: QoS Policies			
DNS	Create/Edit Policies			
Filters	Create/Edit Baliav	Vaice		
нттр	create/Eult Folicy.	Voice		
QUS				
SNMP	Policy Name:	Voice		
SNTP				
VLAN	Classifications:	DSCP - COS Controlled Load (4) DSCP - COS Video < 100ms Latence	vy (5)	
ARP Caching		DSCP - COS Voice < 10ms Latency	(6)	
Band Select				
Auto Config		Delete Classification		
	Match Classification	IS:	Apply Class of	Service
	IP Precedence:	Routine (0)	Best Effort (0)	Add
	IP DSCP:	 Best Effort 	Sest Effort (0)	Add
		0	-63)	
	IP Protocol 119		Best Effort (0)	Add
	Filter:	No Filters defined. Define Filters.		
	Default Classification	on for Packets on the VLAN:	Best Effort (0)	Add
	Rate Limiting:			
	Bits per Sec.:	(8000-20000000	0) Burst Rate (Bytes):	(1000-512000000)
	Conform Action:	Transmit ᅌ	Exceed Action: Drop ᅌ	Add
	Apply Policies to Interfa	ce/ VLANs		Apply Delete Cancel
	VLAN 2	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHZ}	GigabitEthernetu
			Data 😒	Data 📀
	Outgoing		Data 📀	Data 📀
	VLAN 3	Radio0-802.11N ^{2.4GHz}	Radio1-802 114C ^{5GHz}	GigabitEthernet0
	Incoming		Voice	Voice 🗘
	Outgoing		< NONE > 🗘	< NONE > 🗘
	VLAN 10	Radio0-802.11N ^{2.4GHz}	Radio1-802.11AC ^{5GHz}	GigabitEthernet0
	Incoming		< NONE > ᅌ	< NONE > ᅌ
	Outgoing		< NONE > ᅌ	< NONE > 📀
				Apply Cancel

To enable QBSS, select Enable and check Dot11e.

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

Ensure IGMP Snooping is enabled.

Ensure Wi-Fi MultiMedia (WMM) is enabled.

սիսիս	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efres
CISCO	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Services	QoS POLICIES RADIO0-802.11N2 ^{4GHZ} ACCESS CATEGORIES ADVANCED
Telnet/SSH	Hostname ap-1 ap-1 uptime is 1 day, 4 hours, 47 minutes
Hot standby	
CDP	Services: QoS Policies - Advanced
DNS	IP Phone
Filters	
НТТР	QoS Element for Wireless Phones : O Enable Z Dot11e
QOS	O Disable
Stream	
SNMP	IGMP Snooping
SNTP	Snooping Helper: O Enable () Disable
VLAN	
ARP Caching	
Band Select	AVVID Priority Mapping
Auto Config	Map Ethernet Packets with CoS 5 to CoS 6: O Yes No
	WiFi MultiMedia (WMM)
	Enable on Radio Interfaces:
	Radio0.802 11N2.4GHz
	Radio1-802.11AC ^{5GHz}
	Apply Cancel

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.

ululu cisco	HOME NETWORK ASSOCIATI	ON WIRELESS SECURITY	SERVICES	Sa <u>v</u> e Co MANAGEMENT	nfiguration <u>P</u> ir	ig Logout <u>R</u> efresh VENT LOG
Services	RADIO0-802.11N2.4GHZ	RADIO1-802.11AC5GHZ				
Telnet/SSH	Hostname ap-1			ap-1	uptime is 1 day,	4 hours, 48 minutes
Hot standby	Comissos Stream					
CDP	Services. Stream					
DNS	Packet Handling per User Pr	iority:				
Filters	User Priority	Packet Handling	Max Retries for Pa	cket Discard		
НТТР	CoS 0 (Best Effort)	Reliable	NO DISCARD	(0-128)		
QOS	CoS 1 (Background)	Paliable		(0-128)		
Stream	,	Kellable	NO DISCARD	(0-120)		
SNMP	CoS 2 (Spare)	Reliable	NO DISCARD	(0-128)		
SNTP	CoS 3 (Excellent)	Reliable	NO DISCARD	(0-128)		
VLAN	CoS 4 (Controlled Load)	Dellable		(0.128)		
ARP Caching	,	Reliable	NO DISCARD	(0-120)		
Band Select	CoS 5 (Video)	Reliable	NO DISCARD	(0-128)		
Auto Config	CoS 6 (Voice)	Reliable	NO DISCARD	(0-128)		
	CoS 7 (Network Control)	Reliable	NO DISCARD	(0-128)		
	Low Latency Packet Rates:					
	6.0Mb/sec :	Nominal Non-Nominal	 Disable 			
	9.0Mb/sec :	Nominal Non-Nominal	 Disable 			
	12.0Mb/sec :	Nominal Non-Nominal	 Disable 			
	18.0Mb/sec :	Nominal Non-Nominal	 Disable 			
	24.0Mb/sec :	Nominal Non-Nominal	 Disable 			
	36.0Mb/sec :	Nominal Non-Nominal	 Disable 			
	48.0Mb/sec :	O Nominal O Non-Nominal	 Disable 			
	54.0Mb/sec :	Nominal Non-Nominal	 Disable 			
					A	pply Cancel

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.

							Sa <u>v</u> e (Configuration	Ping Logout	<u>R</u> efresh
cisco	<u>H</u> OME	<u>N</u> ETWORK	<u>A</u> SSOCIATION	W <u>I</u> RELESS	<u>S</u> ECURITY	<u>S</u> ERVICES	<u>M</u> ANAGEMENT	<u>S</u> OFTWARE	<u>E</u> VENT LOG	
Services	Host	name ap-1					ap	o-1 uptime is 1 d	lay, 4 hours, 50 m	inutes
Teinet/SSH										
Hot standby	Ser	vices: ARP C	aching							
CDP	Cli	ent ARP Cacl	ning: O En	able 🔿 Disa	able					
DNS										
Filters										
нттр			For	ward ARP Red	quests To Rad	o Interfaces V	hen Not All Client	IP Addresses A	vre Known	
QOS										
Stream										
SNMP									Apply	Cancel

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**.

ululu cisco Meraki	Q Search Dashboard
NETWORK	Create network
Meraki MX64 🛛 👻	
	Setup network
Network-wide	Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization.
Security & SD-WAN	Network name Scranton Branch Office
Organization	
	Network type Wireless - 0
	Network configuration O Default Meraki configuration
	○ Bind to template No templates to bind to ●
	Clone from existing network Select a network -
	Select devices from inventory
	You have no unused devices Add new devices or go to the inventory page to select devices
	that are already in networks
	Add devices Go to inventory
	Create network

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

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

Cisco Meraki access points can be claimed 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 the	ese numbers?	
	Close	Claim

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

cisco Meraki	Q Search Dashboard	
NETWORK	Inventory	
Meraki WLAN 👻	View used and unused devices in your organization. You can <u>claim</u> new device	s to add the list below.
	Add to Unclaim Unused Used Both Search inventory	
Network-wide	O Existing network Model [▲]	Claimed on
	Meraki WLAN v 9K7 MR53	4/29/2020 2:59 PM
Wireless	New network Add to existing	
Organization		

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

cisco Meraki	Q Search Dashboard				
NETWORK	Add access points	;			
Meraki WLAN 👻	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 in	ventory. Once in your inventory,	you can add dev	ices to your network(s).	
Network-wide	Search inventory				
Wireless	MAC address	Serial number	Model *	Claimed on	
	✓ 88:15:44:60:18:8c	Q2MD-MWQS-J9K7	MR53	4/29/2020 2:59 PM	
Organization					
	Add access points				

SSID Configuration

To create 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 **Renam**e.

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

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

cisco Meraki	Q Search Dashboard	
NETWORK	Access control	
Meraki WLAN 👻	SSID: meraki-voice	Θ
Network-wide Wireless Organization	Network access Association requirements	 Open (no encryption) Any user can associate Pre-shared key (PSK) Users must enter a passphrase to associate MAC-based access control (no encryption) RADIUS server is queried at association time Enterprise with Meraki Cloud Authentication S
	WPA encryption mode 802.11r (9) 802.11w (9)	WPA2 only (recommended for most deployments) Image: Commended for most deployments) Image: Commended for most deployments) Enabled Image: Commended for most deployments) Image: Commended for most deployments) Image: Commended for most deployments) Enabled Image: Commended for most deployments) Image: Commended for most deploymen
	Splash page	• None (direct access) Users can access the network as soon as they associate

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

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

cisco Meraki	Q Search Dashboard				
NETWORK	User management p	portal			
Meraki WLAN 👻	SSID: meraki-voice	with Meraki authentication. The	ese 802.1X accounts are n	nanaged separately from Administrate	r or Guest accounts.
	Authorization - Remove Users	Search			
Network-wide	Description	Email (Username)	Account type	Authorized for SSID *	Authorized by
Wireless					
Organization				Save Changes or cancel	
			(Pl	ease allow 1-2 minutes for changes to take effe	ict.)
		Create user Account type: Meral	ki 802.1X		×
		Description:			
		Email (Username):			_
		Password:	Ge	nerate	
		Authorized: No	9		_
				Close Print Cr	eate user

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

disco Meraki	Addressing and traf	ffic
NETWORK	Client IP assignment	NAT mode: Use Meraki DHCP Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the <u>SSID firewall settings</u> permit.
Meraki WLAN 🔫		O Bridge mode: Make clients part of the LAN Meraki devices operate transparently (no NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and wireless cameras.
Network-wide		C Layer 3 roaming
Wireless		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.
Organization		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 Bridge mode and layer 3 roaming only	Use VLAN tagging
	VLAN ID	AP tags VLAN ID Actions
		All other APs 3
		Add VLAN
	Content filtering O NAT mode only	Don't filter content
	Bonjour forwarding Bridge mode and layer 3 reaming only	Enable Bonjour Gateway
	countly only	There are no Bonjour forwarding rules on this network. Add a Bonjour forwarding rule

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.

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**.

cisco Meraki	Q Search Dashboard	
NETWORK	SSID availability	
Meraki WLAN 🔫	SSID: meraki-voice	0
	Visibility	Advertise this SSID publicly
Network-wide	Per-AP availability	This SSID is enabled on all APs
	Scheduled availability	disabled
Wireless		
Organization		

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.

'dudi' Meraki	Q Search Dash	board						
NETWORK	Radio sett	ings						
Meraki WLAN 👻	Overview R	profiles						
	BAND	CHANNEL		AP TAG	RF PROFILE	REGULATORY DOM	AIN	
Network-wide	5	- All	*	MR53 *	All *	FCC Edit		
Wireless	Search by AP n	ame				Upo	date auto channels	Edit settings
Organization	Status 🕲	AP name ⊾	Channel	Ch. Width (MHz)	Target power (dBm) 🕲	Transmit power (dBm) 🕲	RF Profile	÷
	0	MR53	36 (Auto)	20	8 - 30	8	Basic Indoor	Profile

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

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

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.



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.

ululu cisco Meraki	Q Search Dashboard								
NETWORK Meraki WLAN 🗸	Firewall & traffic s	sha	ping C						
Network-wide	Block IPs and ports Layer 2 LAN isolation	Disa	abled ᅌ (bi	idge mode	only)				
Wireless	Layer 3 firewall rules 0	#	Policy	Protocol	Destination	Port	Comment	Actions	
Organization		Add	Allow 😒 Allow a layer 3 fi	Any Any rewall rule	Local LAN Any	Any Any	Wireless clients accessing LAN Default rule		
	Block applications and content categories								
	Layer 7 firewall rules	The <u>Add</u>	re are no ru <u>I a layer 7 f</u> i	les defined rewall rule	for this SSID.				
	Traffic shaping rules Per-client bandwidth limit	unlin	nited	details	Enable Sp	peedBu	rst 0		
	Per-SSID bandwidth limit ③ Shape traffic	Unlin Sha	nited	details his SSID	0				

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.

Cisco 9861 Online - Phones - Webex Aware - Device platform: th	Actions > (名)
Overview History	
Details 16 84:5A:3E:C2:18:14	Connected Peripherals
Lines MAC address	Hoteling
PHONEOS.3-1-1-0004-20240522- f72ed9f1ba Software Version Software Channel	Allow this device to be used as a Hoteling Host by visiting guests.
Cisco Managed By	24 Hours 🗸
Tags	Configurations
+ Add tag	Configuration templates
	Device Management

Workspace Usage

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

Cisco Webex Control Hub		
G Overview	c Add Device	×
MONITORING	Assign to an existing workspace or a new workspace?	
🗇 Organization Health	Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspace If you add multiple devices in a workspace that are not designed to work together, it may create interference issues	e.
[a] Analytics		
✓ Troubleshooting	۶	
MANAGEMENT		
2 Users	\vee	
Workspaces		
Devices	Existing Workspace New Workspace	
88 Apps		
C Account		
Organization Settings	Which Workspace will the device be assigned to?	
SERVICES	Workspaces containing devices that are not Cisco IP Phones will not be shown, since you can only have one of these devices in a workspace.	
O Messaging	Search for a Workspace	
🛱 Meeting		
% Calling		
Hybrid		
	Back Ne:	

Cisco Webex Control Hub							
G Overview	C Add Device ×						
MONITORING	Assign to an existing workspace or a new workspace? Select Existing Workspace to activate a device if the previous code has been lost or has expired, or to have multiple devices in a workspa If you add multiple devices in a workspace that are not designed to work together, it may create interference issues.						
은 Users							
Devices	Existing Workspace New Workspace						
Account	Where will this device he legated?						
SERVICES	What would you like to call the Workspace that this device will be assigned to?						
○ Messaging ➡ Meeting	insert name of device location, e.g. Reception of Bo						
S Calling △ Hybrid	Back Next						

Wi-Fi Capability

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

Device configurations	📕 Cisco 9861 • Yuhul_hd • • Online								
	O Configure — O Burntary								
	Regional	Control Timer Values							
		Phone Language							
	SIP	ICE				~			
		User Preferred Offhook Timer							
	Saftwara								
	JULIWOIE	Upgrade Channel				×			
	System	Bluetooth Enabled							
		IEEE8021X							
		Optional Network Configuration							
		USB Settings							
		VLAN Settings							
		Web Access							
	Will Erable	Will Enabled							
			Supported device types	Configuration value	Default O Undo				
			Cisco 9861	(Yes (Defauit)	Factory ⊙ Yes				
		1		Yes					
	Thousand Eyes			No					

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	0
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* Enabled 🔉 🗆

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.

Enterprise Parameters Configuration				
Parameter Name	Parameter Value	Suggested Value		
Cluster ID_*	StandAloneCluster	StandAloneCluster		
Max Number of Device Level Trace *	12	12		
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)		
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)		
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)		
Connection Monitor Duration *	120	120		
Auto Registration Phone Protocol *	SCCP C	SCCP		
Auto Registration Legacy Mode *	False	False		
BLF For Call Lists *	Disabled	Disabled		
Advertise G.722 Codec *	Enabled ᅌ	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 Wirless 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	🔚 Save 💥 Delete 📄 Copy 睯 Reset 🥒 Apply Config 🕂 Add New		
Status			
i Status: Ready			
Phone Security Prof	ile 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 v		
Transport Type*	TLS v		
Enable Digest Authentication			
TFTP Encrypted Co	TFTP Encrypted Config		
Enable OAuth Auth	nentication		

- 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	<pre>< None ></pre>	~	
SIP Profile*	Standard SIP Profile	~	View Detail
Digest User	< None >	~	
Media Termination Point Require	red		
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.

cisco	Cisco Unif For Cisco Unified	ied CM Ad	ministration					
System 👻	Call Routing - Me	dia Resources 👻	Advanced Features -	Device 👻	Application -	User Management 👻	Bulk Administration	n 👻 Help 👻
Find and	List Wireless LAN	Profiles						
Add N	lew							
Wireles	s LAN Profile							
Find Wirel	ess LAN Profile wher	e Name	ᅌ begin:	s with 📀		Find	Clear Filter	
				No active	query. Please ent	er your search criteria u	sing the options above	s
Add Ne	ew							

3. 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

CISCO For Cisco U	Inified CM Administration	
System - Call Routing -	Media Resources - Advanced Features -	Device - Application -
Wireless LAN Profile (Configuration	
Save		
Status		
i Status: Ready		
Wireless LAN Profile I	Information	
Name*		
Description		
User Modifiable* Allow	red	
Wireless Settings		
SSID (Network Name)*		
Frequency Band *	Auto	
Authentication Setting	gs ————	
Authentication Method*	EAP-FAST	0
Provide Shared Cred	entials	
Password Description		
Network Access Setti	ngs	
Network Access Profile	< None >	View Details
Save		

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

Name*	
Description	

• 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.

Wireless LAN Pro	ofile Configuration		
Save 🗶 D	elete [Copy 🕂 Add New		
Status	Status Status: Ready		
Wireless LAN Pr	Wireless LAN Profile Information		
Name*	lsc-test		
Description User Modifiable [*]			
Wireless Setting Restricted			
SSID (Network Name)* Isc-test			
Frequency Band*	Auto		

- 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 *	Auto	٢

• 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.

Authentication Method* EAP-	FAST
Provide Shared Credentials Password Description	
Authentication Method* PEAP	-GTC 📀
Provide Shared Credentials	
Password Description	
Authentication Method* PEAP	-MSCHAPv2
Provide Shared Credentials	
Password Description	

• 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**.

Authentication Method*	EAP-FAST	٥
Provide Shared Crede	entials	
Username		
Password		
	show password	
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 Certicate) or User Installed.

Authentication Method*	EAP-TLS
User Certificate*	MIC
Authentication Method*	EAP-TLS
User Certificate*	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.

Authentication Method *	PSK
PSK Passphrase*	
	show passphrase
Password Description	

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

Authentication Method* None	٢
-----------------------------	---

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 Wirless 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.

cisco	Cisco U For Cisco U	nified CM Ad	ministration ons Solutions					
System 👻	Call Routing 👻	Media Resources 👻	Advanced Features 👻	Device 👻	Application -	User Management 👻	Bulk Administration 👻	Help 👻
Find and	List Wireless	LAN Profile Group	s					
Add N	lew							
Wireles	s LAN Profile (Group						
Find Wirel	ess LAN Profile	Group where Group	Name ᅌ begins wit	h ᅌ		Find Cl	ear Filter 🔒 😑	
				No active	query. Please ent	er your search criteria u	sing the options above.	
Add Ne	ew							

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

Wireless LAN Prof	ile Group Configuration
Save 🗙 Dele	ete 🗋 Copy 🐈 Add New
_ Status	
(i) Update success	ful
┌ Wireless LAN Prof	ile Group Information
Name* 9871 Description	
Profiles for this W	ireless LAN Profile Group
Available Profiles	Gorilla-dot1x-hide
	Test
	for_test
	gulian_eap
Selected Profiles**	BTHub5-86GN

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 Ma	anager Group*	Default		~
Calling Search Space for Auto-reg	gistration	< None >		~
Adjunct CSS		< None >		~
Reverted Call Focus Priority		Default		~
Intercompany Media Services En	rolled 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		
V Device is Active		
Device is trusted		
MAC Address*	845A3EC211B6	(SEP845A3EC211B6)
Description	Auto 99899	
Current On-Premise Onboarding Method is	s set to Autoregistration. Activation Code will only apply	to onboarding via MRA.
Require Activation Code for Onboarding		
Allow Activation Code via MRA		
Activation Code MRA Service Domain	Not Selected V	View Details
Device Pool*	9871 ~	View Details
Common Device Configuration	< None > ~	View Details
Phone Button Template*	DocTest ModelD 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** dropdown 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.

- Enter the IP address of the phone in your web browser address bar. For example, <u>http://10.64.84.147/</u>
- 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

$\leftarrow \rightarrow $ C	○ 掻 10.74.	151.106/admin/ad	ivanced												ŝ	
uluulu ^{ca} cisco D	sco IP Phone for 3r DP-9871(^{rd Party Call}	^{Control} urat	ion	Jtilit	y										
No password provided Info Voice C	Call History Personal Direct	tory														
System SIP	Provisioning Region	al Phone	Ext 1	Ext 2	Ext 3	Ext 4	Ext 5	Ext 6	Ext 7	Ext 8	Ext 9	Ext 10	Ext 11	Ext 12	Ext 13	Ext 14
	Seco	ndary NTP Server:											Use Config TOS	No 👻		
		Siplog Server:														
VLAN Settings																
		VLAN ID:	1									P	C Port VLAN IE	c 1		
		Enable CDP:	Yes -									Ena	able LLDP-MED	Yes -		
	DH	ICP VLAN Option:														
Wi-Fi Settings																
		Phone-wifi-on:	Yes -													
Wi-Fi Profile 1																
		Network Name:	xin-wpa3	-23-SAE									Security Mode	PSK -		
		Wi-Fi User ID:											Wi-Fi Password			
		Eronuoneu Bondi	E CHa													

6. Click Submit All Changes.

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

\leftrightarrow \rightarrow (♡ 🔒 10.74.151.106		☆
ciso	II. Cisco IP Phone for 3rd Party Call ODP-9871 Configu	Control uration Utility	
🔺 No passv	vord provided		
Info	Voice Call History Personal Directory		
Status	Debug Info Download Status Network Statistics		
System Inf	ormation		
	Host Name:	SEP845A3EC2302B Domain:	crdc.cisco.com
	Primary NTP Server:	10.64.58.51 Secondary NTP Server:	
	Bluetooth Enabled:	No Bluetooth Connected:	No
	Bluetooth MAC:	Connected Device ID:	
	Active Interface:	Wireless Wireless MAC:	84:5A:3E:C2:30:2D
	SSID:	xin-wpa3-23-SAE AP MAC:	6C:8B:D3:F0:02:EF
	Channel:	64 Frequency:	5320 MHz
	Security Mode:	PSK	

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.

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



- 5. 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.
- 6. 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.

¢	-)	Security mode	
	Auto		~
	EAP-FAST		
	EAP-PEAP		
	EAP-TLS		

7. 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.

Join other ne	etwork	← Join other	network Apply
1 Network name		Enter network	information
2 Security mode	psk >	Network name	
3 Password		Security mode	psk >
4 Frequency band	Auto 📏	Password	•
		Frequency band	Auto >
Apply	🗵 🛛 Back		

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.

BTHub5-86GN • Connected		← TP-LINK_24G ● Connected	
1 Security mode	PSK	Security mode	PSK
2 Advanced Wi-Fi details	>	Forget this network	
Forget	Back		

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.

	Web Admin* Admin Password	Enabled	\$		
Open manual install page via https://x.x.x.x8443					

ululu cisco	Sign in User Sign In Cisco IP Phone DP-9861 (SEP845A3EC22785)
Device information	Username
Network setup	
Satur	Password
Setup	
Certificates	Submit

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.

de de					Signed in as a	idmin, <u>Sign o</u> i
cisco			Certificates			
cisco		Cisco	IP Phone DP-9861 (SEP845A3EC22785)			l
Device information	Type	Common name	Issuer name	Valid from	Valid to	
Network setup	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	
Certificates	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
Network statistics	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
Ethernet information	User installed	<not installed=""></not>	<not installed=""></not>			Install
Access	Authentication server CA	<not installed=""></not>	<not installed=""></not>			Install

This root CA should 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.

	Signed in as admin. Sign out
cisco	Cisco IP Phone DP-9861 (SEP845A3EC22785)
Device information	Select file (.p12 or .pfx) to upload: Browse No file selected.
Network setup	Fetrad nesswork
Setup	
Certificates	Upload

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

ahaha	Signed in as admin, Sign.com Certificates
cisco	Cisco IP Phone DP-9861 (SEP845A3EC21655)
Device information	Authentication Server CA certificate has been updated.
Network setup	Phone will use the new certificate after reboot. You can restart the phone with:
Setup	"System/Restart"
Certificates	

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.

	Cisco Unified CM	Administratio	Skin to	Content	Navigation	Cisco Unified CM Ac	Iministration	
cisco	For Cisco Unified Communi	cations Solutions		Content	lavigation	admin	About	Locout
							About	LUguu
System Ca	all Routing - Media Resource	es Advanced Features	Device Application	User Manag	ement 👻	Bulk Administration	неір 🕶	_
ervice Para	meter Configuration			Rela	ated Links	s: Parameters for	All Servers	✓ G
📄 Save 🤞	Set to Default							
Status ——								
i Status: F	Ready							
Select Serve	er and Service							
Server*	10.77.46.225CUCM Voi	ce/Video (Active)	~					
Forvico*	Cisco Certificate Authorit	v Proxy Function (Active)	~					
Service	Cisco Ceruincate Authority Proxy Function (Active)							
All parameter	icate Authority Proxy Fun	ction (Active) Parameters	that are in the cluster-wide g	roup(s). 5CUCM Vo	pice/Video	o (Active)		ę
All parameter Cisco Certific Parameter Nar	icate Authority Proxy Fun	ction (Active) Parameter Val	that are in the cluster-wide g ers on server 10.77.46.225	roup(s). 5CUCM Vo	pice/Video Sugge	o (Active)		g
All parameters Cisco Certific Parameter Nar Certificate Iss	cate Authority Proxy Fun me suer to Endpoint.*	ction (Active) Parameters Parameter Val Online CA	that are in the cluster-wide g ers on server 10.77.46.225 ue	iroup(s). 5CUCM Vo	Dice/Video Sugge V Cisco	o (Active) ested Value Certificate Authorit	y Proxy Fun	ction
All parameters Cisco Certific Parameter Nar Certificate Iss Duration Of C	ser to Endpoint *	ction (Active) Parameters Parameter Val Online CA * 1825	that are in the cluster-wide g	roup(s). 5CUCM עמ	Sugge Cisco	o (Active) ested Value Certificate Authorit	y Proxy Fun	ction
All parameters Cisco Certific Parameter Nar Certificate Iss Duration Of C Maximum Allo	ser to Endpoint. * Certificate Validity (in days). Devale Fine For Key Genera	ction (Active) Parameters Parameter Val Online CA * 1825 ttion. * 30	that are in the cluster-wide g	iroup(s). 5CUCM Vo	Sugge Cisco 1825 30	o (Active) ested Value Certificate Authorit	y Proxy Fun	ction
All parameter Cisco Certific Parameter Nar Certificate Iss Duration Of Co Maximum Allo Maximum Allo	ser to Endpoint. * Certificate Validity (in days). Dowable Time For Key Genera Dowable Attempts for Key Genera	ction (Active) Parameters Parameter Val Online CA * 1825 tion.* 30 neration.* 3	that are in the cluster-wide g ers on server 10.77.46.22! ue	iroup(s). 5CUCM Vo	Sugge Cisco 1825 30 3	o (Active) asted Value Certificate Authorit	y Proxy Fun	ction
All parameter Cisco Certific Parameter Nar Certificate Iss Duration Of C Maximum Allo Maximum Allo	ser to Endpoint. * Cate Authority Proxy Fun me suer to Endpoint. * Certificate Validity (in days). In the For Key Genera In the For Key Genera In the For Key Genera In the For Key Genera	ction (Active) Parameters Parameter Val Online CA * 1825 tion.* 30 neration.* 3	that are in the cluster-wide g ers on server 10.77.46.225 ue	iroup(s). 5CUCM Vo	Sugge Cisco 1825 30 3	o (Active) ested Value Certificate Authorit	y Proxy Fun	ction
All parameter Cisco Certific Parameter Nar Certificate Iss Duration Of C Maximum Allo Maximum Allo Online CA H	ser to Endpoint. * Certificate Validity (in days). Dowable Time For Key Genera Dowable Attempts for Key Genera Dowable Attempts for Key Genera Dostname	server except parameters ction (Active) Parameter Parameter Val Online CA * 1825 tion.* 3 CUCM62.CA.	that are in the cluster-wide g ers on server 10.77.46.225 ue	iroup(s). 5CUCM Vo	Sugge Cisco 1825 30 3	o (Active) ested Value Certificate Authorit	y Proxy Fun	ction
All parameter All parameter Cisco Certific Parameter Nar Certificate Iss Duration of C Maximum Allo Maximum Allo Online CA He Online CA Pe	icate Authority Proxy Fun me suer to Endpoint. * Certificate Validity (in days). owable Time For Key Genera owable Attempts for Key Genera owable Attempts for Key Genera lostname ort	server except parameters ction (Active) Parameter Parameter Val Online CA * 1825 tion.* 30 neration.* 3 CUCM62.CA. 443	that are in the cluster-wide g ers on server 10.77.46.225 ue	iroup(s).	Sugge Cisco 1825 30 3	o (Active) ested Value Certificate Authorit	y Proxy Fun	ction
All parameter All parameter Cisco Certific Parameter Nar Certificate Iss Duration Of C Maximum Allo Maximum Allo Maximum Allo Conline CA H Online CA H Online CA Pe Online CA Te	icate Authority Proxy Fun me suer to Endpoint. * Certificate Validity (in days). owable Time For Key Genera owable Attempts for Key Genera owable Attempts for Key Genera lostname ort emplate	server except parameters ction (Active) Parameter Parameter Val Online CA * 1825 tion.* 3 CUCM62.CA. 443 CIscoRA_1	that are in the cluster-wide g ers on server 10.77.46.225 ue	roup(s).	Sugge Cisco 1825 30 3	o (Active) ested Value Certificate Authorit	y Proxy Fun	ction
All parameter All parameter Cisco Certific Parameter Nar Certificate Iss Duration Of C Maximum Allo Maximum	icate Authority Proxy Fun me suer to Endpoint. * Certificate Validity (in days). owable Time For Key Genera owable Attempts for Key Genera owable Attempts for Key Genera lostname ort emplate ype. *	server except parameters ction (Active) Parameter Parameter Val Online CA * 1825 tion.* 3 CUCM62.CA. 443 CIscoRA_1 Microsoft CA	that are in the cluster-wide g ers on server 10.77.46.225 ue	iroup(s).	Sugge Cisco 1825 30 3 Microz	o (Active)	y Proxy Fun	ction
All parameter All parameter Cisco Certific Parameter Nar Certificate Iss Duration Of C Maximum Allo Maximum	icate Authority Proxy Fun me suer to Endpoint. * Certificate Validity (in days) owable Time For Key Genera owable Attempts for Key Genera owable Attempts for Key Genera lostname ort emplate ype. * Isername	server except parameters ction (Active) Parameter Parameter Val Online CA * 1825 tion.* 3 CUCM62.CA. 443 CIscoRA_1 Microsoft CA	that are in the cluster-wide g ers on server 10.77.46.229 ue	roup(s). 5CUCM Vo	v Cisco 1825 30 3 Micro:	o (Active)	y Proxy Fun	¢
All parameter All parameter Cisco Certifica Parameter Nar Certificate Iss Duration Of Cr Maximum Allo Maximum Allo Maxim	icate Authority Proxy Fun me suer to Endpoint. * Certificate Validity (in days) owable Time For Key Genera owable Attempts for Key Genera owable Attempts for Key Genera owable Attempts for Key Genera owable Attempts for Key Genera lostname ort emplate ype. * Isername assword	server except parameters ction (Active) Parameter Parameter Val Online CA * 1825 tion.* 3 CUCM62.CA. 443 CiscoRA_1 Microsoft CA	that are in the cluster-wide g ers on server 10.77.46.229 ue	roup(s). 5CUCM Vo	v Cisco 1825 30 3 Wilcro: ••••	o (Active)	y Proxy Fun	¢

Save Set to Default

Relat				
🔚 Save 🤣 Set to Default				
- Chatur				
Status Status: Ready				
- Select Server and Service				
Server* 10.79.57.147CIICM Voice/Video (Active)				
Service* Circo Cartificate Authority Provy Supplier (Active)				
All parameters apply only to the current server excent parameters that are	in the cluster-wide groun(s).			
in parameters opping only to be carried on the strategy parameters that are	n die easter mae Brook(s).			
Cisco Certificate Authority Proxy Function (Active) Parameters on s	server 10.79.57.147CUCM Voice/Video (Active)			
Parameter Name Certificate Issuer to Endpoint *	Parameter Value	Suggested Value Cisco Certificate Authority Proxy Function		
Duration Of Certificate Validity (in days) *	Clace Certaincate Additionally Proxy Function	1825		
Maniatum Alleurable Time Facility Consention	1825	1025		
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	ccmadministrator			
Online CA Type *	Microsoft CA v	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 Pro	xy 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 Contain	ns Addition CAPF Settings.				

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

	Security settings			
1	Security mode	Non sec	ure	
2	LSC	Installed	>	
3	Trust list		>	
4	802.1X Authentication		>	
	Select	Ba	ck	

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 I	List (1 -	14 of 14)							
Find Certificate	e List where	Certificate	~	begins with v	CAPF	ct item	or enter	Find Cl	lear Filter 🔂 📼
Certificate 🕇		Common Name/Common Name_SerialNumbe	er	Usag	e	Туре	Кеу Туре		Distribution
CAPF	CAPF-50aa	<u>97cf</u>		Ident	ity S si	elf- igned	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.

duale Identity Services Engine	Home	Policy	tion Work Centers			
▼ System → Identity Management →	Network Resources Device Portal Management	pxGrid Services F	eed Service	Centric NAC		
Deployment Licensing - Certificate	s → Logging → Maintenance Upgrade → Back	up & Restore + Admi	Access > Settings			
0						
✓ Certificate Management	Trusted Certificates					
System Certificates	🖊 Edit 🕂 Import 🕼 Export 🗙 Delete 🔎 View					
Trusted Certificates	Friendly Name	 Status 	Trusted For	Serial Number	Issued To	Issued By
OCSP Client Profile	802.1x_mingjzho_4096CA	Enabled	Cisco Services Endpoints Infrastructure	0F 3A 91 F2 B3 63	test.sipura.cisco.com	test.sipura.cisco.com
Certificate Signing Requests	ASULIU-SCEP-CA#ASULIU-SCEP-CA#00009	Enabled	Infrastructure	62 F7 54 B0 81 B9	ASULIU-SCEP-CA	ASULIU-SCEP-CA
Certificate Periodic Check Setti	asuliu-SUBCA#ASULIU-SCEP-CA#00008	Enabled	Infrastructure	14 72 4E 9A 00 01	asuliu-SUBCA	ASULIU-SCEP-CA
Certificate Authority	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro
	CAPF-50aa97cf	Enabled	Infrastructure Cisco Services Endpoints	6A 4F 99 F8 B9 C0	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.

cisco	Signed in as admin, Sign out Certificates
Device information	Cisco in Priotic DP-9801 (SDF645A3DC22765)
Network setup	
Setup	Ohingan

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

	Signed in as admin, <u>Sign out</u>
ahaha	Certificates
cisco	Cisco IP Phone DP-9861 (SEP845A3EC21655)
Device information	Authentication Server CA certificate has been updated.
Network setup	Phone will use the new certificate after reboot. You can restart the phone with:
Setup	<u>"System/Restart"</u>
Certificates	

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		Cisco	Certificates IP Phone DP-9861 (SEP845A3EC21655)		Signed in a	as admin, <u>Sign c</u>
Device information	<u>Type</u>	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	
Cartificatas	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
Network statistics	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
Ethernet information	User installed	<not installed=""></not>	<not installed=""></not>			Install
Access	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**.

Certificate Operation*	Delete	~
Authentication Mode*	By Null String	~
Authentication String		
Generate String		
Key Order*	RSA Only	~
RSA Key Size (Bits)*	2048	~
EC Key Size (Bits)		~
Operation Completes By	2024 07 03 12 (YYYY:MM:DD:HH)	
Certificate Operation Status Note: Security Profile Conta	s: None ains 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		
WLAN Root CA Fingerprint (SHA256 or SHA1)	81512B4316429092925C6891701B374EBD254447	 	

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....

Add Roles Wizard	×
Specify User Acc	ount
Before You Begin Server Roles AD CS Role Services User Account CA for NDES RA Information Cryptography Confirmation Progress Results	Select the user account Network Device Enrollment Service should use when authorizing certificate requests. The user must be a member of the Domain and must be added to the local ITS_TUSRS group.
	< Previous Next > Install Cancel

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

Windows Securi	ty	×			
Add Role Serv	Add Role Services				
Speciry a name	and password.	-			
	lser name				
	Password				
	Domain: YD-MSCA				
	Insert a smart card				
	OK Cancel				

11. Enter the Registration Authority information.

Add Role Services	×
Specify Registrat	ion Authority Information
Role Services User Account RA Information Cryptography Confirmation Progress Results	A registration authority will be set up to manage Network Device Enrollment Service certificate requests. Enter the requested information to enroll for an RA certificate. Required Information RA Name: VD-MSCA-W2K8-MSCEP-RA Country/Region: US (United States) Coptional Information E-mai: Company: Department: Company: State/Province:
	< Previous Next > Install Cancel

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

Add Role Services		×
Configure Crypto	graphy for Registration Authority	
Role Services User Account RA Information	To configure cryptography, you have to select cryptographic service providers and key lengths for the signature key and the encryption key used to sign and encrypt communications between the device and the CA.	
Cryptography	Signature key is used to avoid repetition of communication between the CA and the RA.	
Confirmation	Signature key CSP: Key character length:	
Progress	Microsoft Strong Cryptographic Provider	
Results	Encryption key is used for secure communication between the RA and the network device. Encryption key CSP: Microsoft Strong Cryptographic Provider Microsoft Strong Cryptographic Provider More about signature and encryption keys	
	< Previous Next > Install Cancel	

14. Select Install.



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)

—	• •	·		
🎪 Registry Editor				
File Edit View Favorites Help				
🛱 🌗 Cryptography	Name	Туре	Data	ĺ
🕀 🌗 AutoEnrollment	(Default)	REG_SZ	(value not set)	
🕀 🄑 Calais	30 EnforcePassword	REG DWORD	0×00000000 (0)	
		-		
🕀 🍌 CertificateTemplateCache				
🕀 🆺 Defaults				
😑 🔒 MSCEP				
CAType				
CertsInMYStore				
EnforcePassword				
PasswordVDir				
UseSinglePassword				

- 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)

			1 8 1 1
💰 Registry Editor			
File Edit View Favorites Help			
🕀 🌗 Defaults	Name	Туре	Data
	(Default)	REG_SZ	(value not set)
CAType	EncryptionTemplate	REG_SZ	IPSECIntermediateOffline
CertsInMYStore	Abj GeneralPurposeT	REG_SZ	IPSECIntermediateOffline
EnforcePassword	ab Signature Template	REG_SZ	IPSECIntermediateOffline
LiceSingleDactword			

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

🗶 Certificate Templates Console			
File Action View Help			
Certificate Templates (YD-MSCA-W2K8	Template Display Name 🔺	Minimum Supported CAs	Versic 🔺
	Cross Certification Authority	Windows Server 2003 Ent	105.C
	Directory Email Replication	Windows Server 2003 Ent	115.C
	🚇 Domain Controller	Windows 2000	4.1
	Domain Controller Authentication	Windows Server 2003 Ent	110.C
	🗟 EFS Recovery Agent	Windows 2000	6.1
	🗟 Enrollment Agent	Windows 2000	4.1
	River Agent (Computer)	Windows 2000	5.1
	🚇 Exchange Enrollment Agent (Offline request)	Windows 2000	4.1
	Rechange Signature Only	Windows 2000	6.1
	🚇 Exchange User	Windows 2000	7.1
	IPSec	Windows 2000	8.1
	PSec (Offline request)	Windows 2000	7.1
	Rerberos Authentication	Windows Server 2003 Ent	110.C
	Rey Recovery Agent	Windows Server 2003 Ent	105.C
	QCSP Response Signing	Windows Server 2008 Ent	101.C
		Windows Server 2008 Ent	100.5
	RAS and IAS Server	Windows Server 2003 Ent	101.C
	Root Certification Authority	Windows 2000	5.1
	Router (Offline request)	Windows 2000	4.1
	Reference Scep User	Windows Server 2008 Ent	100.2
	SCEP-User	Windows Server 2008 Ent	100.3
	🖳 server Template	Windows Server 2003 Ent	100.2
	Real Smartcard Logon	Windows 2000	6.1
	🚇 Smartcard User	Windows 2000	11.1
	Subordinate Certification Authority	Windows 2000	5.1
	Real Trust List Signing	Windows 2000	3.1
	User Duplicate Template	Windows 2000	3.1
	User :	Windows 2000	4.1
	🖳 Web : All Tasks 🔹 🕨	Windows 2000	4.1
	Web: Properties	Windows Server 2003 Ent	100.3
	Web:	Windows Server 2008 Ent	100.5
	WiFi F Help	Windows Server 2008 Ent	100.4
	😬 WiFi Server Certificate template	Windows Server 2008 Ent	100.€
	Workstation Authentication	Windows Server 2003 Ent	101.C
	•		

22. Configure the Validity Period on the General tab as necessary.

CEP-User Properties 🛛 😤 🔀
Superseded Templates Extensions Security Server Cryptography Subject Name Issuance Requirements General Request Handling
Template display name: SCEP-User
Minimum Supported CAs: Windows Server 2008 Enterprise
SCEP-User
Validity period: Renewal period: 2 years 6 weeks
 Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

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.

CEP-User Properties			? ×
Superseded Templa General Cryptography	ates Extensions	Security Request Handlin Issuance Req	Server g juirements
Algorithm name: Minimum key size: Choose which crypto © Requests can us © Requests must us Providers:	RSA 2048 graphic providers can be e any provider available se one of the following p	e used for requests on the subject's co roviders:	▼ mputer
Microsoft Software	e Key Storage Provider		
Request hash:	SHA1		•
Use alternate sign For more informal	, nature format. ion about restrictions an	d compatibility clicl	< <u>here.</u>

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

Server Manager (YD-MSCA-W2K8)	Certificate Templates	
	Name	Intended Purpose
Active Directory Certificate Service Figure 1	Rep-User	Encrypting File System, Secure Email, Clien
i yichun-CA (V0.0)	CEP Encryption	Certificate Request Agent
🖳 Certificate Templates (YD-MS	Exchange Enrollment Agent (Offline req	Certificate Request Agent
🖃 🚽 yichun-CA	IPSec (Offline request)	IP security IKE intermediate
Revoked Certificates	Web ServerV3	Server Authentication
🧾 Issued Certificates	Web ServerV2	Server Authentication
🧮 Pending Requests	🖳 🚇 WiFi Server Certificate template	Server Authentication
Failed Requests	🖳 🖳 Directory Email Replication	Directory Service Email Replication
Certifica Mapage	Domain Controller Authentication	Client Authentication, Server Authenticatio
Sective Directory	EFS Recovery Agent	File Recovery
E Active Direct New	Certificate Template to Issue	Encrypting File System
🖃 🉀 yd-msca View	Domain Controller	Client Authentication, Server Authentication
	Web Server	Server Authentication
🖽 🔤 Com Refresh	Computer	Client Authentication, Server Authentication
Export List.	. User	Encrypting File System, Secure Email, Clien
	Subordinate Certification Authority	<all></all>
	Administrator	Microsoft Trust List Signing, Encrypting File
Active Directory Sites and Sector		
🖃 🧰 Sites		
🕀 🧰 Subnets		

27. Select SCEP User template.

Enable Certificate Templates	
Select one Certificate Template to en Vote: If a certificate template that wa nformation about this template has be All of the certificate templates in the o For more information, see <u>Certificate T</u>	able on this Certification Authority. s recently created does not appear on this list, you may need to wait until sen replicated to all domain controllers. rganization may not be available to your CA. remplate Concepts.
Name	Intended Purpose
Router (Offline request)	Client Authentication
🚇 SCEP User	Client Authentication, Secure Email, Encrypting File System
🗷 server Template	Server Authentication
🗷 Smartcard Logon	Client Authentication, Smart Card Logon
🗷 Smartcard User	Secure Email, Client Authentication, Smart Card Logon
碅 Trust List Signing	Microsoft Trust List Signing
風 User Signature Only	Secure Email, Client Authentication
🕺 WiFi Phone Certificate template	Server Authentication
風 Workstation Authentication	Client Authentication
4	
	OK Cancel

28. Associate the newly created template to SCEP via regedit.

🔐 Registry Editor			
File Edit View Favorites Help			
File Edit View Favorites Help	Name (Default) TencryptionTemplate SignatureTemplate Edit String Value name: EncryptionTem Value data: SCEPLISEE	Type REG_52 REG_52 REG_52 REG_52	Data (value not set) IPSECIntermediateOffline IPSECIntermediateOffline IPSECIntermediateOffline
UseSinglePassword			OK Cancel

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.

 Navigate to Administration > Network Device Profiles, add a new profile or levering existing profile Cisco. If create a new profile, remember to configure Supported Protocols, Authentication/Authorization and Permission properly.

=	dentity Services F	Engine			Administration / Ne	twork Resource	es		Q	۵	0	Q	I.
н	Bookmarks	Network Dev	vices Network Device Grou	ps	Network Device Profiles	External RADI	US Servers	RADIUS Server Sequences	More ~				
55	Dashboard												
1 ¹¹	Context Visibility	Net	work Device Profi	les									
×	Operations									Selec	ted 0 T	otal 9	Ø
U	Policy	/ Edit	+ Add Duplicate J Imp	ort d	Cisco Communities Import 🕧	Export Selected	Delete Selecte	d			A		8
20	Administration		Name	^	Description		Vendor		Source				
	Week Conten		AlcatelWired		Profile for Alcatel switches		Alcatel		Cisco Provi	ded			
nill	Work Centers		ArubaWireless		Profile for Aruba wireless ne	twork access devi	Aruba		Cisco Provi	ded			
			BrocadeWired		Profile for Brocade switches		Brocade		Cisco Provi	ded			
?	Interactive Features		atta Cisco		Generic profile for Cisco net	work access devi	Cisco		Cisco Provi	ded			

≡	dentity Services	Engine		Administration / Net	work Resources	
н	Bookmarks	Network Devices Net	twork Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences
55	Dashboard	Network Device Profile List	> Cisco			
14	Context Visibility	Network Device Pr	ofiles		Sat	Reset
×	Operations	* Nom	Cieco			
-0	Policy	Nam	Generic profile for Cisco networ	k access devices		
20	Administration	Description	n		li.	
đ	Work Centers	Ico	n Change icon	Set To Default		
		Vendo	r Cisco			
		Supported Protoc	cols			
(?)	Interactive Features	RADIUS	\checkmark			
		TACACS+	\checkmark			
		TrustSec				
		RADIUS Dictionari	es Cisco ×			

2. Navigate to Administration > Network Resources > Network Devices and add a device for Cisco IOS RA like yan_RA_sudi as shown bellow

dentity Services Engine	Home Context	Visibility ► Operations ► Policy	✓ Administration		
System Identity Management	▼Network Resources	Device Portal Management pxGrid S	ervices Feed Service Threat Centric	NAC	
Network Devices Network Device	Groups Network Device	e Profiles External RADIUS Servers	RADIUS Server Sequences NAC Managers	External MDM	
	oping_switch	10.74.133.13 🎂 Cisco 🕀	All Locations	All Device Types	
Network Devices	rimo_switch	10.74.23.50/32 🛛 🎂 Cisco 🕀	All Locations	All Device Types	10.74.23.50
	shihan-test	10.74.10.220/32 🛛 🏭 Cisco 🕀	All Locations	All Device Types	
Detault Device	shugwang-rou	10.74.133.115 👑 Cisco 🕀	All Locations	All Device Types	
Device Security Settings	ting_cube_sw2	10.74.53.202/32 🛛 🖶 Cisco 🕀	All Locations	All Device Types	ting_cube_sw2
	ting_wlc9800	10.74.151.66/26 🛛 🗯 Cisco 🕀	All Locations	All Device Types	
	tiren_shield_wlo	c 100.100.101 ditto Cisco ⊕	All Locations	All Device Types	
	tru-test-au	10.74.10.219/24 🛛 👑 Cisco 🕀	All Locations	All Device Types	
	wangh_switch	100.100.30.7 👑 Cisco 🕀	All Locations	All Device Types	wangh_switch
	wenjuaga_swi	. 10.74.10.72/32 👑 Cisco 🕀	All Locations	All Device Types	
	weny_switch	10.74.19.19/26 🚟 Cisco 🕀	All Locations	All Device Types	
	wexiao2_switch	10.79.57.18/24 🛛 👑 Cisco 🕀	All Locations	All Device Types	wexiao2_switch
	whale_WLC	10.74.18.31/32 🔐 Cisco 🕀	All Locations	All Device Types	
	wic-public	100.100.66.1 👑 Cisco 🕀	All Locations	All Device Types	
	yan-auto	100.100.116.2 🚲 Cisco 🕀	All Locations	All Device Types	
	yan-auto-3502	100.100.116.1 🎂 Cisco 🕀	All Locations	All Device Types	
	yan_RA_ca2	10.79.57.89/32 🚟 Cisco 🕀	All Locations	All Device Types	
	yan_RA_ca3	10.75.185.48/32 🗰 Cisco 🕀	All Locations	All Device Types	
	yan_RA_sudi	10.79.57.93/32 🚟 Cisco 🕀	All Locations	All Device Types	scep-for-sudi

3. Navigate to Policy > Authentication, set a Default rule to use Default Network Access and use All_Uesr_ID_Stores.

=	dentity Services Eng	ine Po	licy / Policy Sets	Q & @ & A
н	Bookmarks	Policy Sets→ Default	Reset	Reset Policyset Hitcounts Save
5	Dashboard	Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits
0	Context Visibility	Same		
×	Operations	SQUI		
0	Policy	O Default Default policy set		Default Network Access 🥒 🕂 2
80	Administration	∨Authentication Policy(3)		
ส์เ	Work Centers	+ Status Rule Name Conditions	Use	Hits Actions
?	Interactive Features		All_User_ID_	Stores 🥜
		O Default	> Options	0 {Õ}

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.

		If Auth fail		-
	A	REJECT		
	~	DROP		
		CONTINUE		
P. (REJECT		
Default			0	

4. Navigate to Administration > Identity Management > Identity Source Sequence.

Щ	Bookmarks	Identities	Groups	External Identity Sources	Identity Source Sequences	Settings			
55	Dashboard	Identity So	urce Sequence	es List > All_User_ID_Stores					
ы	Context Visibility	Identity	Source S	equence					
х	Operations	∨ Iden	tity Sourc	e Sequence					
U	Policy	* Name		All_User_ID_Stores					
20	Administration	Descrip	otion A	built-in Identity Sequence to include all User Id	lentity Stores				
đ	Work Centers					11.			
?	Interactive Features	∽ Cer	tificate Ba	ased Authentication	adad Cartificy				
			Select Certific						
		∽ Aut	✓ Authentication Search List A set of identity sources that will be accessed in sequence until first authentication succeeds						
			Available		Selected				
			Internal E	Indpoints	Internal Users				

5. Under Policy > Policy Elements > Results > Authentication > Allowed Protocols, edit Default Network Access as shown below

Policy Sets Profiling Posture Cl	ient Provisioning	Policy Elements				
Dictionaries Conditions Result	S					
G						
- Authentication	Allowed Protocols S	Services List > Default Network Access				
	Allowed Protoc	cols				
Allowed Protocols	Name	Default Network Access				
	Description	Default Allowed Protocol Service				
) Profiling						
Froming						
▶ Posture	 Allowed Protoc 	cols				
Client Provisioning	Auth	nentication Bypass				
r Client Provisioning	\checkmark					
	Auth	nentication Protocols				
	Auti					
	<u> </u>	Allow PAP/ASCII				
		Allow CHAP				
		Allow MS-CHAPv1				
		Allow MS-CHAPv2				
	\checkmark	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								
Dictionaries Conditions - Results									
0									
Authentication Standard Authorization Profiles Explain Experime Explaine Explaine Standard Authorization > Switem > Backup & Bestore > Policy Export Page									
* Authorization									
Authorization Profiles	/ Edit 🕂 Add 🖳 Duplicate 🗙 Delete								
Downloadable ACI s	Name	Profile	Description						
Downloadable ACES	Blackhole_Wireless_Access	🐝 Cisco 🕀	Default profile used to blacklist wireless devices.						
➤ Profiling	Cl_bbb_voice_vlan	🐝 Cisco 🕀	Cl_bbb_voice_vlan						
▶ Posture	Cisco_IP_Phones	🐝 Cisco 🕀	Default profile used for Cisco Phones.						
	Cisco_Temporal_Onboard	🐝 Cisco 🕀	Onboard the device with Cisco temporal agent						
Client Provisioning	Cisco_WebAuth	👑 Cisco 🕀	Default Profile used to redirect users to the CWA						
	Eagle PC VLAN	ditto Cisco 🕀	Access PC VLAN 165 of Eagle Team						
	Eagle Wired Phone VVLAN	🗰 Cisco 🕀	Access VVLAN 604 of Eagle Team						
	FT pc vlan 96	ditto Cisco 🕀	access vlan 96 for phonenix register						
	NSP_Onboard	👑 Cisco 🕀	Onboard the device with Native Supplicant Provi						
	Non_Cisco_IP_Phones	dete Cisco 🕀	Default Profile used for Non Cisco Phones.						
	Phone_SCEP_profile	就 Cisco 🕀	for scep						

cisco Identity Services Engine	Home → Con	text Visibility	Operations	✓ Policy	Administration	▶ Work Cen
Policy Sets Profiling Posture C	lient Provisioning	 Policy Elements 				
Dictionaries → Conditions	ts					
G						
Authentication	Authorization Pro	ntiles > Phone_SCE	P_profile			
- Authorization	Authorization	* Namo	ana SCED profile		1	
✓ Authorization		Name Pr	ione_SCEP_prome	2		
Authorization Profiles		Description fo	r scep			
Downloadable ACLs	*	Access Type AC	CCESS_ACCEPT			
▶ Profiling	Network De	evice Profile	🖁 Cisco 💌 🕀			
▶ Posture	Ser	vice Template				
Client Provisioning	Tra	ck Movement	<i>i</i>)			
	Passive Ide	entity Tracking	<i>i</i>)			
	Common 1	「asks				
	▼ Advanced	Attributes Sett	ings			
	Cisco:cisco-a	av-pair	⊘ = pki:cert	-application=a		ŀ

7. Navigate to Administration > Identity Management > Groups > User Identity Groups and add a user group for SCEP, like scep-group displayed in below picture.

cisco Identity Services Engine Home	Context Visibility Operations	► Policy	Work Centers	
→ System → Identity Management → Network Re	sources	pxGrid Services Feed Se	rvice	
Identities Groups External Identity Sources	Identity Source Sequences	;		
Identity Groups Image: Constraint of the second s	User Identity Groups > scep-group Identity Group * Name scep-group Description for SCEP Save Reset Member Users Users			
GROUP_ACCOUNTS (default)	+ Add - X Delete -			
GuestType_Contractor (default) GuestType_Daily (default)	Status En	nail Usernan	First Name	Last Name
GuestType_SocialLogin (default) GuestType Weekly (default)			P-8821 SN:FC	
<pre>kaipen_wired_pc_group</pre>		2 PID:C	P-8832 SN:FC	
Neshu_wired_pc_group	Enabled	👤 PID:C	P-8875 SN:FC	
OWN_ACCOUNTS (default)	Enabled	👤 PID:C	P-8875 SN:FC	
🚰 scep-group	Enabled	👤 PID:D	P-9861 SN:FV	

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**.

cisco Identity Services Engine Home Context Visibility Operations Policy	y Administration	▶ Work Centers			Q	0 0
Policy Sets Profiling Posture Client Provisioning Policy Elements						
> Authentication Policy (4)						
Authorization Policy - Local Exceptions						
> Authorization Policy - Global Exceptions						
Authorization Policy (13)						
			Results			
Status Rule Name Conditions			Profiles	Security Groups	Hits	Actions
Search						
SCEP_Access yan_scep			* Phone_SCEP_profile +	Select from list	+ 39	٥
Conditions Studio						\mathbf{O}
Library	Editor					
						*
Search by Name		IdentityGroup·Name				
◐▤∩▰▰◻◾▱▱◗▯心◗⊘ょ◈	8					
	Ľ.	Equals ~	User Identity Groups:scep-gr	roup	;	
AutonomousAP 7 103		Set to 'Is not'		Du	uplicate	Save
				ba	pilouro -	

9. 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).

cisco Iden	tity Services E	ingine	Hom	e ▶ Cont	ext Visibility ► O	perations	▶ Policy	✓ Administ	ration	Work Centers			
▶ System	◄ Identity Mana	igement 🕨	Netw	ork Resources	B Device Portal I	Management	pxGrid S	ervices F	eed Service	Threat Centric	NAC		
✓ Identities	Groups Ext	ternal Identity	y Sourc	es Identity	Source Sequences	 Settings 							
		G											
Users			Net	work Acce	ss Users								
Latest Manual	Network Scan R	tesults	/ E	dit 🕂 Add	🔀 Change Status 👻	🕞 Import	🚯 Export 👻	X Delete	Duplicate	e			
				Status	Name			Description		First Name	Last Name	Email Address	User Identity Group
					PID:CP-8875 SI	V:FCH26173	SXI						
				Enabled	2 PID:CP-8875 SI	N:FCH26283	IMF						scep-group
				Enabled	2 PID:CP-8875 SI	N:FCH263038	BNM						
				Enabled	9 PID:CP-8875 S	N:FCH263038	BUY						scep-group
				Enabled	👤 PID:CP-8875 SI	N:FCH263332	2VH	cisco					scep-group
				Enabled	9 PID:CP-8875 SI	N:FCH264520)24						scep-group
				Enabled	9 PID:CP-8875 S	N:FCH264520	NS						
				Enabled	2 PID:CP-8875 SI	N:FCH264520	DNT	cisco					scep-group
				Enabled	2 PID:DP-9861 S	N:FCH274720	020	cisco					scep-group
				Enabled	2 PID:DP-9861 S	N:FVH280322	2J6	cisco					scep-group
				Enabled	9 PID:DP-9861 S	N:FVH281623	BFQ	cisco					scep-group
				Enabled	9 PID:DP-9861 S	N:FVH281623	BFV	cisco					scep-group
				Enabled	2 PID:DP-9861 S	N:FVH281623	8U3	cisco					scep-group
				Enabled	2 PID:DP-9861 SI	N:FVH281623	BYE	cisco					scep-group
				Enabled	2 PID:DP-9871 SI	N:FCH273820)0Y	cisco					scep-group
				Enabled	2 PID:DP-9871 S	N:FCH274620)2B	cisco					scep-group
				Enabled	2 PID:DP-9871 S	N:FCH274620)48	cisco					scep-group
				Enabled	9 PID:DP-9871 SI	N:FVH28080F	NY	CISCO					scep-group

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
✓ Identities Groups External Identi	ty Sources Identity Source Sequences
Users Latest Manual Network Scan Results	Network Access User • Name PID: DP-9871 SN:FCH2738200Y Status Status Email • Passwords Password Type: Internal Users • Password Re-Enter Password • Login Password • User Information First Name Last Name 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

Cisco Desk Phone 9800 Series Wireless LAN Deployment Guide

bzEZMBcGA1UEAxMOO2lzY28gUm9vdCBDOSBNMjAeFw0xMjExMTIxMzUwNThaFw0zNZEXMTIxMzAwMTdaMDYxDjAMBgNVBAoTBUNpc2NvMSQwIgYDVQQDExtDaXNjbyBN YW51ZmFjdHVyaW5nIENBIFNIQTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK AoIBAQD0NktCAjJn3kk98hU7wUVp6QlOFrlItEce6CpbfYpeLdUeZduAo+S0otzT lJwS2BlMhZtacu9vUpfmW9w7nOo9zVT3evPuhF/6/9TEdVBn75zb5CfV+E6ld+fH nuPiFyBu+HDDJRd373Op+957IdoWyPvD8hHR1HJGFJ3JJKBg0UScL4JCwleu98Xq /vPlAqBhExa7a2/fqSmZA0vZIG1bBfWZY8ZtSeTxKg3eWvnV+xElabHqTDMYWf+2 obs4YB5lINTbYgHyRETP6T8Xr6TtD0h3654OUHcW+1meBu/jctluMKppeSjVtrof 5vt+pbkCg0iQAAjsL0qczT3yaNXvAgMBAAGjggGHMIIBgzAOBgNVHQ8BAf8EBAMC AQYwEgYDVR0TAQH/BAgwBgEB/wIBADBcBgNVHSAEVTBTMFEGCisGAQQBCRUBEgAw OzBBBggrBgEFBOcCARY1aHR0cDovL3d3dv5jaXNjbv5jb20vc2VidXJpdHkvcGtp L3BvbGljaWVzL2luZGV4Lmh0bWwwHQYDVR0OBBYEFHrXeZXKu0gruFUU/aPAD7yn D5YZMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy aXR5L3BraS9jcmwvY3JjYW0yLmNybDB8BggrBgEFBQcBAQRwMG4wPgYIKwYBBQUH MAKGMmh0dHA6Lv93d3cuY2lzY28uY29tL3NlY3VvaXR5L3BraS9jZXJ0cv9jcmNh bTIuY2VyMCwGCCsGAQUFBzABhiBodHRwczovL3Rvb2xzLmNpc2NvLmNvbS9wa2kv b2NzcDAfBgNVHSMEGDAWgBTJAPkfih/CZr2l0m1lDiIuNMMFoDANBgkqhkiG9w0B AQsFAAOCAQEAc1k2rH6YT4juFxs9q7ObzfcKbNvOvDsaU7av4IHFXmn/JxfnBmUv YxAI2Hx3xRb0KtG1JGkffQjVAtBboTXynLaQso/jj46ZOubIF8y6Ho3nTAv7Q6VH kqSCdZClVu91zbHV9FFYQzJxjw1QgB0a4ItS4yhdmgl3oDNEcb3trQezrQ3/857/ ISqBGVLEbKHOu8H6zOLhxAgZ08ae1oQQQJowki0Ibd+LRLGovtEwLg8yyqiTIGve 7VFL2sRa8Z3rK9tlwKVH2kpFKNAeN3rfKFqr0/weR0cvKpmLMrSBTBZcxQcJCYF4 X6FO/32KOqcxJFIOKGVIUjvAvioOqoducw== -----END CERTIFICATE-----

Trustpoint 'MIC_trustpoint' is a subordinate CA and holds a non self-signed cert. Certificate has the following attributes:

Fingerprint MD5: AC14F08F C3780F8F D9EEE6C9 39111280

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

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.

	Report prob	olem	
1	Date of problem (mm/dd)	06/21	
2	Time of problem (hh:mm + AM/PM)	7:18 PM	
3	Problem description	Failed to place a	call >
4	Last PRT file name		
5	Last uploaded time		
	Submit	Select	Back
	lesues and dia	apostico	
		gnostics	
1	Issues	gnostics	None
1 2	Issues Problem submitted	gnostics	None
1 2 3	Issues and diagonal submitted The PRT file is available at http://1 prt-20240621-192126-845A3EC	0.79.63.52/FS/ 22785.tar.gz	None
1 2 3	Issues and diag	0.79.63.52/FS/ 22785.tar.gz	None
1 2 3	Issues and diag	0.79.63.52/FS/ 22785.tar.gz	None

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.

CISCO DP-9871 Config	uration Utility		Admin Logir
Info Voice Call History Personal Directory			
Status Debug Info Download Status Network Statistics			
Console Loge			
Debug Message 1	messages	Debug Message 2:	
Debug Message 3		Debug Message 4:	
Debug Message 5		Debug Message 6:	
Debug Message 7		Debug Message 8:	
ThousandEyes Logs			
Agent Message 1		Agent Message 2:	
Problem Reports			
Report Problem	Generate PRT	Prt File:	prt-20240621-042152-845A3EC2302B.tar.gz
Mini Prt File	miniprt-20240621-042152-845A3EC2302B.tar.gz		



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	0000000
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.

$\leftarrow \rightarrow$ C \bigcirc \gtrless 100.100.122.153		\$
Cisco IP Phone for 3rd Party Call Cisco DP-9871 Configu	Control Uration Utility	
Info Voice Call History Personal Directory		
Status Debug Info Download Status Network Statistics		
Hoteling State:	Disabled Extended Function Status:	None
Line 1 Call 1 Status		
Call State:	Called Party Ringing Call Appearance:	Line 1 Call 1
Tone:	None Encoder:	PCMU
Decoder:	PCMU Type:	Outbound
Remote Hold:	No Caliback:	
Mapped RTP Port:	19626 >> 0 Peer Name:	+17139326004
Peer Phone:	+17139326004 Duration:	
Packets Sent:	335 Packets Received:	308
Bytes Sent:	53600 Bytes Received:	52804
Decode Latency:	20 ms Jitter:	44 ms
Round Trip Delay:	0 ms Packets Lost:	0
Loss Rate:	0.00 Packet Discarded:	1
Discard Rate:	0.32 Burst Duration:	0 ms
Gap Duration:	0 ms R Factor:	87
MOS-LQ:	4.26 MOS-CQ:	4.26

$ \rightarrow$ G	Lo.79.63.51/CGI/Java/Serviceability?adapter=device.statistics.streaming.0		
ahaha		Streaming	statistics
cisco		Cisco IP Phone DP-9861	(SEP845A3EC229D4)
Device information		Remote address	173.36.143.200/51302
Network setup		Local address	10.79.63.51/22570
Network statistics		Start time	9:31:25am
Ethernet information		Stream status	Active
Access		Host name	SEP845A3EC229D4
<u>Network</u>		Sender packets	237269
Device logs		Sender octets	12263901
Console logs		Sender codec	OPUS
Core dumps		Sender reports sent	835
Status messages		Sender report time sent	10:50:31am
Debug display		Receiver lost packets	583
Streaming statistics		Avg jitter	8
Stream 1		Receiver codec	OPUS
Stream 2		Receiver reports sent	0
Stream 3		Receiver report time sent	00:00:00
Stream 4		Receiver packets	236709
Stream 5		Rcvr 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.

BTHub5-86GN • Connected		Advanced W	/i-Fi details
1 Security mode	PSK	AP name	
2 Advanced Wi-Fi details	>	MAC address	00:20:c7:64:ad:86
		Frequency	2.462Ghz
		Current channel	11
		Last RSSI	-58
		Beacon interval	100
Forget Select	Back		Back

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 vist /admin/screendump.bmp">http://sphone_IP_address>/admin/screendump.bmp in a web browser. For exmaple, <a href="http://http:/http://http://http://http://http://http://http://http://http://http://http://http://http://http://http://http:/http://htt

For phones that are registered to Cisco Unified Communications Manager, get the IP address of your phoen and <a href="http://<phone_IP_address>/CGI/Screenshot">http://<phone_IP_address>/CGI/Screenshot. For example, http://transformation.com 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 <u>http://<phone_IP_address>/admin</u> in a web browser.

1. Navigate to Info > Debug Info and clicke Start Packet Capture.

Info Voice Call History Personal Directory	
Status Debug Info Download Status Network Statistics	
Console Logs	
Debug Message 1: messages	Debug Message 2:
Debug Message 3:	Debug Message 4:
Debug Message 5:	Debug Message 6:
Debug Message 7:	Debug Message 8:
Problem Reports	
Report Problem: Generate PRT	Prt File 1: prt-20190324-141057-002F5C6121C2.tar.gz
Prt File 2:	Packet Capture: Start Packet Capture
Capture File:	

2. Click **Submit** in the prompt.

Packet Captur	e	х
Filter:	All	
	Cancel	

3. When the process completes, click Stop Packet Capture to stop capturing.

Info	Voice Call History Personal Directory						
Status	Status Debug Info Download Status Network Statistics						
Console Logs							
	Debug Message 1:	messages Debug Message 2:					
	Debug Message 3:	Debug Message 4:					
	Debug Message 5:	Debug Message 6:					
	Debug Message 7:	Debug Message 8:					
Problem Reports							
	Report Problem:	Generate PRT Prt File 1: prt-20190324-141057-002F5C6121C2.tar.gz					
	Prt File 2:	Packet Capture: Stop Packet Capture					
	Capture File:						

The captured file is available for downloading.

- 61-24			,		
Info	Voice Call History Personal Directory				
Status	Debug Info Download Status Network Sta	tistics			
Console I	Logs				
	Debug Message 1:	messages		Debug Message 2:	
	Debug Message 3:			Debug Message 4:	
	Debug Message 5:			Debug Message 6:	
	Debug Message 7:			Debug Message 8:	
Problem	Reports				
	Report Problem:	Generate PRT		Prt File 1:	prt-20190324-141057-002F5C6121C2.tar.gz
	Prt File 2:			Packet Capture:	Start Packet Capture
	Capture File:	pkt-20190403-011835-002F5C6121C2.pcap			

Additional Documentation

Cisco Desk Phone 9800 Series Datasheet: <u>https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/ip-phones/desk-phone-9800-series-ds.html</u>

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/xe-3s/sec-pki-xe-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: <u>http://www.cisco.com/go/trademarks</u>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2024 Cisco Systems, All rights reserved.