Cisco Wireless Phone 9821

Wireless LAN Deployment and Connection Guide



Cisco is bringing a new standard to portable phones with a portfolio built for working in modern office environments. Cisco Wireless Phone 9821 is designed with IT and facilities in mind to deliver a new phone model. Included on each phone is the newly released PhoneOS software that simplifies the user experience and compliments our other portfolios devices to give seamless experience from desk spaces to mobile device in an area. With expanded functionality – Cisco Wireless Phone 9821 combines secure enterprise calling, meetings, 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 Handset.

Cisco Wireless Phone 9821 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, or other 3rd party cloud calling platforms. Alongside our extensive portfolio of desk devices, the 9821 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 Cisco Wireless Phone 9821 into a wireless LAN environment.

Revision History

Date	Comments
07/29/26	Initial version

Contents

Cisco Wireless Phone 9821 overview **6**

Bands *6*

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

Protocols *9*

Wi-Fi *10*
6 GHz Specifications 10
5 GHz Specifications 10
2.4 GHz Specifications 12
Regulatory 13

Bluetooth *14*
Bluetooth Profiles 14
Coexistence (802.11b/g/n + Bluetooth) 14

Languages *14*

Battery Life *15*

Device Care *16*

Accessories *16*

Other Accessories *16*

Wireless LAN Design **17**

802.11 Network *17*
6 GHz (802.11ax) 17
5 GHz (802.11a/n/ac/ax) 17
2.4 GHz (802.11b/g/n/ax) 18
Cells Deployment 19
Power Balancing 20
Signal Strength and Coverage 20
Data Rates 21
Rugged Environments 21
Multipath 22

Security *23*
Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST) 24
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) 25
Protected Extensible Authentication Protocol (PEAP) 25

Quality of Service (QoS) *26*
Call Admission Control (CAC) 26
Wired QoS 26
Configuring Cisco Switch Ports for WLAN Devices 27
Configuring Cisco Switch Ports for Wired IP Phones 27

Roaming *27*
Fast Secure Roaming (FSR) 28
Interband Roaming 29

Delivery Traffic Indicator Message (DTIM) *30*

Call Capacity *30*
Multicast *30*

Configuring the Cisco Wireless LAN **31**
Cisco AireOS Wireless LAN Controller and Lightweight Access Points *31*
Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points *32*
802.11 Network Settings 33
WLAN Settings 48
Controller Settings 64
Mobility Settings 65
Call Admission Control (CAC) 66
Multicast 67
Advanced Settings 69
Cisco Mobility Express and Lightweight Access Points *70*
Cisco Autonomous Access Points *71*
Cisco SSID on Meraki Dashboard *71*

Configuring Cisco Call Control **74**
Cisco Webex Calling *74*
Personal Usage 75
Cisco Unified Communications Manager *77*
Device Enablement 77
QoS Parameters 78
Wireless LAN Profiles 78

Configuring Cisco Wireless Phone 9821 ..... **86**
Wi-Fi Profile Configuration *86*
Automatic Provisioning *86*
Config and Modify Wi-Fi Profile via Phone Administration Web Page *87*
Webex Calling 87
CUCM 88
Configure Wi-Fi Settings on the Phone UI *90*
Network configuration 92
Certificate Management *94*
Manual Installation 94
Server Certificate 100
Certificate Removal 100
CDC cert installation (Webex Calling) 101
Simple Certificate Enrollment Protocol (SCEP) 101

Troubleshooting **120**
Problem Report Tool *120*
Wi-Fi statistics *123*
Streaming Statistics *123*
Wi-Fi Signal Indicator *125*
Current Access Point *125*

Neighbor list *126*
Diagnostics *126*
Audio Diagnostics 126
WLAN Diagnostics 127
Capturing a Screenshot of the Phone Display *128*
Capturing packets *128*
Additional Documentation 129

Cisco Wireless Phone 9821 overview

Cisco's implementation of 802.11 standards enables time-sensitive applications, such as voice and video, to operate efficiently across campus-wide wireless LAN (WLAN) deployments. These enhancements provide fast roaming and seamless multimedia traffic flow while maintaining robust security as users transition between access points.

WLANs operate in unlicensed spectrum and are susceptible to interference from other devices. The 2.4 GHz band is often congested due to the proliferation of devices such as Bluetooth headsets, microwave ovens, and cordless phones. The 5 GHz band is less congested and is the preferred spectrum for Cisco Wireless Phone 9821, allowing the device to leverage the higher data rates provided by the 802.11a/n/ac/ax standards.

Cisco Wireless Phone 9821 supports Wi-Fi 6 and 6E, including 6 GHz band capabilities. Where regulatory domains permit, the 6 GHz spectrum is the recommended choice. However, note that 6 GHz signals exhibit higher attenuation than 5 GHz signals. To maintain a consistent coverage footprint, you may need to increase access point (AP) density by approximately 5% to 10%.

Despite the optimizations that Cisco has implemented in the Cisco IP Phone Series, the use of unlicensed spectrum means that uninterrupted communication cannot be guaranteed. Users may experience intermittent voice gaps during calls. Adhering to these deployment guidelines will minimize the likelihood of such occurrences, but they cannot be entirely eliminated.

Due to the inherent nature of unlicensed spectrum and the inability to guarantee packet delivery to a WLAN device, the Cisco Wireless Phone 9821 is not intended for use as a medical device and should not be used to support clinical decision-making.

Bands

The following table outlines the peak antenna gain and frequency ranges/channels supported by Cisco Wireless Phone 9821.

Part Number	Description	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
WP-9821-K9=	Cisco Wireless Phone 9821	2.400-2.483 GHz: 2.0 dBi	2.412 - 2.472 GHz	13	1-13
		5.150-5.250 GHz: 2.0 dBi	5.180 - 5.240 GHz	4	36,40,44,48
		5.250-5.350 GHz: 2.2 dBi	5.260 - 5.320 GHz	4	52,56,60,64
		5.470-5.725 GHz: 3.2 dBi	5.500 - 5.720 GHz	12	100-144
		5.725-5.850 GHz: 3.0 dBi	5.745 - 5.825 GHz	5	149,153,157,161,165
		5.945-6.425 GHz: 2.2 dBi	5.955 - 6.415 GHz	24	1, 5, 9, 13, ..., 93
		6.425-6.525 GHz: 1.4 dBi	6.435 - 6.515 GHz	5	97, 101, 105, 109, 113
		6.525-6.885 GHz: 3.2 dBi	6.535 - 6.875 GHz	18	117, 121, ..., 185
		6.885-7.125 GHz: 2.5 dBi	6.895 - 7.115 GHz	12	189, 193, ..., 233

Note: Channel availability is subject to local regulatory restrictions. Cisco Wireless Phone 9821 does not support Channel 14 in the Japan regulatory domain.

Requirements

Cisco Wireless Phone 9821 is an IEEE 802.11a/b/g/n/ac/ax-compliant collaboration device that provides voice and data communications. Before deployment, the wireless LAN infrastructure must be validated to ensure it meets the required specifications for the 9821.

Site Requirement

Before deploying the Cisco Wireless Phone 9821 into a production environment, a site survey must be completed by a Cisco-certified partner. The site survey must include heatmaps that illustrate the intended coverage plan and determine the appropriate access point (AP) platform, antenna type, and configuration (channel and transmit power) for the location.

During the site survey, the RF spectrum must be analyzed to identify usable channels within the 2.4 GHz, 5 GHz, and 6 GHz bands.

- **6 GHz:** Where regulatory domains permit, the 6 GHz spectrum is the recommended choice. It provides a "greenfield" environment, which is significantly cleaner than legacy Wi-Fi bands.
- **5 GHz:** This is the preferred secondary band, as it offers more non-overlapping channels and less interference than the 2.4 GHz band.
- **2.4 GHz:** Use this band only when necessary, as it is prone to high interference from non-Wi-Fi devices.

Select hardware based on the environment:

- **Non-rugged environments (e.g., office, healthcare, education, hospitality):** Use APs with integrated antennas.
- **Rugged environments (e.g., manufacturing, warehouse, retail):** Use AP platforms that support external antennas.

The site survey must accurately reflect the hardware and configuration of the final installation. Do not use legacy radio equipment to survey coverage for a modern 802.11ac/ax/be network. Ensure that:

- AP orientation and mounting height match the final installation.
- Data rates are configured according to your application, bandwidth, and coverage requirements.
- The wireless LAN is validated post-installation to ensure it meets all requirements for Cisco Wireless Phone 9821.

6GHz Design

Due to higher signal attenuation, 6 GHz radio signals exhibit slightly less range than 5 GHz signals, assuming identical antenna patterns and transmit power levels. To achieve equivalent coverage, you have two primary options:

- **Increase AP Density:** Deploy 10–20% more access points (APs) within the coverage area.
- **Adjust Transmit Power:** Increase the 6 GHz transmit power by approximately 3–6 dBm relative to the 5 GHz configuration.

Maintain a minimum distance of 1 meter from glass surfaces. Glass can cause significant signal reflection at 6 GHz frequencies, which may lead to multipath interference. Avoid mounting APs behind heavy obstructions, such as metal ductwork or concrete pillars, as these significantly degrade signal propagation.

For optimal performance and roaming stability, maintain consistency across your wireless infrastructure. Mixing APs of different generations or capabilities—specifically 6 GHz-capable and non-6 GHz-capable APs—

within the same roaming area is not recommended. Inconsistent hardware capabilities can lead to unpredictable client roaming behavior and performance degradation.

Signal

The cell edge should be designed to -67 dBm where there is a 15-20% overlap of adjacent access point at that signal level.

This ensures that Cisco Wireless Phone 9821 always has adequate signal and can hold a signal long enough in order to roam seamlessly where signal based triggers are utilized vs. packet loss triggers.

Also need to ensure that the upstream signal from the 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 -80 dBm or **Auto**.

It is recommended to design the cell size to ensure that the phone can hold a signal for at least 5s.

Channel Utilization

Channel Utilization levels should be kept under 40%.

Noise

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

Also need to ensure that the upstream signal from the Cisco Wireless Phone 9821 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 15%.

Multipath

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

Call Control

The Cisco Wireless Phone 9821 is supported on the following call control platforms.

- Cisco Webex Calling
- Cisco Unified Communications Manager (CUCM) (15.0.1 or above)

Note: Cisco Unified Communications Manager (CUCM) requires the installation of a specific device package or service release update to enable support for Cisco Wireless Phone 9821.

Device packages for Cisco Wireless Phone 9821 are available at the following location.

https://software.cisco.com/download/home/286331940/type/282074299/release/15.0(1.15036)

Wireless LAN

The Cisco Wireless Phone 9821 is supported on the following Cisco Wireless LAN solutions.

- Cisco IOS Wireless LAN Controller and Cisco Lightweight Access Points
  - Minimum = 17.12
  - Recommended = 17.18.2
- EWC (Embedded Wireless Controller)
- Cisco Meraki Access Points
  - Minimum = MR 27.X, MX 13.33
  - Recommended = MR 30.6, MX 18.211.2

Access Points

The following table lists the supported Cisco access points.

Controller Model	**AP Models**
IOS XE	9105, 9115, 9117, 9120, 9130, 9136, 9162, 9164, 9166, 917x
Meraki	9162, 9164, 9166, 917x, MR20, MR28, MR30H, MR32, MR33, MR34, MR36, MR36H, MR42, MR44, MR45, MR46, MR52, MR53, MR55, MR56, MR57

Note:

- Cisco Wireless Phone 9821 has been tested for interoperability with Cisco Catalyst and Meraki access points that have not reached their End-of-Sale or End-of-Support dates. If an access point model is not explicitly listed in the supported hardware documentation, it may still provide basic functionality; however, such configurations are not officially supported.
- Cisco Wireless Phone 9821 is designed for use with indoor access points. Mesh deployments and outdoor access point configurations are not supported, as these environments have not been validated for this device.
- Interoperability with 3rd-party APs cannot be guaranteed as we have limited testing ability. As long as the 3rd party AP is Wi-Fi specification compliant, basic operations will work.
- Cisco does not perform interoperability testing with third-party access points. While the 9821 may provide basic functionality when connected to Wi-Fi-compliant third-party hardware, Cisco cannot guarantee performance, stability, or feature parity.

Antenna System

Some Cisco access points require or allow external antennas.

Please refer to the Cisco Aironet and Catalyst Antennas and Accessories Reference Guide for the list of supported antennas for Cisco Aironet access points and how the external antennas should be mounted.

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,ax
- Wi-Fi MultiMedia (WMM)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)

  Opus, G.722, G.711, G.722.1, G.722.2, G.729
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- HyperText Transfer Protocol (HTTP)

Wi-Fi

Cisco Wireless Phone 9821 works with 2.4 GHz (HT/VHT/HE 20), 5 GHz (HT/VHT/HE 20/40/80) and 6 GHz (HE 20/40/80) mode. To achieve 802.11n/ac/ax connectivity, it is recommended that Cisco Wireless Phone 9821 is within 30 feet of the access point.

6 GHz Specifications

6 GHz - 802.11ax	**Data Rate**	**Spatial Streams**	**HE20 (Mbps)**	**HE40 (Mbps)**	**HE80 (Mbps)**	**Modulation**
Max Tx Power=13.6 dBm (Power depends on the region. 13.6dBm is for CE area, while FCC/RCM is 9.46dBm)	HE0	1	8.6	17.2	34.4	OFDM-BPSK
	HE1		17.2	34.4	68.8	OFDM-QPSK
	HE2		25.8	51.6	103.2	OFDM-QPSK
	HE3		34.4	68.8	137.6	OFDM-16QAM
	HE4		51.6	103.2	206.5	OFDM-16QAM
	HE5		68.8	137.6	275.3	OFDM-64QAM
	HE6		77.4	154.9	309.7	OFDM-64QAM
	HE7		86.0	172.1	244.1	OFDM-64QAM
	HE8		103.2	206.5	412.9	OFDM-256QAM
	HE9		114.7	229.4	458.8	OFDM-256QAM
	HE10		129.0	258.1	516.2	OFDM-1024QAM
	HE11		143.4	286.8	600.5	OFDM-1024QAM

5 GHz Specifications

5 GHz - 802.11a	**Data Rate**	**Spatial Streams**	**Modulation**

Max Tx Power=16 dBm (Depends on region)	6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps		1 1 1 1 1 1 1 1			OFDM-BPSK OFDM-BPSK OFDM-QPSK OFDM-QPSK OFDM-16QAM OFDM-16QAM OFDM-64QAM OFDM-64QAM
5 GHz (802.11n/ac/ax)	**Date Rate**	**Spatial Streams**	**HT20 (Mbps)**	**VHT20 (Mbps)**	**HE20 (Mbps)**	**Modulation**
Max Tx Power=15.5 dBm (Depends on region)	MCS 0 MCS 1 MCS 2 MCS 3 MCS 4 MCS 5 MCS 6 MCS 7 MCS 8 MCS 9 MCS 10 MCS 11	1	7.2 14.4 21.7 28.9 43.3 57.8 65.0 72.2	7.2 14.4 21.7 28.9 43.3 57.8 65.0 72.2 86.7	8.6 17.2 25.8 34.4 51.6 68.8 77.4 86.0 103.2 114.7 129.0 143.4	OFDM-BPSK OFDM-QPSK OFDM-QPSK OFDM-16QAM OFDM-16QAM OFDM-64QAM OFDM-64QAM OFDM-64QAM OFDM-256-QAM OFDM-256-QAM OFDM-1024-QAM OFDM-1024-QAM
5 GHz (802.11n/ac/ax)	**Date Rate**	**Spatial Streams**	**HT40 (Mbps)**	**VHT40 (Mbps)**	**HE40 (Mbps)**	**Modulation**
Max Tx Power=15 dBm (Depends on region)	MCS 0 MCS 1 MCS 2 MCS 3 MCS 4 MCS 5 MCS 6	1	15.0 30.0 45.0 60.0 90.0 120.0 135.0	15.0 30.0 45.0 60.0 90.0 120.0 135.0	17.2 34.4 51.6 68.8 103.2 137.6 154.9	OFDM-BPSK OFDM-QPSK OFDM-QPSK OFDM-16QAM OFDM-16QAM OFDM-64QAM OFDM-64QAM

	MCS 7 MCS 8 MCS 9 MCS 10 MCS 11		150.0	150.0 180.0 200.0	172.1 206.6 229.4 258.1 286.8	OFDM-64QAM OFDM-256-QAM OFDM-256-QAM OFDM-1024-QAM OFDM-1024-QAM
5 GHz (802.11ac/ax)	**Date Rate**	**Spatial Streams**	**VHT80 (Mbps)**	**HE80 (Mbps)**		**Modulation**
Max Tx Power=15 dBm (Depends on region)	MCS 0 MCS 1 MCS 2 MCS 3 MCS 4 MCS 5 MCS 6 MCS 7 MCS 8 MCS 9 MCS 10 MCS 11	1	32.5 65.0 97.5 130.0 195.0 260.0 292.5 325.0 390.0 433.0	34.4 68.8 103.2 137.6 206.5 275.2 309.6 344.1 412.9 458.8 516.2 600.5		OFDM-BPSK OFDM-QPSK OFDM-QPSK OFDM-16QAM OFDM-16QAM OFDM-64QAM OFDM-64QAM OFDM-64QAM OFDM-256QAM OFDM-256QAM OFDM-1024-QAM OFDM-1024-QAM

2.4 GHz Specifications

2.4 GHz - 802.11b	**Data Rate**	**Spatial Streams**	**Modulation**
Max Tx Power=16 dBm (Depends on region)	1 Mbps 2 Mbps 5.5 Mbps 11 Mbps	1 1 1 1	DSSS-BPSK DSSS-QPSK DSSS-CCK DSSS-CCK
2.4 GHz - 802.11g	**Data Rate**	**Spatial Streams**	**Modulation**
Max Tx Power=16 dBm (Depends on region)	6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps	1 1 1 1 1	OFDM-BPSK OFDM-BPSK OFDM-QPSK OFDM-QPSK OFDM-16QAM

	36 Mbps 48 Mbps 54 Mbps		1 1 1		OFDM-16QAM OFDM-64QAM OFDM-64QAM
2.4 GHz (802.11n/ax)	**Data Rate**	**Spatial Streams**	**HT20 (Mbps)**	**HE20 (Mbps)**	**Modulation**
Max Tx Power=16 dBm (Depends on region)	MCS 0 MCS 1 MCS 2 MCS 3 MCS 4 MCS 5 MCS 6 MCS 7 MCS 8 MCS 9 MCS 10 MCS 11	1	7.2 14.4 21.7 28.9 43.3 57.8 65.0 72.2	8.6 17.2 25.8 34.4 51.6 68.8 77.4 86.0 103.2 114.7 129.0 143.4	OFDM-BPSK OFDM-QPSK OFDM-QPSK OFDM-16QAM OFDM-16QAM OFDM-64QAM OFDM-64QAM OFDM-64QAM OFDM-256-QAM OFDM-256-QAM OFDM-1024-QAM OFDM-1024-QAM

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

Regulatory

World Mode (802.11d) allows a wireless client to adapt to the regulatory requirements of the local environment by utilizing the channels and transmit power levels advertised by the access point (AP). For optimal performance, ensure that 802.11d is enabled on your wireless infrastructure for the country where the AP is deployed.

Operation in the 6 GHz band is prohibited until the AP has confirmed the local regulatory domain.

Many 5 GHz channels are shared with radar technology. To utilize these Dynamic Frequency Selection (DFS) channels, both the client and the AP must be 802.11h compliant. Note that 802.11h requires 802.11d to be enabled. The 9821 performs a passive scan of DFS channels before attempting active scans.

If 802.11d is not enabled, the Cisco Wireless Phone 9821 may attempt to connect to the AP using passive scanning and reduced transmit power.

The Cisco Wireless Phone 9821 supports country codes defined by the Wi-Fi Alliance (WFA). The following table details the countries and their corresponding 802.11d codes supported by the device.

Australia (AU)	Canada (CA)	Europe (EU)	New Zealand (NZ)
Saudi Arabia (SA)	Turkey (TR)	United Kingdom (GB)	United States (US)

Bluetooth

Cisco Wireless Phone 9821 supports Bluetooth technology allowing for wireless headset communications.

Bluetooth enables low bandwidth wireless connections within a range of 1 to 3 meters.

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 in the 2.4 GHz band. Because this spectrum is shared with 802.11b/g/n devices and other common equipment—such as microwave ovens and cordless phones—Bluetooth performance may be subject to signal interference.

Bluetooth Profiles

Cisco Wireless Phone 9821 supports the following Bluetooth profiles.

- Audio/Video Remote Control Profile (AVRCP)
- Generic Access Profile (GAP)
- Generic Audio/Video Distribution Profile (GAVDP)
- Hands-Free Profile (HFP)
- Device Identification (DID)

Coexistence (802.11b/g/n + Bluetooth)

When Bluetooth and 802.11b/g/n operate simultaneously, both technologies contend for the 2.4 GHz ISM band. This coexistence introduces specific performance limitations and deployment requirements.

Capacity

Call capacity is reduced when using Bluetooth in the 2.4 GHz band. This is due to the overhead required by Clear to Send (CTS) frames, which are necessary to protect both 802.11 and Bluetooth transmissions from collision.

Multicast Audio

Multicast audio applications—including Push-to-Talk (PTT) and Music on Hold (MOH)—are not supported when Bluetooth and 802.11b/g/n are used simultaneously.

Voice Quality

Depending on your data rate configuration, the system may trigger CTS frames to protect Bluetooth traffic. In some environments, enabling the 6 Mbps mandatory data rate may be necessary to maintain stability.

Note: To avoid the limitations associated with the 2.4 GHz band, it is strongly recommended to use 802.11a/n/ac/ax (5 GHz or 6 GHz bands) for all voice traffic when Bluetooth is enabled.

Languages

Cisco Wireless Phone 9821 supports the following languages.

Arabic	Bulgarian	Catalan	Chinese

Croatian	Czech	Danish	Dutch
English	Estonian	Finnish	French
German	Greek	Hebrew	Hungarian
Italian	Japanese	Korean	Latvian
Lithuanian	Norwegian	Polish	Portuguese
Romanian	Russian	Serbian	Slovak
Slovenian	Spanish	Swedish	Thai
Turkish			

Battery Life

Cisco Wireless Phone 9821 is equipped with a 2000 mAh smart battery. Battery capacity is expected to degrade to 80% of its original capacity after 500 full charge cycles; consequently, it is recommended to replace the battery approximately every two years. The battery's manufacture date is printed on the rear of the unit to assist with tracking its age.

With the latest software release, a fully charged battery provides up to 11.5 hours of talk time or 145 hours of standby time. Batteries can be charged while installed in the handset or independently using the Cisco Wireless Phone 9821 Desktop or Multi-Charger.

Note: Actual battery life varies significantly based on the wireless LAN (WLAN) environment and specific usage patterns. Factors that can negatively impact battery performance include frequent DHCP lease renewals, frequent EAP reauthentication, short session timeouts, and poor signal coverage (low RSSI).

To optimize battery life, the following configuration settings are recommended:

- **DHCP Lease Time:** Greater than 8 hours.
- **EAP Reauthentication Timer:** 2 hours or greater.
- **Session Timeout:** 24 hours.
- **Signal Strength:** Maintain an RSSI of –67 dBm or better.

Usage

Battery life is directly impacted by device activity. Power consumption increases during the following operations:

- Active voice calls
- Frequent roaming between access points
- Extended LCD display usage
- Bluetooth headset usage
- Application activity, including XAPI integration and XSI message processing
- Menu navigation and configuration changes

- Outside the wireless coverage area of the access point
- High LCD backlight

Coverage

To maximize battery efficiency, ensure Cisco Wireless Phone 9821 remains within an area with robust RF coverage. The phone must maintain a consistent connection to the Cisco Unified Communications Manager (CUCM) or Cloud service. If the phone moves out of range and remains disconnected for an extended period, the power consumption increases as the phone actively scans to re-establish a network connection.

Multicast streams

Subscribing to multicast streams requires the handset to wake frequently to process incoming frames. This constant state of activity significantly increases power consumption compared to idle operation.

Background Noise Removal (BNR)

Background Noise Removal is a CPU-intensive feature. Enabling this function increases power consumption during active calls due to the additional processing required for real-time audio filtering.

Device Care

To clean Cisco Wireless Phone 9821, use a soft, moist cloth to wipe the device.

- Do not apply liquids or powders directly to the device as it can damage the device.
- Do not use bleach or other caustic products to clean the device.
- Do not use compressed air to clean the device as it can also damage the device.

For more information, refer to Care of your phone.

Accessories

The following accessories are available for Cisco Wireless Phone 9821.

- Batteries
- Phone power adapter
- Holster case
- Leather case
- Lanyard
- Desktop charger
- Multicharger
- Headsets
    - Wired (3.5mm): 520 series
    - Wireless (Bluetooth): 720 series

Other Accessories

Cisco Wireless Phone 9821 supports the following USB to Ethernet adapters:

- Apple USB 2.0 Type-A Ethernet Adapter

- Belkin USB 2.0 Type-A Ethernet Adapter
- TAIKESEN USB 2.0 Type-A Ethernet Adapter
- Davicom DM9601 Type-A Adapter
- USB RJ45-KYRS9600
- UGREEN Type-A Ethernet Adapter
- StarTeck USB 3.0 Type-A Ethernet Adapter
- Amazon USB 3.0 Type-A Ethernet Adapter

Note: Cisco does not endorse, support, or test third-party cases or covers for Cisco Wireless Phone 9821. Using Cisco Wireless Phone 9821 with 3rd-party cases or covers may void the warranty.

Wireless LAN Design

Follow these network design guidelines to ensure adequate coverage, call capacity, and seamless roaming for the Cisco Wireless Phone 9821.

802.11 Network

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

6 GHz (802.11ax)

Where regulatory domains permit, the 6 GHz band is highly recommended. Due to higher free-space path loss and reduced wall penetration compared to 5 GHz, 6 GHz deployment requires careful planning. Use predictive modeling and conduct post-installation passive surveys to validate coverage, particularly in areas with significant physical obstructions.

For optimal network design, use 5 GHz as the primary coverage layer for large areas, and reserve 6 GHz for targeted high-density or capacity-demanding zones. Maintain consistent channel widths across the deployment area and limit the number of SSIDs on the 6 GHz band (maximum of 3) to minimize management overhead.

To facilitate efficient client discovery, configure APs to operate concurrently on 5 GHz and 6 GHz. Clients can discover 6 GHz network via **RNR** on 5 GHz. **PSC enforcement** can limit access points to primary channels. **RNR**+**PSC enforcement** and **FILS discovery** could significantly speed up the time it takes for clients to find the network.

By default, Reduced Neighbor Report (RNR) works when APs broadcast information about 6 GHz network inside beacons of their 2.4 GHz and 5 GHz radios. This is achieved by a co-located SSID (identical name) running on 2.4 GHz or 5 GHz so the client can discover the 6 GHz channel.

Enable 6 GHz client steering to proactively transition capable devices to the cleaner 6 GHz spectrum.

For advanced RF parameters, refer to Cisco’s AI-RRM best practices for Wireless LAN Controllers (WLCs) and Access Points (APs).

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

5 GHz is the recommended frequency band for operating Cisco Wireless Phone 9821.

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

If there is intermittent interference, it may be necessary to statically assign channels to the access point or access points serving that area..

Cisco Wireless Phone 9821 supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, 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 an 802.11a/n/ac/ax environment, it's crucial to have at least 20 percent overlap with adjacent channels. For critical areas, increasing the overlap to 30% or more is recommended to ensure that there can be at least 2 access points available with a signal of -67 dBm or higher. Additionally, Cisco Wireless Phone 9821 complies with the access point's receiver sensitivity (required signal level for the current data rate).

Dynamic Frequency Selection (DFS)

DFS triggers a channel change when radar signal is detected. Upon detection, the access point (AP) radio ceases transmission for at least 60 seconds to perform a scan for another usable channel. Because the AP stops broadcasting beacons during this silent period, the connected Cisco Wireless Phone 9821 will experience a temporary loss of connectivity.

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.

To mitigate the impact of radar-induced channel changes, it is recommended to ensure that at least one access point in each coverage area operates on a non-DFS channel, such as those within the UNII-1 band. This ensures that a channel is available when an access point's radio is in its hold-off period while scanning for a new usable channel.

Optionally, use a UNII-3 channel (5.745 - 5.825 GHz 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.

2.4 GHz (802.11b/g/n/ax)

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

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

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

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

Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying Cisco Wireless Phone 9821 in an 802.11b/g/n/ax environment, which allows for seamless roaming.

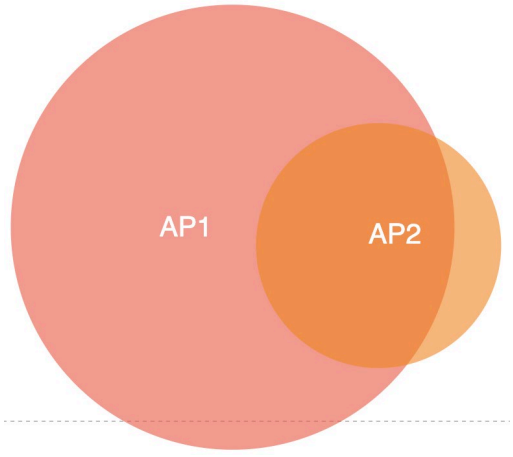
Using an overlapping channel set such as 1, 5, 9, 13 is not suggested, but users can choose them based on their local air environments.

Cells Deployment

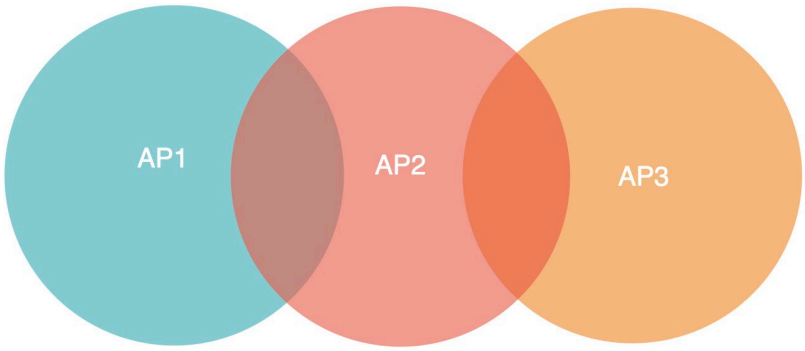
To ensure optimal roaming performance, access point cells must maintain sufficient overlap with adjacent coverage areas. The following examples illustrate sample overlap configurations for client transitions.



No overlap. Cannot roam



Too much overlap. Clients may stick to AP1



Minimum 20% overlap

Power Balancing

Adhere to established RF design principles for voice-over-IP (VoIP) deployments. If there is no specific requirement for 2.4 GHz coverage, it is recommended to disable the 2.4 GHz radio to reduce co-channel interference and optimize airtime efficiency.

Signal Strength and Coverage

To ensure acceptable voice quality, Cisco Wireless Phone 9821 should always have a signal of -67 dBm or higher, while the phone also meets the access point's receiver sensitivity required signal level for the transmitted data rate.

Maintain a Packet Error Rate (PER) of 1% or less for voice traffic, and 5% or less for standard data and web applications. It is important to note that voice traffic is highly sensitive to packet loss; exceeding a 1% PER threshold typically results in degraded audio quality, characterized by 'choppy' or robotic speech, or potential call drops.

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.

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

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

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

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

Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g/n. Some microwaves are shielded more than others and that shielding reduces the spread of energy. Microwave energy can impact channel 11, while some microwaves can affect the entire 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 and 6 GHz frequency. The 802.11a/n/ac/ax technology provides more non-overlapping channels and typically

lower initial RF utilization. For voice deployments, it is suggested to use 802.11a/n/ac/ax for voice and use 802.11b/g/n 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).

Cisco CleanAir can help to detect, classify, locate and mitigate sources of radio frequency (RF) interference that standard Wi-Fi chipsets cannot see. When combined with a management platform (such as Cisco DNA center or Prime Infrastructure), CleanAir can 'triangulate' the interference. You can see a 'heat map' of the interference on your floor plan, showing exactly where the offending device is located.

Data Rates

Management frames and multicast traffic are transmitted at the lowest mandatory data rate. In environments with sufficient RF coverage, it is recommended to incrementally disable lower data rates. Limiting the number of supported data rates reduces management overhead, discourages 'sticky' clients, and ensures that retransmissions occur at more efficient rates, which significantly improves overall airtime utilization.

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 same applies for 6 GHz deployments.

Cisco Wireless Phone 9821 is 1x1 with single antenna, therefore they support up to MCS 7 data rates for 802.11n (up to 150 Mbps). For 802.11ac, Cisco Wireless Phone 9821 supports up to VHT80 MCS 9 1SS (up to 433 Mbps). For 802.11ax, Cisco Wireless Phone 9821 supports up to HE80 MCS 11(up to 600 Mbps).

If 802.11b clients are not allowed in the wireless network, 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, 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, use a limited set of the data rates 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 Cisco Wireless Phone 9821 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 Cisco Wireless Phone 9821 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 6 GHz and 5 GHz. Use of 2.4 GHz, especially when 802.11b rates are enabled, may not work well.

In the 6 GHz band, it is recommended to utilize 80 MHz channel widths, which provide 14 non-overlapping channels in the US regulatory domain and 6 in the EU/UK domains. This abundance of spectrum significantly mitigates co-channel interference (CCI), even in high-density deployments. To ensure optimal client discovery, always configure the primary channel as a Preferred Scanning Channel (PSC).

In the 5 GHz band, it is recommended to utilize an 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, disable the data rates above 24 Mbps to increase first transmission success. If the same band is also used for data, video or other applications, then is suggested to keep the higher data rates enabled.

Transmit Power

Due to the potential of elevated multipath in rugged environments, the transmit power of the access point and Cisco Wireless Phone 9821 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.

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

Quality of Service (QoS)

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. Wi-Fi 6 introduced Long Symbol Duration, Extended GI, OFDMA, advanced beamforming and uplink MU-MIMO all together to resolve multipath problem.

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. Cisco Wireless Phone 9821 supports the following wireless security features.

WLAN Authentication

- WPA2 and WPA3 enterprise (802.1x authentication)
- WPA2-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 and OWE

WLAN Encryption

- AES (minimum 128-bit Advanced Encryption Standard)

- AES-GCM (AES with Galois/Counter Mode)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
- PMF (Protected Management Frames)

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)

- Suite-B (Encryption with GCMP, Digital Signature with ECDSA, Key Exchange with ECDH and Hashing with SHA2)
- Suite-B-192 (longer bits of security strength)

Note: CCMP256 encryption cipher is not supported.

Cisco Wireless Phone 9821 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 Cisco Wireless Phone 9821 and the RADIUS server. The server sends an Authority ID (AID) to the phone, which in turn selects the appropriate PAC. The phone 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 be enabled on the RADIUS server.

To enable EAP-FAST, you must install a certificate on the RADIUS server.

Cisco Wireless Phone 9821 currently supports automatic provisioning of the PAC only. Therefore, enable **Allow anonymous in-band PAC provisioning** on the RADIUS server. When this option is enabled, both EAP-GTC and EAP-MSCHAPv2 must be active.

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

If anonymous PAC provisioning is not allowed in the production wireless LAN environment, set up a staging RADIUS server for initial PAC provisioning of Cisco Wireless Phone 9821.

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

Ensure the production primary EAP-FAST RADIUS server is setup to send the EAP-FAST primary keys and policies to the staging secondary EAP-FAST RADIUS server, which will then allow Cisco Wireless Phone 9821 to use the provisioned PAC in the production environment where **Allow anonymous in-band PAC provisioning** is disabled.

When renewing the PAC, authenticated in-band PAC provisioning is used. Therefore, ensure that **Allow authenticated in-band PAC provisioning** is enabled.

Ensure that Cisco Wireless Phone 9821 has connected to the network during the grace period to ensure it can use its existing PAC —created with either the active or retired primary key—to obtain a new PAC.

It is recommended to point the staging wireless LAN only to the staging RADIUS server and to disable the staging access point radios when not in use.

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 strong security but requires client certificate management. It may also require a user account to be created on the authentication server matching the common name of the certificate imported into Cisco Wireless Phone 9821.

It is recommended that EAP-TLS be the only EAP type enabled on the RADIUS server to ensure optimal security.

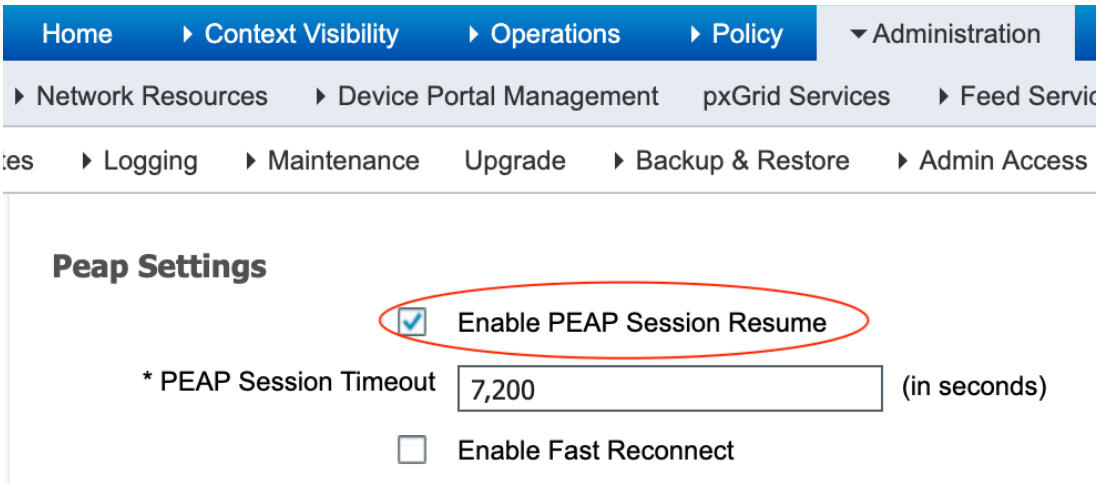
Protected Extensible Authentication Protocol (PEAP)

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by establishing an encrypted SSL/TLS tunnel between the client and the authentication server. This tunnel protects the subsequent exchange of authentication information, ensuring that user credentials remain confidential and secure from eavesdropping.

PEAP supports inner authentication protocols such as PEAP-GTC and PEAP-MSCHAPv2. It requires that a user account be created on the authentication server to facilitate authentication.

Enable Session Resume

It is recommended to enable session resume for the corresponding EAP algorithm on ISE, which reduces Wi-Fi authentication and authorization time. See the following screenshot as an example:



Quality of Service (QoS)

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

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

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

Traffic Type	Call Server	DSCP	802.1p	WMM UP	Port Range
Voice	CUCM	CS4 (32)	4	5	RTP/RTCP port negotiated with remote peer.
	Webex	EF (46)	5	6	RTP/RTCP port negotiated with remote peer
Call Control	CUCM	CS3 (24)	3	4	TCP/UDP port configured by admin
	Webex	default (0)	0	0	HTTPS (TCP 443)

- 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 Wireless Phone 9821 does not support Call Admission Control of voice stream.

If CAC/TSPEC is enabled for voice in the access point, then the priority of related frames will be downgraded.

Wired QoS

Configure QoS settings and policies for the necessary network devices.

Configuring Cisco Switch Ports for WLAN Devices

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

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

Enable COS trust for Cisco Wireless LAN Controller

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

Enable DSCP trust for Cisco Access Points

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

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

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

Cisco Wireless Phone 9821 connects to 6 GHz, 5 GHz or 2.4GHz bands and enables inter-band roaming support.

802.1x without 802.11r (FT) can introduce delay during roaming due to its requirement for full re-authentication. 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 that transition time from one access point to another will not be audible to the user.

Cisco Wireless Phone 9821 supports 802.11r (FT). See the following table for authentication type and the roaming time.

Authentication	Roaming Time
Personal	150 ms
Enterprise	300 ms
802.11r (FT)	< 100 ms

The Cisco Wireless Phone 9821 manages the scanning and roaming events.

The roaming trigger for majority of roams should be due to meeting the required RSSI differential based on the current RSSI, which results in 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.

802.11r (FT) enables fast secure roaming and limits the off-network time to keep audio gaps at a minimum when on call.

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 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 communications 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.

Cisco Wireless Phone 9821 supports 802.11r (FT) with WPA2-PSK, WPA3-SAE or WPA2/WPA3 enterprise, but Suite-B or Suite-B-192 doesn't support FT roam.

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
non-FT	Suite-B	WPA-EAP-SUITE-B	GCMP	Yes
non-FT	Suite-B-192	WPA-EAP-SUITE-B-192	GCMP	Yes

Note: When deploying Cisco Wireless Phone 9821 in an environment with legacy voice devices that do not support 802.11r (Fast Transition), you may utilize the existing SSID. It is recommended to enable 802.11r using the 'Over-the-Air' (OTA) method in conjunction with your existing key management protocols, such as 802.1X. Before implementation, verify that all legacy devices can successfully interoperate within an 802.11r-enabled network, even if they do not actively utilize the FT feature.

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

Interband Roaming

Cisco Wireless Phone 9821 supports interband roaming across the 6 GHz, 5 GHz, and 2.4 GHz frequency bands. By default, the device prioritizes the connection with the strongest Received Signal Strength Indicator (RSSI). Because 2.4 GHz signals generally exhibit superior propagation characteristics compared to 5 GHz and 6 GHz, the phone may favor the 2.4 GHz band when transmit power levels are uniform across all bands. To ensure the client prioritizes 5 GHz or 6 GHz, administrators should carefully calibrate AP transmit power levels and implement infrastructure-side features such as **6G Clients Steering**.

At power on, Cisco Wireless Phone 9821 will scan all 2.4 GHz, 5 GHz and 6 GHz channels, then attempt to associate to an access point for the configured network if available.

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

Delivery Traffic Indicator Message (DTIM)

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

Since Cisco Wireless Phone 9821 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 considering multicast applications, a shorter DTIM period can be used.

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

Call Capacity

Design the network to accommodate the desired call capacity.

It is essential to distinguish between **Association Capacity**—the total number of clients that can maintain an association with an access point—and **Call Capacity**, which refers to the number of concurrent, high-quality voice streams an access point can support. While modern Cisco Catalyst 9100 series access points support a theoretical association limit of 512 clients per radio (totaling over 1,500 clients for a tri-band AP such as the Catalyst 9136 or 9166), the practical capacity for concurrent voice calls is significantly lower. Because voice traffic requires consistent airtime and strict latency guarantees, the actual number of high-quality calls an access point can sustain is only a fraction of its total association capacity.

Wi-Fi mode	**Recommended Max Concurrent Calls (per Radio)**
802.11b (legacy)	7 ~ 8 calls (G.711 codec)
802.11a/g/n	20 ~ 25 calls
802.11ac (Wi-Fi 5)	~ 30 calls
802.11ax (Wi-Fi 6/6E)	~ 40 calls

Note: The capacity estimates provided in this table assume the access point is dedicated exclusively to voice traffic. In environments where concurrent high-bandwidth data applications—such as video streaming or large file transfers—are present, the effective voice capacity may be reduced by 50% or more due to increased airtime contention.

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.

Cisco Wireless Phone 9821 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.

Cisco Wireless Phone 9821 supports the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure that IGMP snooping is also enabled on all switches.

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

Note: Cisco Wireless Phone 9821 supports IGMP v2 only.

Configuring the Cisco Wireless LAN

Cisco AireOS Wireless LAN Controller and Lightweight Access Points

Cisco AireOS-based Wireless LAN Controllers (WLCs) and associated access points have reached End-of-Life (EOL) status and do not support Wi-Fi 6E (6 GHz). However, Cisco Wireless Phone 9821 remains compatible with AireOS infrastructure in environments where 6 GHz connectivity is not required. When configuring AireOS WLCs and lightweight access points for use with Cisco Wireless Phone 9821, adhere to the following guidelines:

- Enable **802.11r (FT)**
- Disable **CCKM**
- Disable **Call Admission Control (CAC)**
- 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 **Enabled**
- Disable **P2P (Peer to Peer) Blocking Action**
- Ensure **Client Exclusion** is configured correctly
- Disable **DHCP Address Assignment Required**
- Set **Protected Management Frame (PMF)** to **Optional** or **Required** for WPA3, and **Disabled** for WPA2
- Set **MFP Client Protection** to **Optional** or **Required** for WPA3, and **Disabled** for WPA2
- Set the **DTIM Period** to **2** if no multicast application.
- Set **Client Load Balancing** to **Disabled**
- Set **Client Band Select** to **Disabled**
- Set **IGMP Snooping** to **Enabled**

- Enable **Symmetric Mobile Tunneling Mode** if Layer 3 mobility is utilized
- Enable **ClientLink** if utilizing Cisco 802.11 n/ac/ax capable Access Points
- Configure the **Data Rates** as necessary
- Configure **Auto RF** as necessary
- Set EDCA Profile to **Voice Optimized**
- Set **Enable Low Latency MAC** to **Disabled**
- Ensure that **Power Constraint** is **Disabled**
- Enable **Channel Announcement** and **Channel Quiet Mode**
- Configure the **High Throughput Data Rates** as necessary
- Configure the **Frame Aggregation** settings
- Enable **CleanAir** if utilizing Cisco access points with CleanAir technology
- Configure **Multicast Direct Feature** as necessary
- Set the **Protocol Type** to **None** for the **Platinum** QoS profile

Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points

When configuring the Cisco Wireless LAN Controller and Lightweight Access Points, adhere to the following guidelines.

- Enable **802.11r (FT)**
- uncheck **Over the DS**
- Disable **CCKM**
- Disable **Call Admission Control (CAC)**
- 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 **Enabled**
- Disable **P2P (Peer to Peer) Blocking Action**
- Ensure **Client Exclusion** Timeout is configured correctly
- Disable **DHCP Required**
- Set **Protected Management Frame (PMF)** to **Optional** or **Required** for WPA3, **Disabled** for WPA2
- Set the **DTIM Period** to **2** if no multicast application
- 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**
- 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

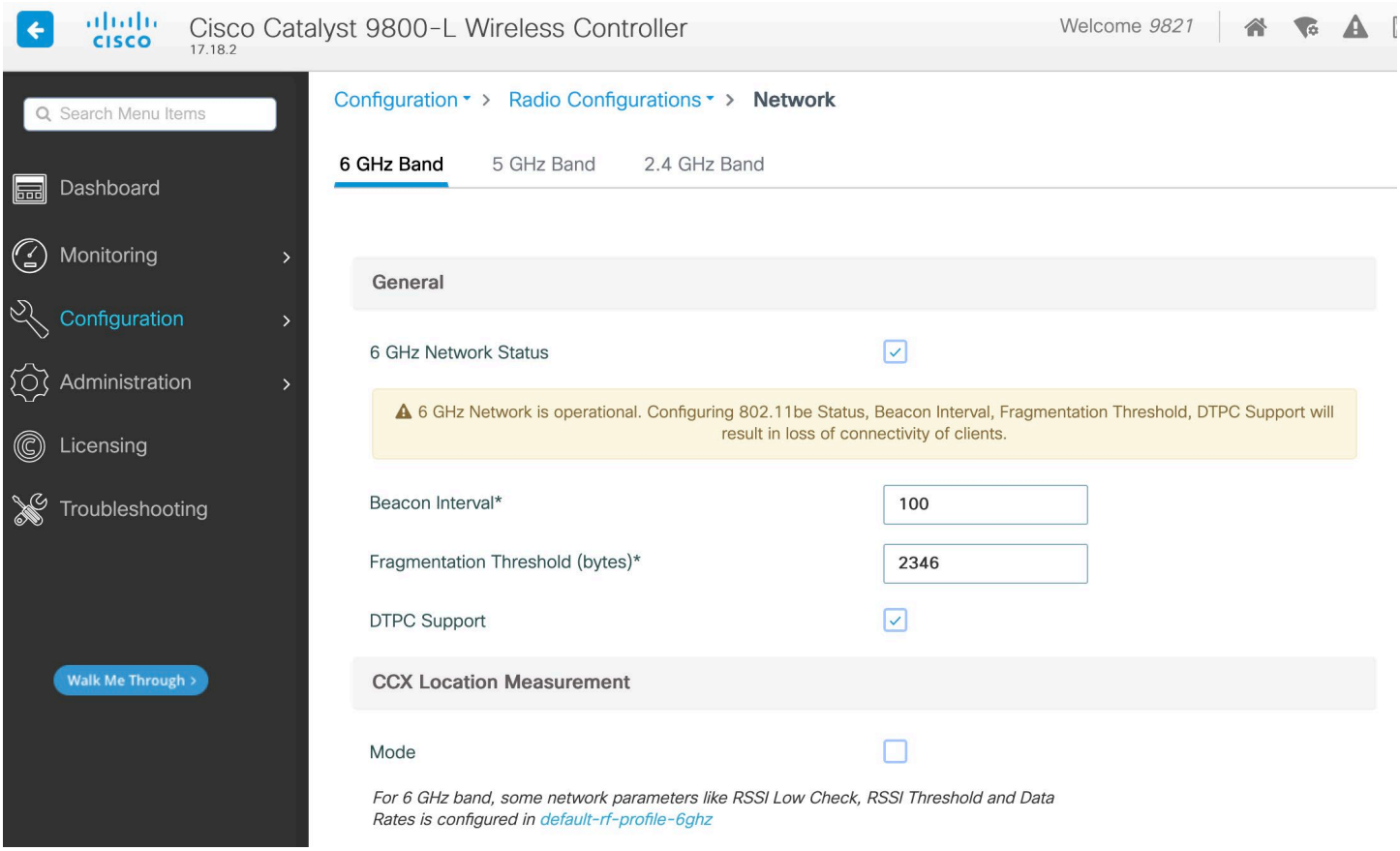
It is recommended to operate Cisco Wireless Phone 9821 on the 5 GHz or 6 GHz band. These bands provide significantly greater spectrum availability and lower levels of non-Wi-Fi interference compared to the 2.4 GHz band, resulting in a more stable and reliable environment for latency-sensitive voice traffic.

To use 5 GHz or 6 GHz frequency, ensure that the 5 GHz or 6 GHz network status is **Enable**d.

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

It is recommended to set 24 Mbps as the mandatory (basic) rate and 36 Mbps and higher as supported (optional) rates. However, some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

The same applies for 6 GHz tab.



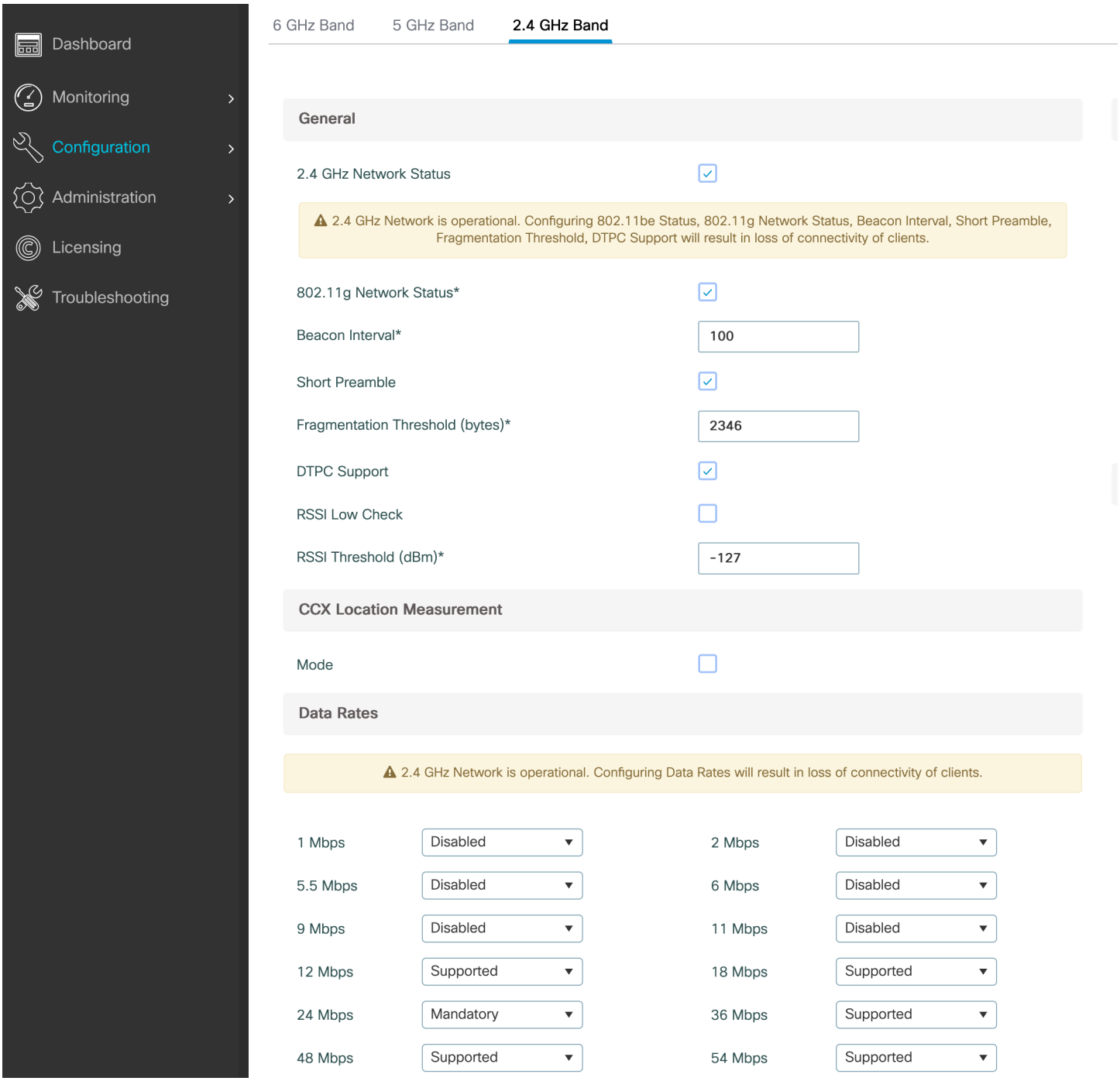
To use 2.4 GHz, ensure the 2.4 GHz network status and 802.11g network status are **Enabled**.

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

Set **Short Preamble** to **Enabled** in the 2.4 GHz radio configuration setting on the access point when no legacy clients that require a long preamble are present in the wireless LAN. By using the short preamble instead of long preamble, the wireless network performance is improved.

It is recommended to set 24 Mbps as the mandatory (basic) rate and 12, 18, 36 Mbps and higher as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN. However, some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

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



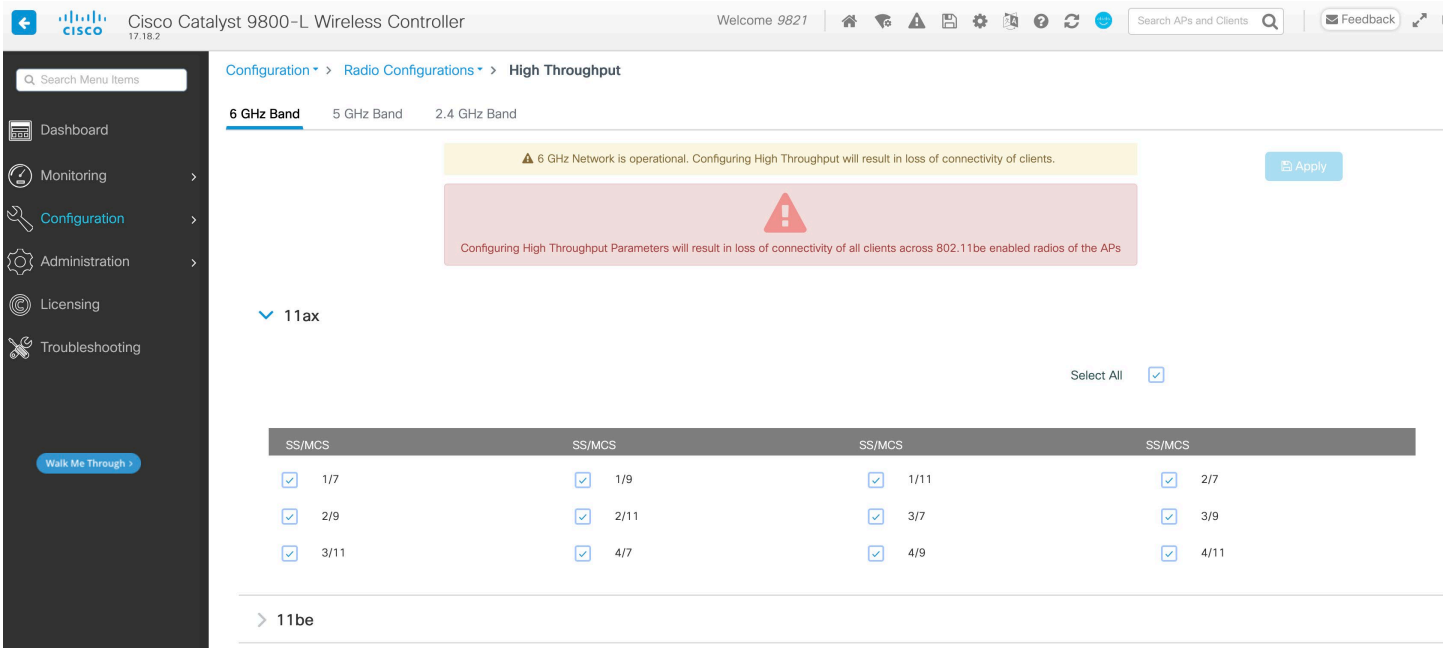
High Throughput (802.11n/ac/ax)

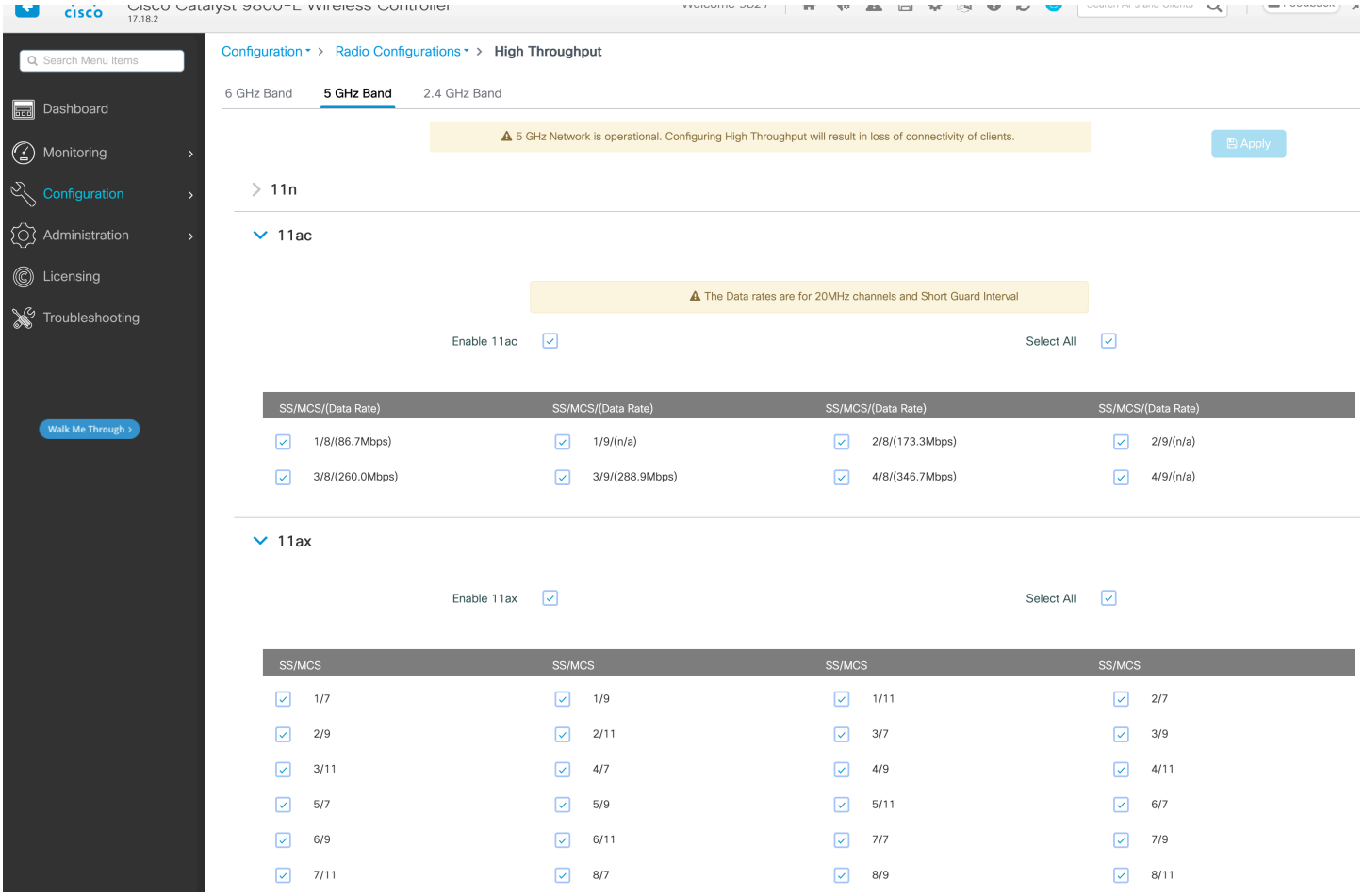
The 802.11n, 802.11ac and 802.11ax data rates can be configured per each band (2.4 GHz, 5 GHz and 6 GHz).

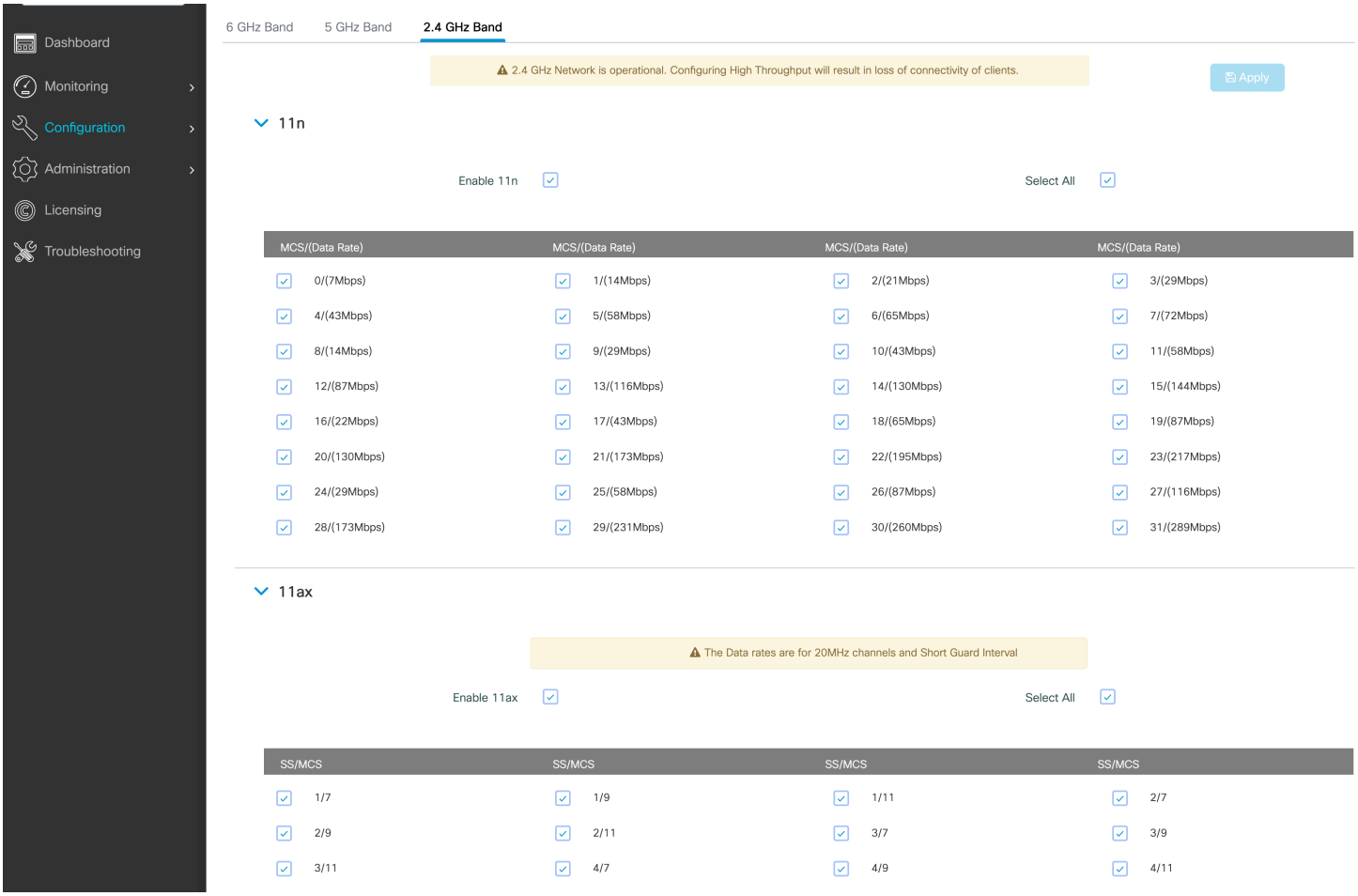
802.11ax data rates are applicable to all 3 bands.

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

Cisco Wireless Phone 9821 supports HT MCS 0 – MCS 7, VHT MCS 0 – MCS 9 and HE0 – HE111SS data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n/ac/ax clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of those higher data rates.




Cisco Catalyst 9800-L Wireless Controller
17.18.2
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through
Configuration
Radio Configurations
High Throughput
6 GHz Band
5 GHz Band
2.4 GHz Band
5 GHz Network is operational. Configuring High Throughput will result in loss of connectivity of clients.
Apply
11n
11ac
The Data rates are for 20MHz channels and Short Guard Interval
Enable 11ac
Select All
SS/MCS/(Data Rate)
1/8/(86.7Mbps)
1/9/(n/a)
2/8/(173.3Mbps)
2/9/(n/a)
3/8/(260.0Mbps)
3/9/(288.9Mbps)
4/8/(346.7Mbps)
4/9/(n/a)
11ax
Enable 11ax
Select All
SS/MCS
1/7
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
7/11
8/7
8/9
8/11



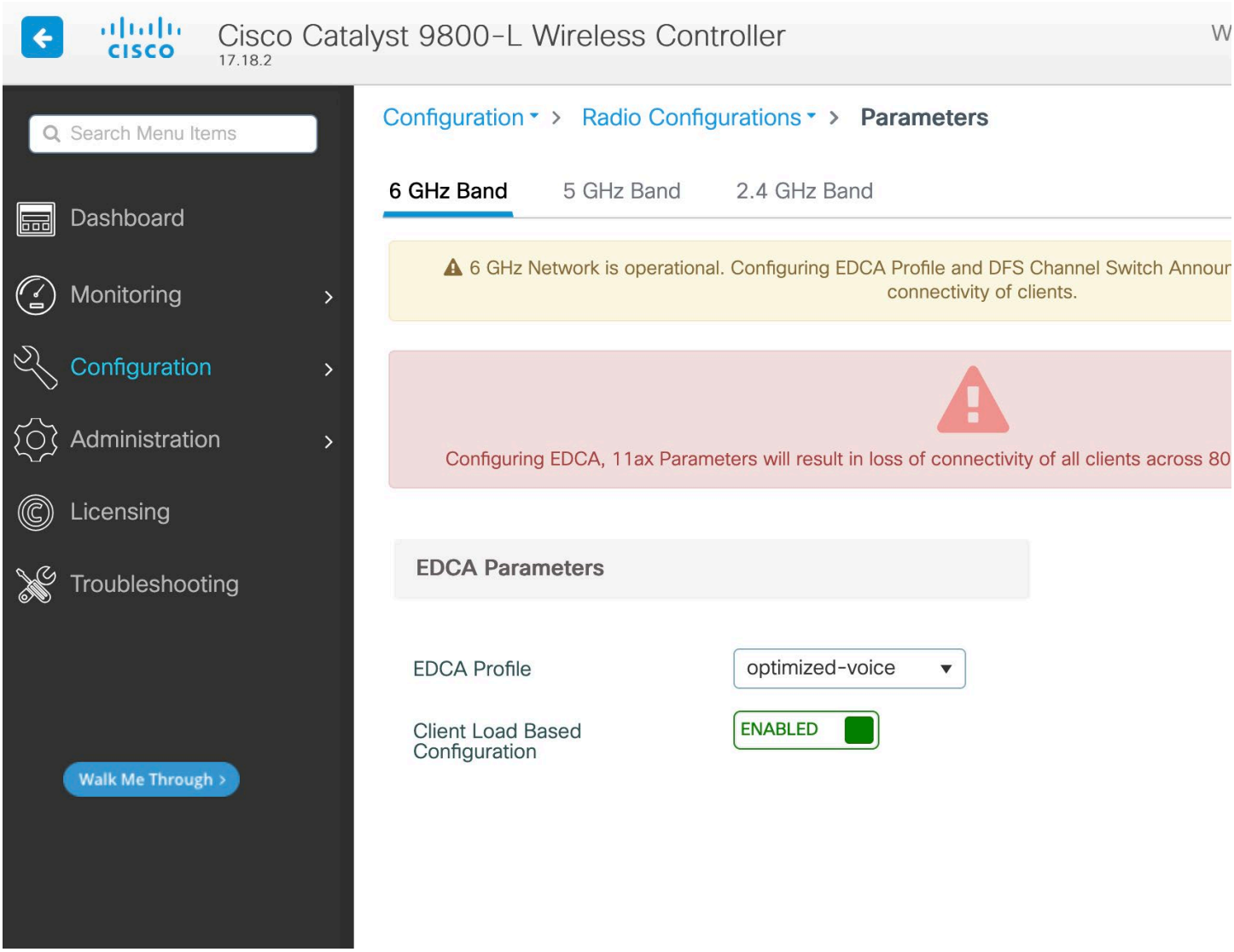
Parameters

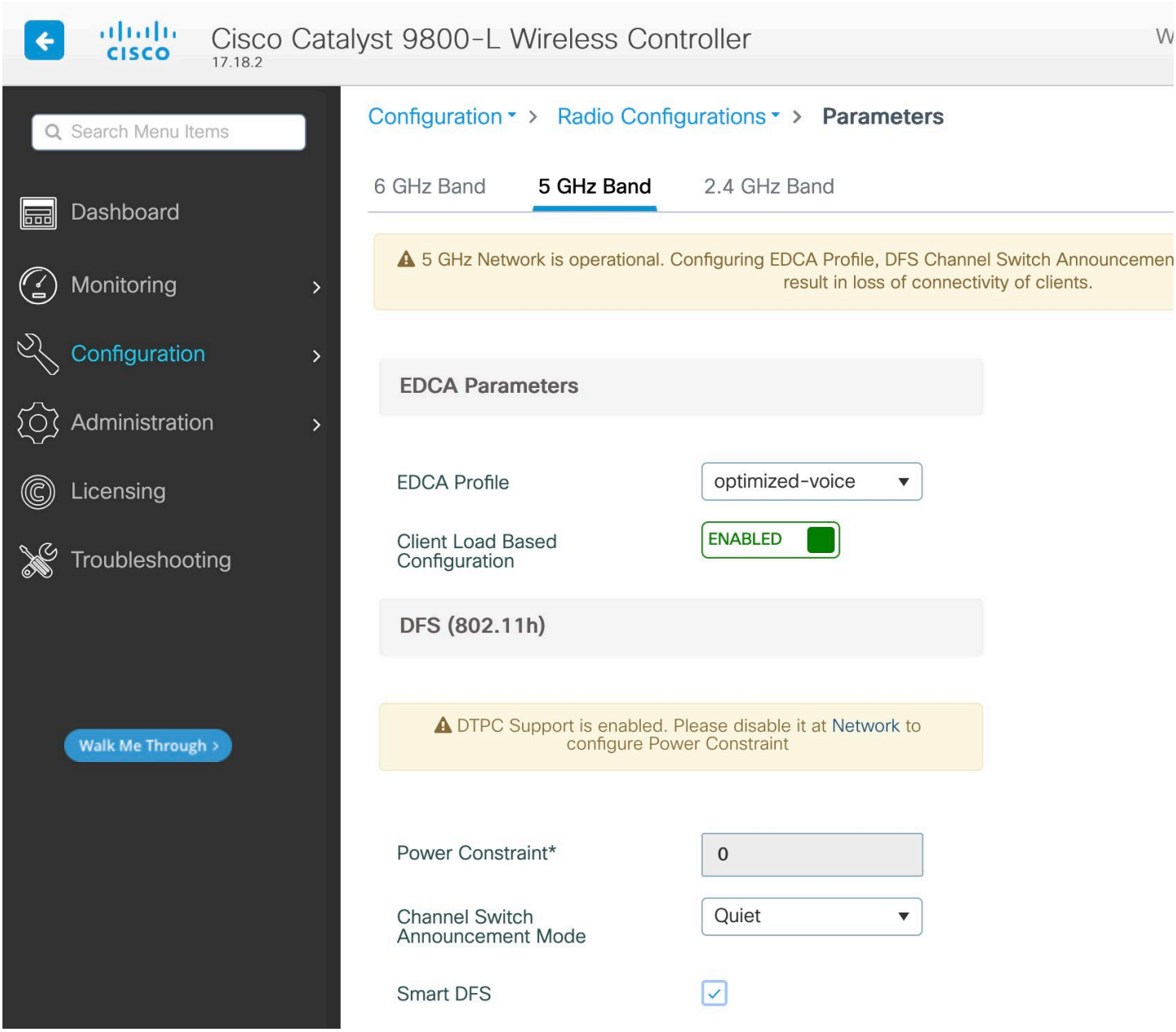
In the EDCA Parameters section, set the EDCA profile to **Optimized-voice** for the band (2.4 GHz, 5 GHz, and 6 GHz) that will support voice traffic.

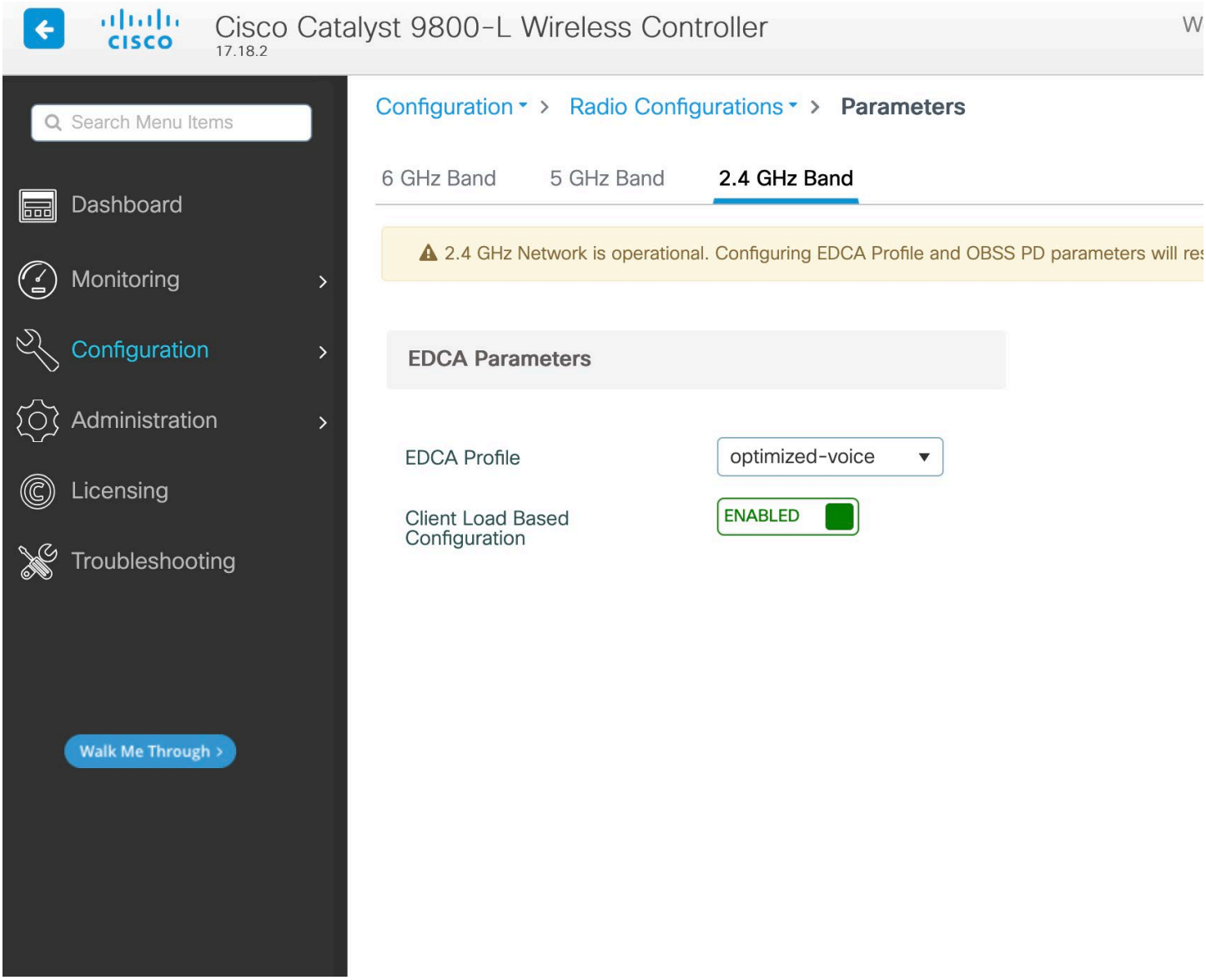
In the DFS (802.11h) section, leave **Power Constraint** un-configured or set the value to 0 dB.

Set **Channel Switch Status** and **Smart DFS** to **Enabled**.

Set **Channel Switch Announcement Mode** to **Quiet**.

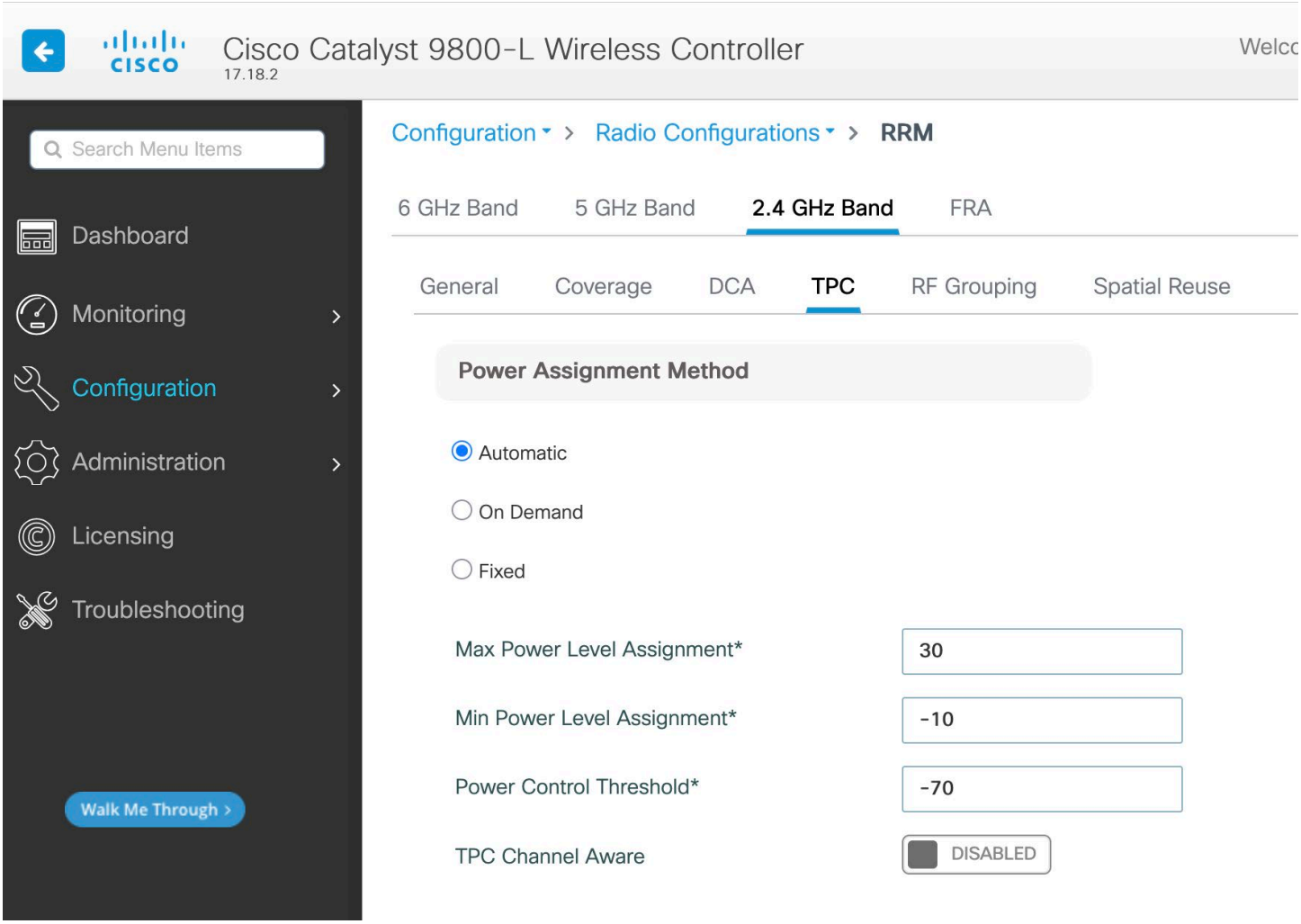

Cisco Catalyst 9800-L Wireless Controller
17.18.2
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through >
Configuration > Radio Configurations > Parameters
6 GHz Band
5 GHz Band
2.4 GHz Band
6 GHz Network is operational. Configuring EDCA Profile and DFS Channel Switch Announ
connectivity of clients.
Configuring EDCA, 11ax Parameters will result in loss of connectivity of all clients across 80
EDCA Parameters
EDCA Profile
optimized-voice
Client Load Based Configuration
ENABLED

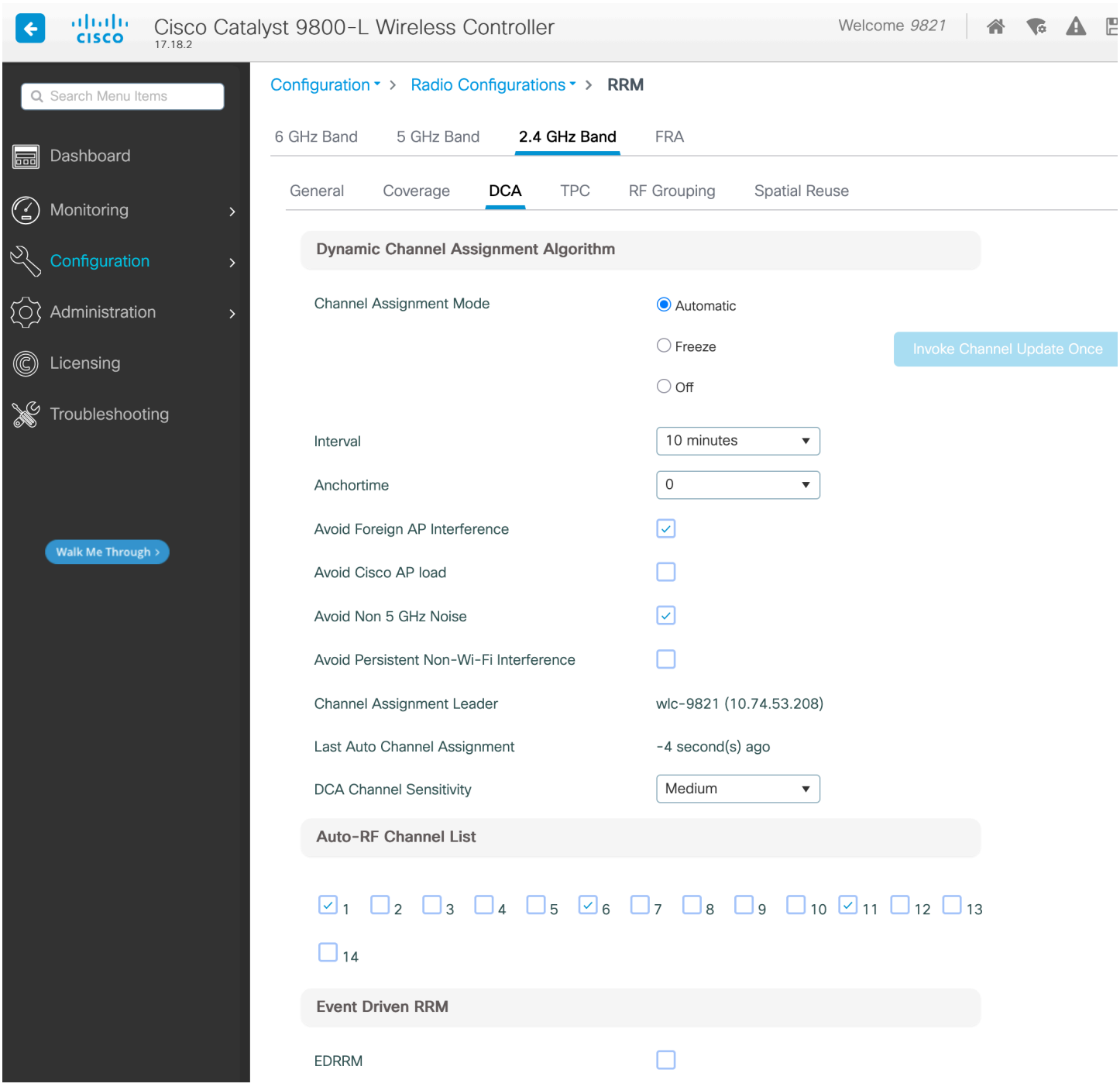

Cisco Catalyst 9800-L Wireless Controller
17.18.2
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through
Configuration
Radio Configurations
Parameters
6 GHz Band
5 GHz Band
2.4 GHz Band
5 GHz Network is operational. Configuring EDCA Profile, DFS Channel Switch Announcemen
result in loss of connectivity of clients.
EDCA Parameters
EDCA Profile
optimized-voice
Client Load Based Configuration
ENABLED
DFS (802.11h)
DTPC Support is enabled. Please disable it at Network to configure Power Constraint
Power Constraint*
0
Channel Switch Announcement Mode
Quiet
Smart DFS

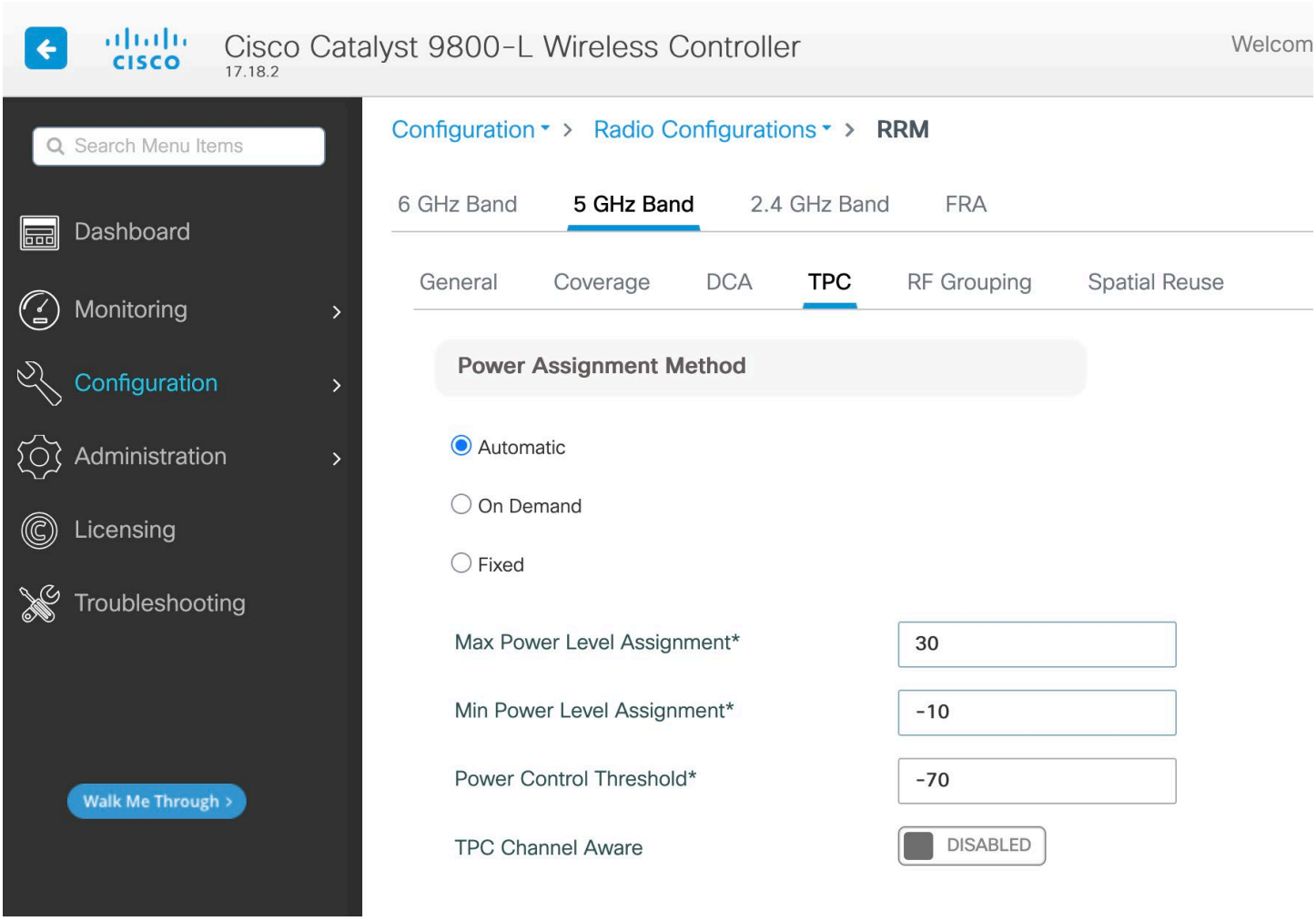


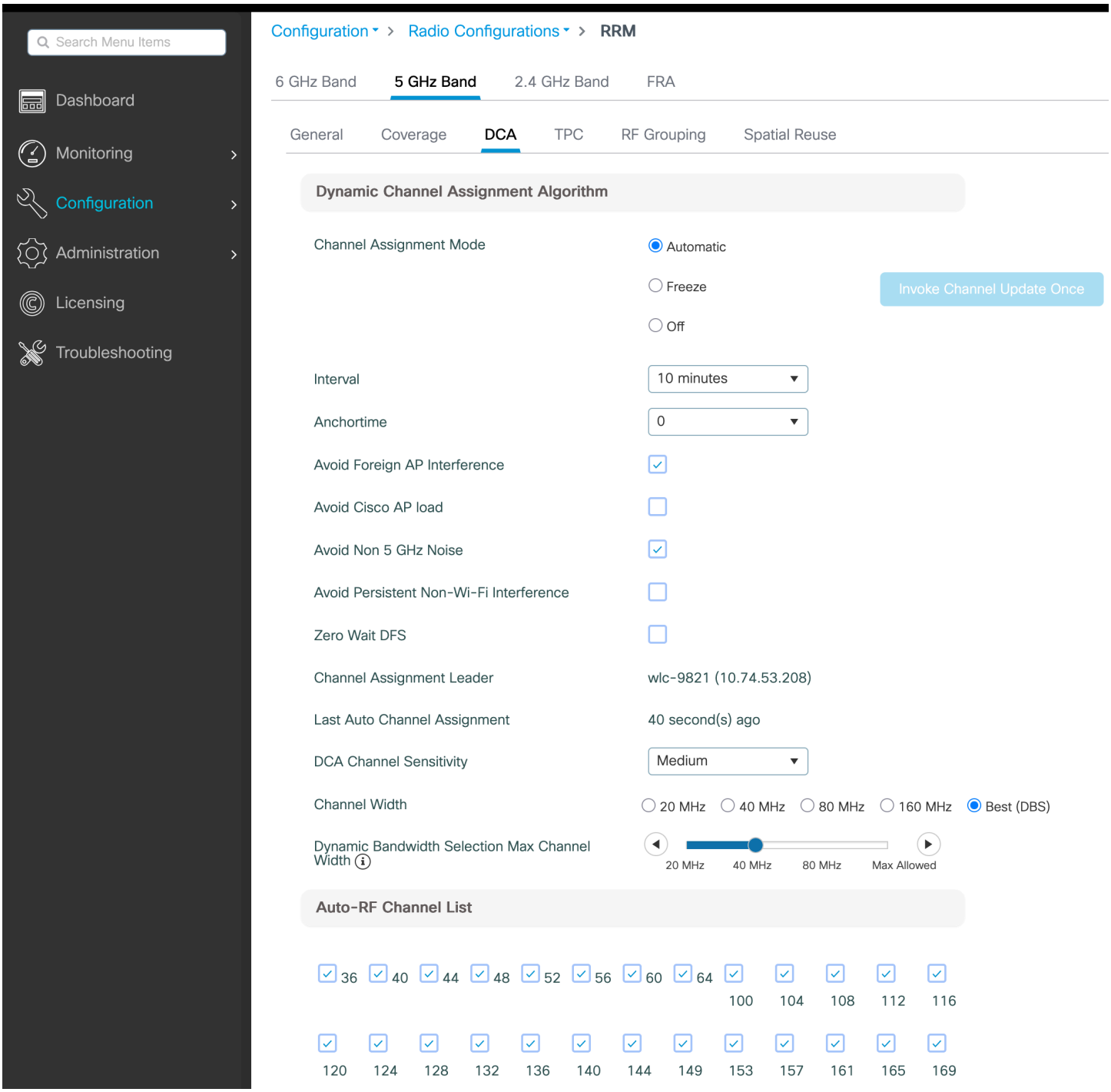
RRM

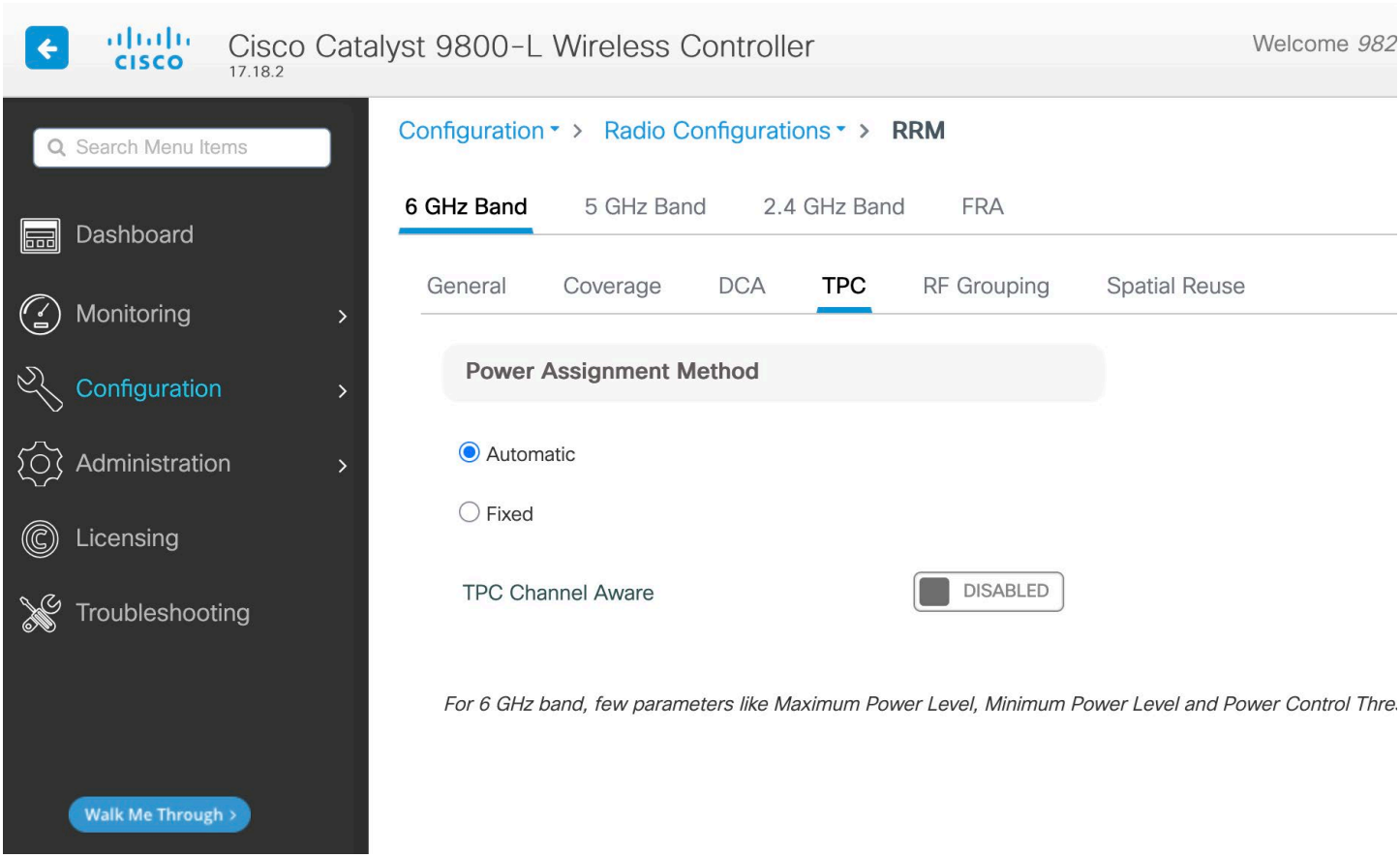
Adhere to established best practices for WLC and AP configurations. In most deployments, it is recommended to leverage Cisco AI-RRM (Radio Resource Management) to automate RF optimization, as dynamic management is generally more effective and reliable than manual tuning.

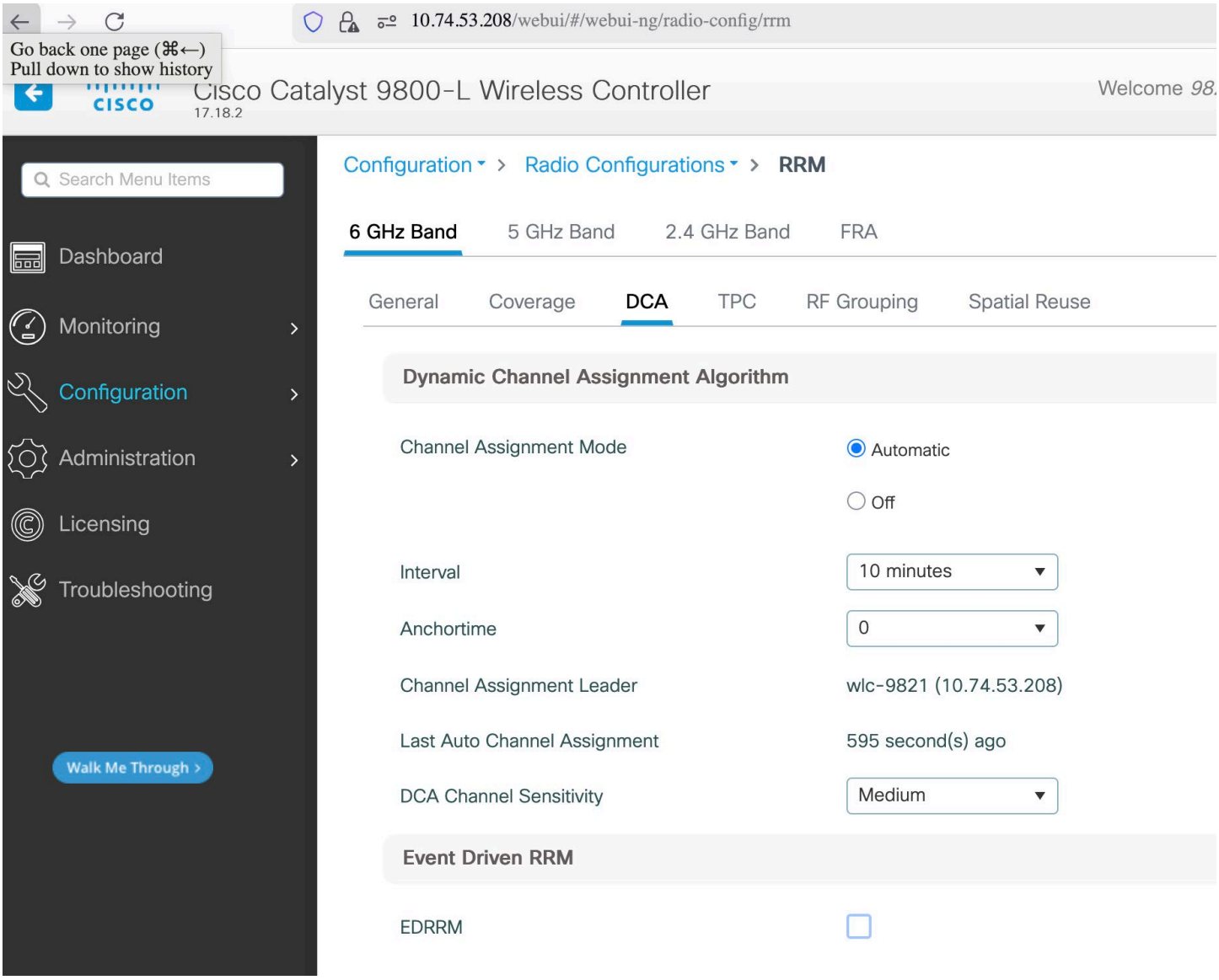

Cisco Catalyst 9800-L Wireless Controller
17.18.2
Welcc
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through >
Configuration > Radio Configurations > RRM
6 GHz Band
5 GHz Band
2.4 GHz Band
FRA
General
Coverage
DCA
TPC
RF Grouping
Spatial Reuse
Power Assignment Method
Automatic
On Demand
Fixed
Max Power Level Assignment*
30
Min Power Level Assignment*
-10
Power Control Threshold*
-70
TPC Channel Aware
DISABLED


Cisco Catalyst 9800-L Wireless Controller
17.18.2
Welcome 9821
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through
Configuration > Radio Configurations > RRM
6 GHz Band
5 GHz Band
2.4 GHz Band
FRA
General
Coverage
DCA
TPC
RF Grouping
Spatial Reuse
Dynamic Channel Assignment Algorithm
Channel Assignment Mode
Automatic
Freeze
Off
Invoke Channel Update Once
Interval
10 minutes
Anchortime
0
Avoid Foreign AP Interference
Avoid Cisco AP load
Avoid Non 5 GHz Noise
Avoid Persistent Non-Wi-Fi Interference
Channel Assignment Leader
wlc-9821 (10.74.53.208)
Last Auto Channel Assignment
-4 second(s) ago
DCA Channel Sensitivity
Medium
Auto-RF Channel List
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Event Driven RRM
EDRRM


Cisco Catalyst 9800-L Wireless Controller
17.18.2
Welcom
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through
Configuration
Radio Configurations
RRM
6 GHz Band
5 GHz Band
2.4 GHz Band
FRA
General
Coverage
DCA
TPC
RF Grouping
Spatial Reuse
Power Assignment Method
Automatic
On Demand
Fixed
Max Power Level Assignment*
30
Min Power Level Assignment*
-10
Power Control Threshold*
-70
TPC Channel Aware
DISABLED

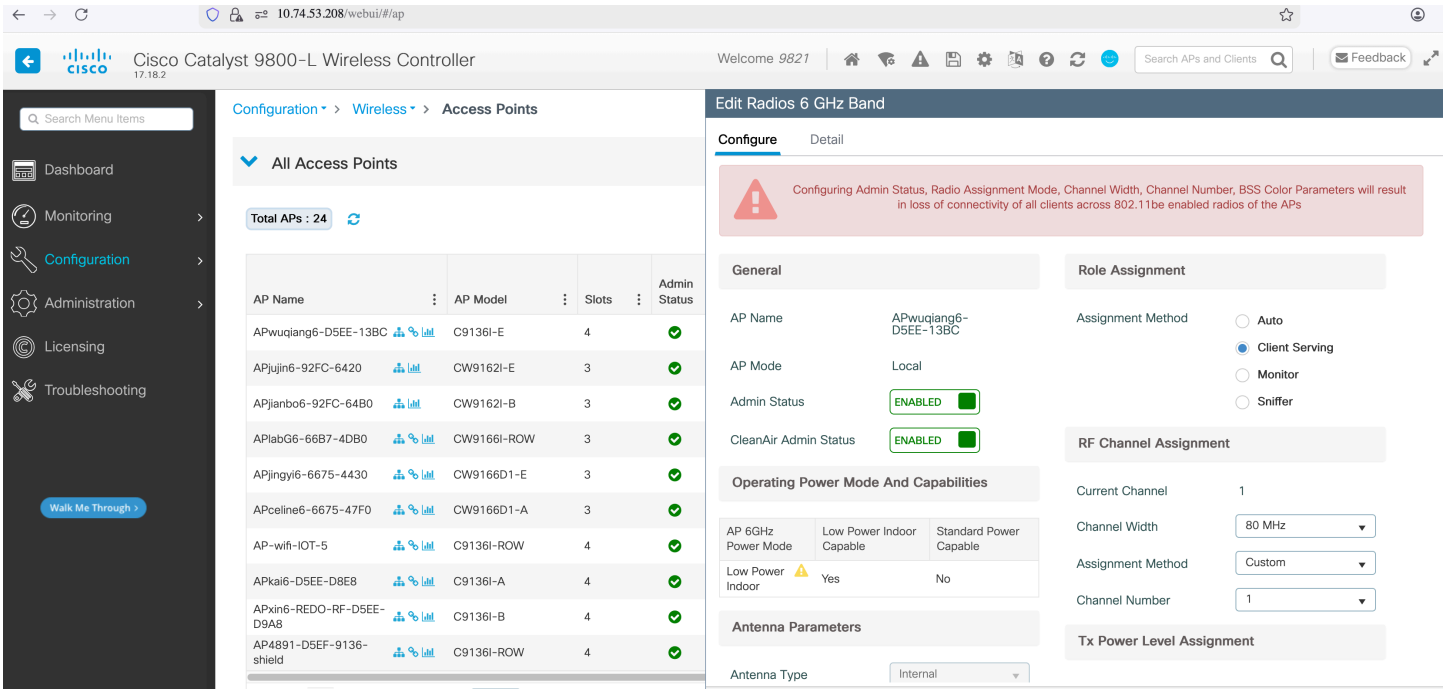

Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Configuration > Radio Configurations > RRM
6 GHz Band
5 GHz Band
2.4 GHz Band
FRA
General
Coverage
DCA
TPC
RF Grouping
Spatial Reuse
Dynamic Channel Assignment Algorithm
Channel Assignment Mode
Automatic
Freeze
Off
Invoke Channel Update Once
Interval
10 minutes
Anchortime
0
Avoid Foreign AP Interference
Avoid Cisco AP load
Avoid Non 5 GHz Noise
Avoid Persistent Non-Wi-Fi Interference
Zero Wait DFS
Channel Assignment Leader
wlc-9821 (10.74.53.208)
Last Auto Channel Assignment
40 second(s) ago
DCA Channel Sensitivity
Medium
Channel Width
20 MHz
40 MHz
80 MHz
160 MHz
Best (DBS)
Dynamic Bandwidth Selection Max Channel Width
20 MHz
40 MHz
80 MHz
Max Allowed
Auto-RF Channel List
36 40 44 48 52 56 60 64 100 104 108 112 116
120 124 128 132 136 140 144 149 153 157 161 165 169


Cisco Catalyst 9800-L Wireless Controller
17.18.2
Welcome 982
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through
Configuration > Radio Configurations > RRM
6 GHz Band
5 GHz Band
2.4 GHz Band
FRA
General
Coverage
DCA
TPC
RF Grouping
Spatial Reuse
Power Assignment Method
Automatic
Fixed
TPC Channel Aware
DISABLED
For 6 GHz band, few parameters like Maximum Power Level, Minimum Power Level and Power Control Thre



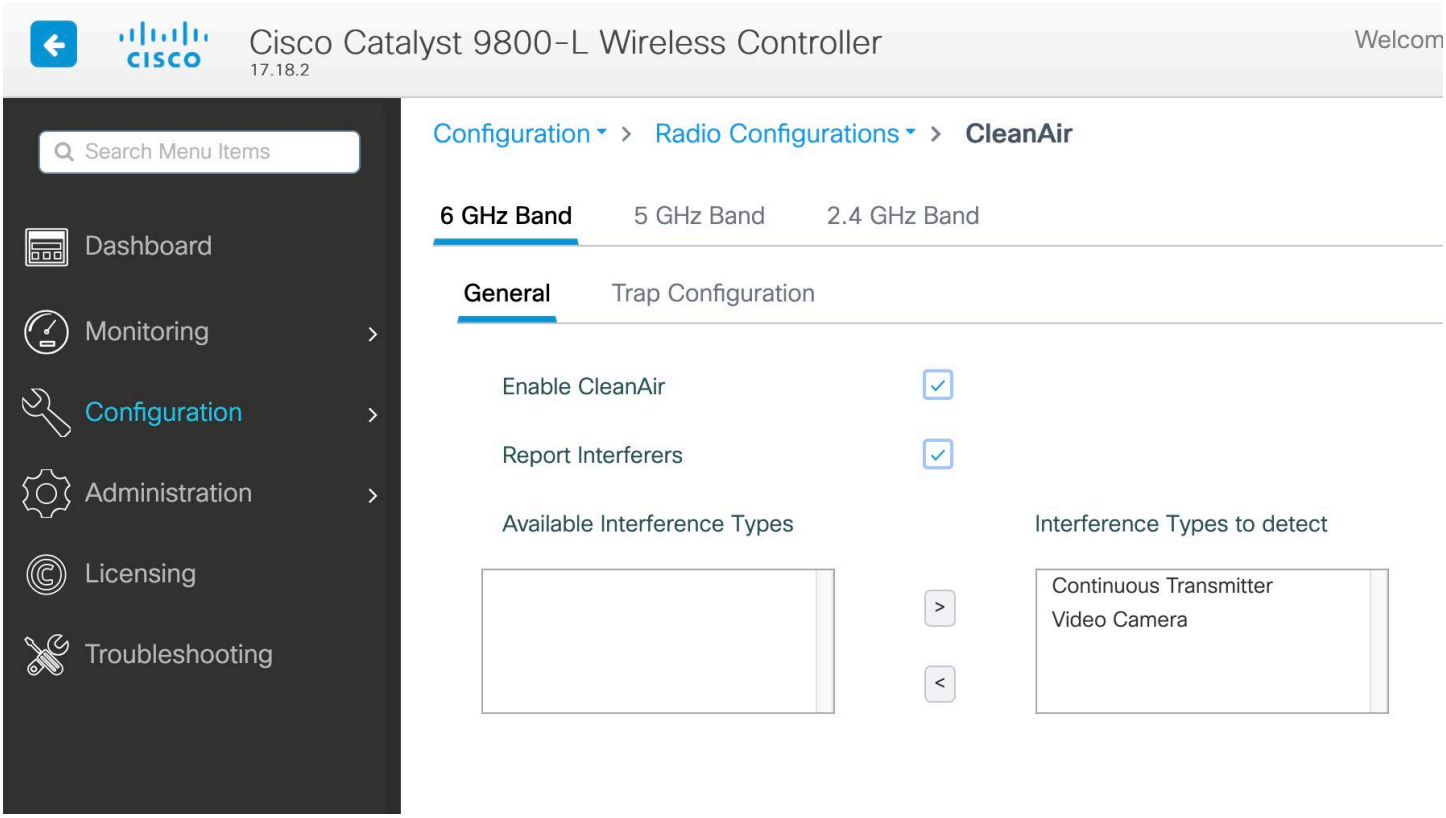
Individual access points can be configured to override global RRM settings with static channel and transmit power assignments.

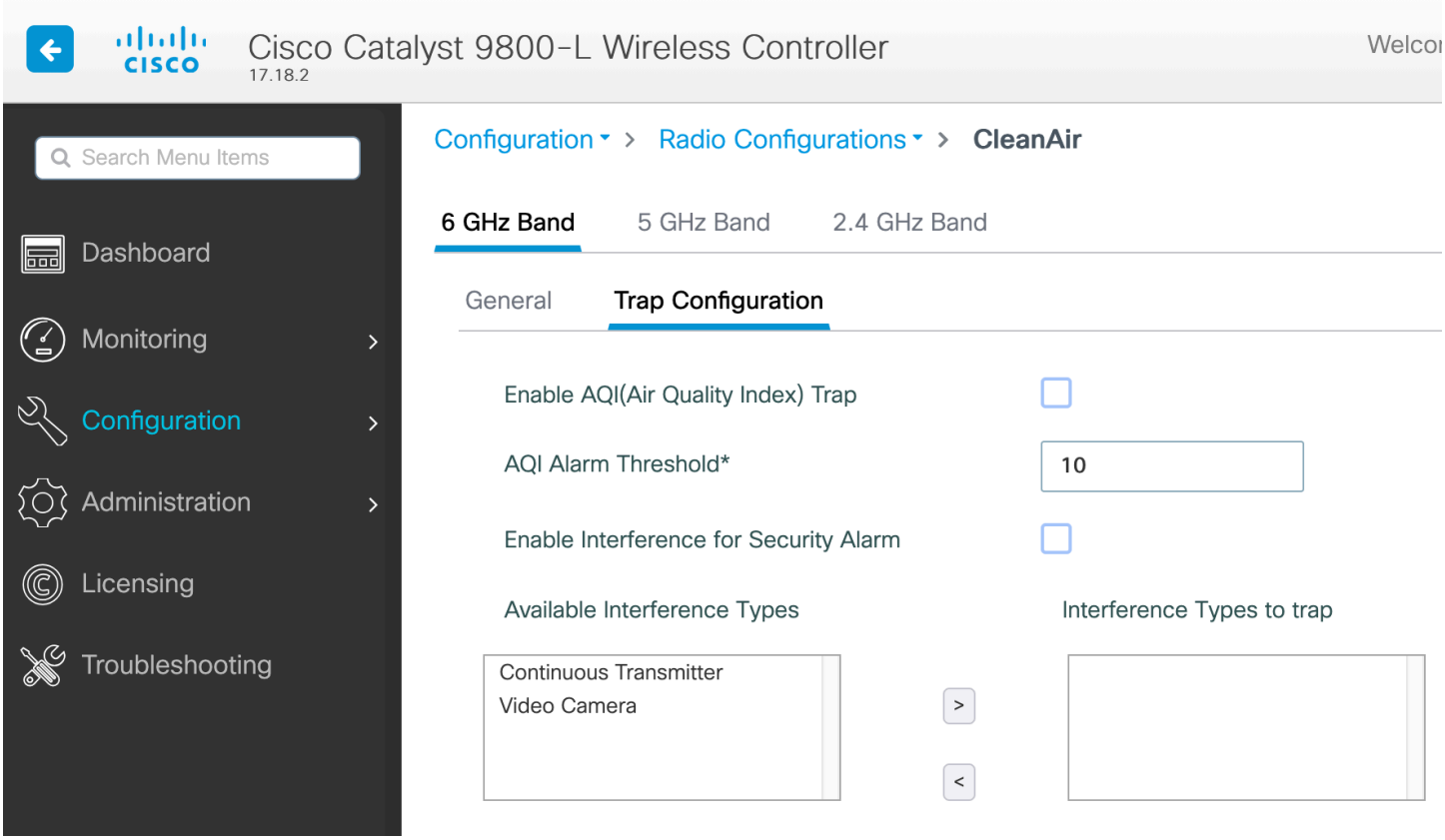
When specific APs are statically configured, the RRM algorithm automatically adjusts its calculations to account for these fixed assignments. This manual override may be necessary to address localized, intermittent interference that cannot be adequately mitigated by automated RRM processes.



CleanAir

Select **Enable CleanAir** when utilizing Cisco access points with CleanAir technology to detect any existing interferers.





WLAN Settings

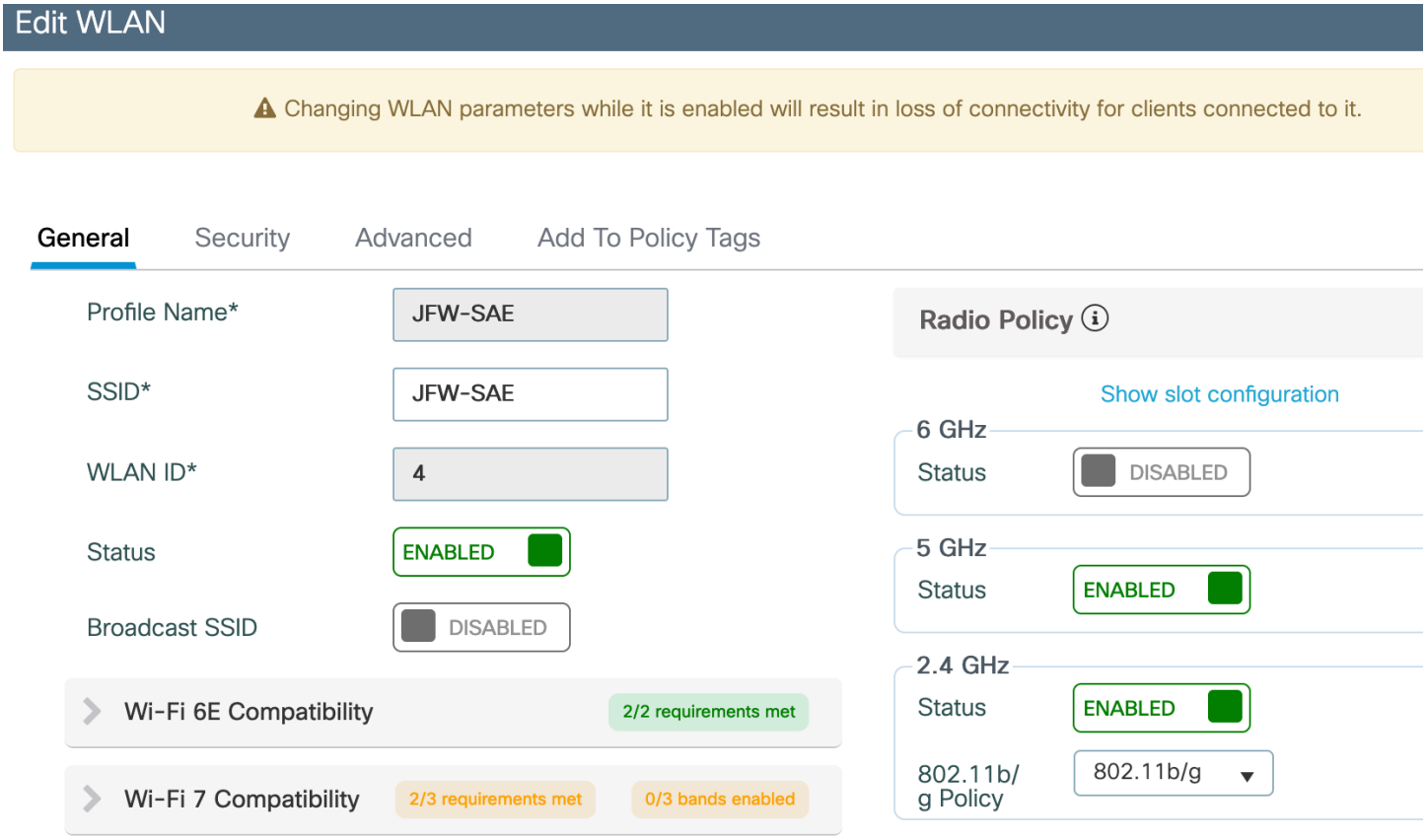
It is recommended to have a separate SSID for Cisco Wireless Phone 9821.

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 Cisco Wireless Phone 9821 can be configured to only apply to a certain 802.11 radio policy (e.g. 5 GHz only).

It is recommended to operate Cisco Wireless Phone 9821 on the 5 GHz or 6 GHz band. These bands provide significantly greater spectrum availability and lower levels of non-Wi-Fi interference compared to the 2.4 GHz band, resulting in a more stable and reliable environment for latency-sensitive voice traffic.

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

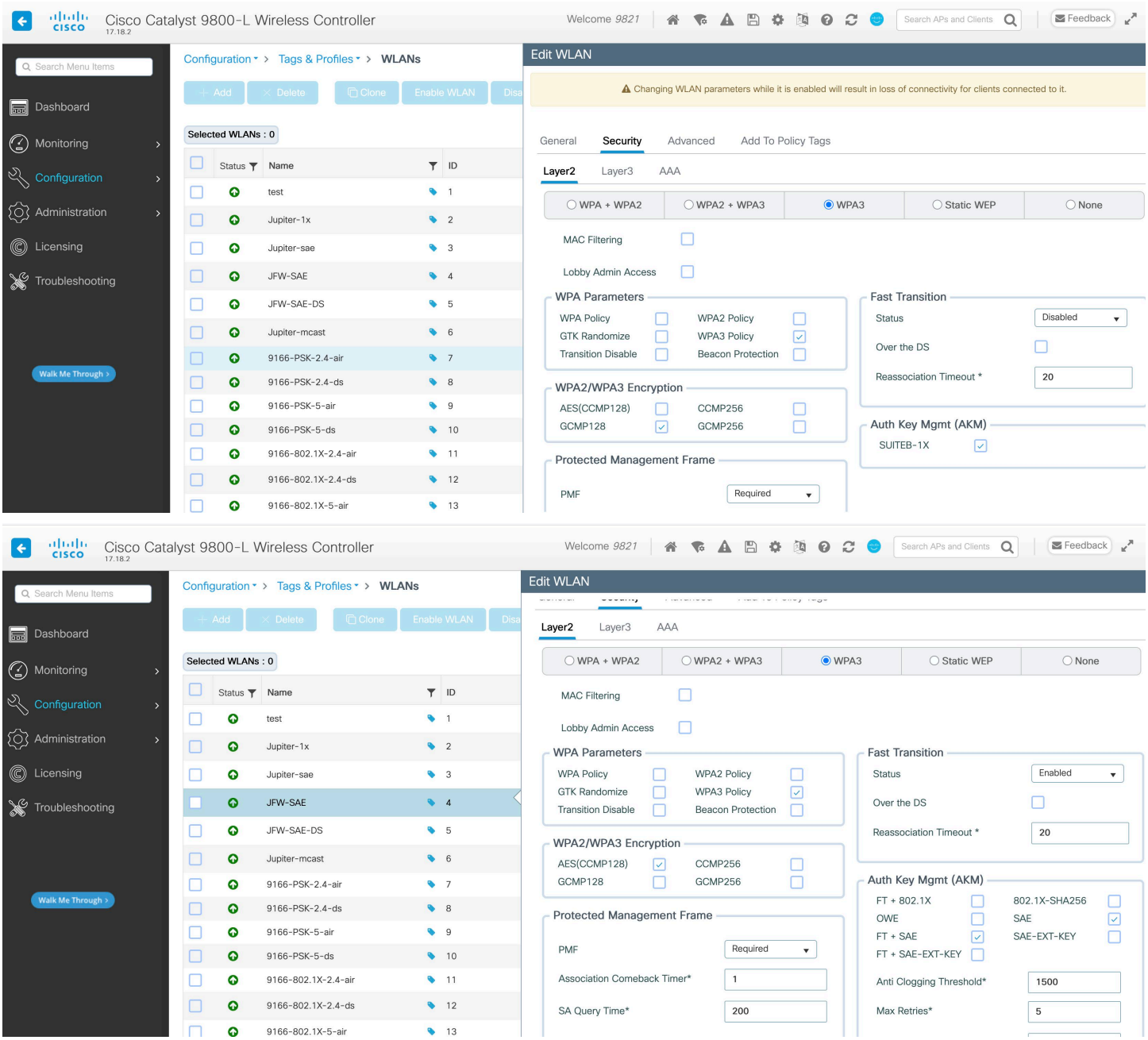


To utilize 802.11r (FT) for fast secure roaming, enable **Fast Transition**.

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

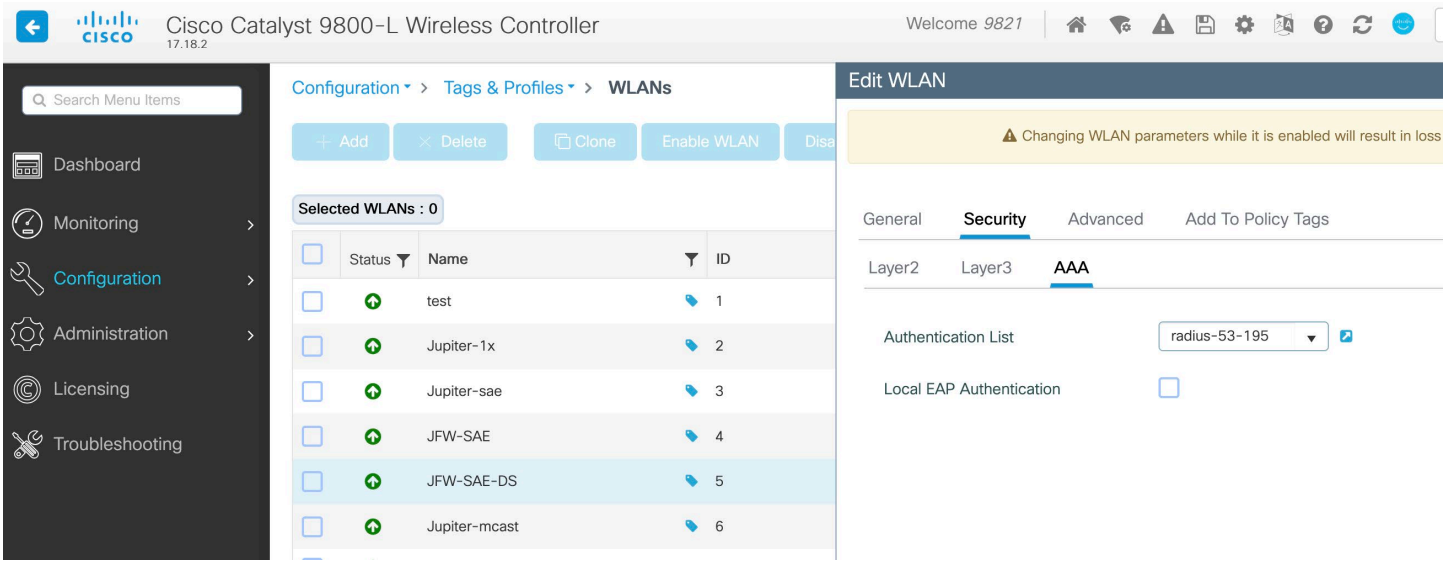
Set **Protected Management Frame** to **Optional** or **Required**.

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



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

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



Aironet IE should be **Enabled**.

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

The **WMM Policy** should be set to **Required** only if Cisco Wireless Phone 9821 or other WMM enabled phones will use this SSID.

If there are non-WMM clients existing in the WLAN, it is recommended to put those clients on another WLAN.

If non-other WMM clients must utilize the same SSID as the Cisco Wireless Phone 9821, ensure the WMM policy is set to **Allowed**.

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

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

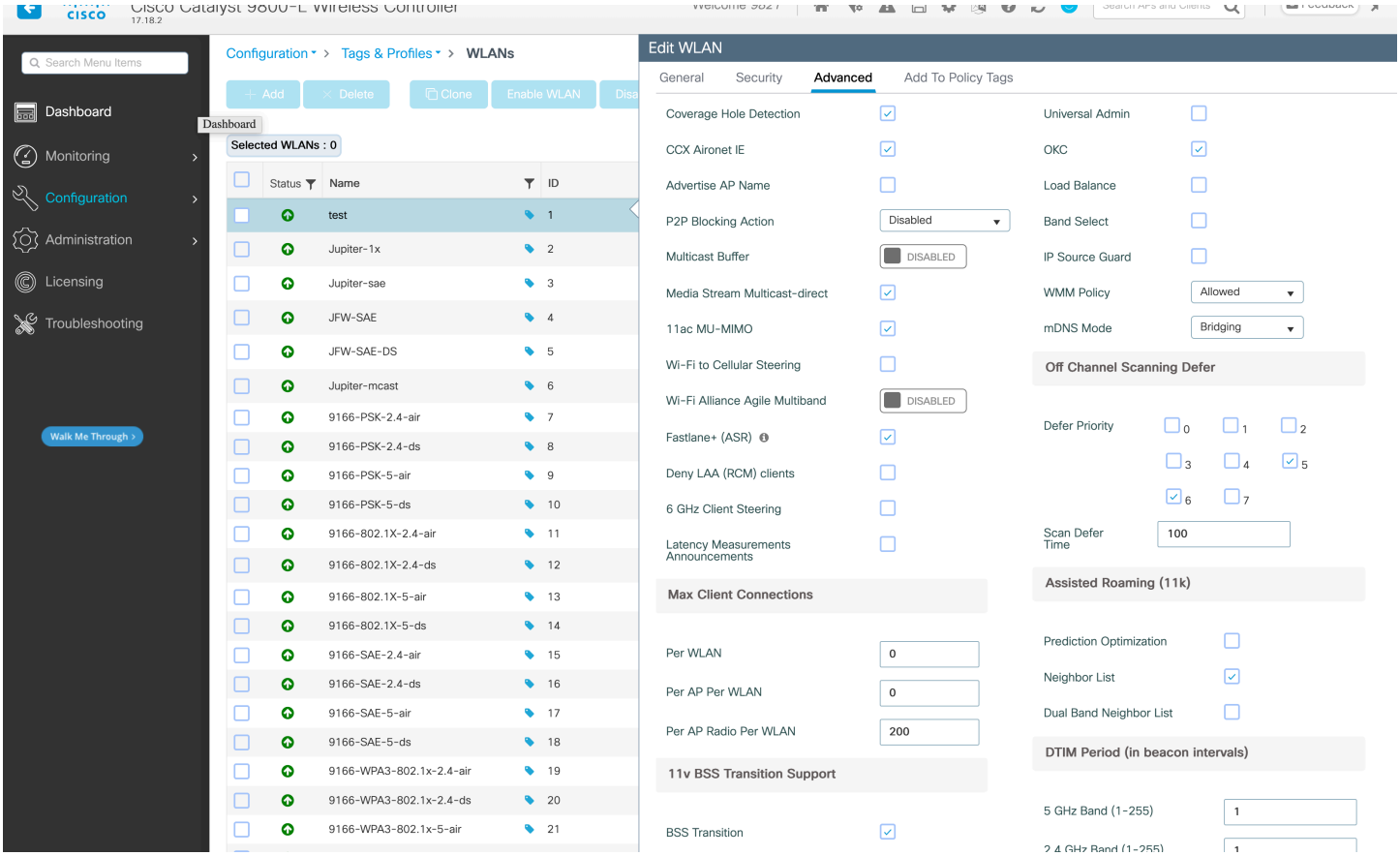
It is recommended to enabled defer priority for queues 4-6.

If using best effort applications frequently or 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.

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

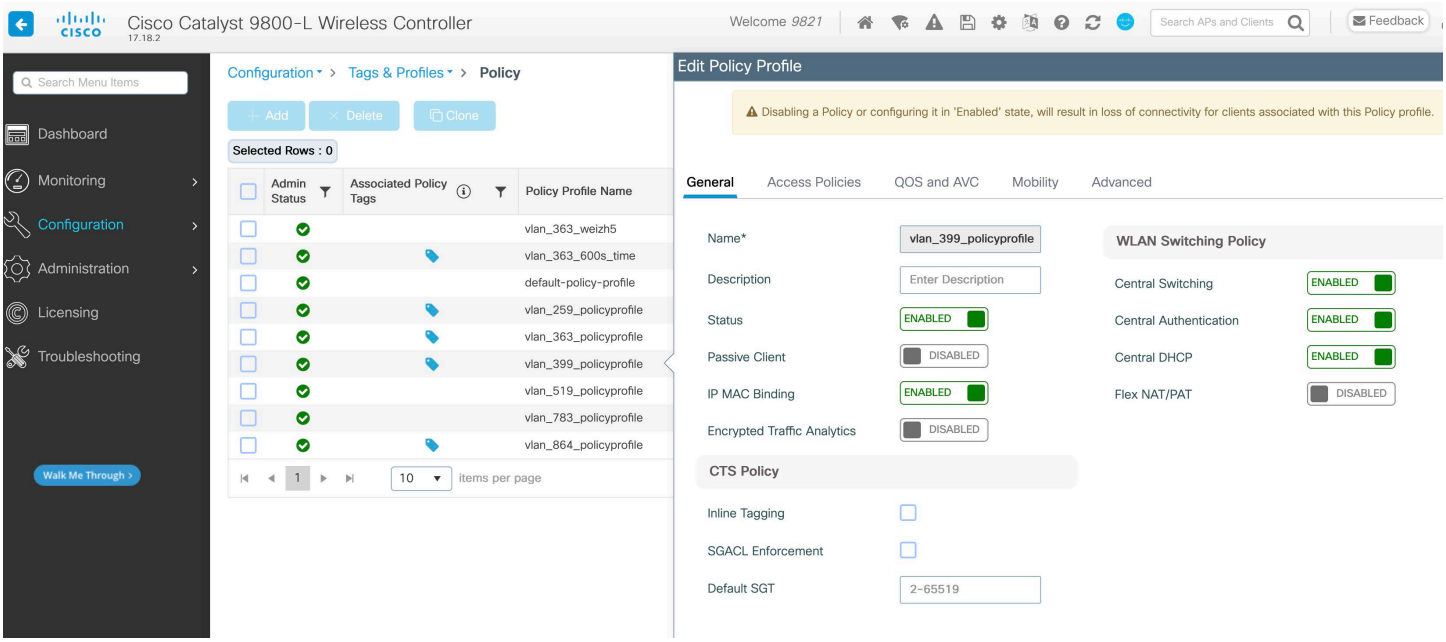
Use a **DTIM Period** of 2 with a beacon period of **100 ms** if no need to consider multicast applications.



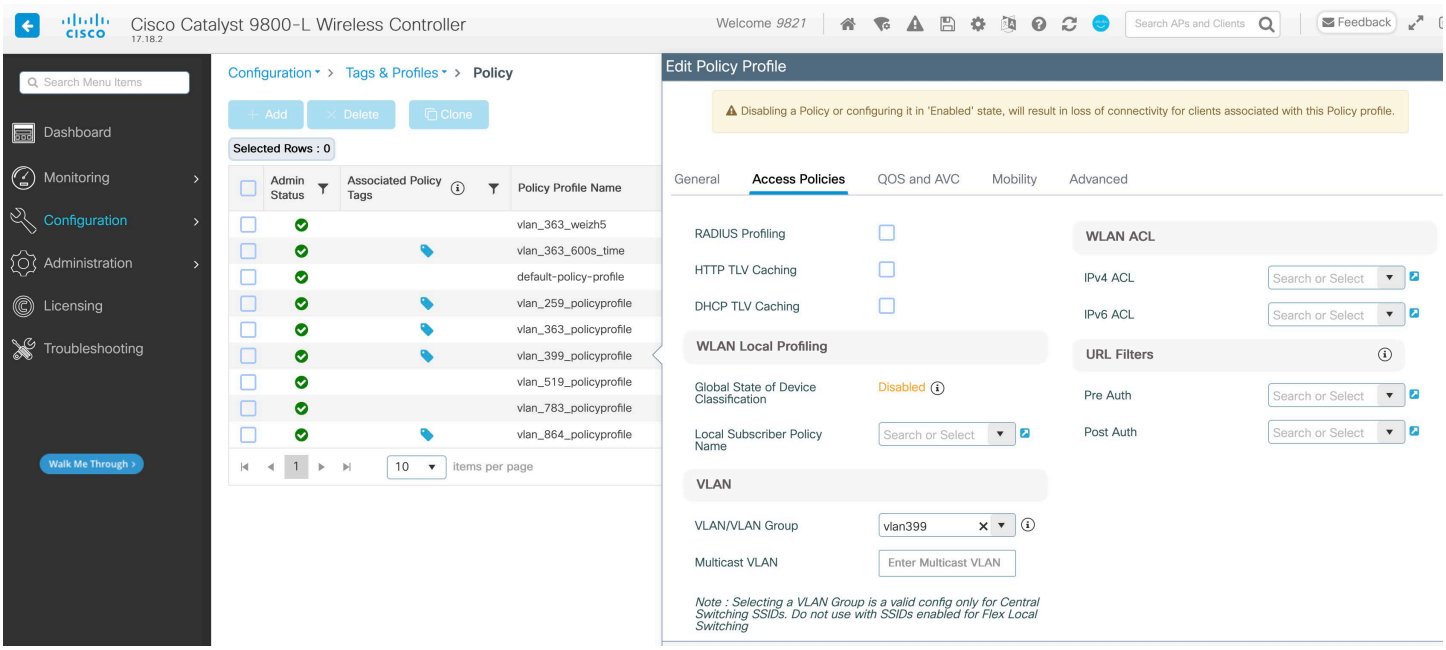
Policy Profiles

Policy Profiles define the operational and security attributes for a wireless session, including access control, Quality of Service (QoS), mobility, and advanced configuration parameters. These profiles are associated with a Policy Tag, which also maps to a WLAN Profile. When this Policy Tag is assigned to an access point, it enforces the combined configuration on the wireless network.

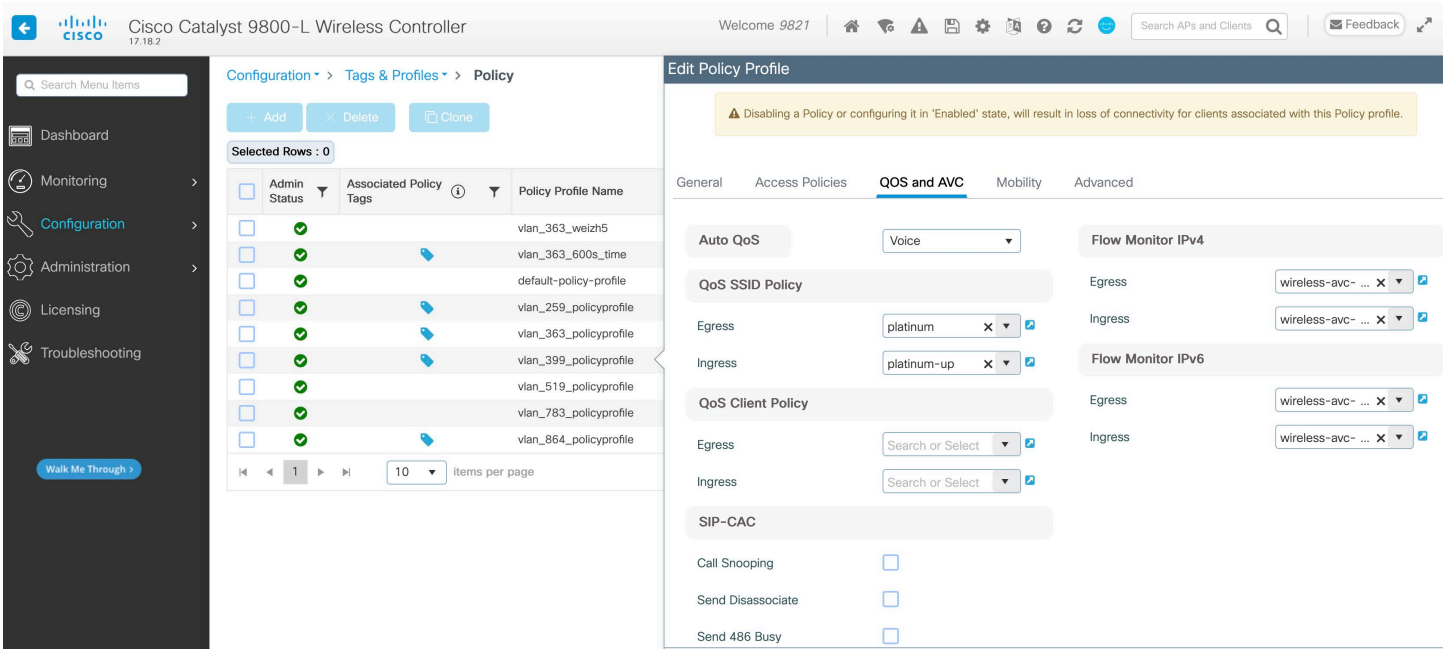
Ensure the **Status** of the policy profile is **Enabled**.



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



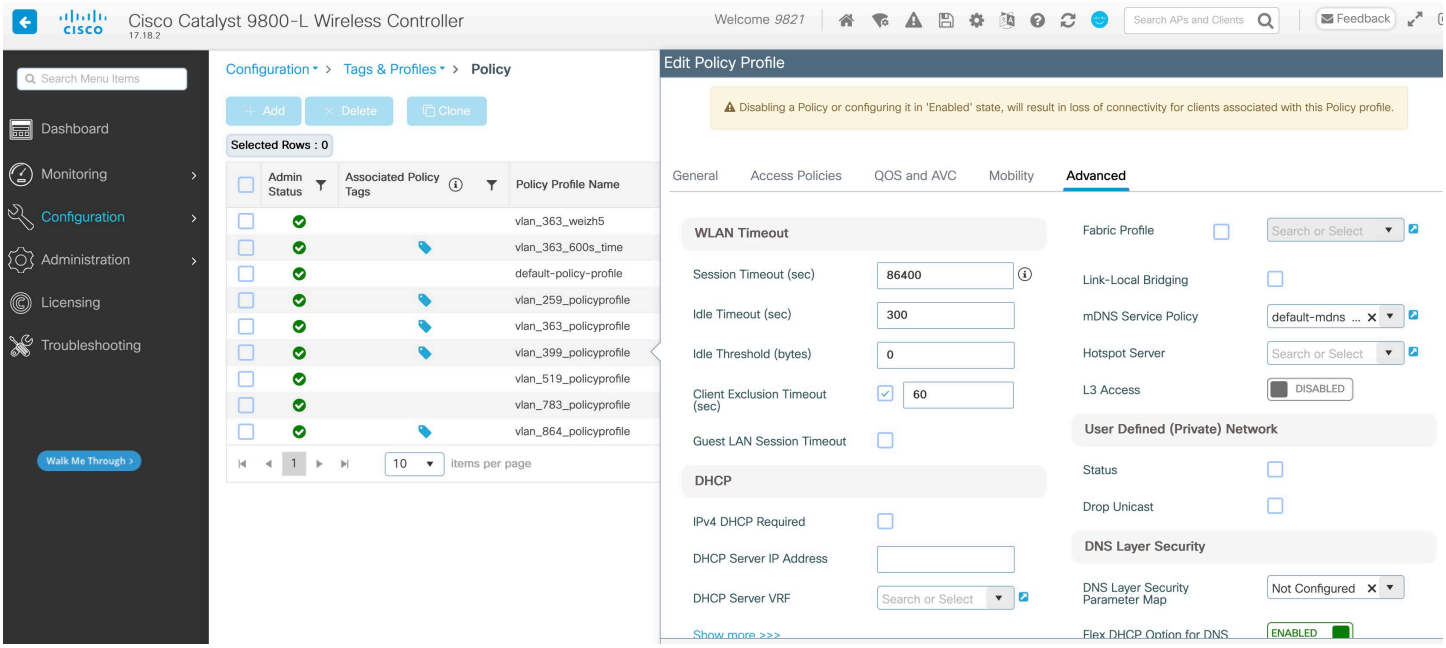
Set the QoS SSID Policy to **Platinum** for egress and **Platinum-up** for ingress.



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

Configure **Client Exclusion Timeout** as necessary.

IPv4 DHCP Required should be disabled.



RF Profiles

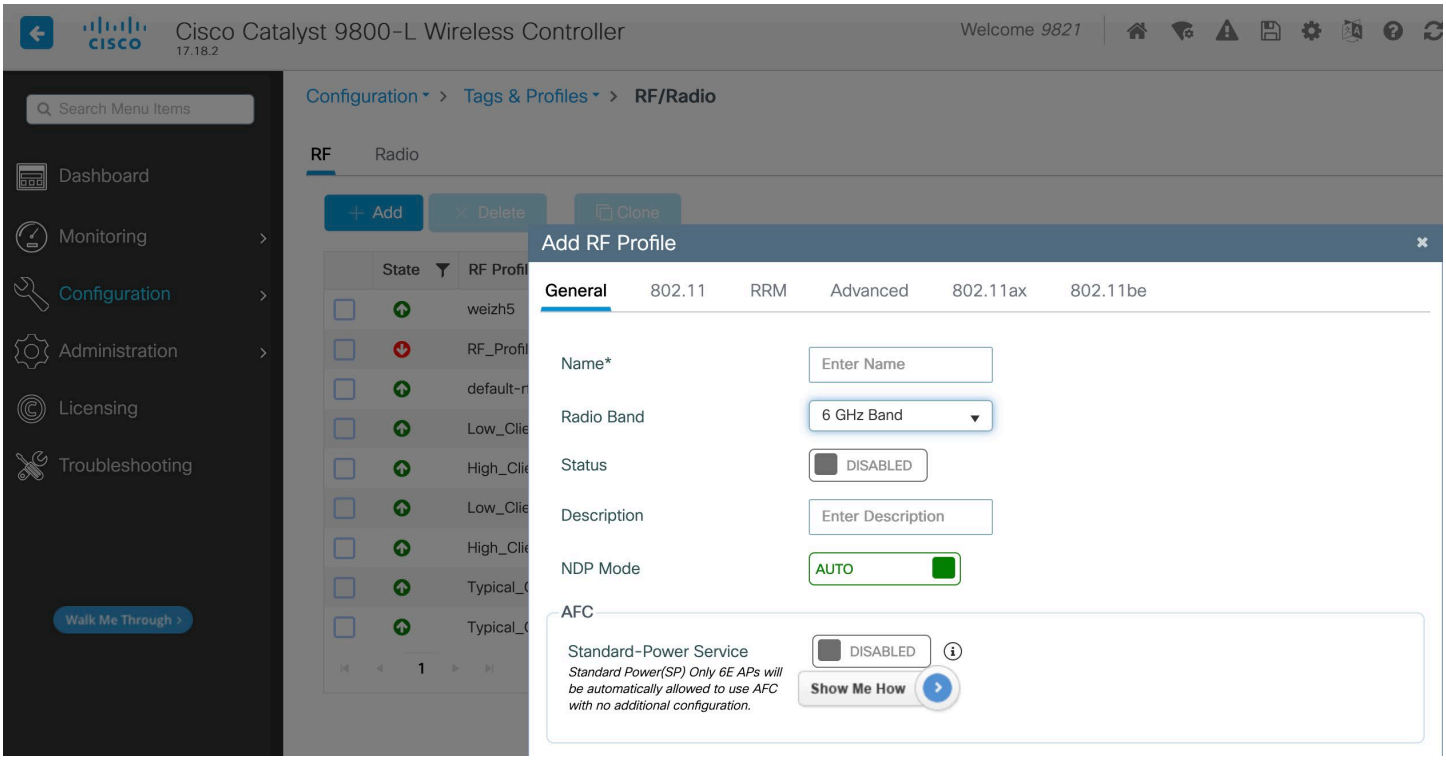
Define RF Profiles to govern frequency bands, data rates, RRM parameters, and advanced radio settings for a designated group of access points.

It is recommended to apply the SSID used by Cisco Wireless Phone 9821 to 5 GHz or 6 GHz bands.

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

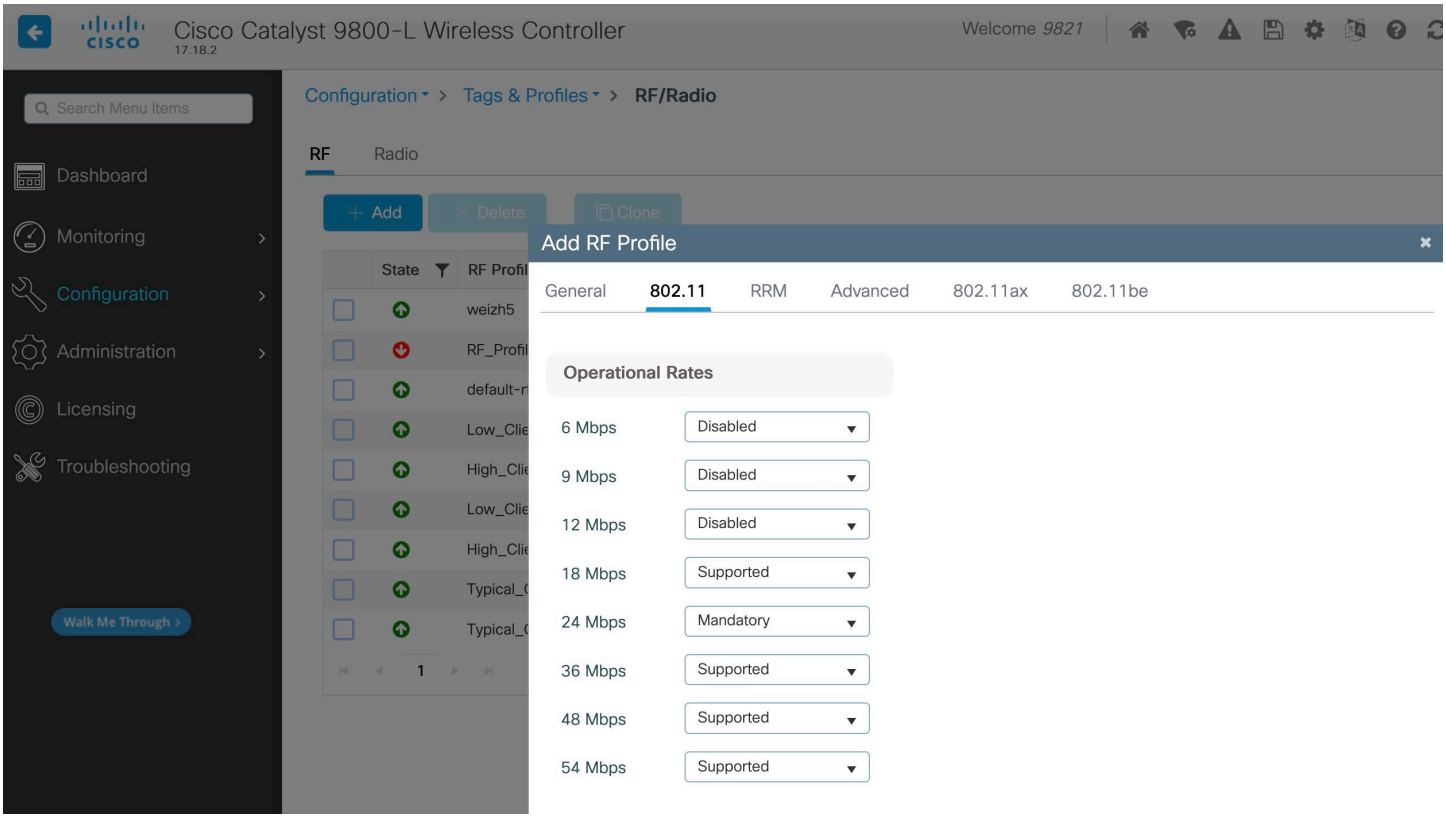
When creating an RF Profile, you must define the **Name** and **Radio Band**.

Select **6 GHz Band**, **5 GHz Band** or **2.4 GHz Band** for the **Radio Band**.

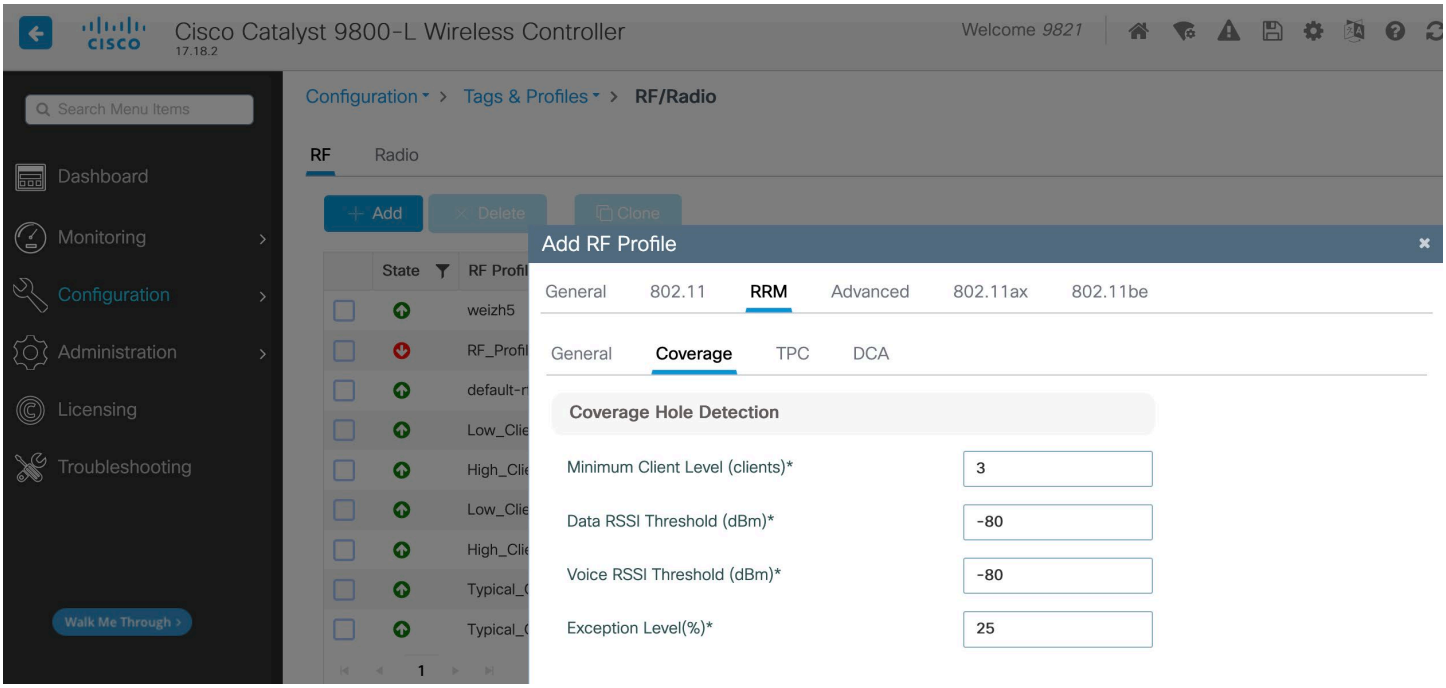


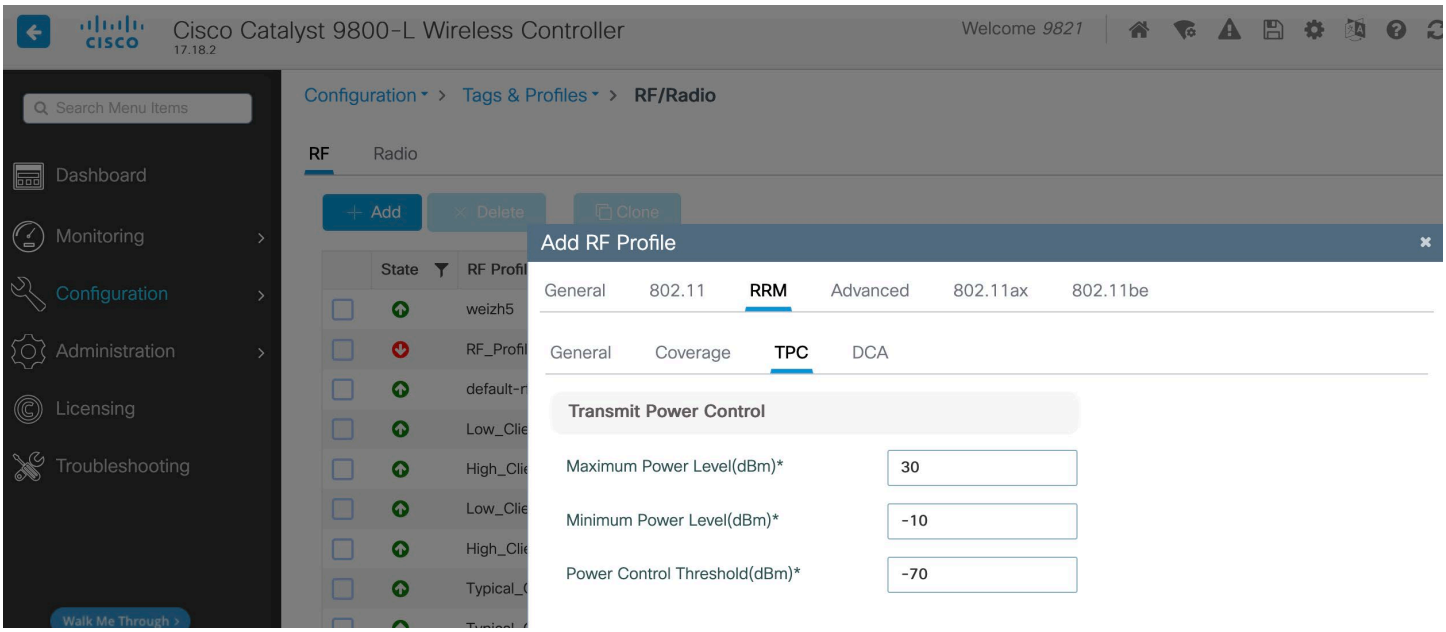
On the **802.11** tab, configure the data rates as necessary.

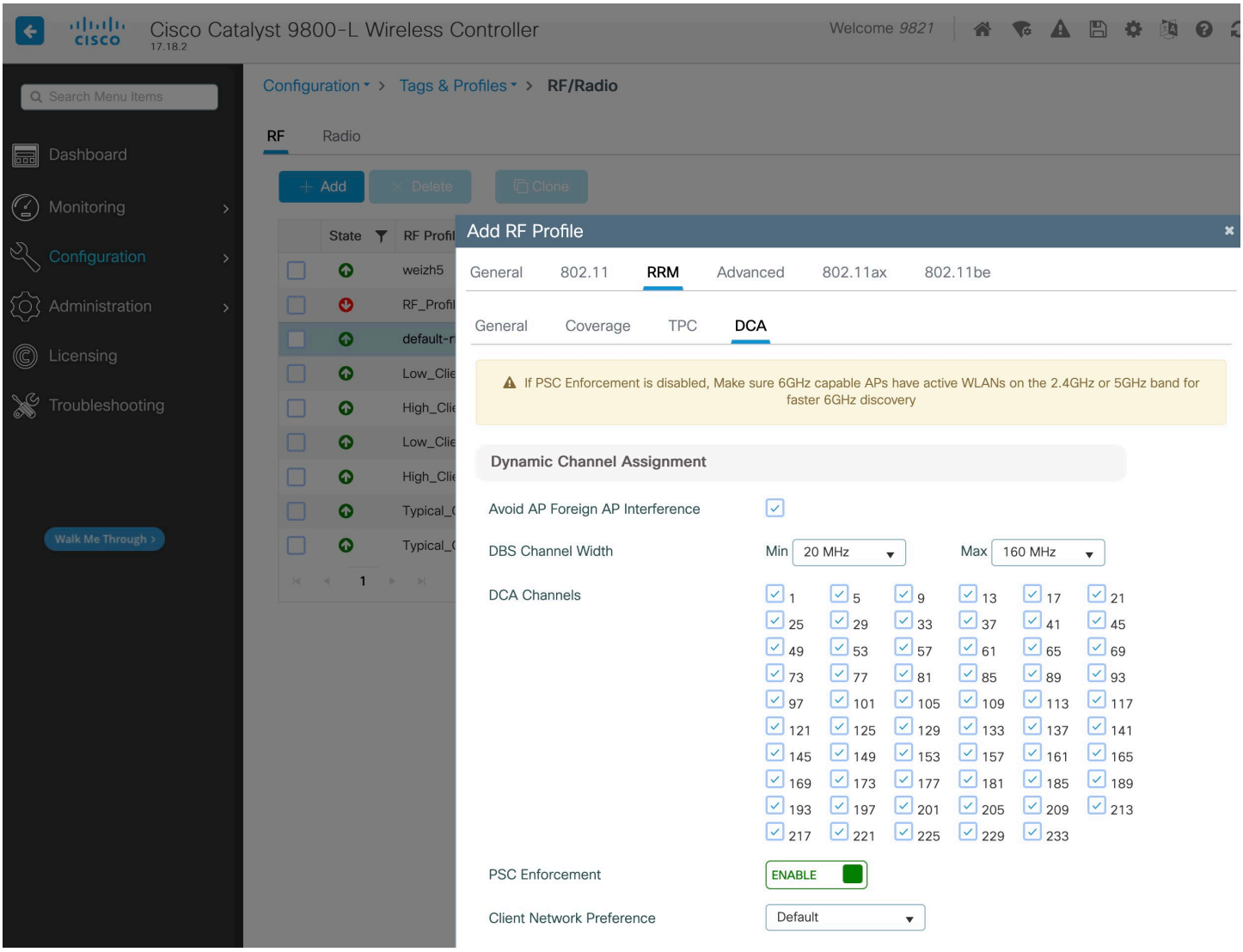
It is recommended to enable 24 Mbps as **Mandatory** and 18, 36 Mbps and higher as **Supported**. However, some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.



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

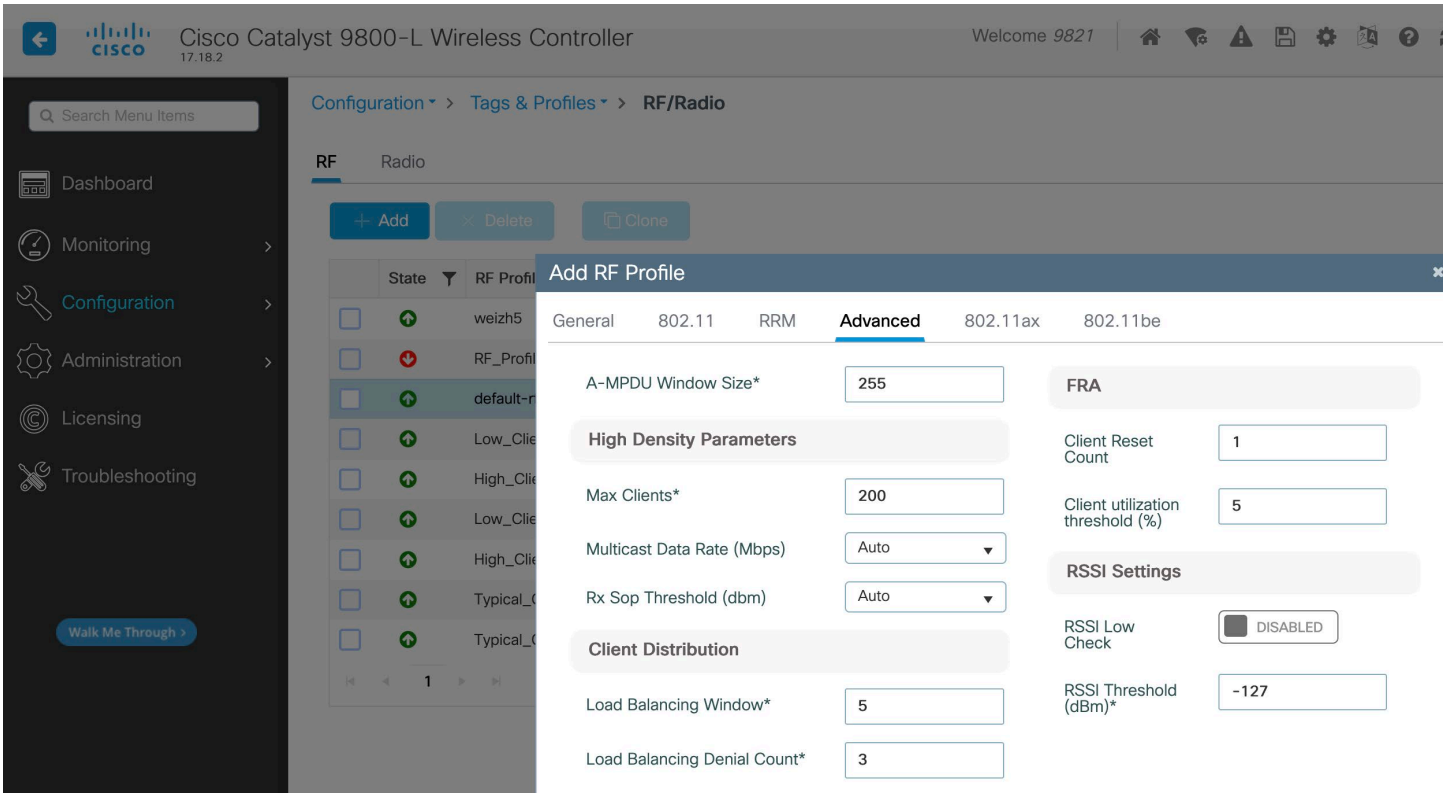



Cisco Catalyst 9800-L Wireless Controller
17.18.2
Welcome 9821
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Walk Me Through
Configuration > Tags & Profiles > RF/Radio
RF
Radio
Add
Delete
Clone
State
RF Profil
weizh5
RF_Profil
default-r
Low_Clie
High_Clie
Low_Clie
High_Clie
Typical_
Add RF Profile
General
802.11
RRM
Advanced
802.11ax
802.11be
General
Coverage
TPC
DCA
Transmit Power Control
Maximum Power Level(dBm)*
30
Minimum Power Level(dBm)*
-10
Power Control Threshold(dBm)*
-70



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

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



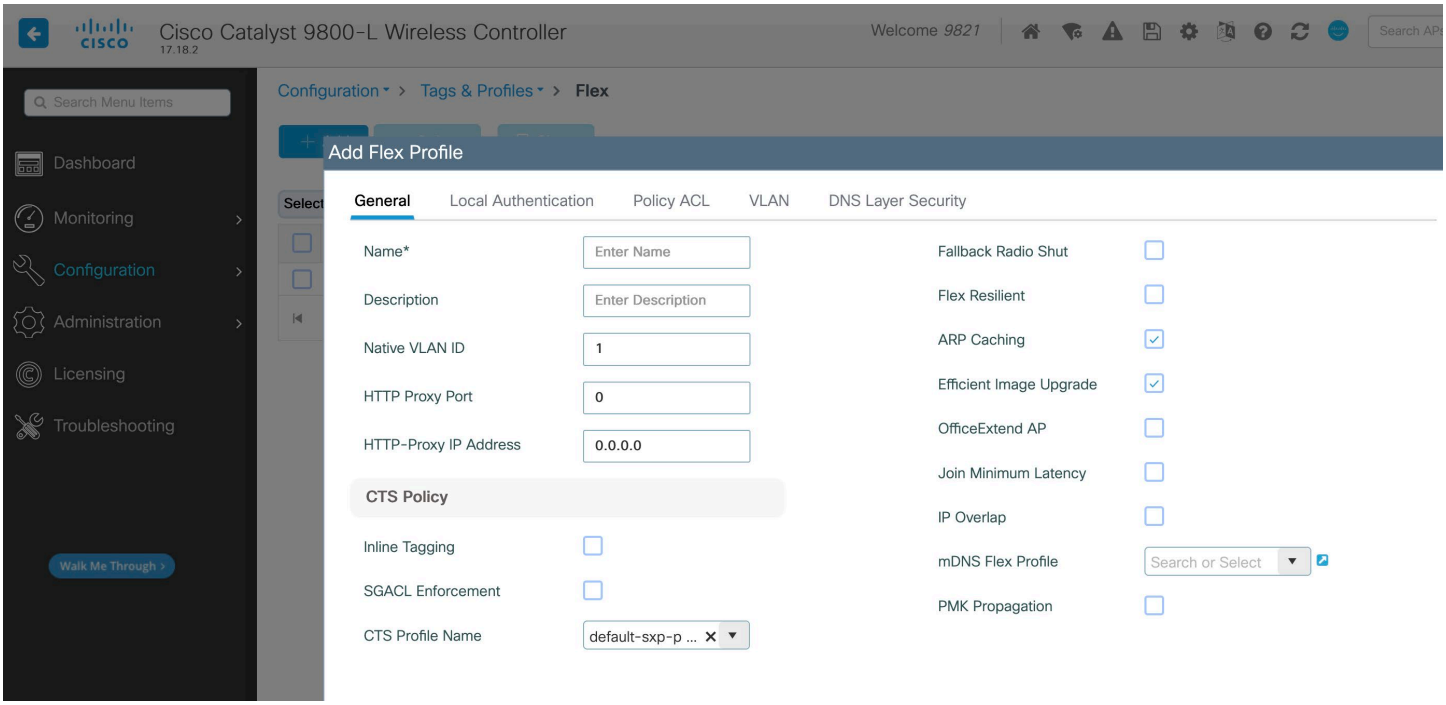
Flex Profiles

Flex Profiles define the operational parameters for access points configured in FlexConnect mode. These profiles are mapped to a Site Tag, which is subsequently assigned to an access point to enforce the defined configuration.

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

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

Enable **Local Authentication** as necessary.



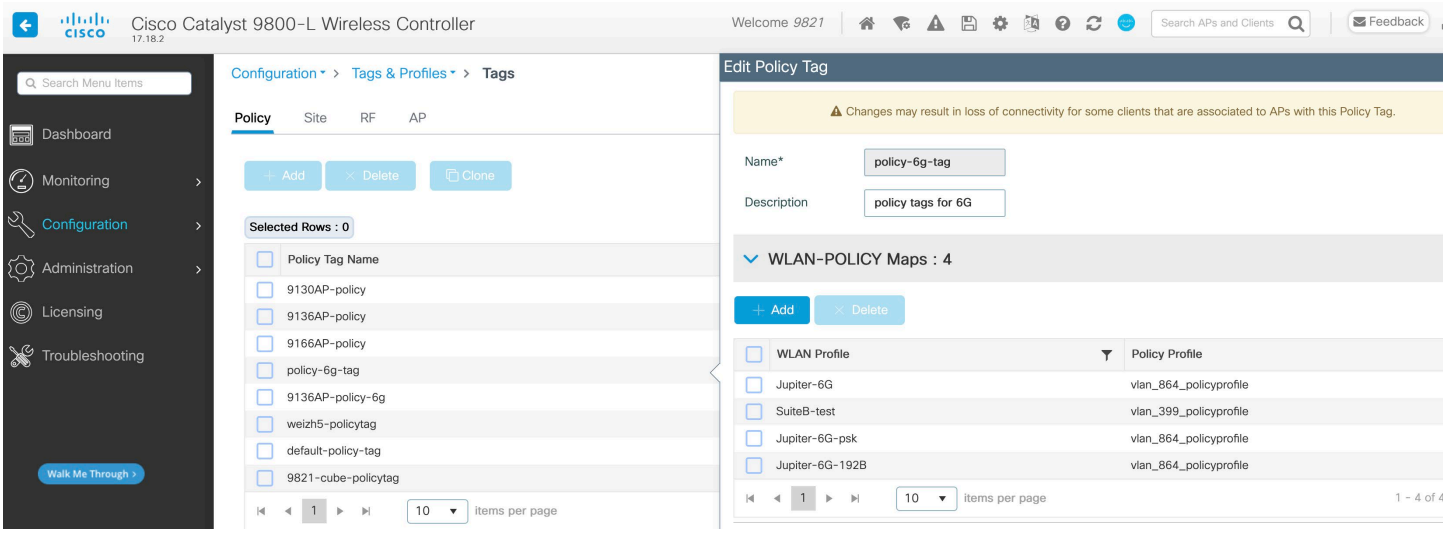
Tags

Policy Tag

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

When assigned to an access point, a Policy Tag dictates which WLANs are broadcast, the associated VLAN or interface mapping, and the specific Quality of Service (QoS) and security policies applied to the wireless traffic.

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



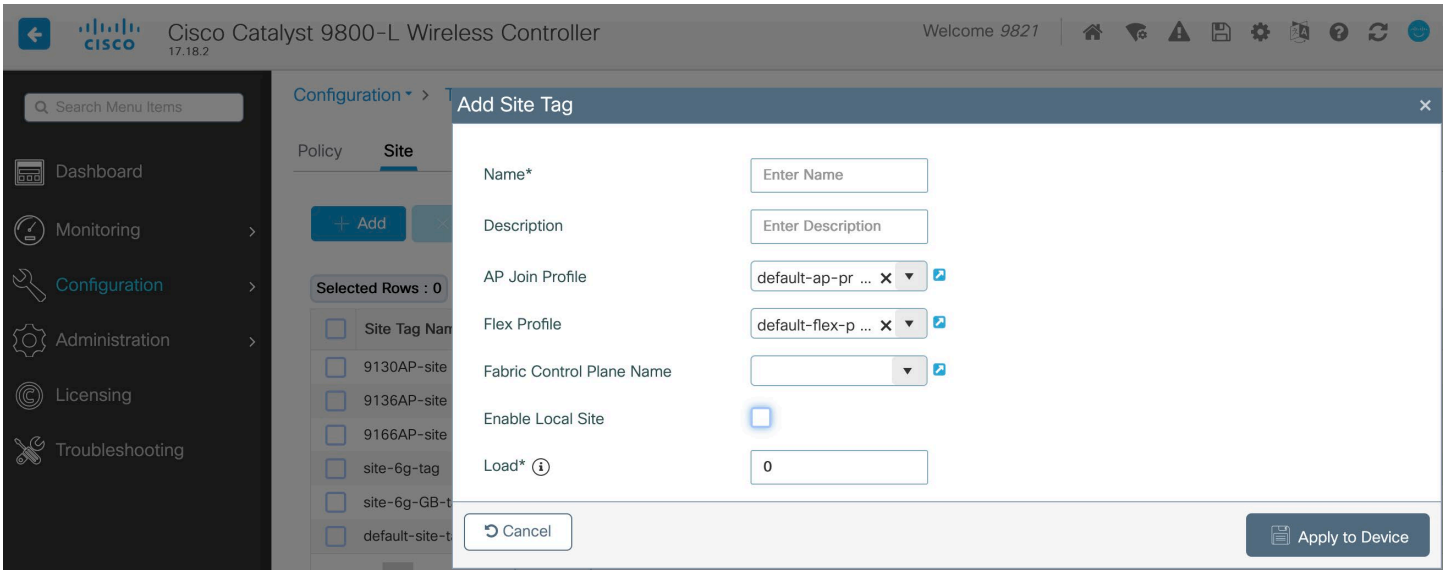
Site Tag

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

When assigned to an access point, Site Tags specify the AP Join Profile and Flex Profile parameters to be used.

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

When creating a Site Tag to include a Flex Profile, leave **Enable Local Site** unselected, and then select the necessary **Flex Profile**.

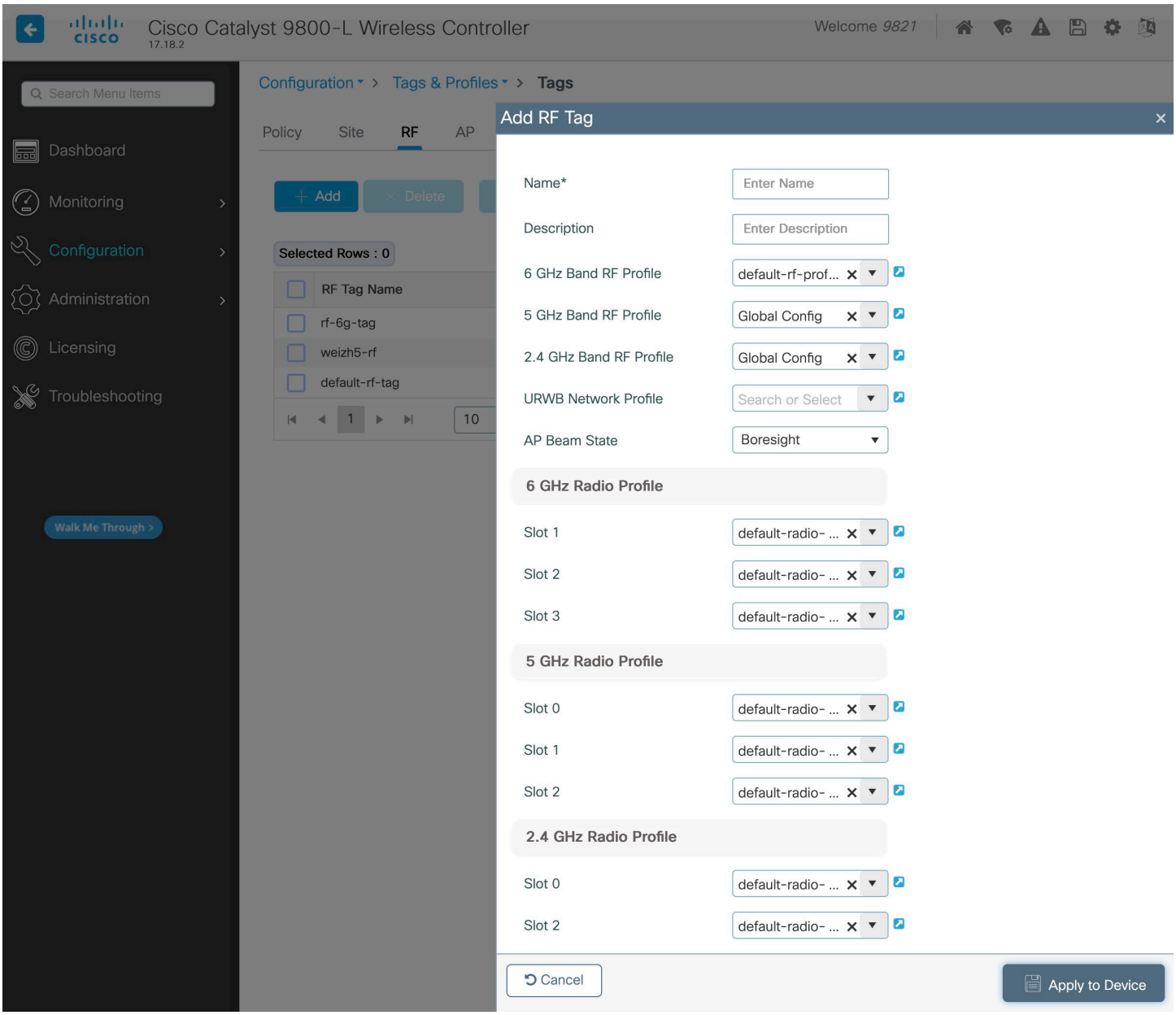


RF Tag

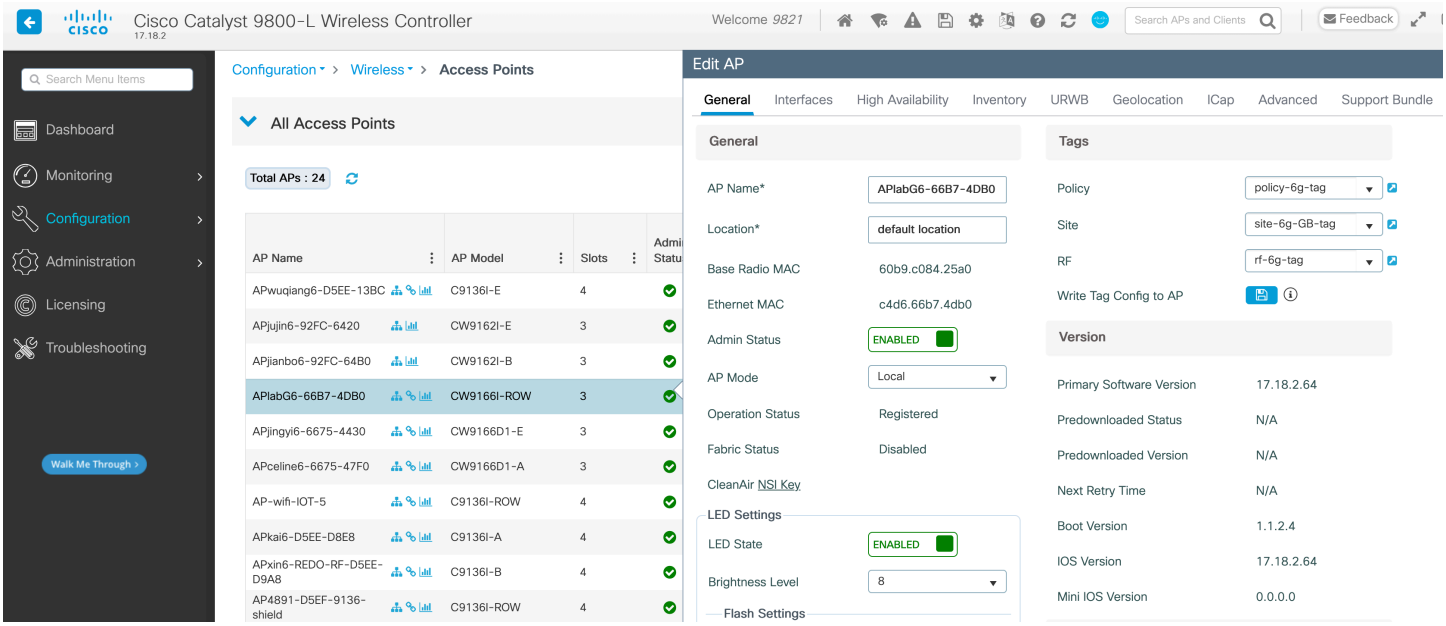
RF Tags define which RF Profiles should be used for 2.4 GHz, 5 GHz and 6 GHz.

When assigned to an access point, RF Tags specify the RF Profile parameters to be used.

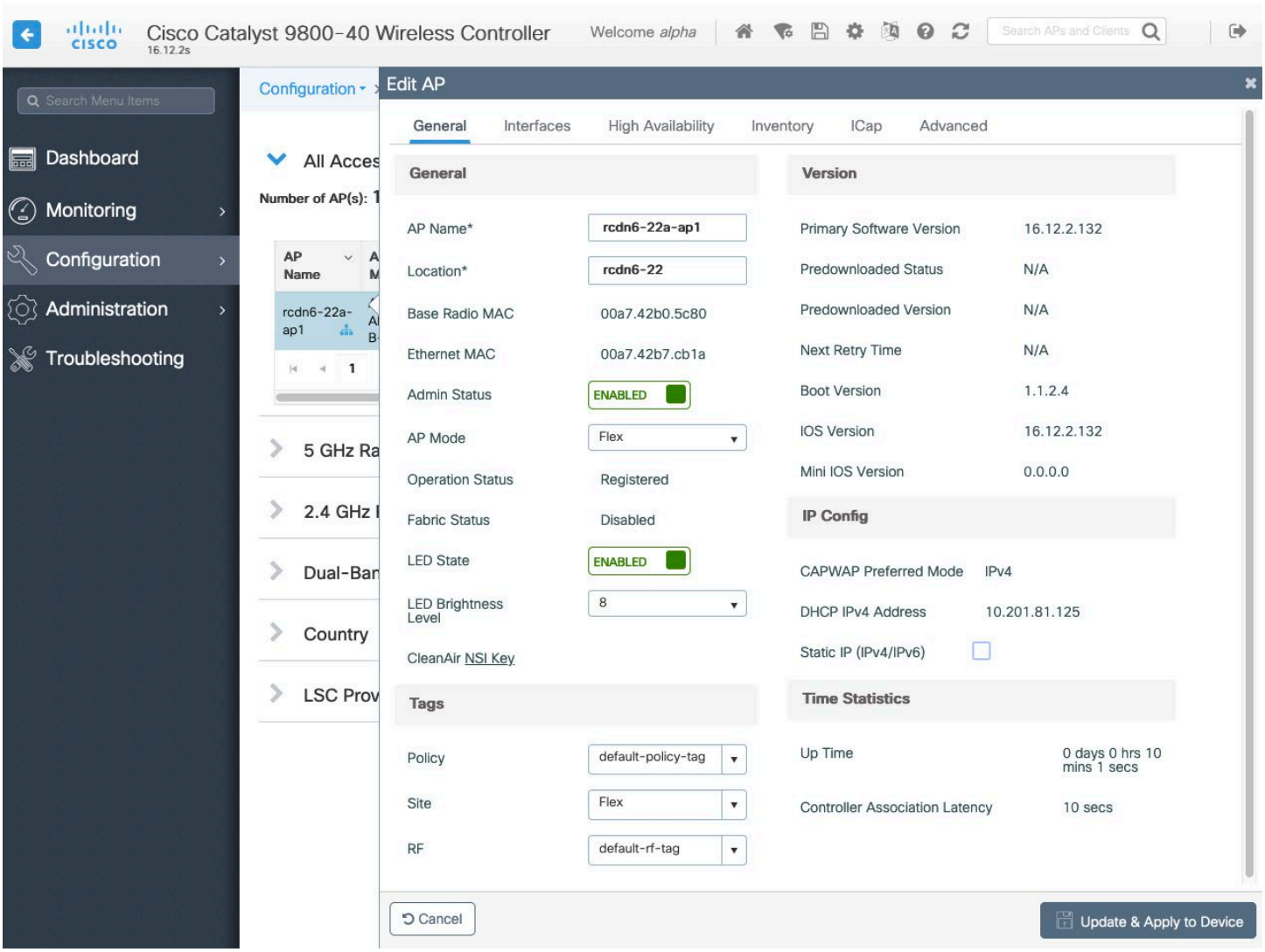
When creating a RF Tag, select the **6 GHz Band RF Profile**, **5 GHz Band RF Profile**, and **2.4 GHz Band RF Profile** to be used.



Once defined, apply the RF Tags to an access point.

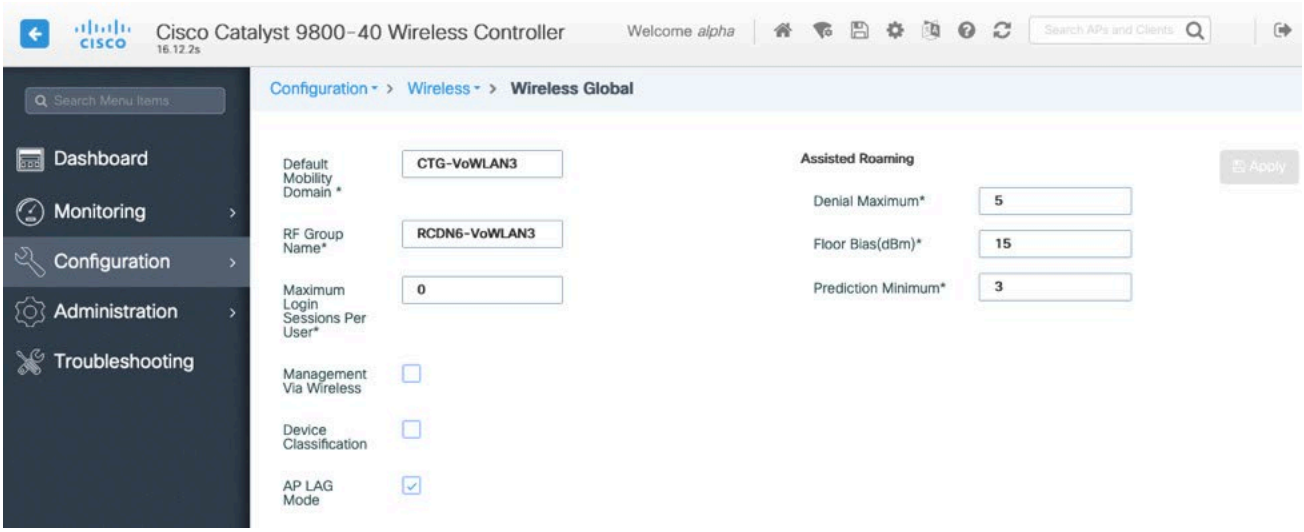


If an applied Site Tag includes a configured Flex Profile, the **AP Mode** will be changed to **Flex** automatically.



Controller Settings

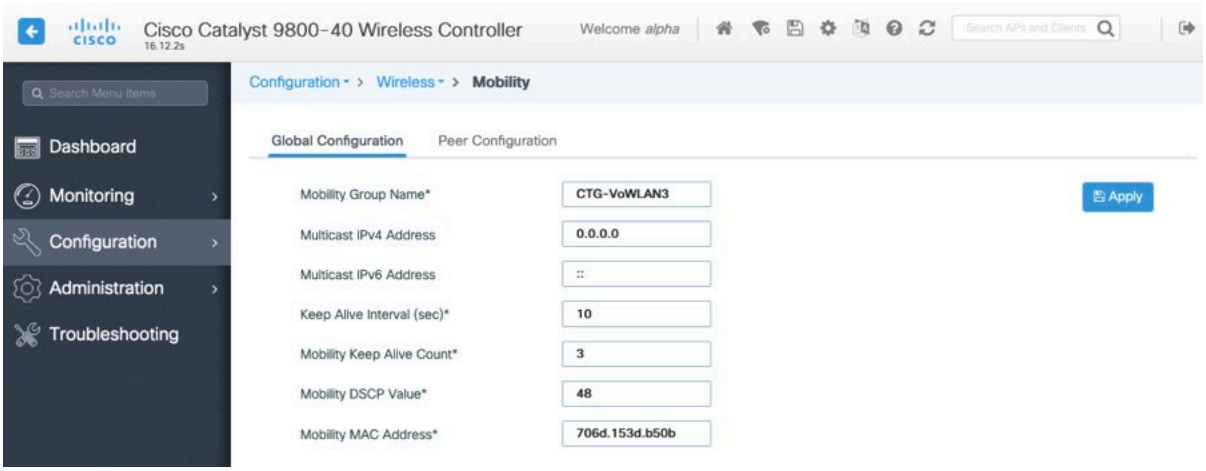
Ensure the **Default Mobility Domain** is configured correctly.

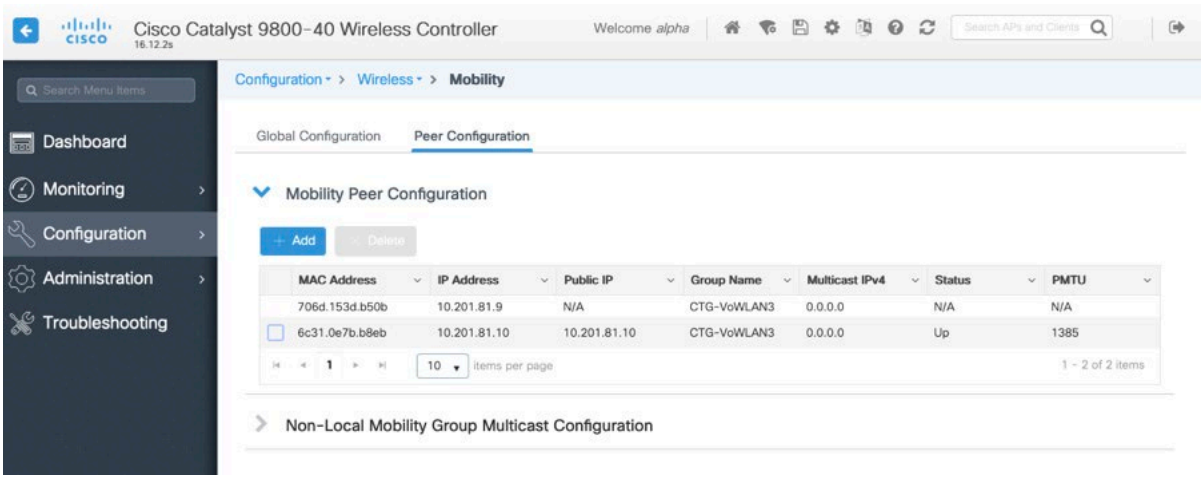


Mobility Settings

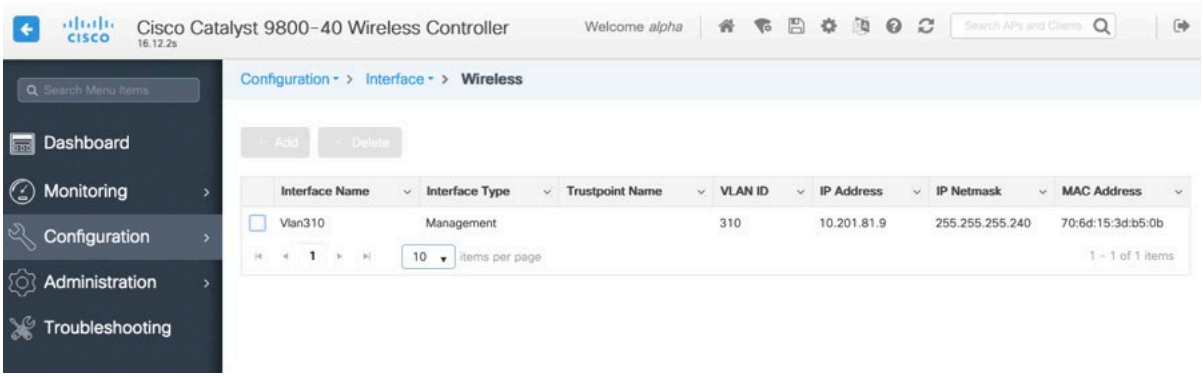
When multiple Cisco Wireless LAN Controllers are in the same mobility group, the IP address and MAC address of each Cisco Wireless LAN Controller should be added to the Mobility Peer configuration.

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





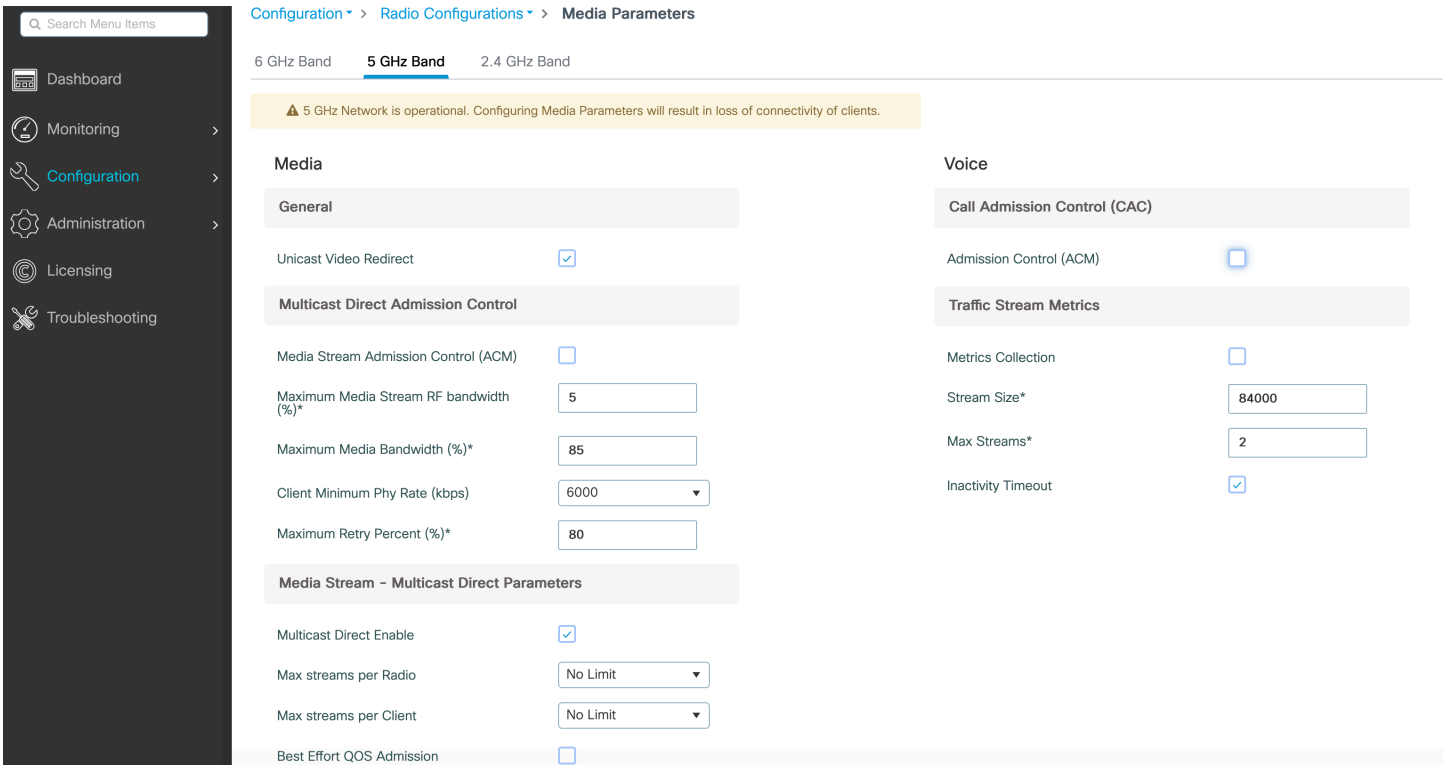
Ensure the **Mobility MAC Address** matches the MAC address of the wireless management interface.

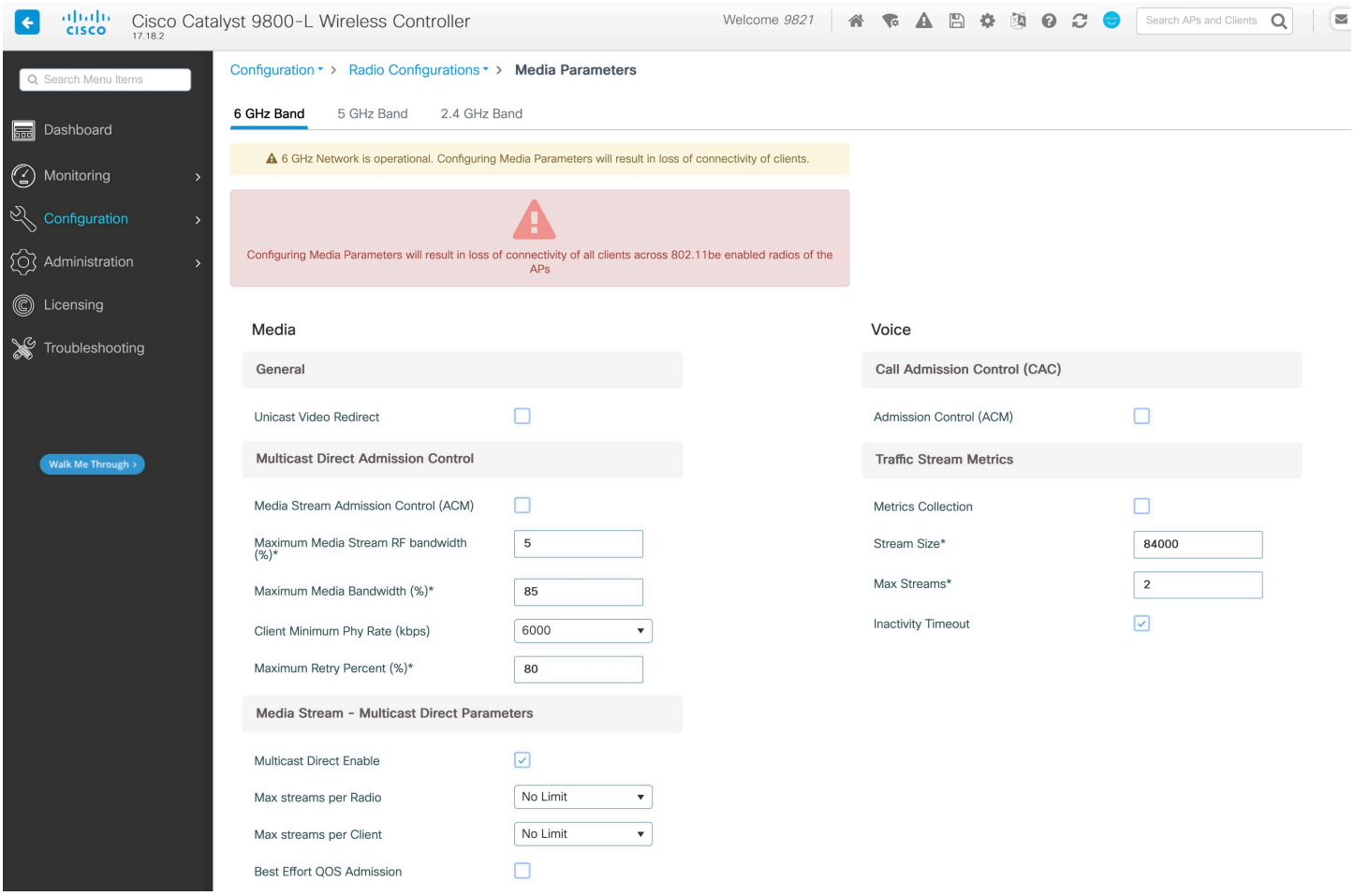


Call Admission Control (CAC)

Disable CAC because Cisco Wireless Phone doesn't support this setting.

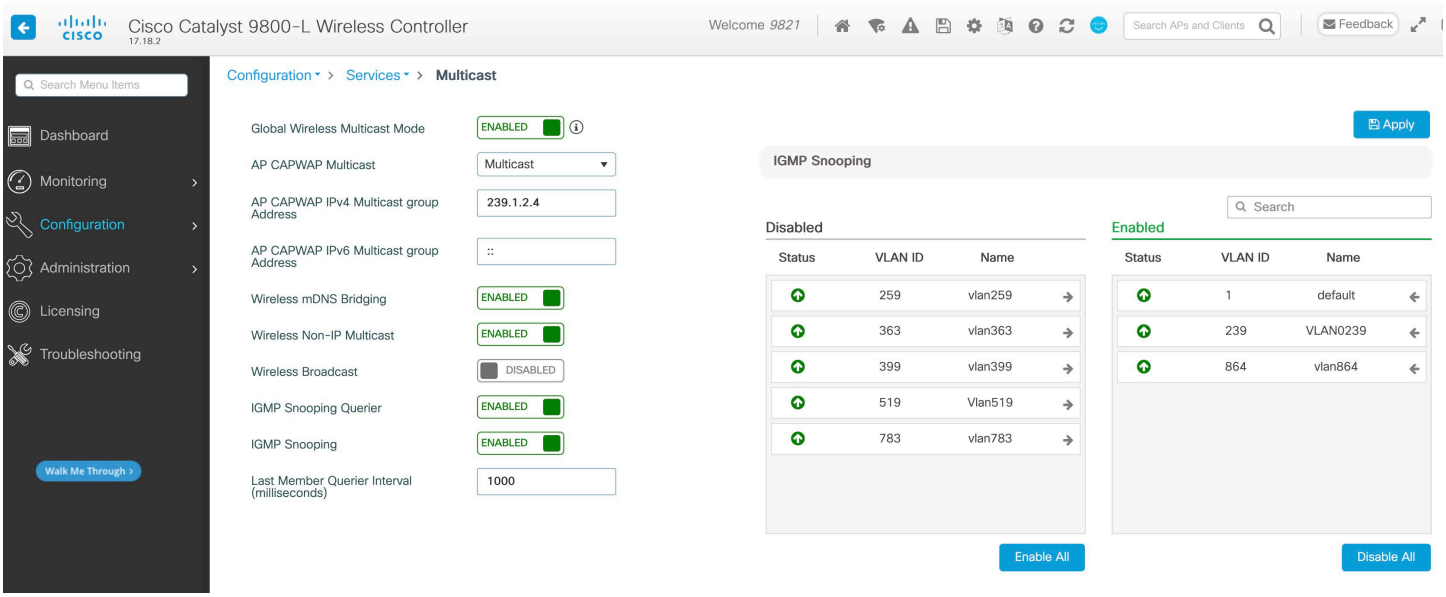
Set **Multicast Direct Enable** to **Enabled**.



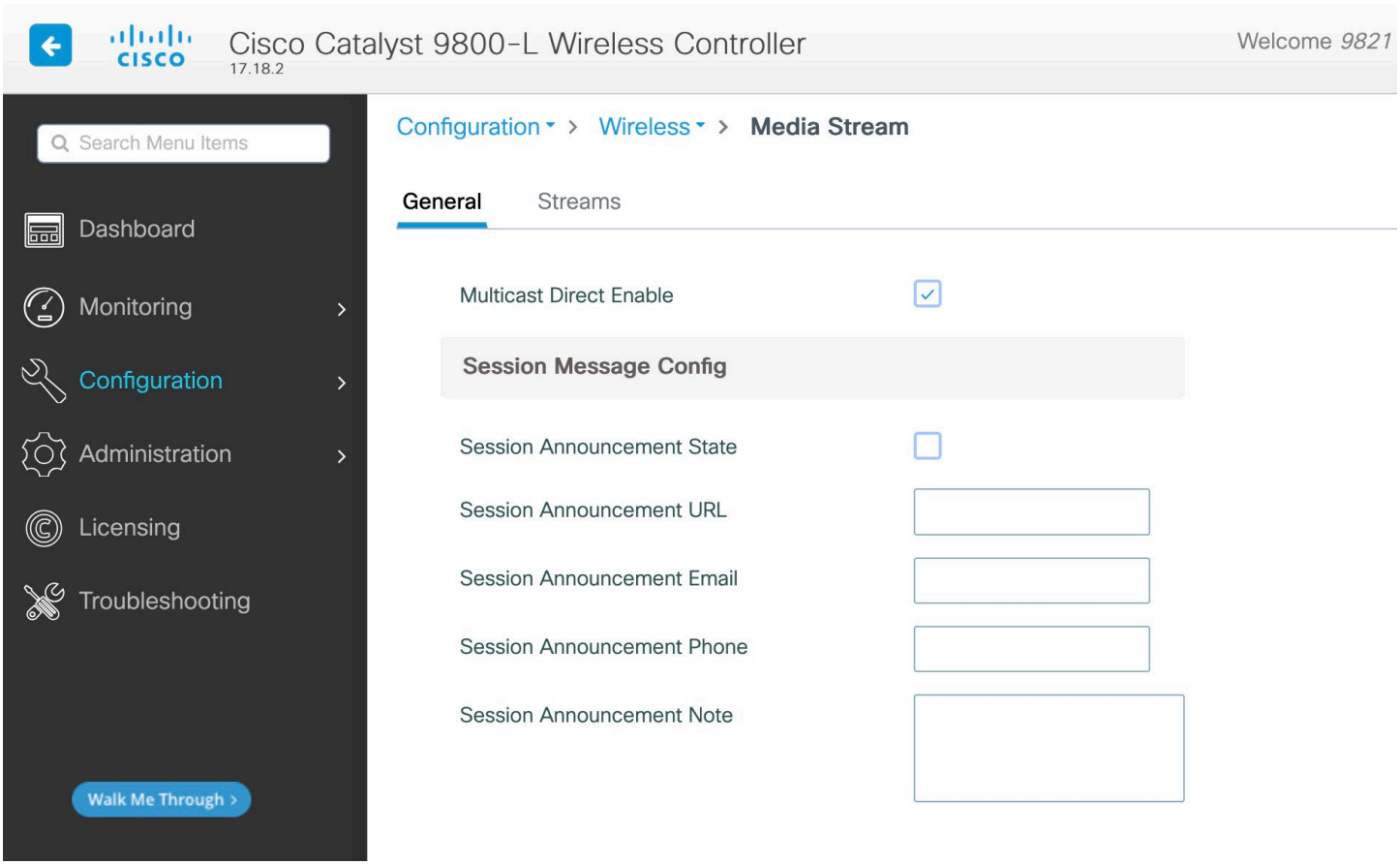


Multicast

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



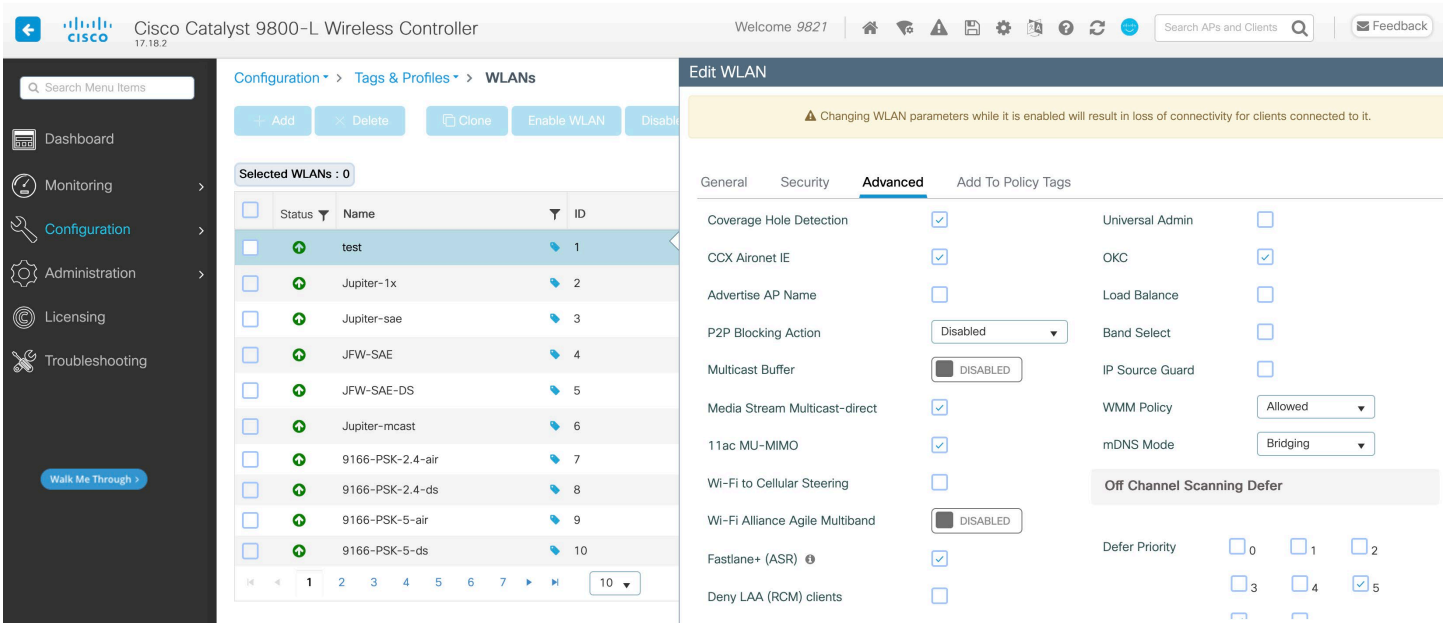
In the Media Stream settings, **Multicast Direct Enable** should be **Enabled**.



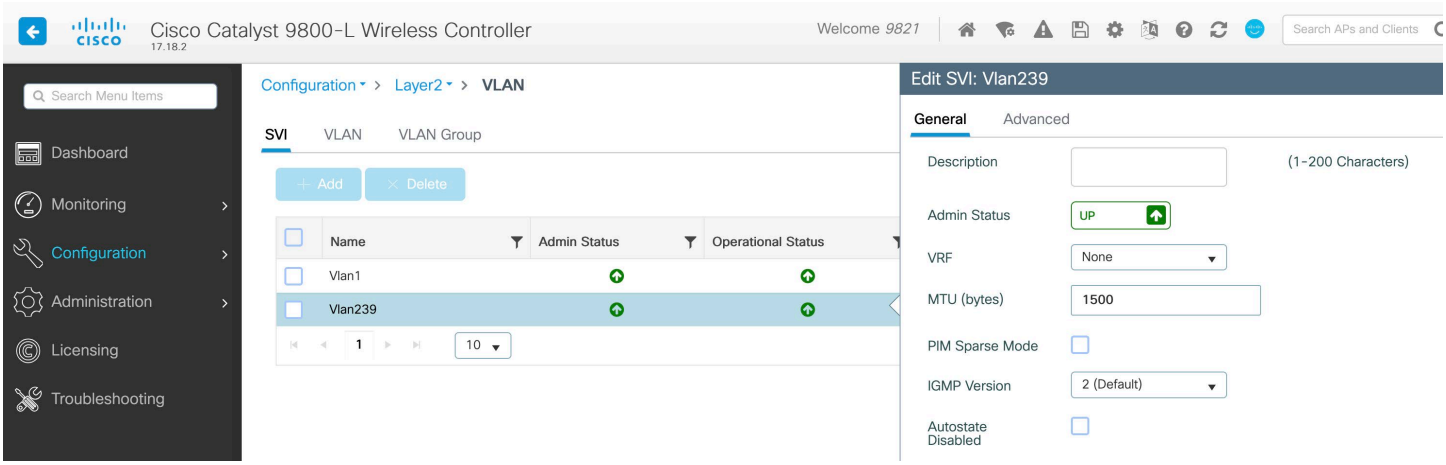
Configure the media streams as necessary.

Once saved, then the media stream will be displayed.

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



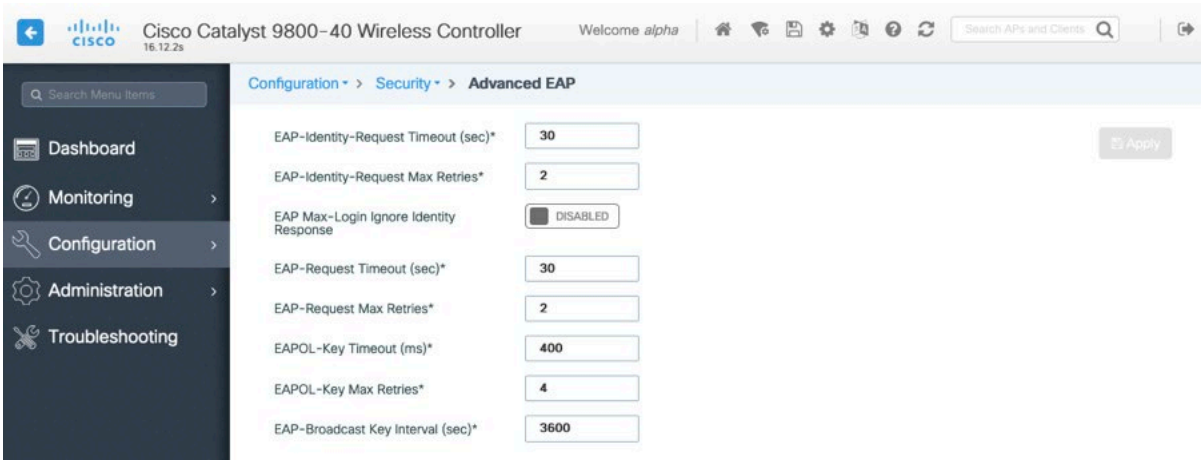
Note that Cisco Wireless Phone 9821 supports **IGMPv2 only**.



Advanced Settings

Advanced EAP Settings

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



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

For deployments where EAP failures occur frequently, the **EAP-Request Timeout** should be reduced to less than 30 seconds.

When utilizing PSK, it is recommended to set the **EAPOL-Key Timeout** to 400 milliseconds (the default is 1000 milliseconds) and then set **EAPOL-Key Max Retrie**s to 4 (the default is 2).

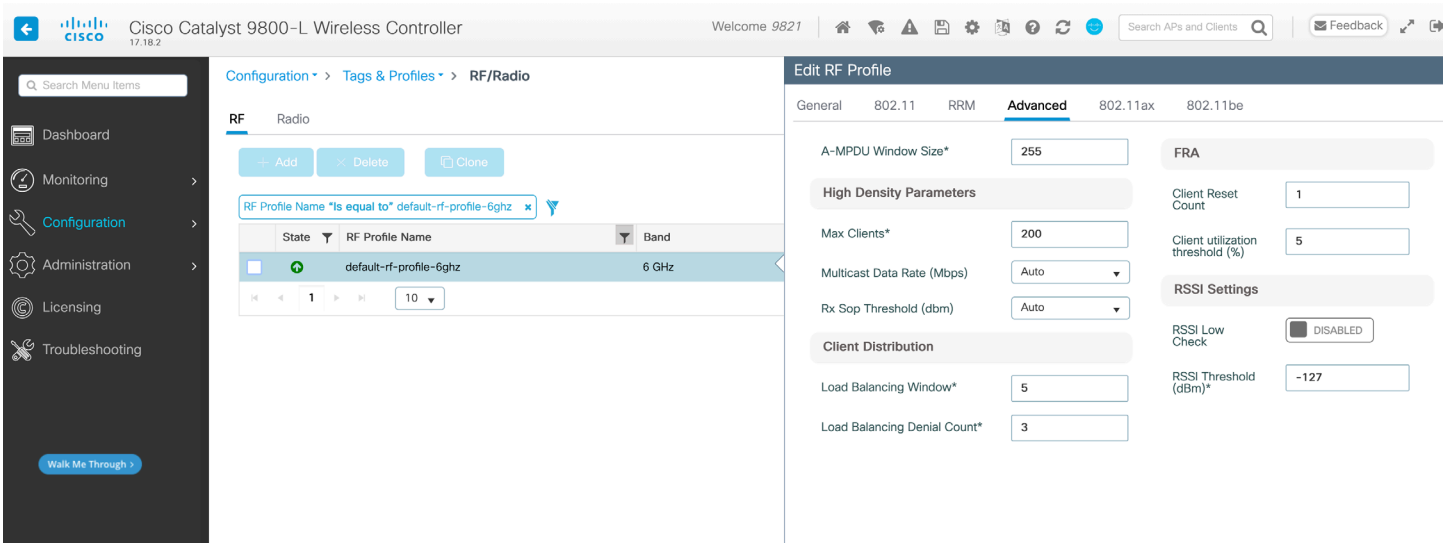
When utilizing 802.1x, though the default parameters—an **EAPOL-Key Timeout** of 1000 ms and 2 **EAPOL-Key Max Retries**—are generally sufficient, it is recommended to optimize these values to a 400 ms timeout and 4 retries for the Cisco Wireless Phone 9821.

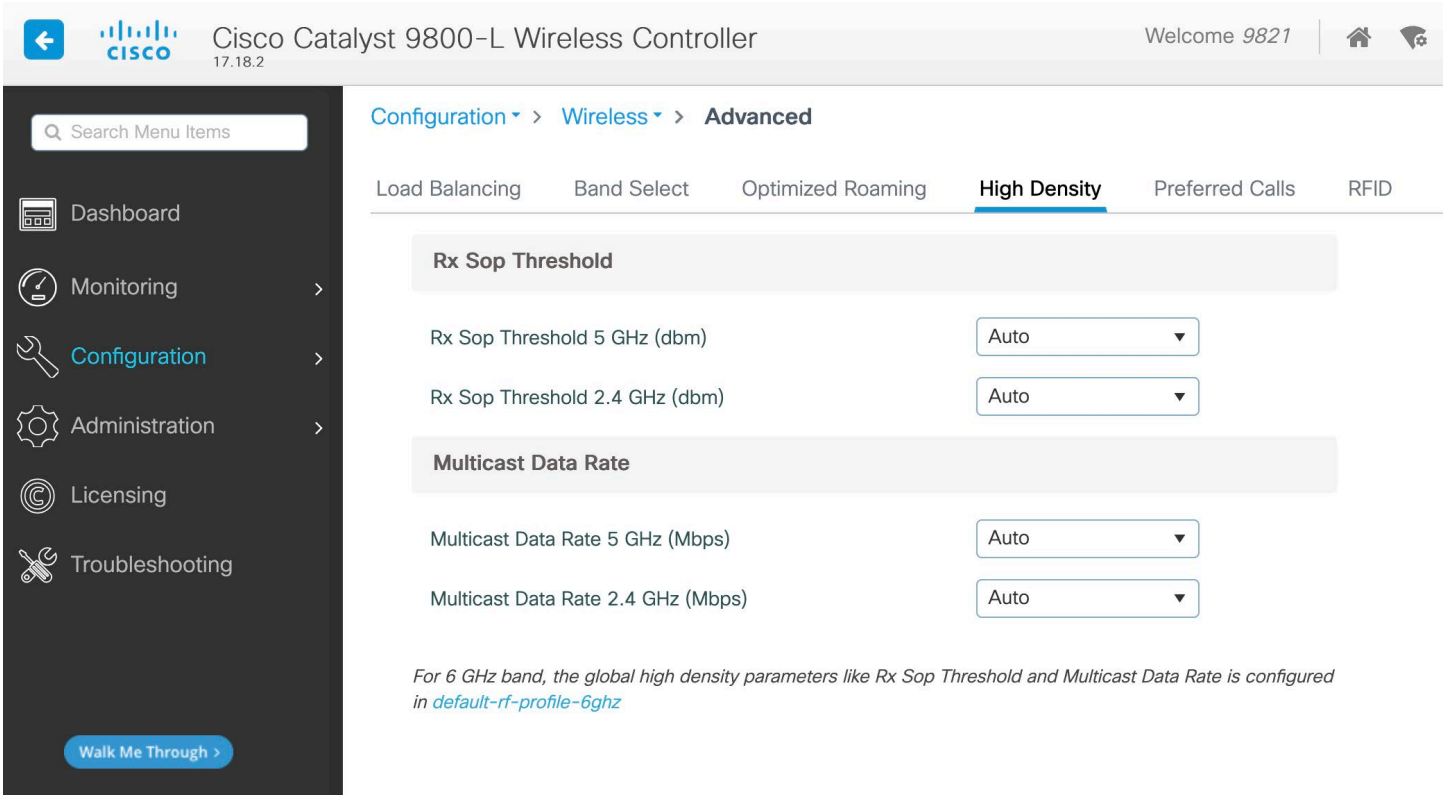
The **EAPOL-Key Timeout** should not exceed 1000 milliseconds (1 second).

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 Mobility Express and Lightweight Access Points

The Cisco Mobility Express solution has reached End-of-Life (EOL) status and does not support Wi-Fi 6E (6 GHz). However, Cisco Wireless Phone 9821 remains compatible with existing Mobility Express deployments

in environments where 6 GHz connectivity is not required. When configuring Mobility Express and its associated access points, adhere to the following guidelines:

- Enable **802.11r (FT)**
- Disable **CCKM**
- Set **Quality of Service (QoS)** to **Platinum**
- 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

Cisco Autonomous Access Points

Cisco Autonomous Access Points have reached End-of-Life (EOL) status and do not support Wi-Fi 6E (6 GHz). However, Cisco Wireless Phone 9821 remains compatible with Autonomous deployments in environments where 6 GHz connectivity is not required. When configuring Cisco Autonomous Access Points, adhere to the following guidelines:

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

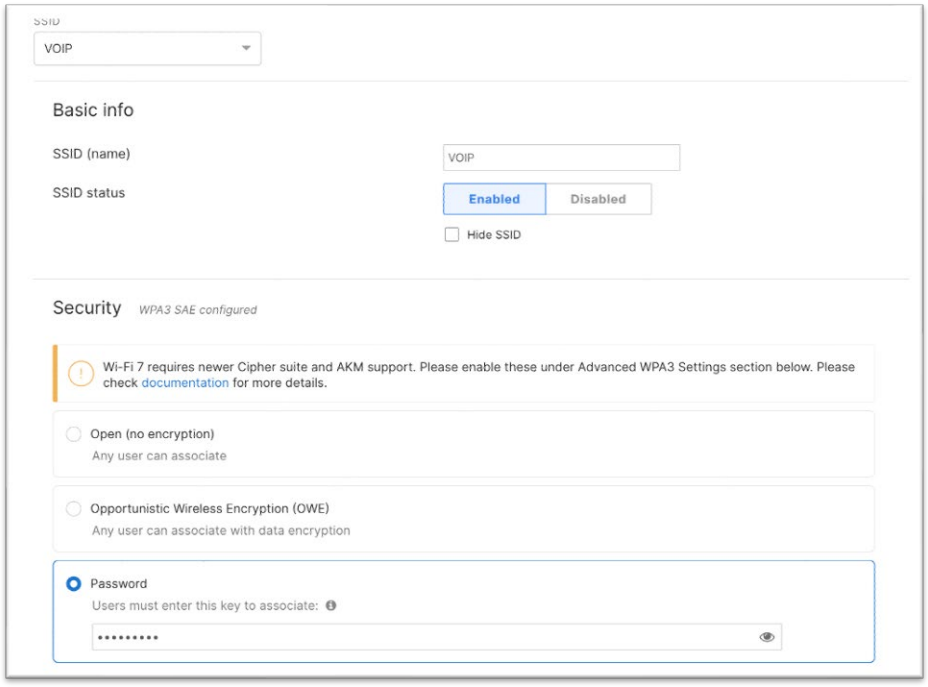
Cisco SSID on Meraki Dashboard

Voice optimization typically requires a different configuration including access control and traffic shaping to address device specific recommendations. It is recommended to have a separate Voice SSID for devices dedicated to voice applications.

It is recommended to operate Cisco Wireless Phone 9821 on the 5 GHz or 6 GHz band. These bands provide significantly greater spectrum availability and lower levels of non-Wi-Fi interference compared to the 2.4 GHz band, resulting in a more stable and reliable environment for latency-sensitive voice traffic.

WLAN Settings

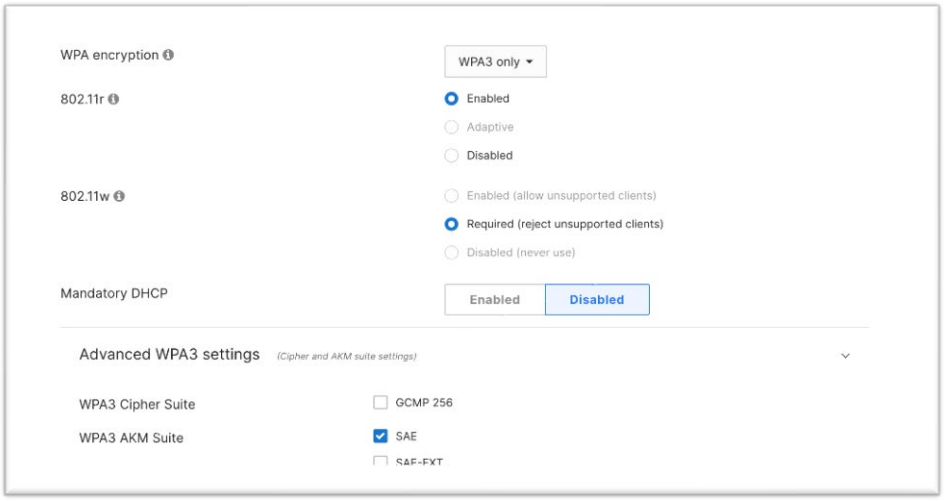
1. Configure a new SSID with WPA3



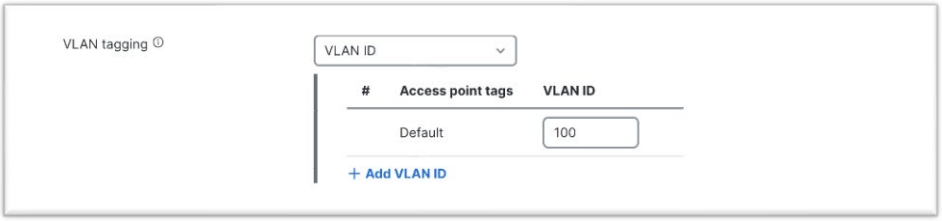
WPA3 Requirements in Wi-Fi 6E (6 GHz):

- WPA3 is mandatory for all Wi-Fi 6E devices operating in 6 GHz band.
- WPA3-Personal (SAE) with H2E for home/personal use.
- WPA3-Enterprise (802.1X, with optional 192-bit security suite) for enterprise deployments.
- Enhanced Open (OWE) for open networks requiring encryption without passwords
- Protected Management Frames (PMF) is mandatory in 6 GHz.
- WPA2 is not permitted in 6 GHz operation.

2. Enable 802.11r for WPA2/WPA3-Enterprise or Pre-shared key. In this example, the WLAN is set the Security Settings to WPA3 only.



3. Set **Splash page** to **None**
4. Enable **Bridge mode**
5. Enable **VLAN tagging**. Segregate Voice traffic Voice by mapping the WLAN with a dedicated VLAN



6. Click **Save**.

Minimum Bitrate

For Voice networks, 12 Mbps is recommended as the minimum bitrate. Increasing this value requires proper coverage in the RF planning. An administrator can improve the performance of clients on the 5 GHz and 6Ghz band by disabling lower bitrates. Adjusting the bitrates can reduce the overhead on the wireless network and also in some cases improve roaming performance.

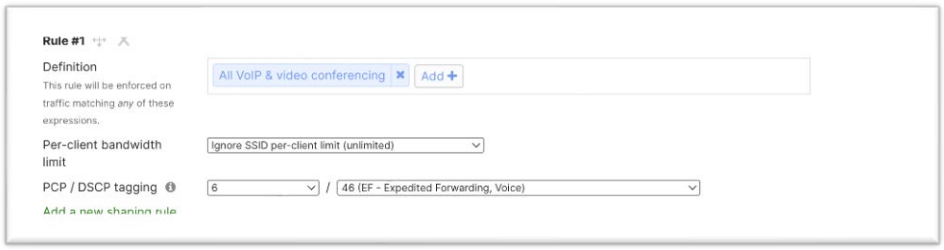
The minimum bitrate is configured in **Wireless** > **Radio Settings** > **RF Profiles** > **[Profile Name]** and can be set on per band or on per SSID basis.



Traffic Shaping Rules

Use traffic shaping to offer voice traffic the necessary bandwidth. It is important to ensure that your voice traffic has enough bandwidth to operate. As such, traffic shaping rules can be implemented to allow voice traffic to use additional bandwidth, or limit other types of traffic to help prioritize voice traffic.

1. Go to **Wireless** > **Configure** > **Firewall & traffic shaping** and choose your SSID from the **SSID** drop-down menu at the top of the screen.
2. Click the drop-down menu next to **Shape traffic** and choose Shape traffic on this SSID, then click **Create a new rule**.
3. Click **Add +** and select **All VoIP & video conferencing**.
4. Set Per-client bandwidth limit to **Ignore SSID per-client limit (unlimited)** and click **Save changes**.



PCP, DSCP, and WMM mapping

Many devices support Quality of Service (QoS) tags to maintain traffic priority across the network. WMM improves the reliability of applications in progress by preventing oversubscription of bandwidth. WMM accomplished this by enhancing the prioritization of traffic using the access categories: voice, video, best effort, and background data. WMM has mapped values which can be found in this article. To configure correct mapping for PCP and DSCP values, follow these steps:

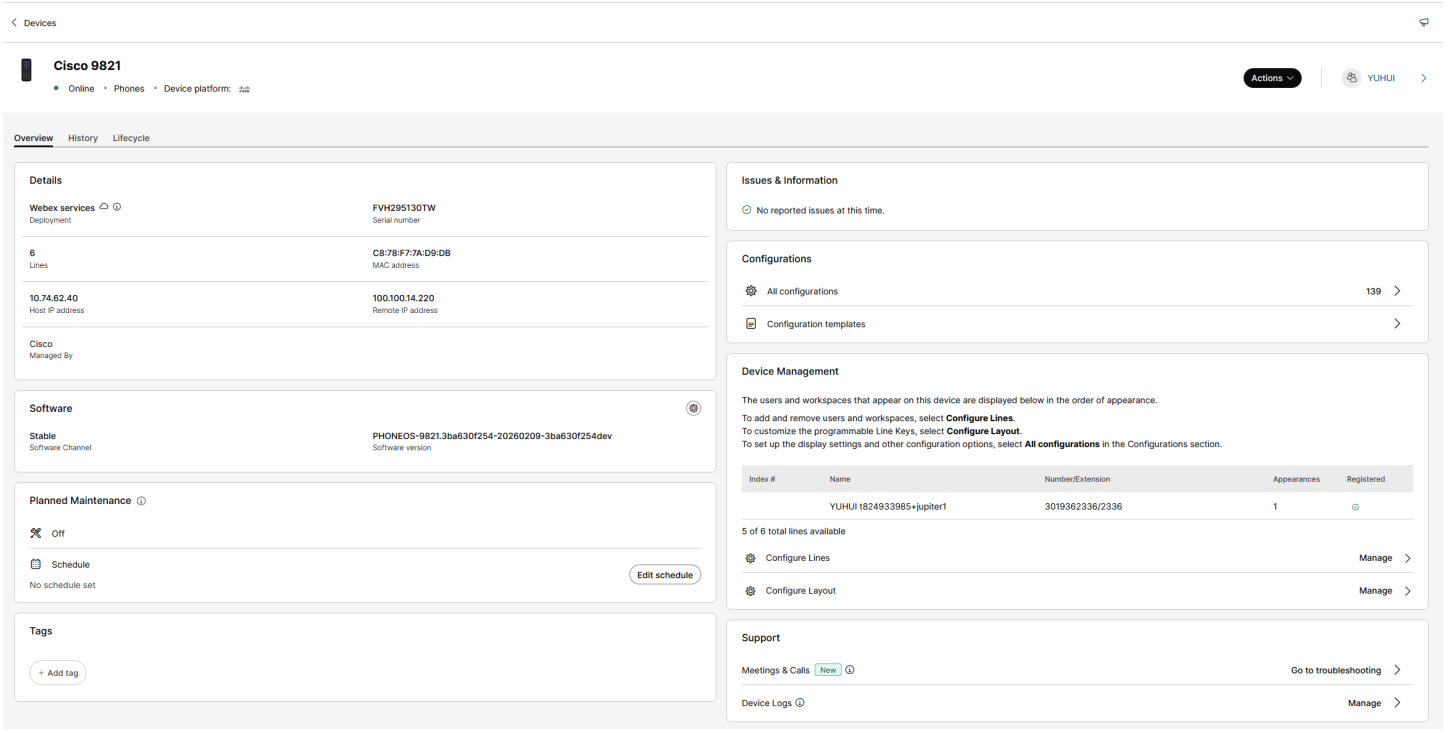
1. Go to **Wireless** > **Configure** > **Firewall & traffic shaping** and choose your SSID from the **SSID** drop-down menu at the top of the screen.
2. Under the traffic shaping rules, make sure **Shape Traffic for this SSID** is selected and that there's a rule for All voice & video conferencing.
3. Set PCP to **6** or the setting recommended by your device/application vendor.

   Note that PCP values can only be changed if the SSID has VLAN tagging enabled. This ensures there's a field to which the CoS value can be written).
4. Set DSCP to **46** (EF - Expedited Forwarding, Voice).

Configuring Cisco Call Control

Cisco Webex Calling

You can add Cisco Wireless Phone 9821 to Cisco Webex Calling and assigned it to a user for personal usage.

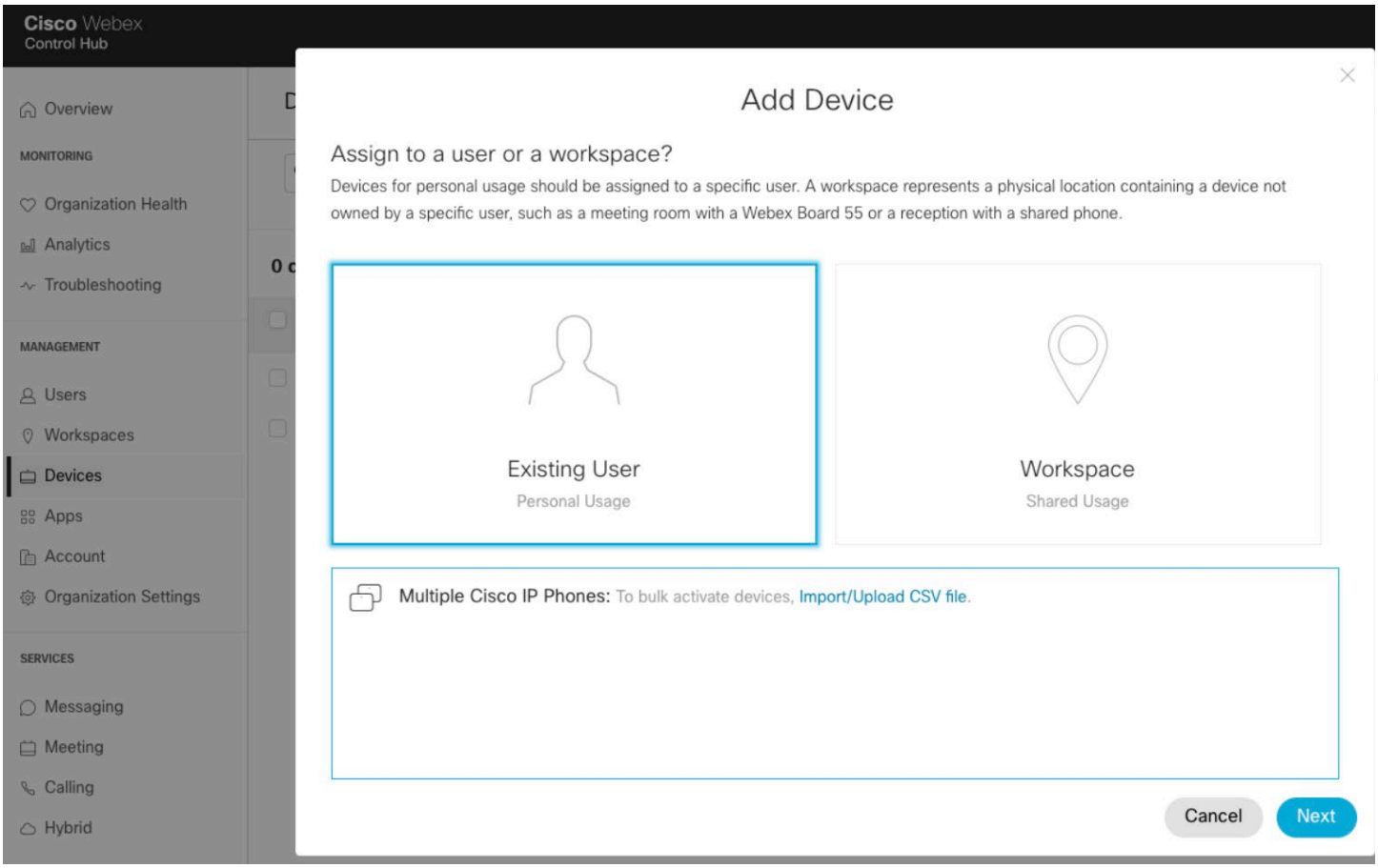


Personal Usage

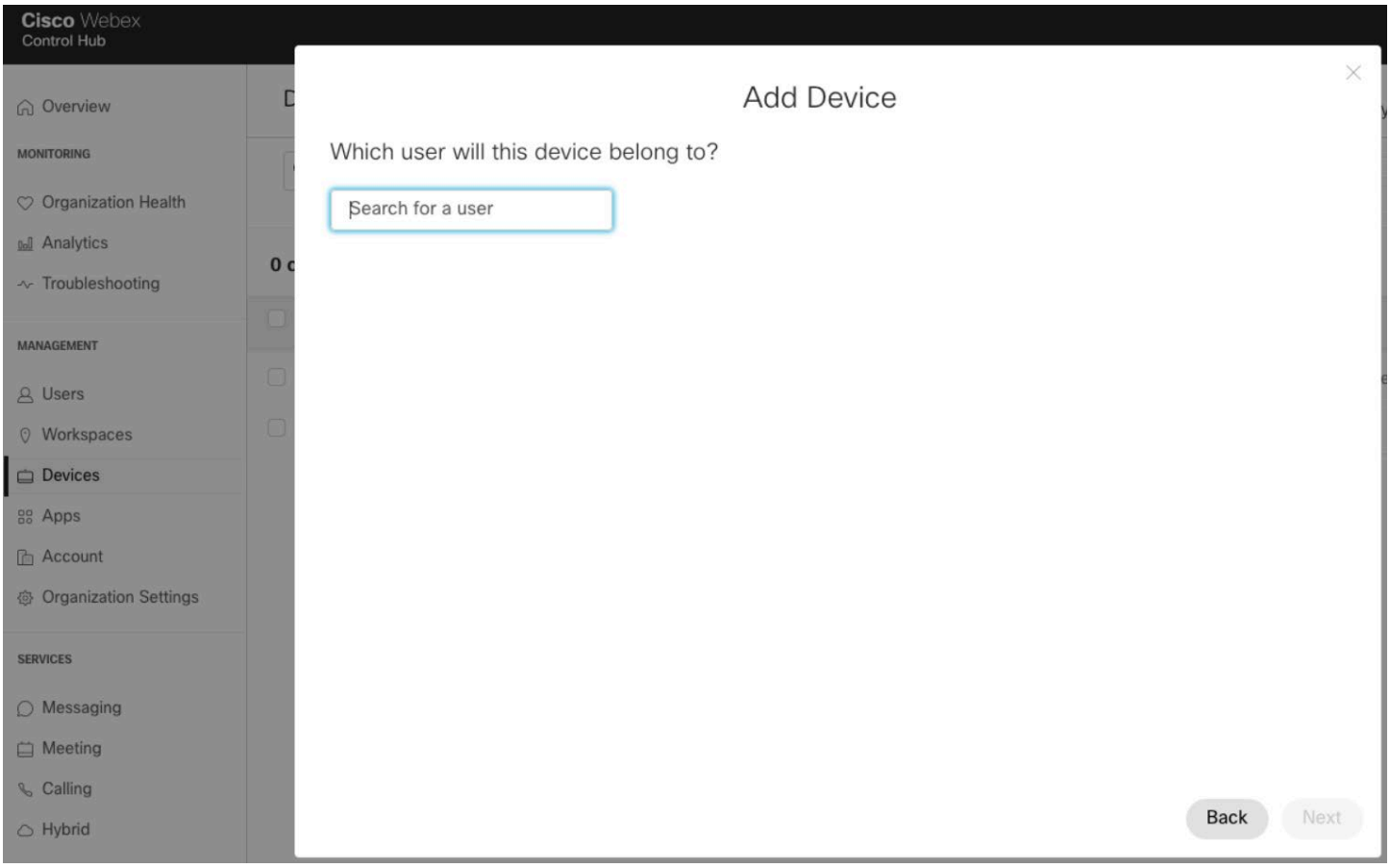
You can assign Cisco Wireless Phone 9821 to a user and configure the settings on Control Hub.

Follow these steps to add a device for a user:

1. Navigate to **Devices**, and then select **Add Device**.
2. Select **Existing User**, and then click **Next**.



3. Search for the user, and then click **Next**.



Cisco Unified Communications Manager

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

Device Enablement

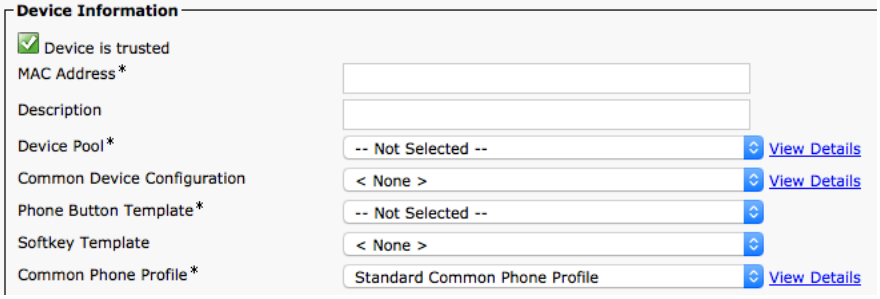
To enable the Cisco Wireless Phone 9821 device type in Cisco Unified Communications Manager, the corresponding device package COP file must be installed via the Cisco Unified Operating System Administration webpage for each Cisco Unified Communications Manager server.

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

For information on how to install COP file, refer to the Cisco Unified Communication Manager Operation System Administration Guide.

When adding Cisco Wireless Phone 9821 to Cisco Unified Communications Manager, you must provision the phone using the Wi-Fi MAC address.

The Wi-Fi MAC address of Cisco Wireless Phone 9821 can be found by navigating to **Settings** > **Phone information** > **Device information**.

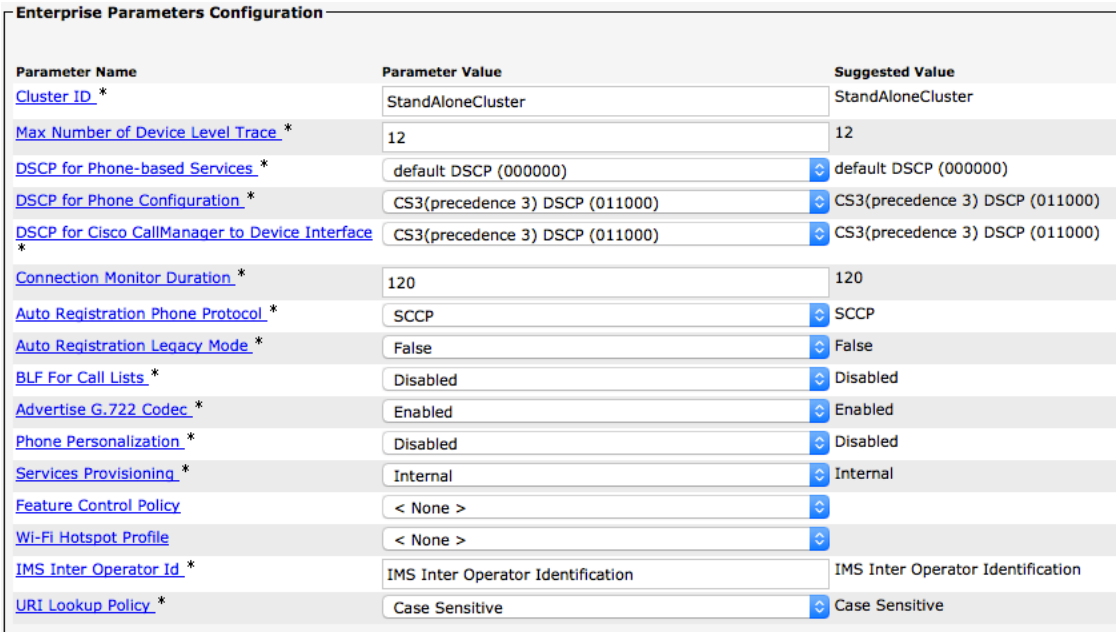


QoS Parameters

The DSCP values to be used for SIP communications, phone configuration, and phone-based services to be used by the phone are defined in 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.

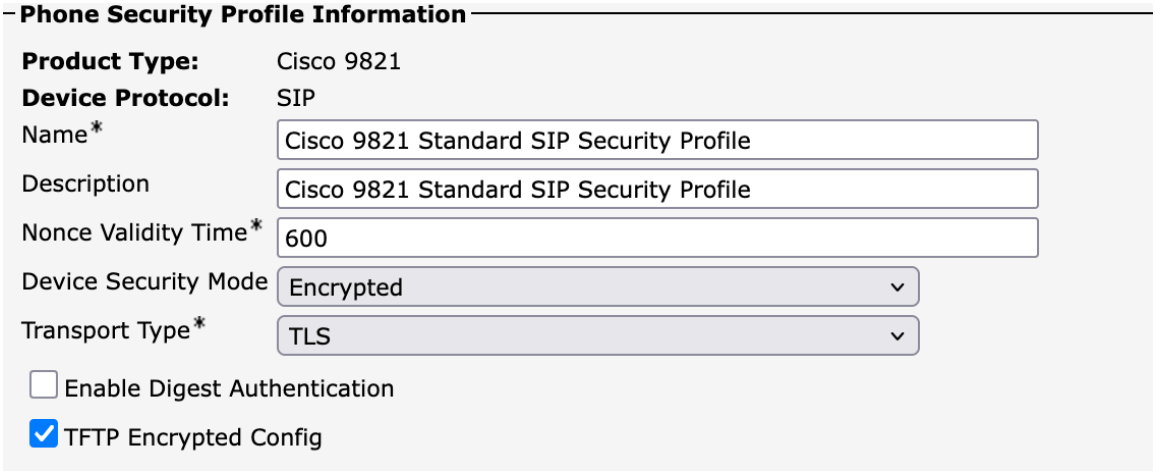


Wireless LAN Profiles

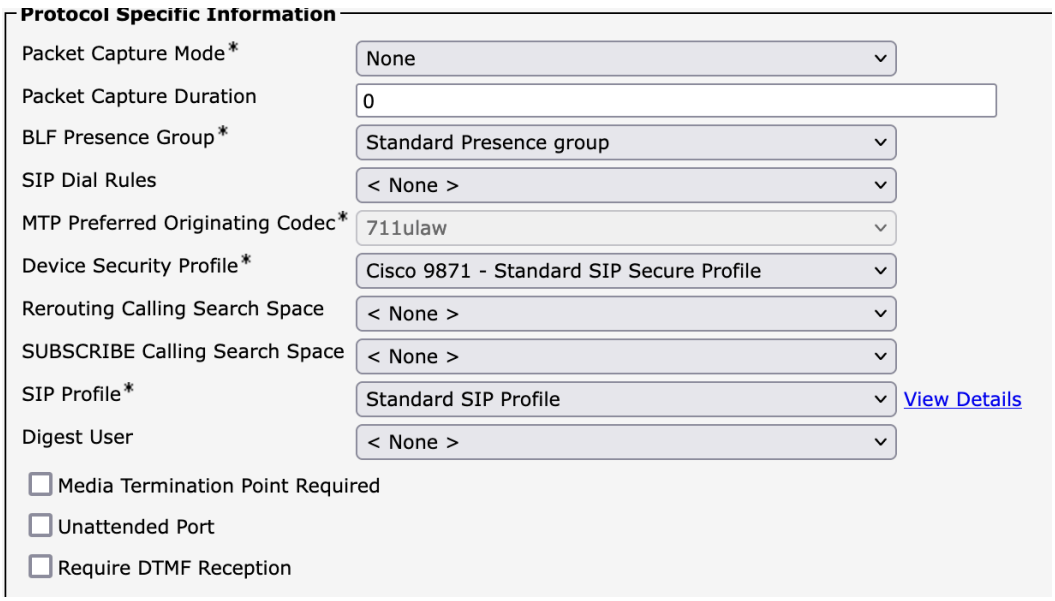
With Cisco Unified Communications Manager 15.0.1 release and later, you can provision Cisco Wireless Phone 9821 with Wireless LAN Profiles. EAP-TLS support is included.

Create a Wireless LAN Profile

Prior to creating a Wireless LAN Profile and associating it to Cisco Wireless Phone 9821, 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.

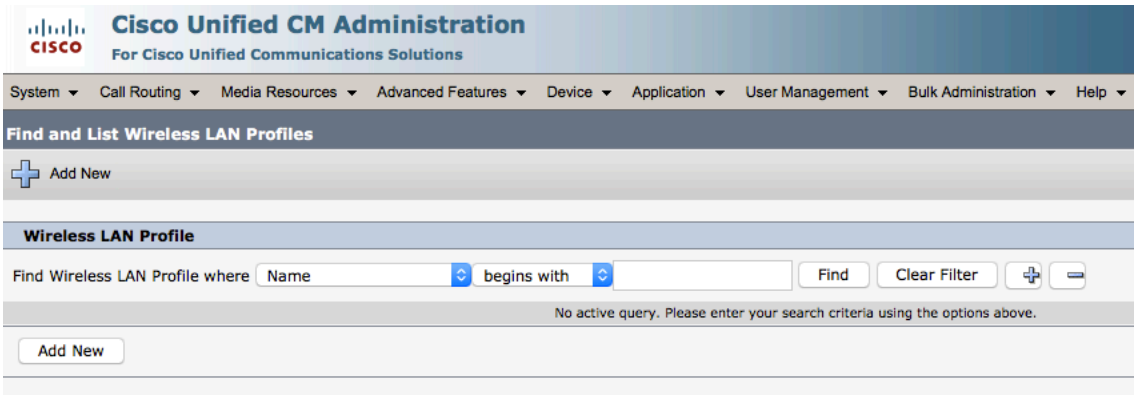


Once the security profile has been created, it must be applied to the phone to enable TFTP encryption for the phone's configuration files. Select the configured security profile from the **Device Security Profile** drop-down menu.



Follow these steps to create a Wireless LAN profile on Cisco Unified Communications Manager.

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**.



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

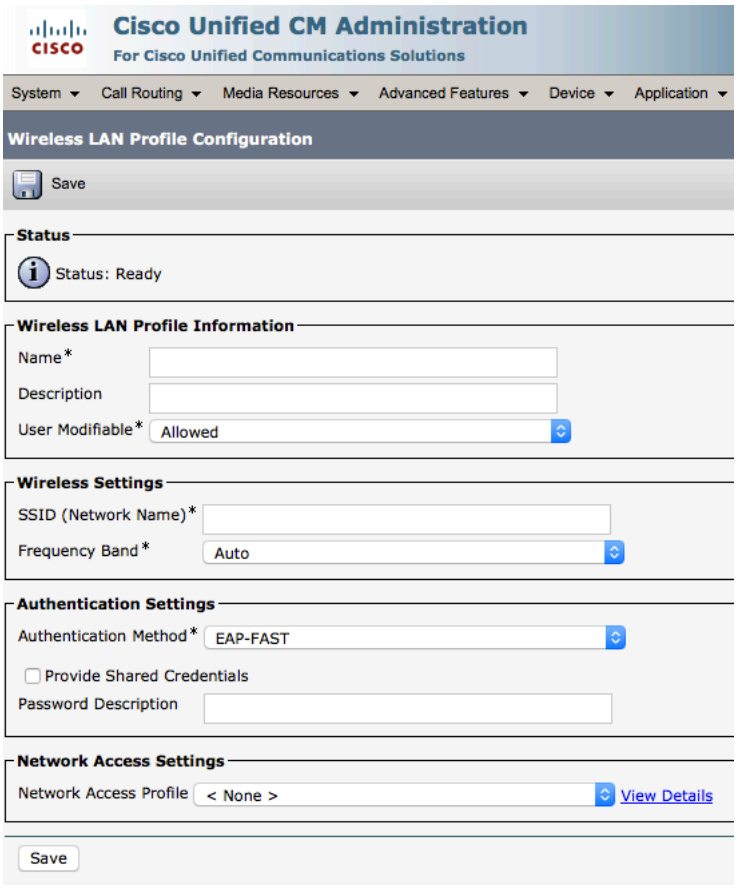
   Below are Wireless LAN Profile defaults:

   Frequency Band = Auto

   User Modifiable = Allowed

   Authentication Method = EAP-FAST

   Note: Wired Equivalent Privacy (WEP) is a legacy security protocol and is not supported by Cisco Wireless Phone 9821. Cisco Wireless Phone 9821 categorizes both PEAP-GTC and PEAP-MSCHAPv2 under the PEAP authentication framework. Additionally, the device groups both 5 GHz and 6 GHz frequency bands under the **5G** designation within the user interface.



a) Enter a name for the Wireless LAN profile. The name can be up to 50 characters in length.
b) (Optional) Enter a description that can be up to 63 characters in length.

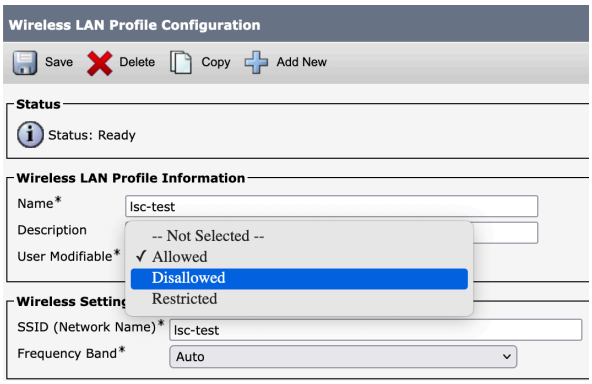


c) Select the desired **User Modifiable** option.

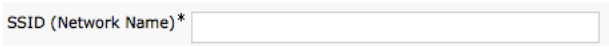
• **Allowed** - The user has the capability to change any Wireless LAN settings (e.g. Enable/Disable, SSID, Frequency Band, Authentication Method, Username and Password, PSK Passphrase) locally on the phone.

• **Disallowed** - The user is unable to change any Wireless LAN settings.

• **Restricted** - The user is only able to change certain Wireless LAN settings (e.g. Username and Password).

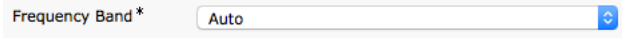


d) Enter an **SSID** that can be up to 32 ASCII characters in length.



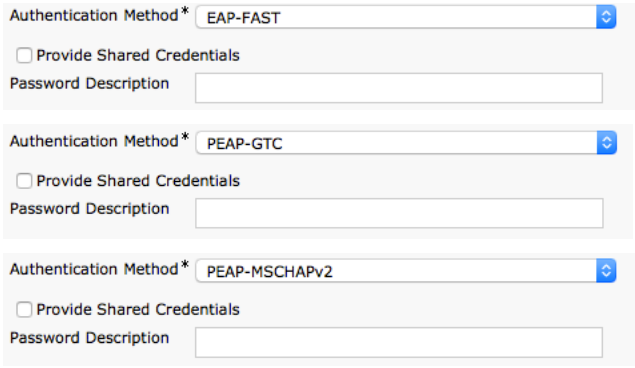
e) Select the desired **Frequency Band** option.

- **Auto** = Give preference to 5 GHz channels, but operates on both 5 GHz and 2.4 GHz channels
- **2.4 GHz** = Operates on 2.4 GHz channels only
- **5 GHz** = Operates on 5 GHz and 6 GHz channels

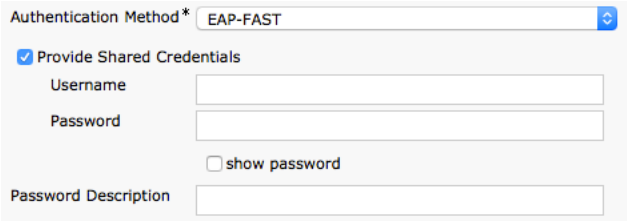


f) Select the desired **Authentication Method** option.

- 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 selected, the Username and Password will need to be configured locally on the phone by the admin or user.



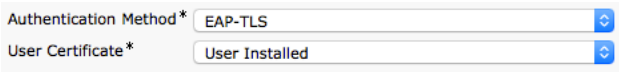
- If **Provide Shared Credentials** is selected, the specified **Username** and **Password** will be utilized for all Cisco Wireless Phone 9821 that utilize this Wireless LAN Profile.
- Up to 64 characters can be entered for the Username and Password.
- (Optional) Enter a **Password Description**.



• If **EAP-TLS** is selected, you must configure **User Certificate** to specify the type of user certificate to utilize for EAP-TLS authentication.

• Set **User Certificate** to **MIC** (Manufacturing Installed Certificate), **LSC** (Locally Significant Certificate) or **User Installed**.



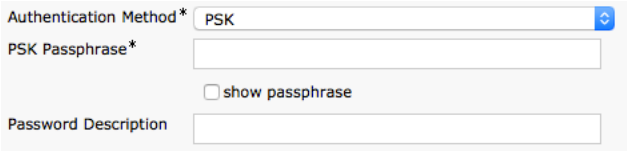


• If **PSK** is selected to utilize Pre-Shared Key authentication, you must enter a **PSK Passphrase**. The **PSK Passphrase** must be in one of the following formats:

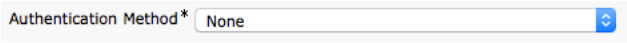
  • 8-63 ASCII character string

  • 64 HEX character string

• (Optional) Enter a **Password Description**.

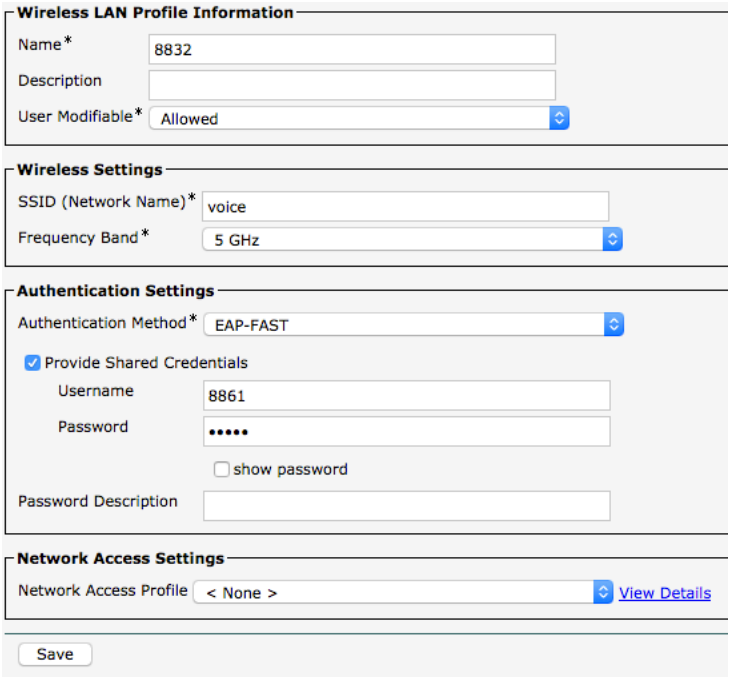


• If **None** is selected, no authentication is required and no encryption will be utilized.



Cisco Wireless Phone 9821 does not support the Network Access Profile option.

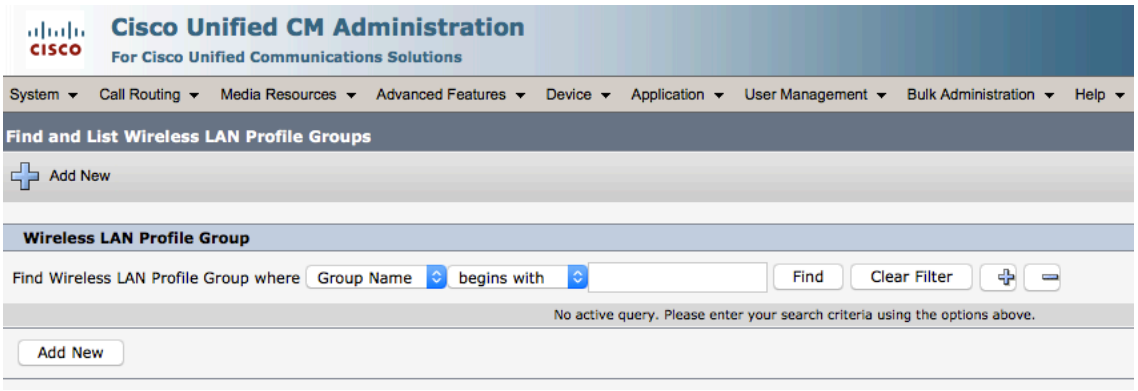
4. Select **Save** once the Wireless LAN Profile configuration is complete.



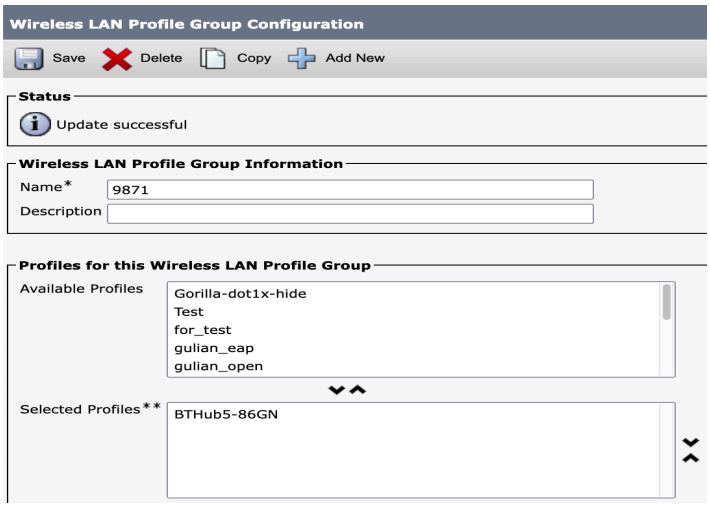
Create a Wireless LAN Profile Group

Follow these steps to create a Wireless LAN Profile Group:

1. Navigate to **Device** > **Device Settings** > **Wireless LAN Profile Group** in Cisco Unified Communications Manager Administration.
2. From the Wireless LAN Profile Group page, select **Add New**.



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



Totally **up to 4** Wireless LAN Profiles could be added to a Wireless LAN Profile Group.

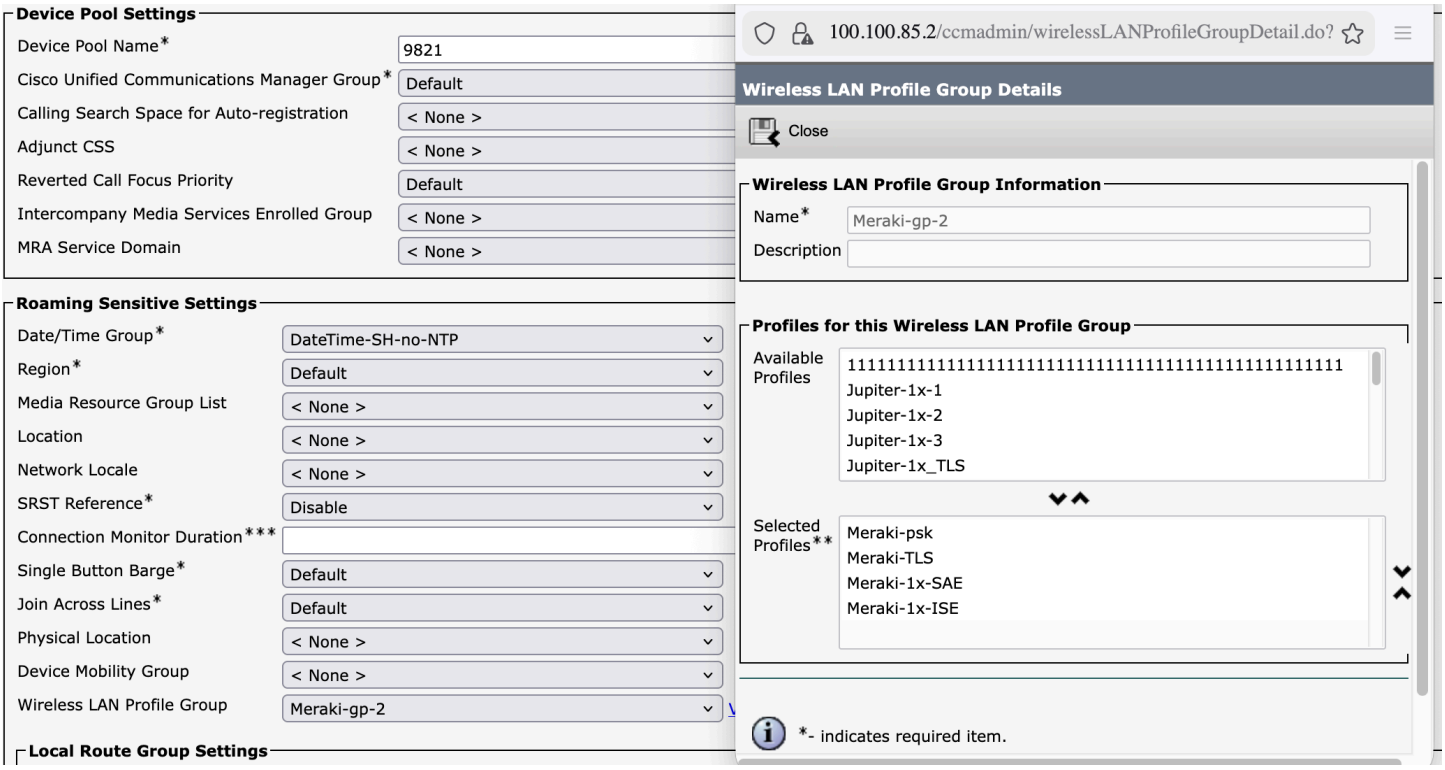
4. Select **Save** once the Wireless LAN Profile Group configuration is complete.

Apply a Wireless LAN Profile Group to a Device Pool

Once the Wireless LAN Profile Group has been created, you can apply it to a Device Pool or an individual Cisco Wireless Phone 9821.

Follow these steps to apply a Wireless LAN Profile Group to a device pool:

1. Navigate to **System** > **Device Pool** in Cisco Unified Communications Manager Administration.
2. Create a Device Pool as necessary and add the desired Cisco Wireless Phone 9821 to this Device Pool.
3. Once the Device Pool has been created, configure the Wireless LAN Profile Group and then select **Save**.
4. Once the Wireless LAN Profile Group has been applied to the Device Pool, select **Apply Config** for the Cisco Wireless Phone 9821 to download the Wireless LAN Profile Group configuration.



Apply a Wireless LAN Profile Group to an Individual Phone

Follow these steps to apply a Wireless LAN Profile Group to an individual Cisco Wireless Phone 9821:

1. Navigate to **Device** > **Phone** in Cisco Unified Communications Manager Administration.
2. Find your phone and open the Phone Configuration page.
3. In the **Device Information** section, select your WLAN profile group in the **Wireless LAN Profile Group** drop-down list.
4. Select **Save**.
5. Select **Apply Config** for the Cisco Wireless Phone 9821 to download the Wireless LAN Profile Group configuration.

Configuring Cisco Wireless Phone 9821

Wi-Fi Profile Configuration

You can add, delete, or edit Wi-Fi profiles using either the Cisco Wireless Phone 9821 administration web page or the on-device LCD menu. The phone supports up to four Wi-Fi profiles. We recommend assigning a unique SSID to each profile; if multiple profiles share the same SSID, the phone will prioritize the highest-ranked enabled profile.

Automatic Provisioning

This method is currently available only for phones registered to Cisco Unified Communications Manager. For automatic provisioning of the Wi-Fi Profiles, you can connect Cisco Wireless Phone 9821 to a network by either docking in the desktop charger with a supported USB-to-Ethernet adapter or using the default Wi-Fi settings (**SSID** = cisco and **Security Mode** = none). Both methods ensure connectivity to the Cisco Unified Communications Manager (CUCM). Ensure the network provides DHCP Option 150 to direct the device to the target CUCM.

With connectivity to Cisco Unified Communications Manager 15.0.1 or later, Wi-Fi profile configuration data can be downloaded and applied to Cisco Wireless Phone 9821. For more information, see the Wireless LAN Profiles section.

Certificates can also be automatically installed utilizing a network connection. For more information, see the Simplified Certificate Enrollment Protocol (SCEP) section.

Config and Modify Wi-Fi Profile via Phone Administration Web Page

Once the Cisco Wireless Phone 9821 onboarding process is complete, you can modify Wi-Fi profiles via the phone administration web page. Ensure that the phone has obtained a valid IP address.

Webex Calling

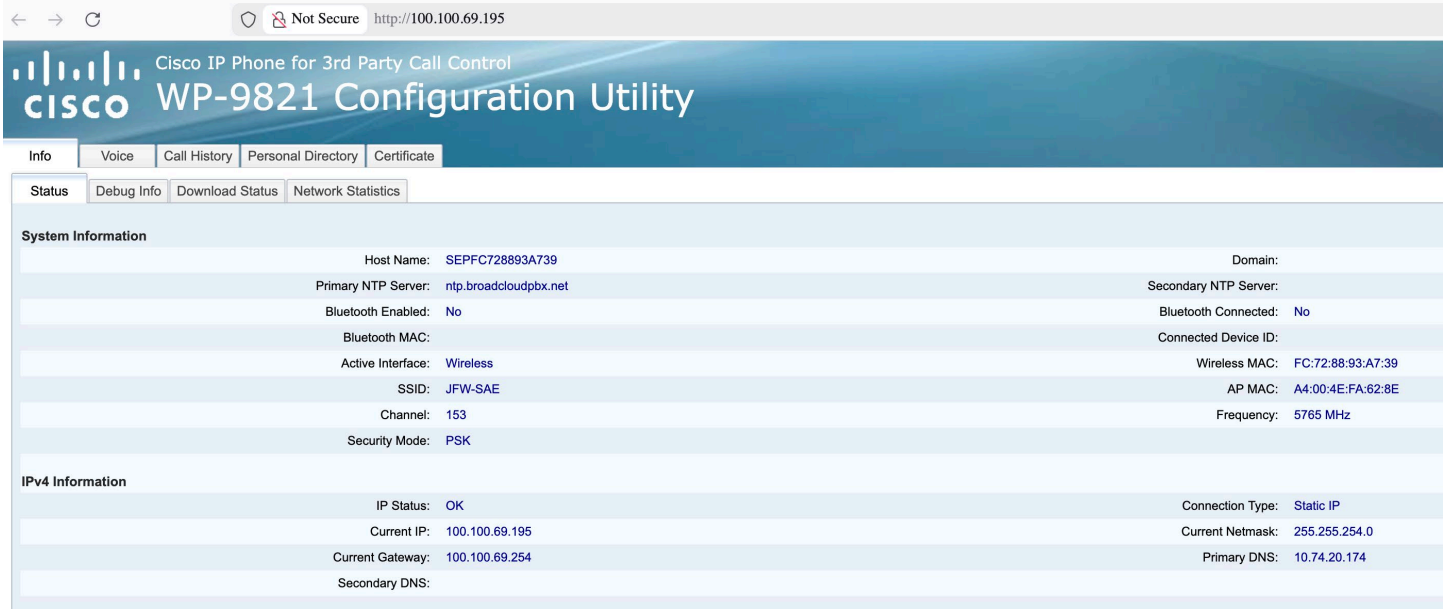
1. Enter the IP address of the phone in your web browser address bar in this format.

   [web service]://A.B.C.D

   Replace [web service] with http or https, which depends on the exact web service opened on your phone, and replace A.B.C.D with your phone's valid IP address. For example, http://10.64.84.147/.

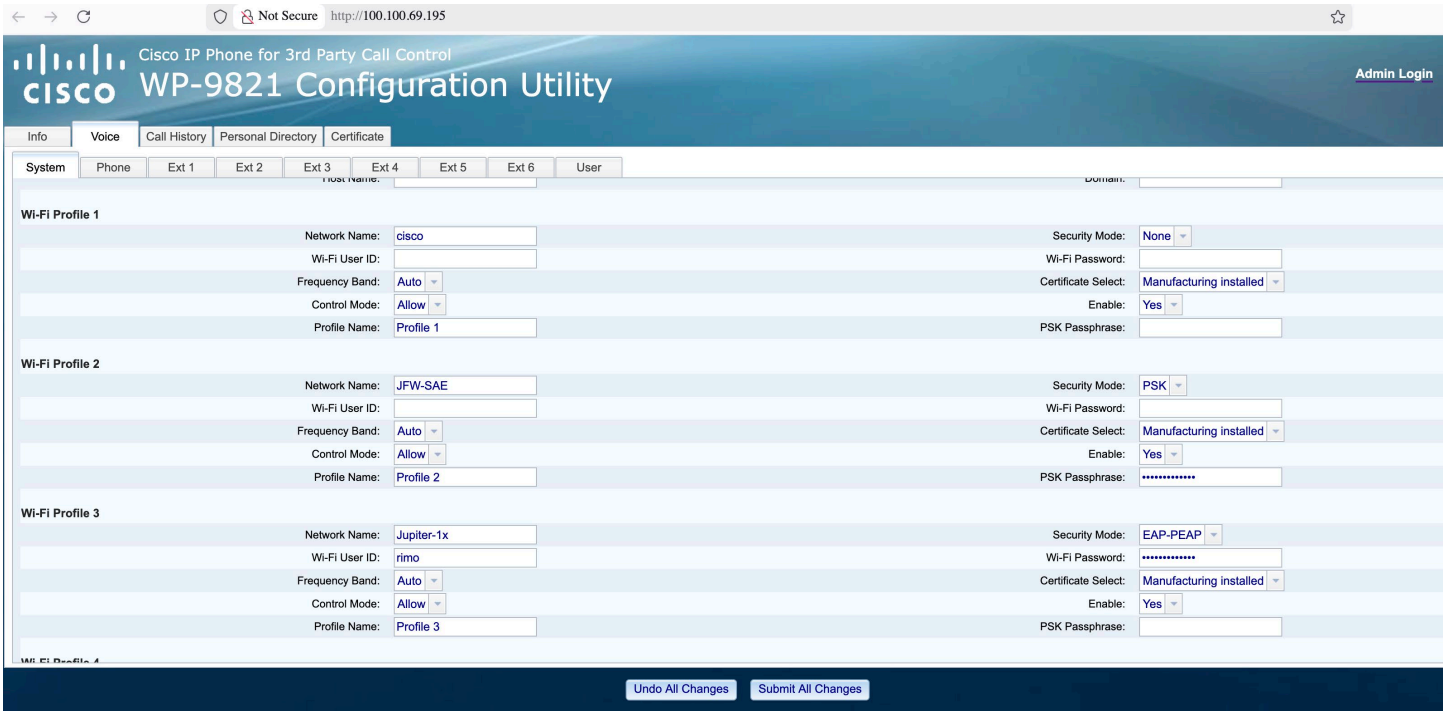
2. Click **Admin Login** and then click **advanced** to access the configurations as an administrator.

   Refer to the following screenshot as an example:



3. Go to **Voice** > **System**.

Currently Cisco Wireless Phone 9821 has four Wi-Fi profiles. Refer to the following screenshot as an example:



4. Specify the Wi-Fi network name and credentials for the phone to connect to the wireless access point.

   The **Security Mode** can be **EAP-Fast**, **EAP-PEAP**, **PSK**, **EAP-TLS** or **NONE**, depending on the authentication method settings on your access point.

   - If **EAP-FAST**, or **PEAP** is selected, **Wi-Fi User ID** and **Wi-Fi Password** are required.
   - If **PSK** is selected to utilize Pre-Shared Key authentication, you must enter a **PSK Password**.
   - The **PSK Password** must be 8-63 ASCII character string.
   - If **None** is selected, no authentication is required and no encryption will be utilized.
   - If **EAP-TLS** is selected, currently **MIC** or **Customer Installed** certificate is supported for Cisco Webex Calling.
5. Select the desired **Frequency Band**.
   - **Auto:** Give preference to 5 GHz and 6 GHz channels, but operates on all 3 bands
   - **2.4 GHz:** Operates on 2.4 GHz channels only
   - **5 GHz or 6 GHz:** Operates on 5 GHz and 6 GHz channels
6. Click **Submit All Changes**.

CUCM

Note: Ensure that **Web Admin** is set to **Enabled** on your Cisco Wireless Phone 9821 in Cisco Unified Communications Manager Administration. The username is fixed to **admin**, and you have configured the **Admin password**.



1. Enter the IP address of the phone in your web browser address bar in this format.

https://A.B.C.D:8443

Replace A.B.C.D with your phone's valid IP address. For example, http://10.64.84.147:8443/.

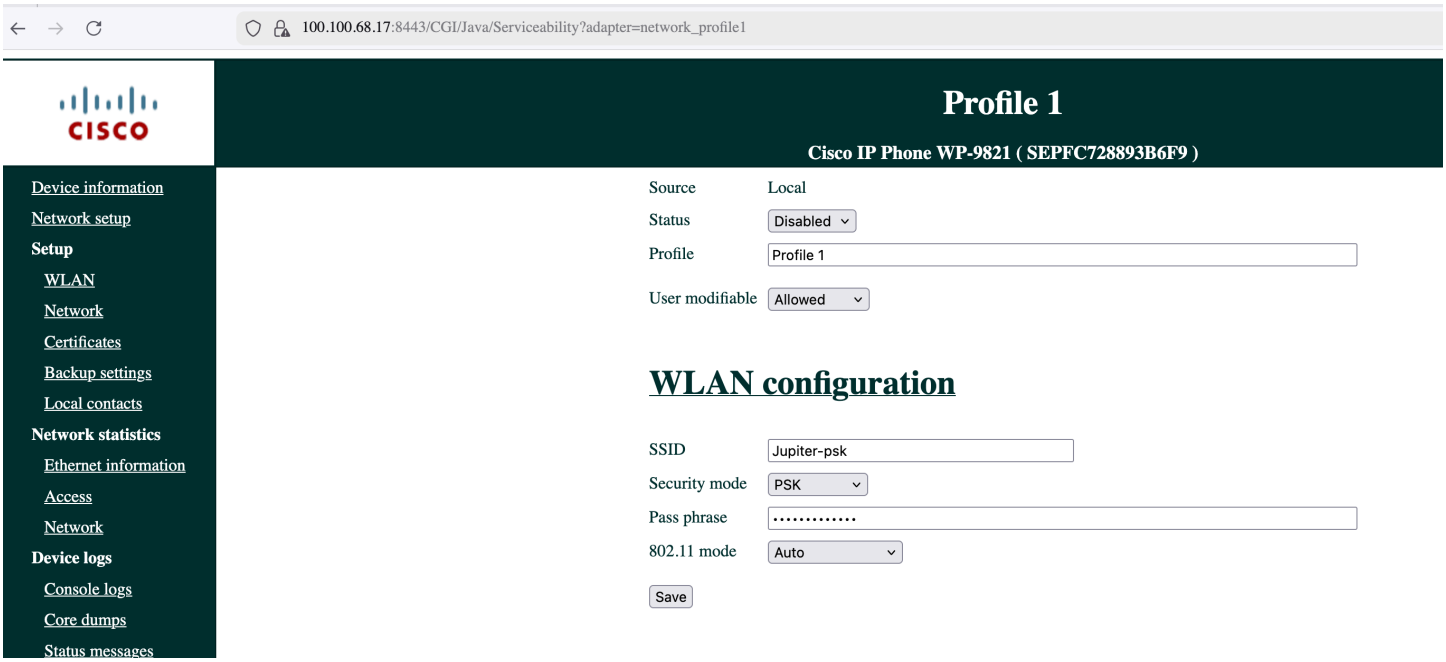
2. Enter admin in the **Username** field, enter the password in the **Password** field. Click **Submit**.
3. Select **Network setup**.

   Refer to the following screenshot as an example:



4. Select a profile to access the WLAN and network configuration parameters.

   Refer to the following screenshot as an example:



Note:

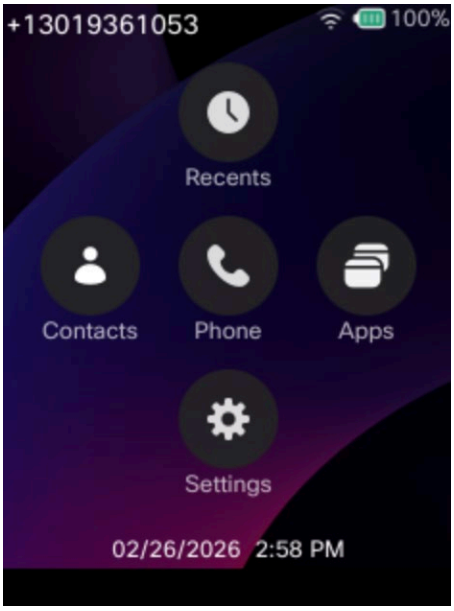
- Any changes made to the currently active Wi-Fi profile will cause the phone to disconnect from the current access point (AP) and re-establish a connection using the updated parameters.
- Wired network connectivity takes precedence over wireless. When the phone is placed in a desktop charger connected with a USB-to-Ethernet adapter, the Wi-Fi radio is automatically disabled. Removing the phone from the desktop charger triggers an automatic transition back to the wireless connection.
- Wi-Fi profiles configured via the web page are automatically synchronized with those configured on the phone UI.

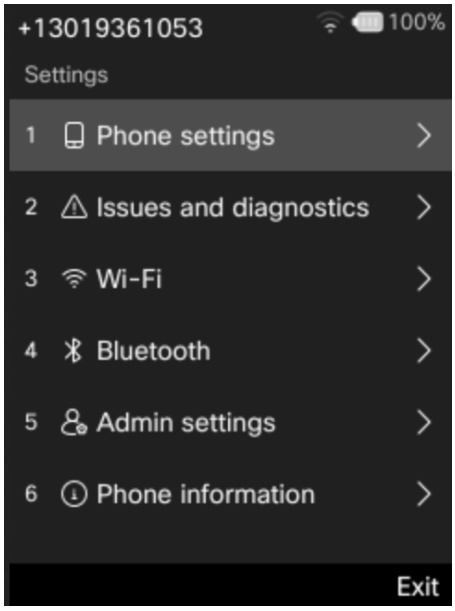
Configure Wi-Fi Settings on the Phone UI

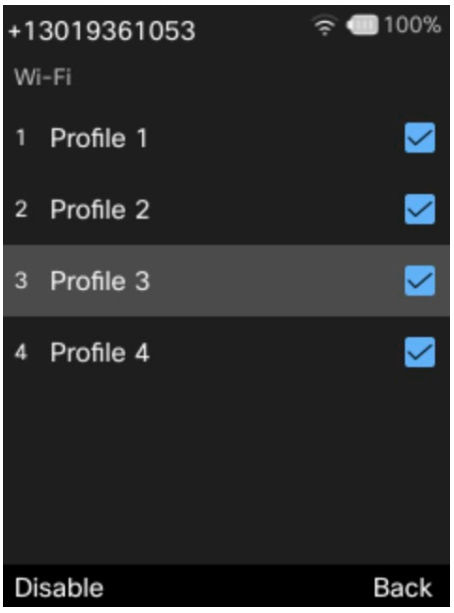
Use the following guidelines to configure Wi-Fi Profiles through the phone UI menu.

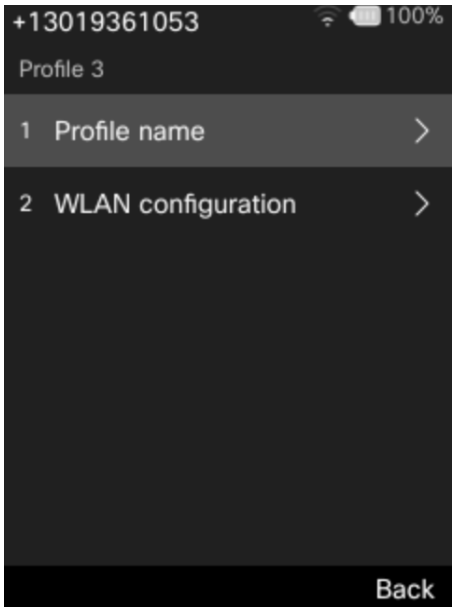
1. Access the **Settings** app.
2. Select **Wi-Fi**, then select the desired profile to configure. You can configure four profiles in total.

   Refer to the following screenshots as an example:



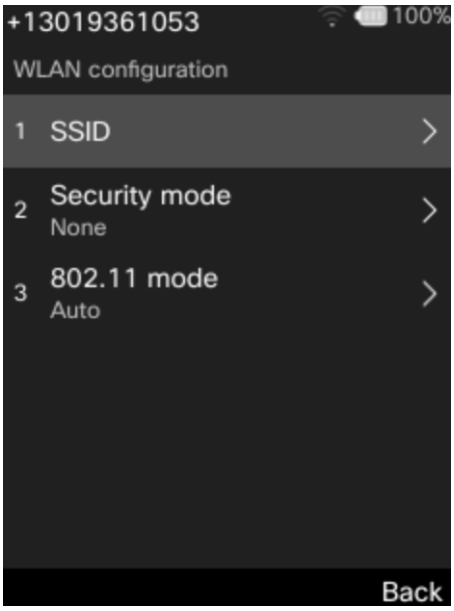




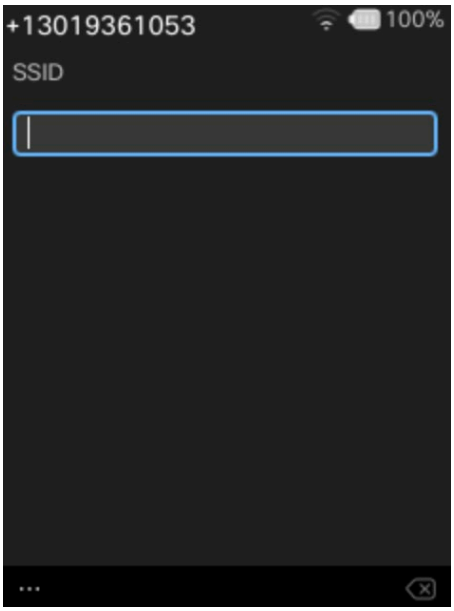


3. (Optional) Press **Select** to enter a profile name. Press **More** (…) and select **Save**.
4. Highlight **WLAN configuration** and then press **Select** to configure the WLAN parameters including **SSID**, **Security mode**, and **802.11 mode**.

   Refer to the following screenshots as an example:



a) Select SSID and then enter the SSID of the desired WLAN. Press **More** (…) and select **Save**.



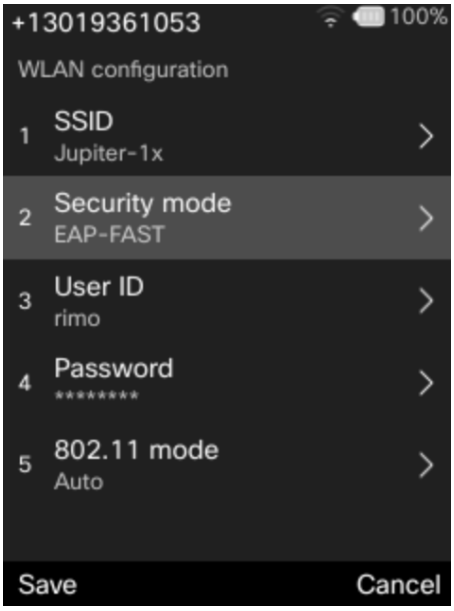
b) Select a **Security mode** as required. The following table shows the valid input for each security mode.

Security mode	Password	User ID	Certificate
None			
PSK	yes		
EAP-FAST	yes	yes	
EAP-PEAP	yes	yes	

EAP-TLS			yes

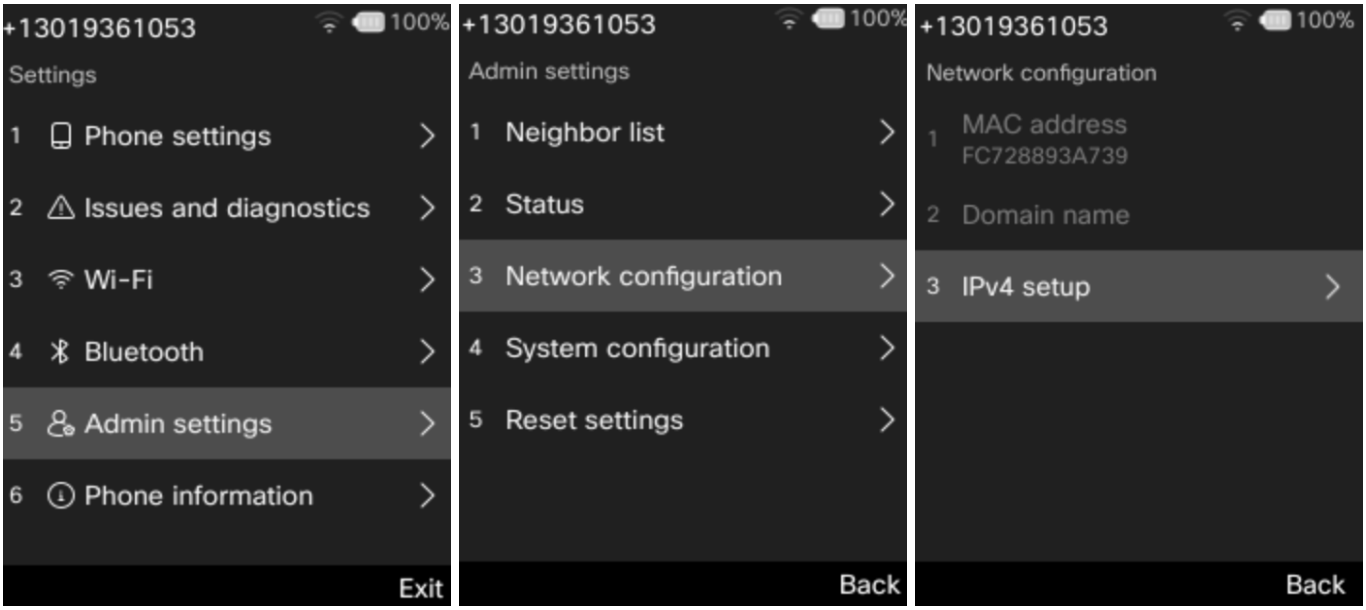
5. Press **Save**.

   Refer to the following screenshots as an example:

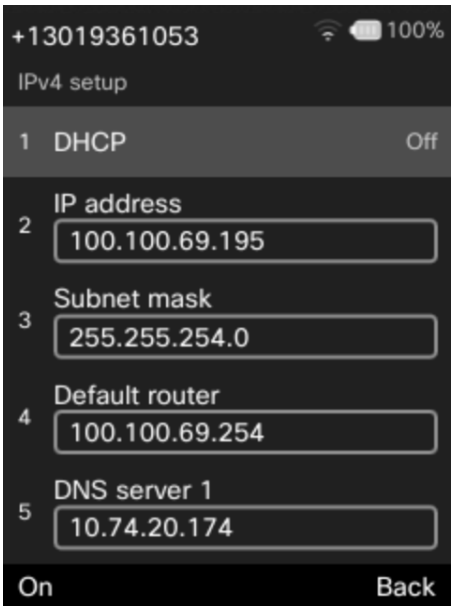


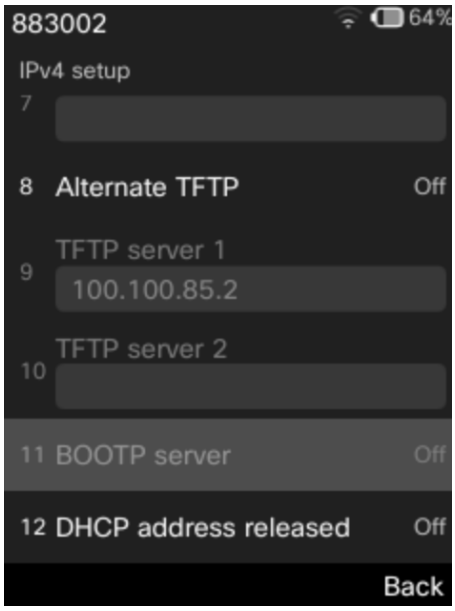
Network configuration

Network configuration is the common setting for all WLAN profiles. You can set up DHCP, IP Address, Gateway, DNS and Alternate TFTP parameters from **Settings** > **Admin settings** > **Network configuration** > **IPv4 setup**.

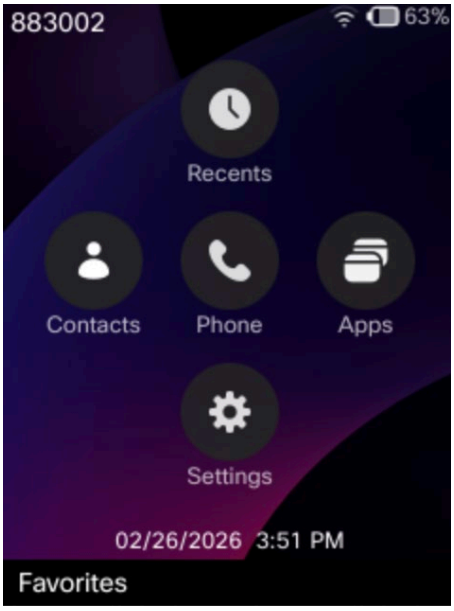


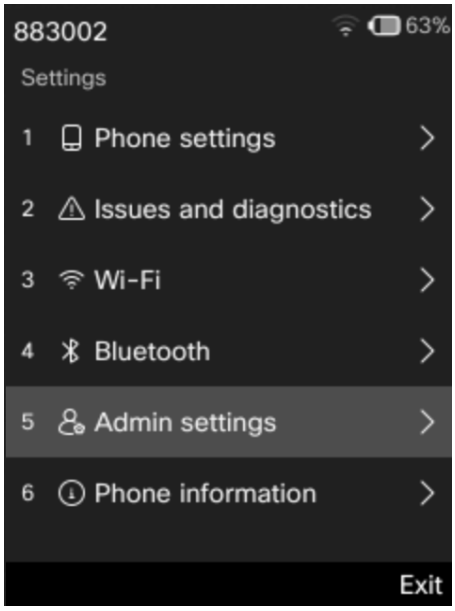
Refer to the following screenshots as an example:

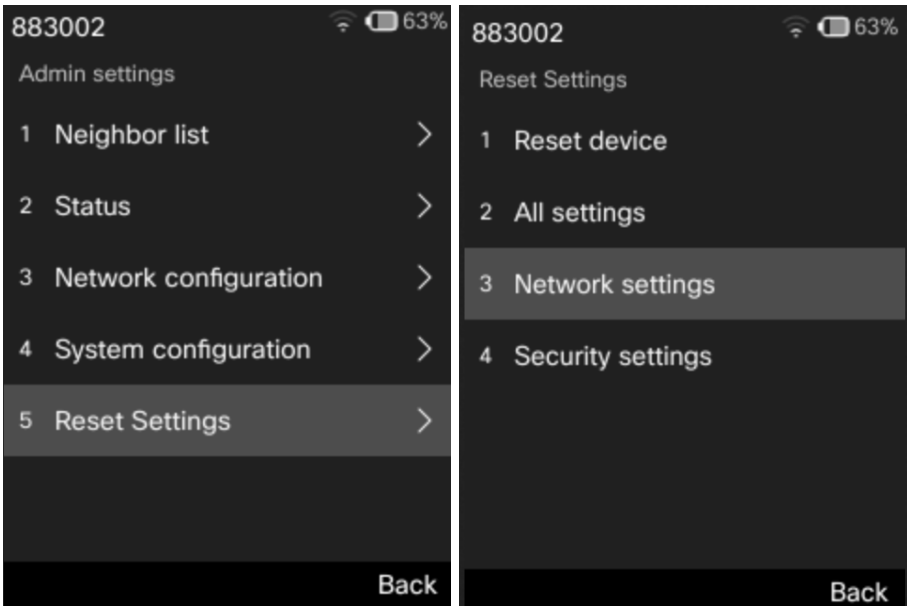




To reset all WLAN and network configurations, access **Settings** > **Admin settings** > **Restart and Reset** > **Network settings**.







Certificate Management

Cisco Wireless Phone 9821 utilizes X.509 digital certificates for EAP-TLS or to enable Server Validation.

User certificates can be installed automatically using the Simple Certificate Enrollment Protocol (SCEP) or manually via the phone administration web page.

The phone supports a maximum of one certificate per type: one User Certificate and one Server Certificate. These may be provisioned using either SCEP or manual upload methods.

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 Cisco Wireless Phone 9821.

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

Note: Ensure that **Web Admin** is set to **Enabled** on your Cisco Wireless Phone 9821 in Cisco Unified Communications Manager Administration. The username is fixed to **admin**, and you have configured the **Admin password**.



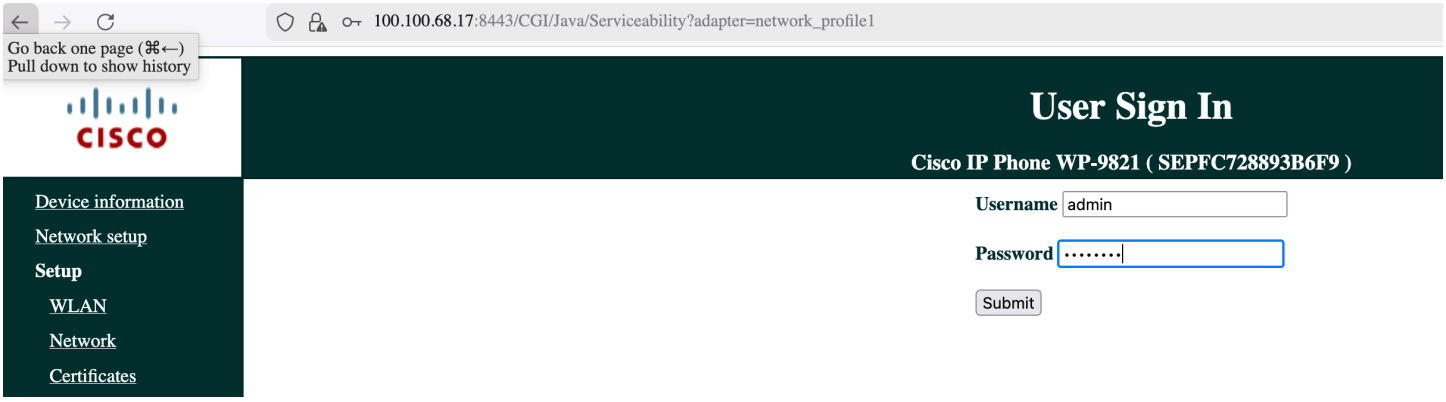
1. Enter the IP address of the phone in your web browser address bar in this format.

https://A.B.C.D:8443

Replace A.B.C.D with your phone's valid IP address. For example, http://10.64.84.147:8443/.

2. Enter admin in the **Username** field, enter the password in the **Password** field. Click **Submit**.
3. Select **Certificates**.

   Refer to the following screenshot as an example:



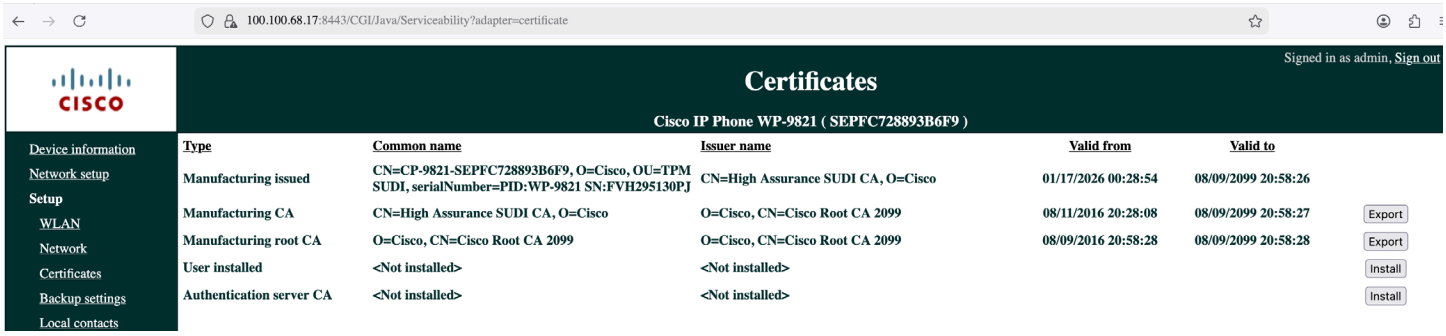
You can utilize the internal Manufacturing Installed Certificate (MIC), LSC or a custom User Installed certificate to be used as the User Certificate for EAP-TLS.

Manufacturing Installed Certificate (MIC)

You can use the pre-installed Manufacturing Installed Certificate (**MIC**) as the **User Certificate** for **EAP-TLS**.

To use the MIC as the User Certificate for **EAP-TLS**, you must export the MIC's CA chain and add it to the RADIUS server's trust list.

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



This Manufacturing root CA should be added to the RADIUS server's trust list.

MFG Root CA on User's Radius Server

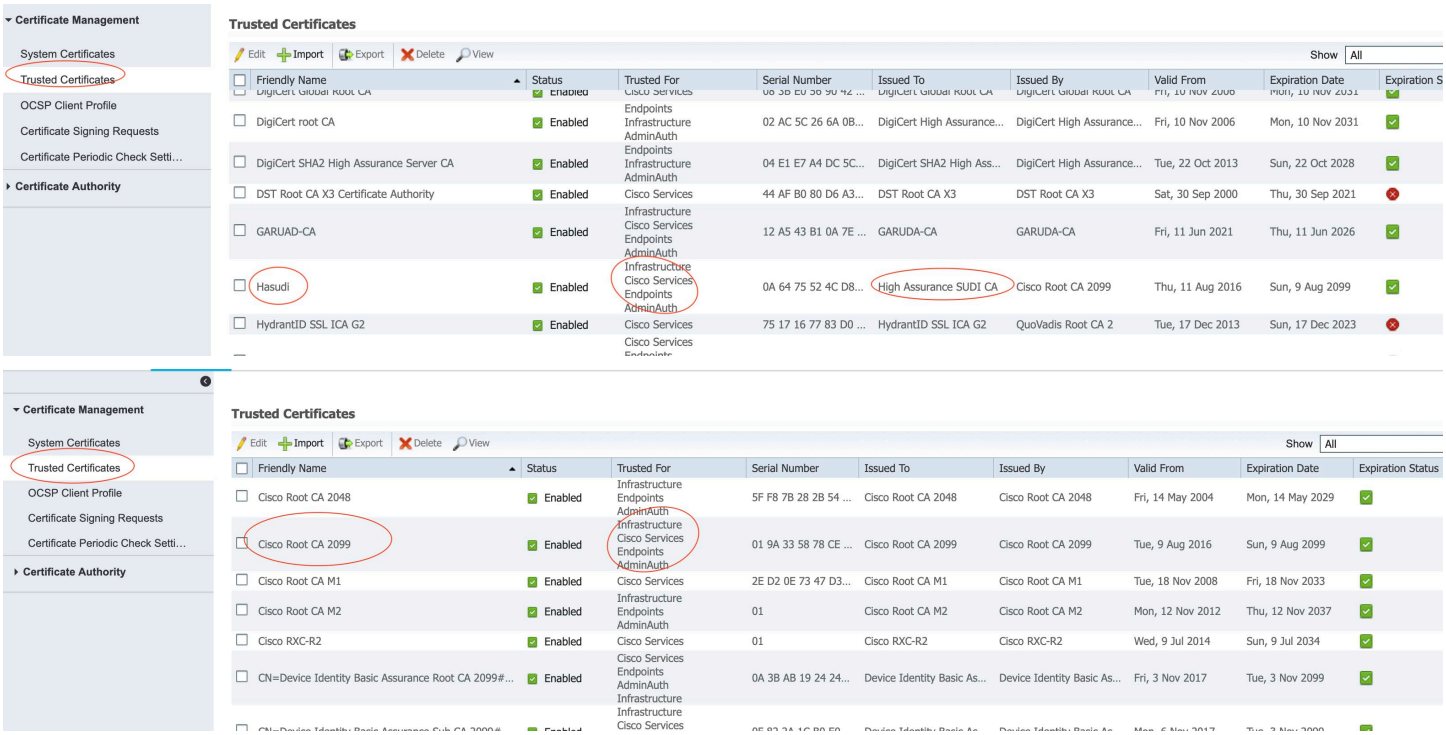
Manufacturing Installed Certificate should be installed and trusted by the end user's RADIUS Server.

1. Download two root CA certs for Cisco Wireless Phone 9821 from the following links.

   https://www.cisco.com/security/pki/certs/hasudi.cer

   https://www.cisco.com/security/pki/certs/crca2099.cer

2. Import these two certificates into the user's RADIUS server, such as the Cisco Identity Services Engine (ISE).
3. Apply the correct privilege to these two trusted certs. Pay attention to the red circles highlighted in the following screenshots.



User Installed Certificate

Follow these steps to manually install a user certificate for **EAP-TLS**:

1. Select **Install** for **User Installed** on the **Certificates** page.
2. Select **Browse** to point to the user certificate in **PKCS #12** format (.p12 or .pfx).
3. Enter the **Extract password**, and then select **Upload**.

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



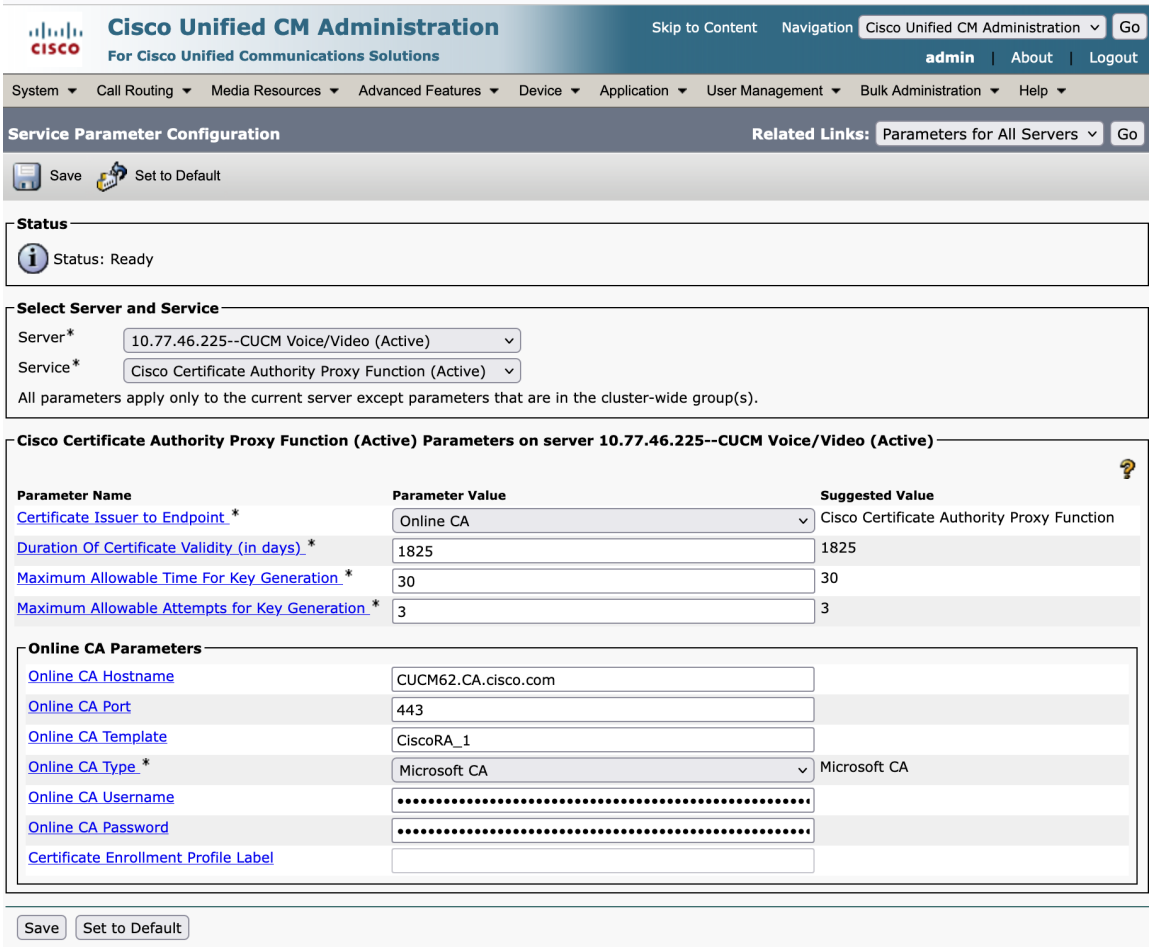
4. Restart Cisco Wireless Phone 9821 after all certificates are installed.

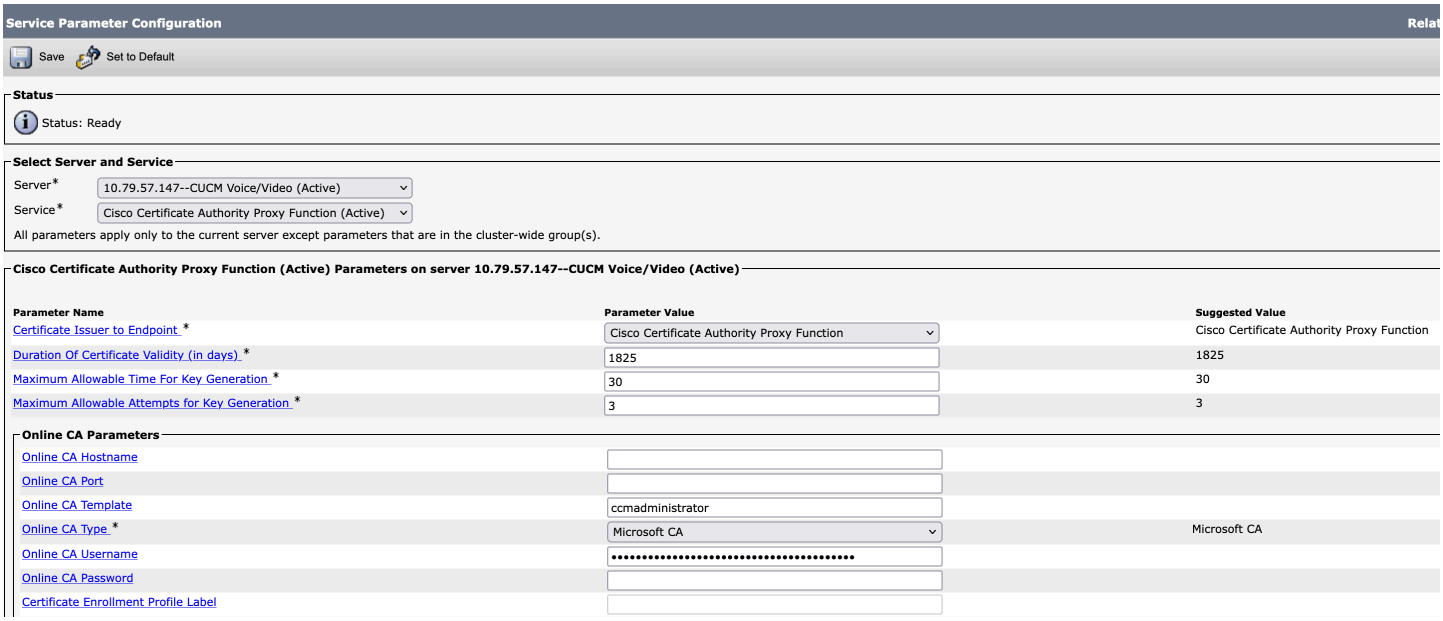


LSC Certificate

Follow these steps to enable CAPF service on CUCM:

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



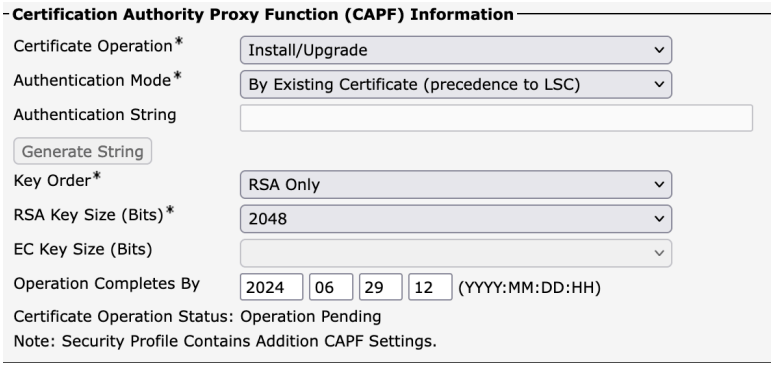


Follow these steps to active or restart the CAPF server:

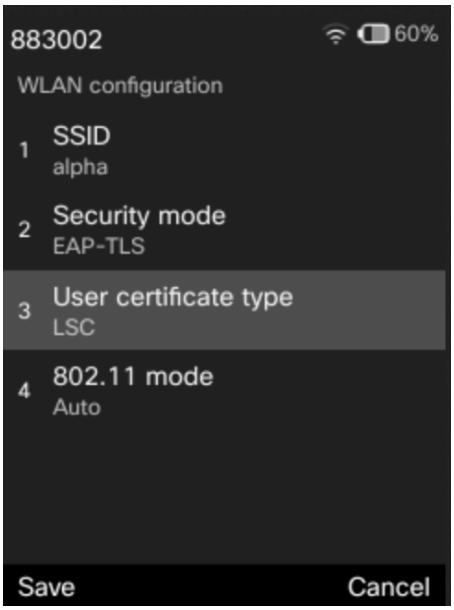
1. Login to **Cisco Unified Serviceability**.
2. Select **Tools** > **Service Activation**.
3. Select your CUCM server.
4. Ensure that **Cisco Certificate Authority Proxy Function** is **Activated**.
5. Select **Tools** > **Control center Feature Service**.
6. Select and restart **Cisco Certificate Authority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

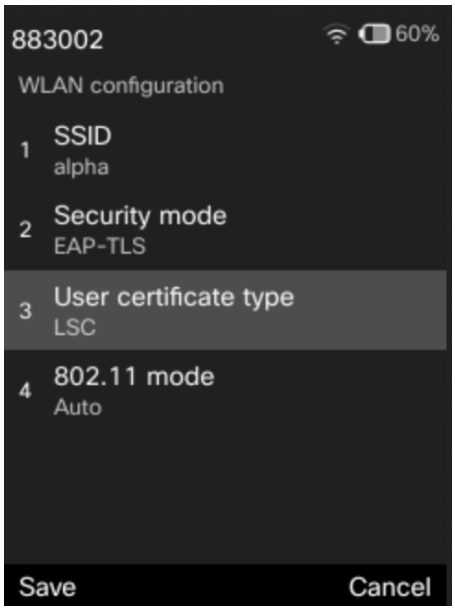
Follow these steps to install LSC certificate on Cisco Wireless Phone 9821:

1. Login to **Cisco Unified CM Administration**.
2. Select **Device** > **Phone**.
3. Click **Find** to display the list of configured phones, and then choose the phone to which you want to install LSC certificate.
4. Select **Install/Upgrade** in **Certificate Operation**.



5. Select **Save** and **Apply**.
   The phone will install the LSC and then reboot. You can check the phone **LSC** status by accessing **Settings** > **Wi-Fi** > **Profile** > **WLAN Configuration** > **Security mode**.





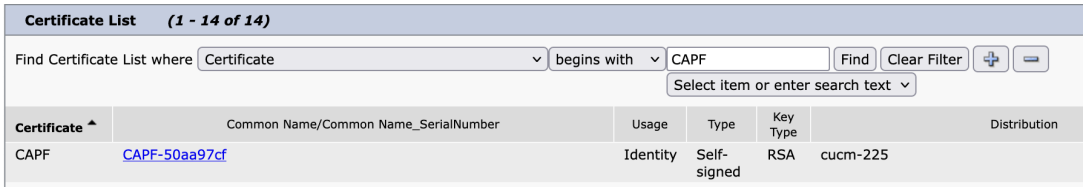
Import CAPF CA to ISE

Follow these steps:

1. Export LSC CA cert from CUCM.

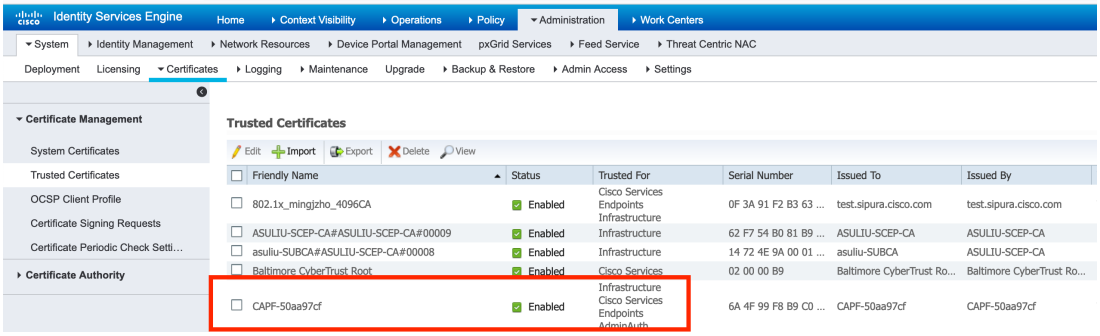
   If **Online** CAPF is used, users should ask for external CA cert from admin. If **build-in** CAPF is used, users can download CA cert from CUCM.

   a) Login to **Cisco Unified OS Administration**.
   b) Select **Security** > **Certificate Management**.
   c) Download the CAPF Identity certificate.



2. Import LSC certificate to trust list.

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

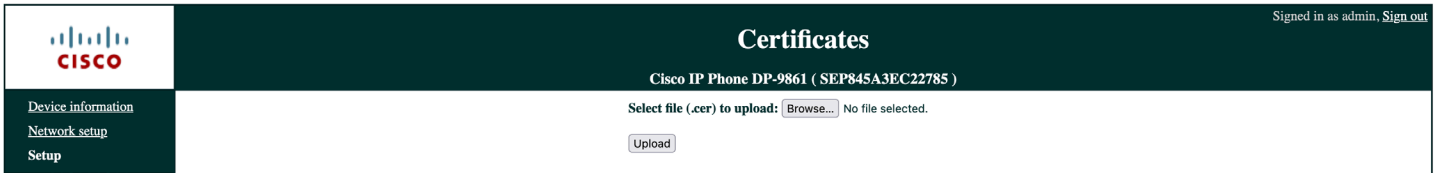


Server Certificate

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, skip this step.

To manually install a server certificate, select **Install** for **Authentication Server CA** on the **Certificates** web page.

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

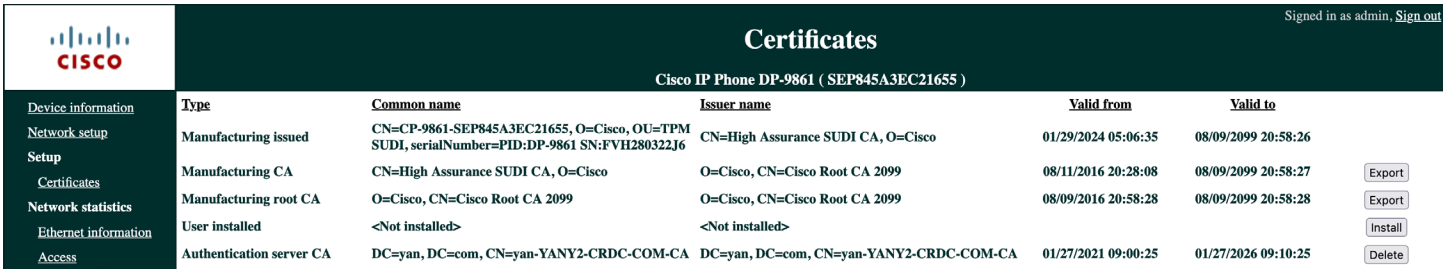


Restart Cisco Wireless Phone 9821 after all certificates are installed.

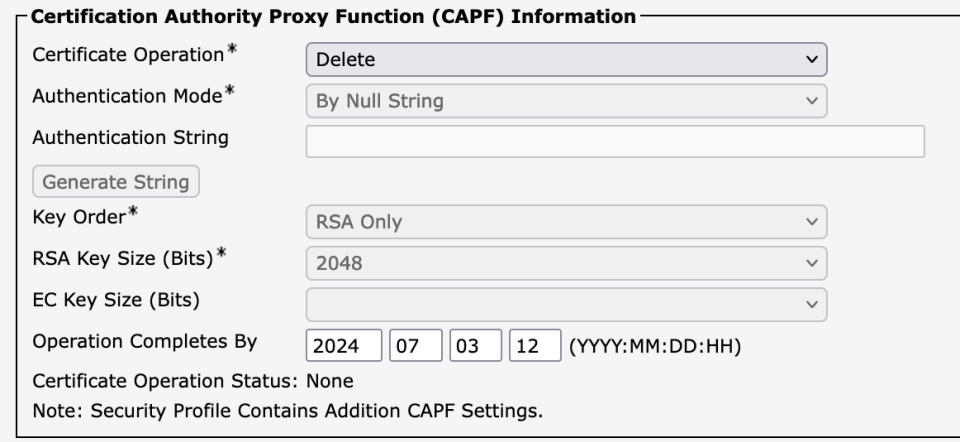


Certificate Removal

You can remove the **User Installed** certificates from the phone administration web page. To remove a certificate, select **Delete** for the corresponding certificate, then restart the phone once a certificate has been removed.

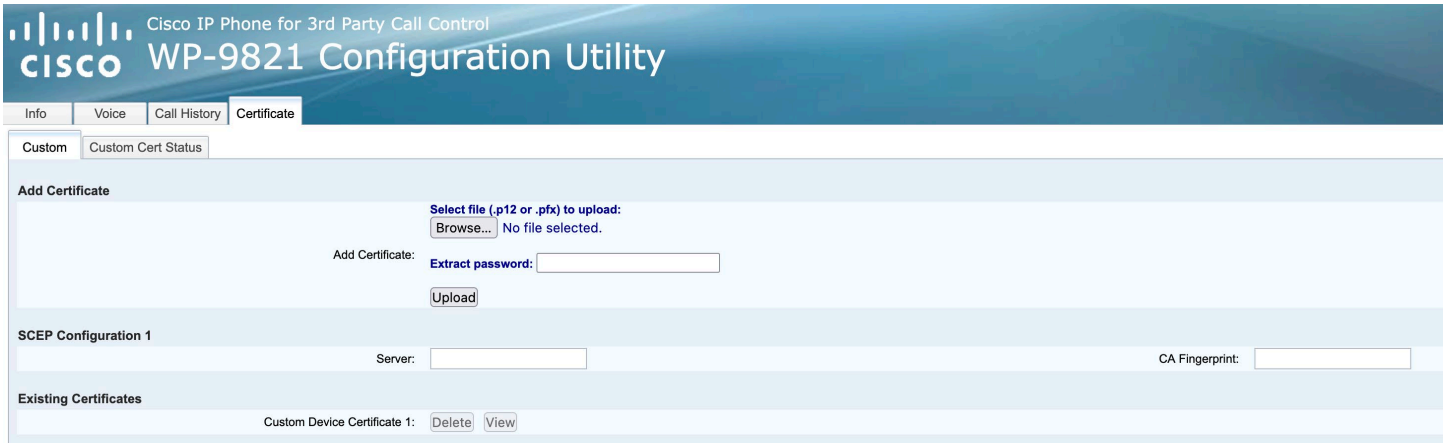


You can remove the LSC certificate in Cisco Unified Communications Manager Administration. Select **Save** and **Apply**.



CDC cert installation (Webex Calling)

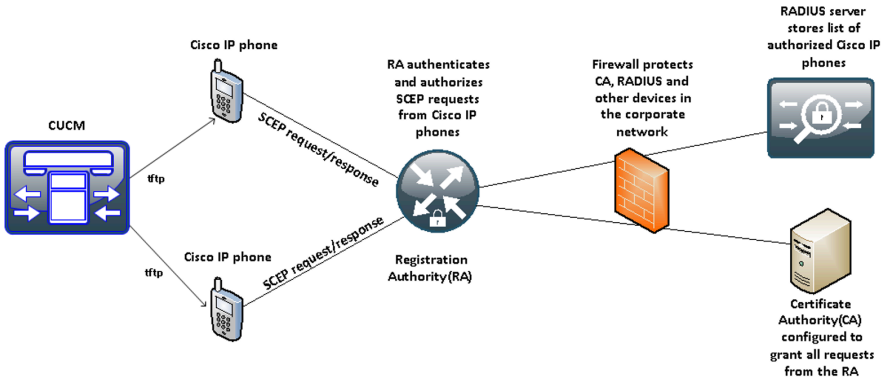
On the phone administration web page, an administrator can install a cert manually or provide SCEP parameters to trigger the phone to fetch the cert from server. We have another separate doc describes the CDC process.



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. Refer to the following topology as an example.



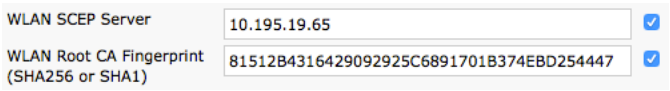
Ensure that the same CA chain is used for issuing certificates to the phones as well as for the RADIUS servers. Otherwise, server validation could fail.

For initial certificate enrollment via SCEP, the Cisco Wireless Phone 9821 needs to be connected to a network which has connectivity to the Cisco Unified Communications Manager.

Cisco Wireless Phone 9821 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 issues the certificates. If the issuing CA in which the SCEP RA is enrolled to is a subordinate CA, then enter its fingerprint and not the fingerprint of the root CA. The defined fingerprint is used to validate the received certificate.

  Removing these parameters will disable SCEP.



Cisco Wireless Phone 9821 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 enrollment 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.

Cisco Wireless Phone 9821 will periodically check the user and server certificate expiration periods.

Certificate renewal will occur every 24 hours until success 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 enrollment 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.

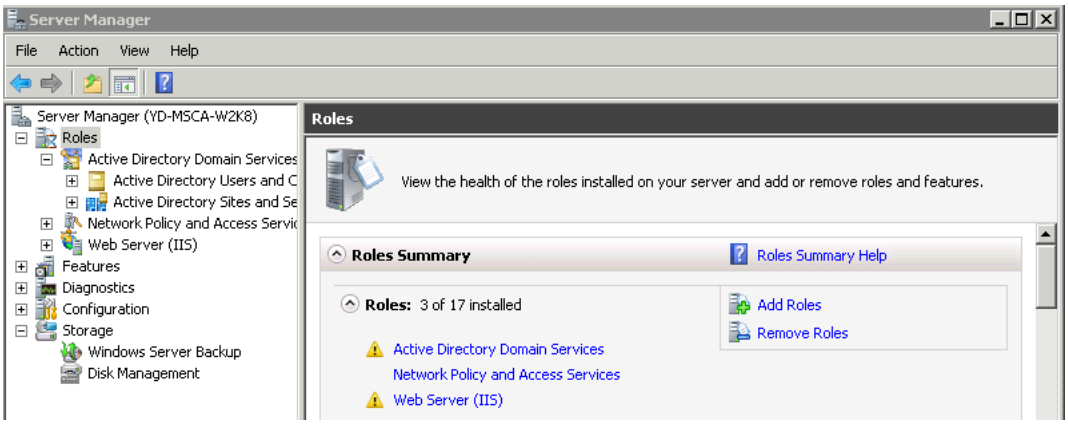
If **WLAN SCEP Server** or **WLAN Root CA Fingerprint (SHA256 or SHA1)** has been modified, then the Cisco Wireless Phone 9821 will attempt to update the CA and user certs immediately.

Certificate Authority (CA) Configuration

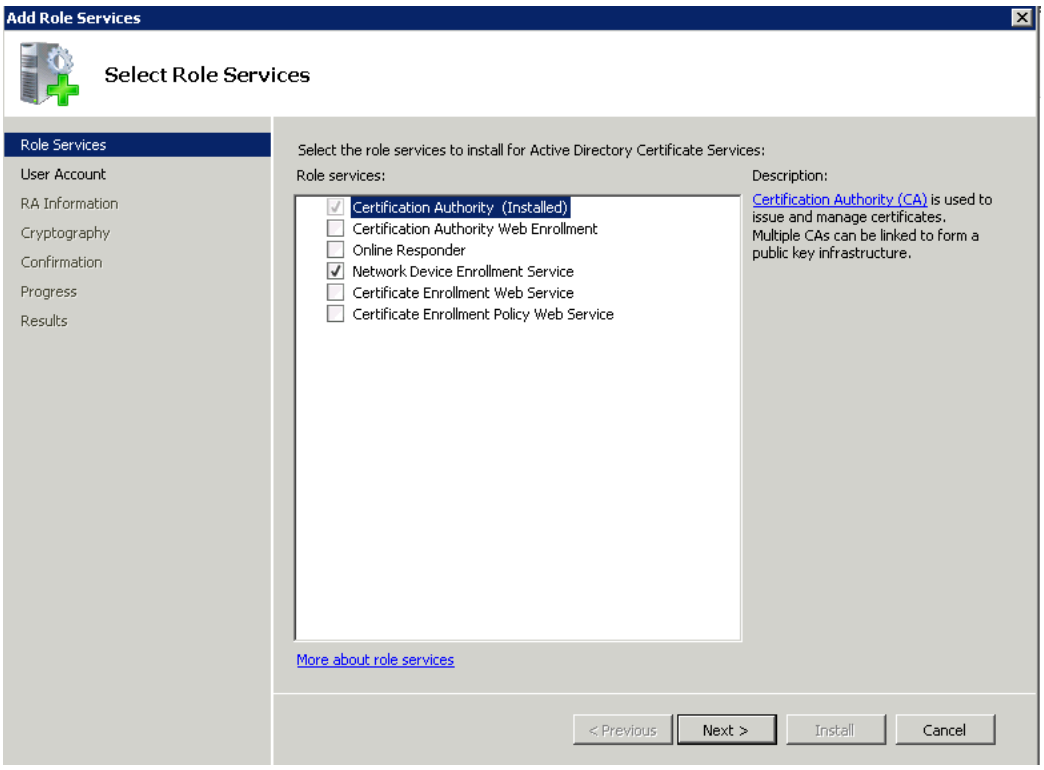
It is recommended to use Microsoft® Certificate Authority (CA) servers.

Use the following guidelines to configure the Microsoft CA.

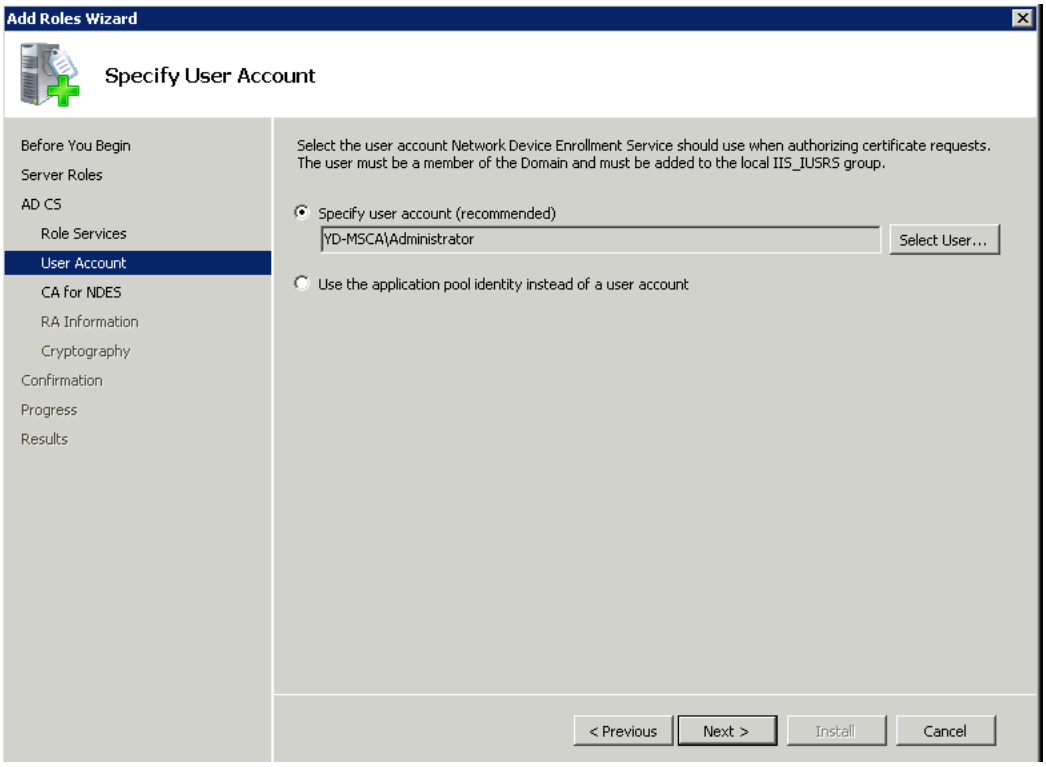
1. Create Certificate Authority and Active Directory Domain Service on a Microsoft Windows server.
2. Enable Network Device Enrollment Service.
3. Make **Administrator** a member of **IIS_IUSERS** group by going to **MemberOf** tab of user property screen.
4. Launch **Server Manager**, and then click **Add roles**.



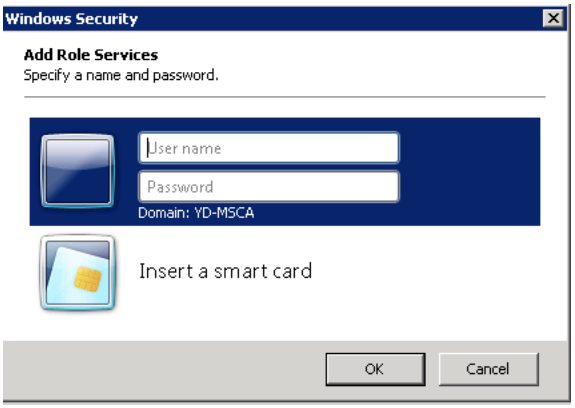
5. On the **Select Server Role** page, select the **Active Directory Certificate Services** role, and then click **Next**.
6. On the **Select Role Services** page in the **Add Roles Services** Wizard, the default service selected is **Certification Authority**, clear the check box.
7. Select the **Network Device Enrollment Service** check box, and then click **Next**.



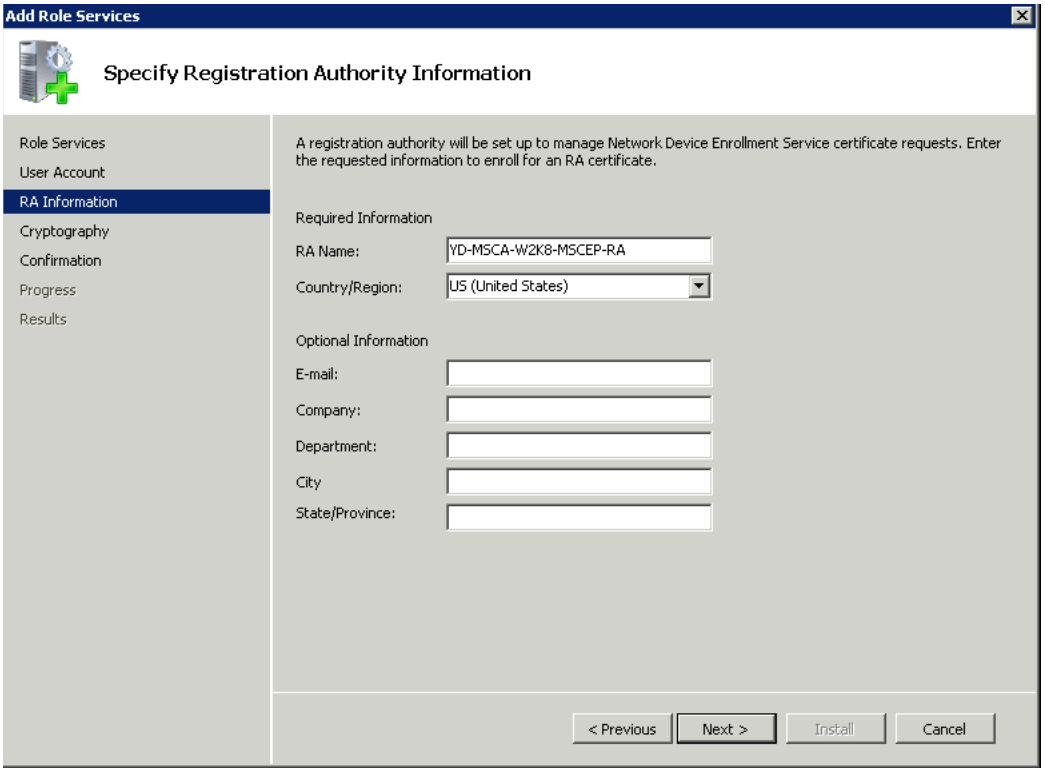
8. The wizard will detect whether all the required dependencies are installed. If any dependencies are missing, you will be prompted with a dialog box explaining what is missing and requesting your permission to install the dependencies. Click **Yes** to continue the installation.
9. Select **User Account** under **Role Services** and then click **Select User**….



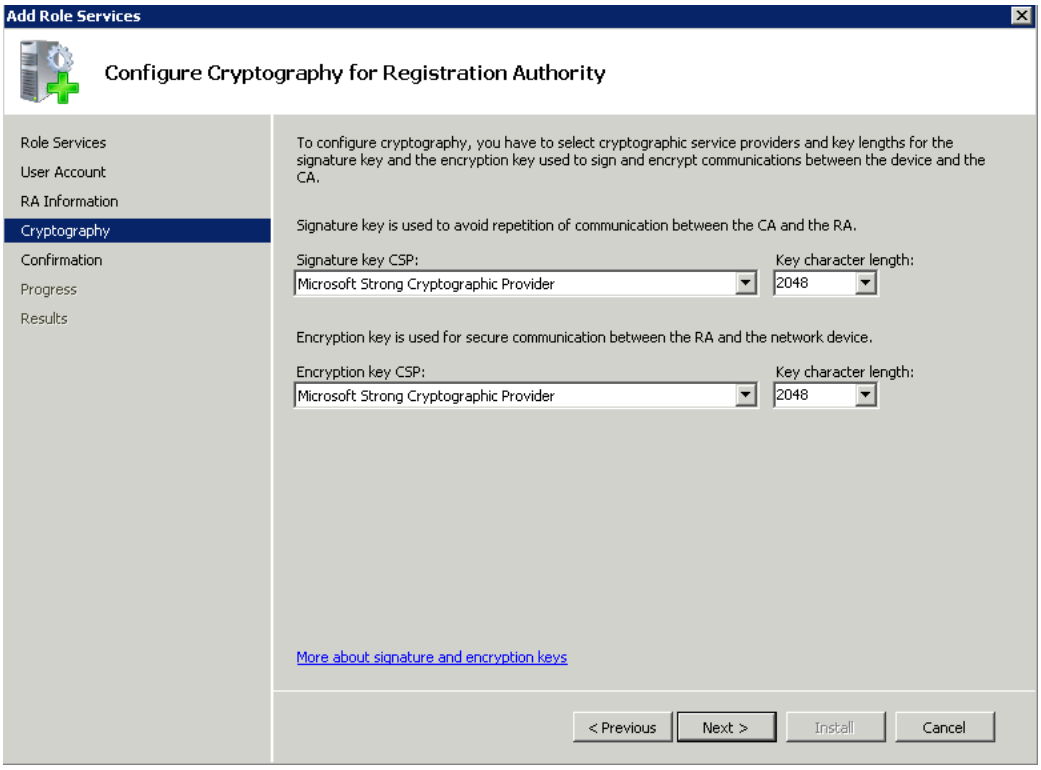
10. Enter **Administrator** as the user name, then enter the password.



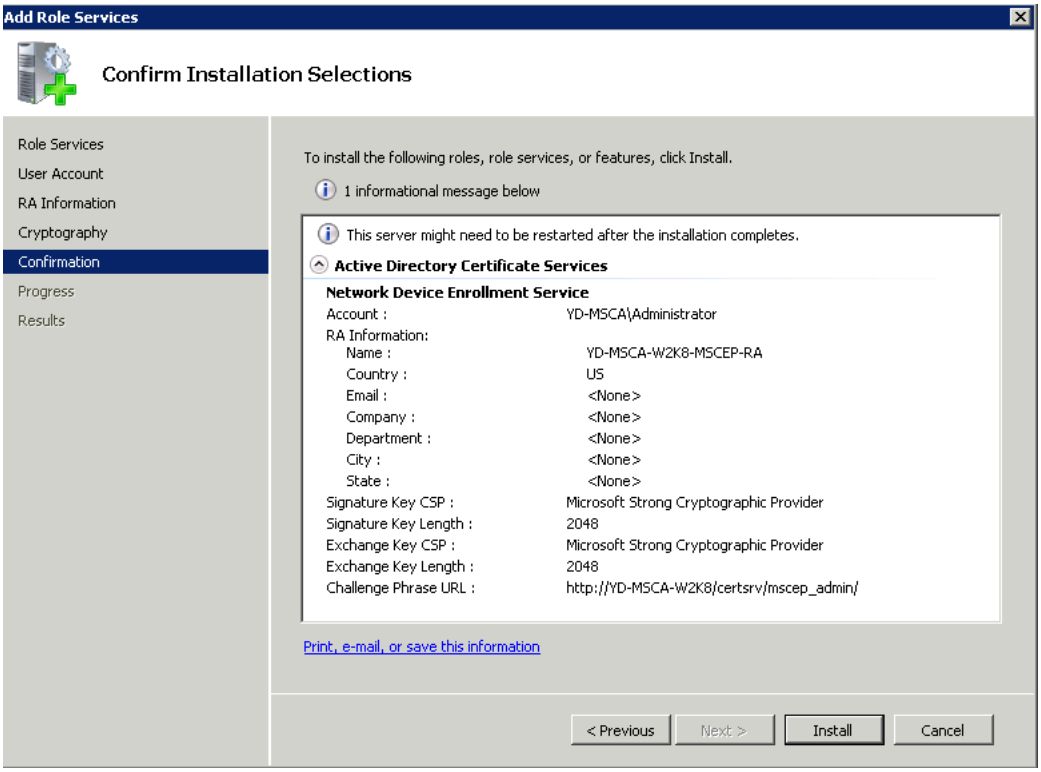
11. Enter the Registration Authority information, and then click **Next**.



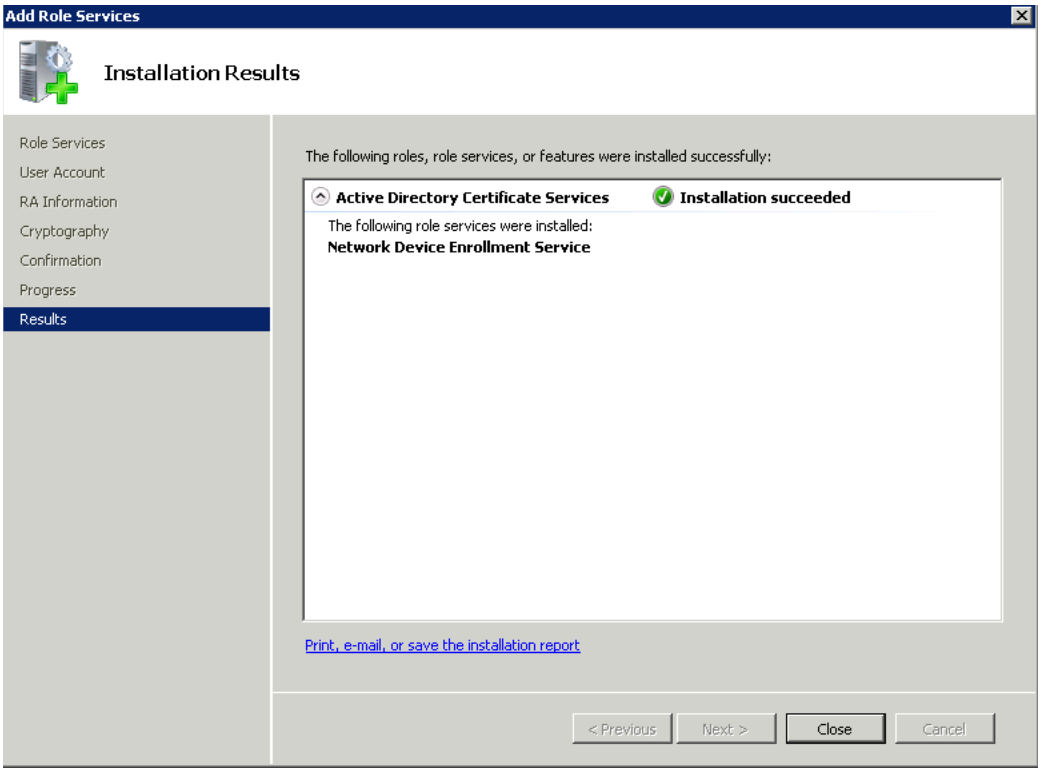
12. Select **Microsoft Strong Cryptographic Provider** for **Signature Key CSP** and **Encryption key CSP**.
13. Select **2048** for **Key character length**, and then click **Next**.



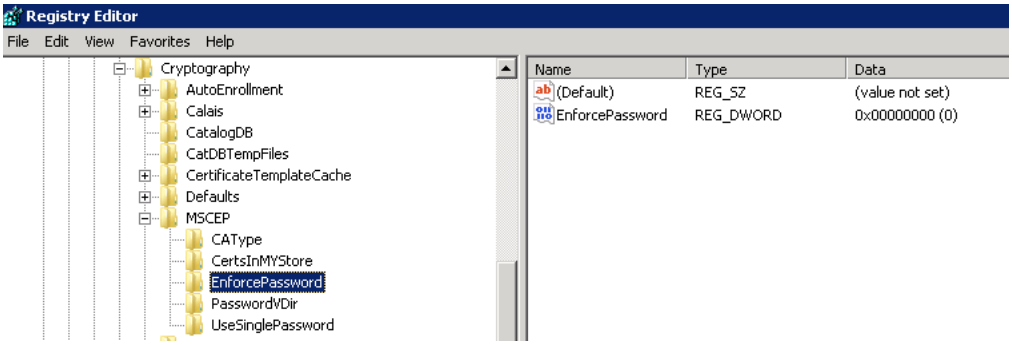
14. Click **Install**.



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

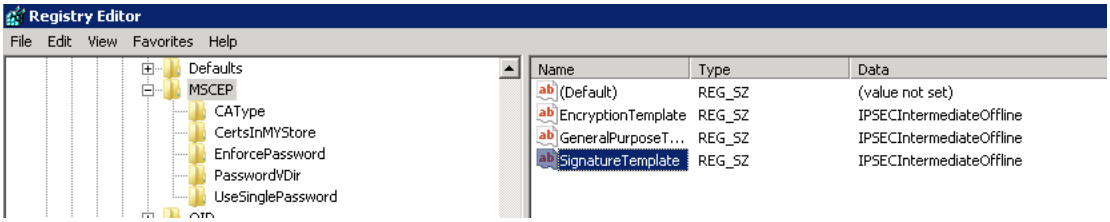


15. In **Regirstry Editor**, browse to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Cryptography** > **MSCEP** > **EnforcePassword**. Disable SCEP enrollment challenge password requirement by setting **EnforcePassword** to **0**.



16. Specify certificate templates for SCEP.

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

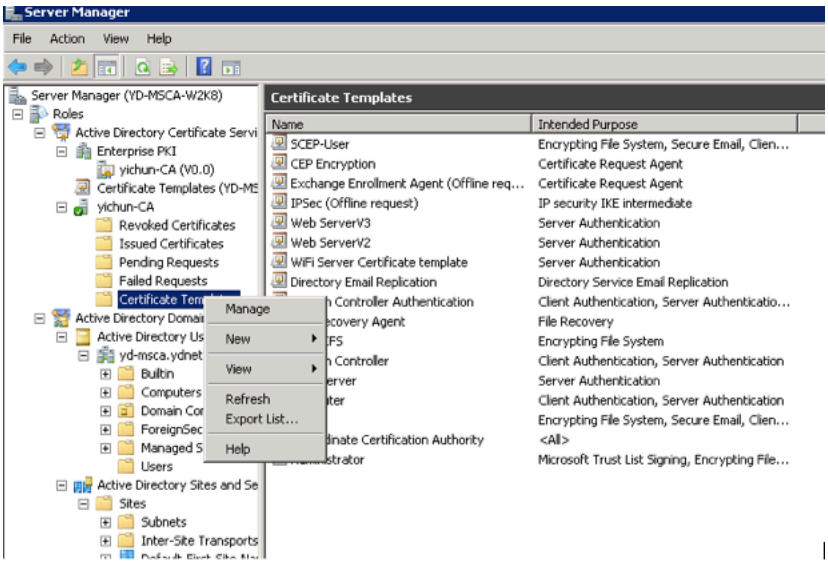


    Typically the RA will have a longer period (same as that of the CA certificate). The default template used for RA to be enrolled to the SCP server is **IPSECIntermediateOffline** as highlighted in the

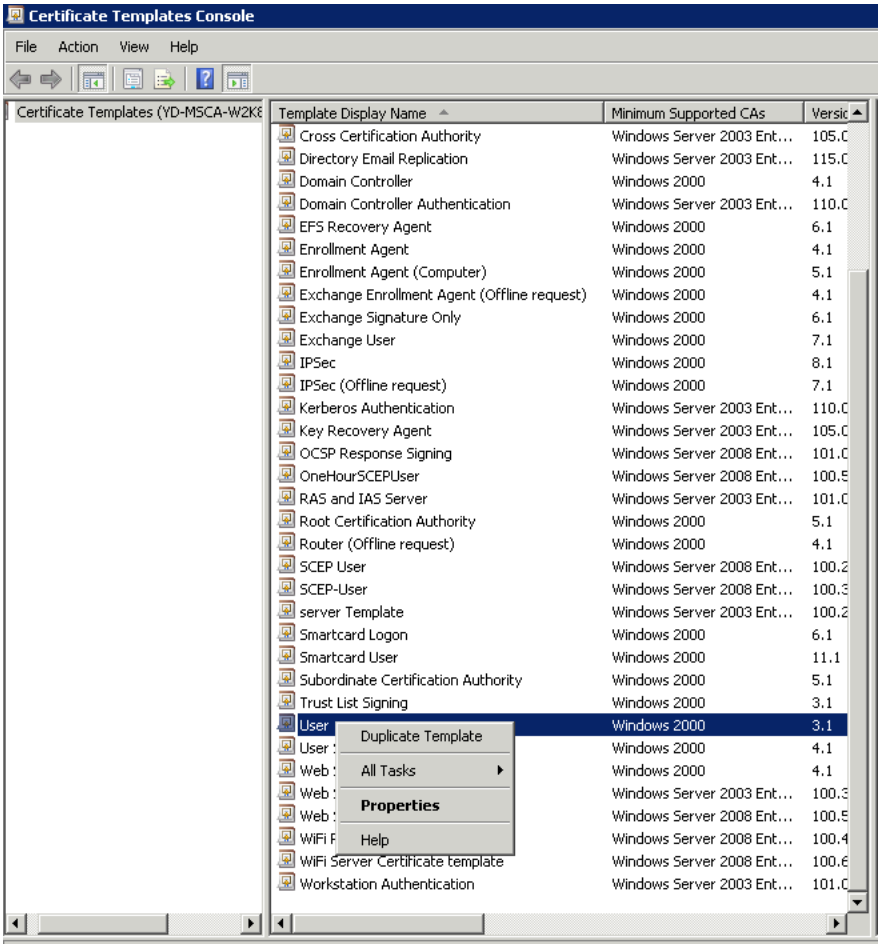
screenshot above. Make sure a correct template is set to the above registries before enrolling Cisco RA to the SCEP server.

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).

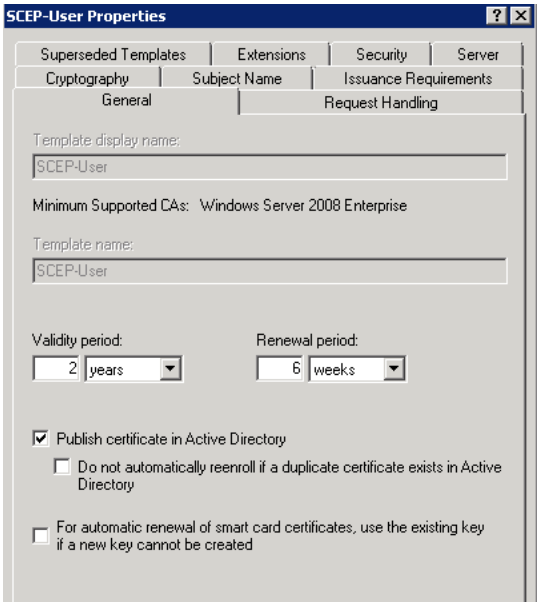
17. Right-click **Certificate Templates** and then select **Manage**.



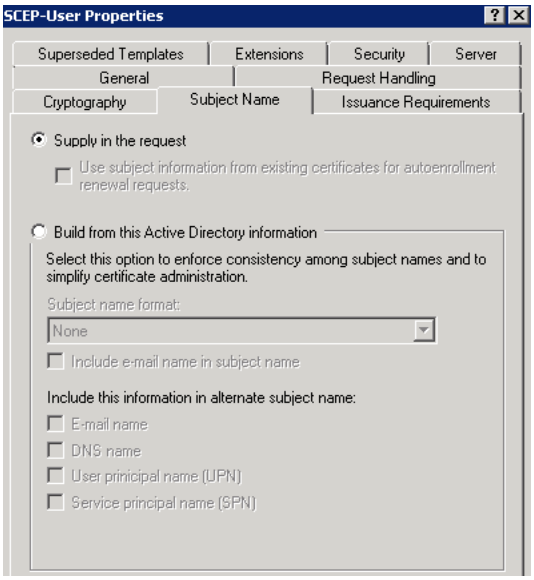
18. Right-click **User template** and then select **Duplicate Template**.
19. Select **Windows Server 2003 2008 Template**.
20. Under the **General** tab, change template name and validity period.
21. On the **Extensions** tab, ensure the following:
    - **Client Authentication** is set as one of the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



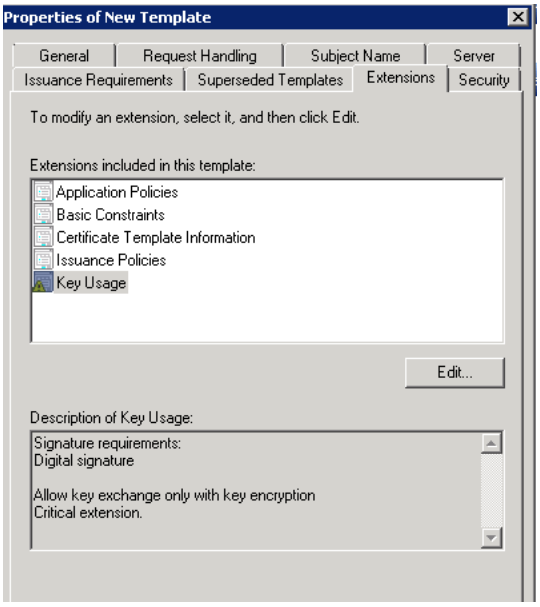
22. Configure the **Validity Period** on the **General** tab as necessary.



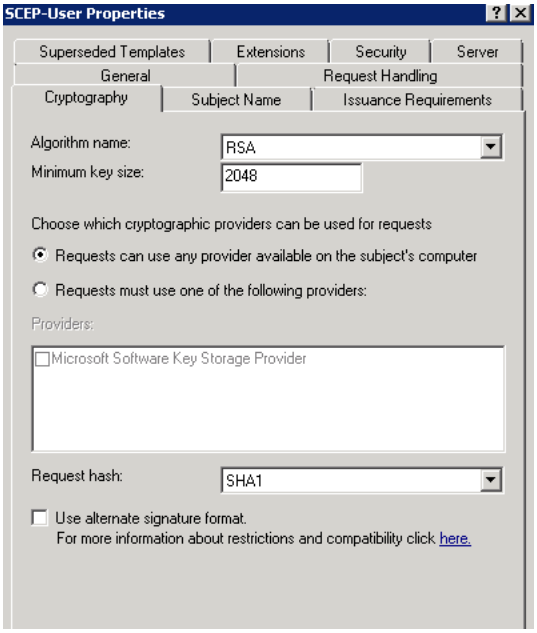
23. Configure **Subject Name** tab as shown below.



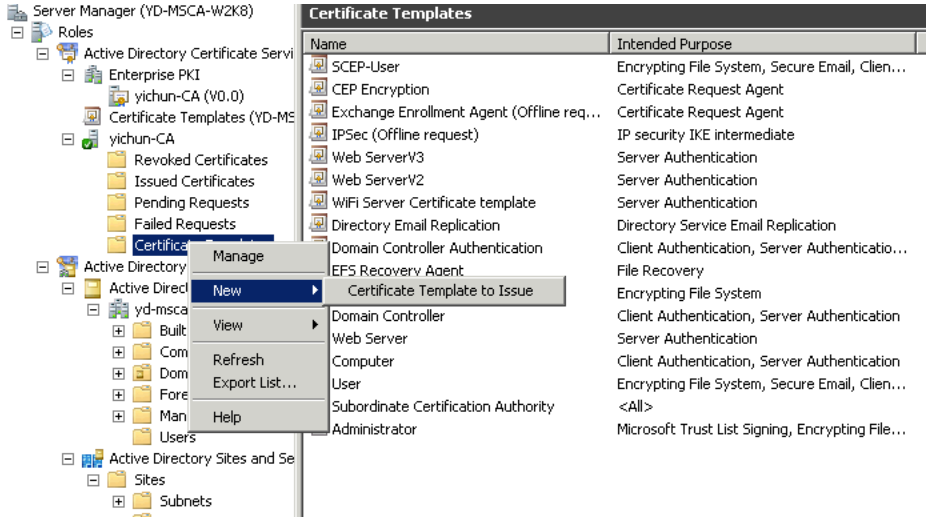
24. Configure the **Extensions** tab as shown below.



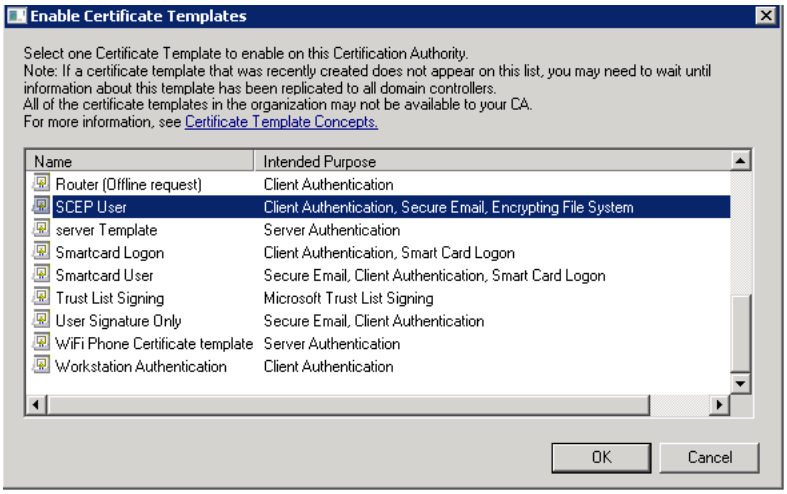
25. Configure **Algorithm Name**, **Minimum Key Size**, and **Request Hash** as necessary on the **Cryptography** tab.



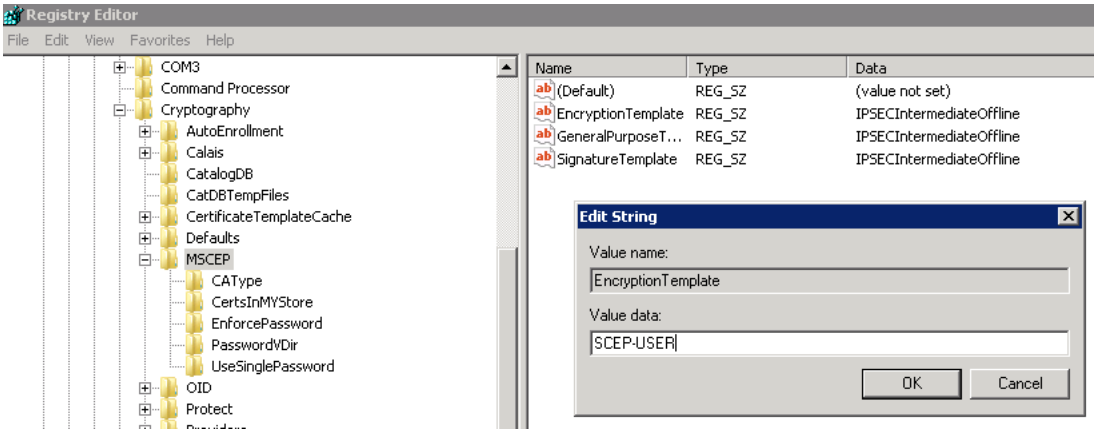
26. Right-click **Certificate Templates** then select **New** > **Certificate Template to Issue** to enable the newly created template.



27. Select the **SCEP User** template.



28. In **Registry Editor**, associate the newly created template to SCEP.

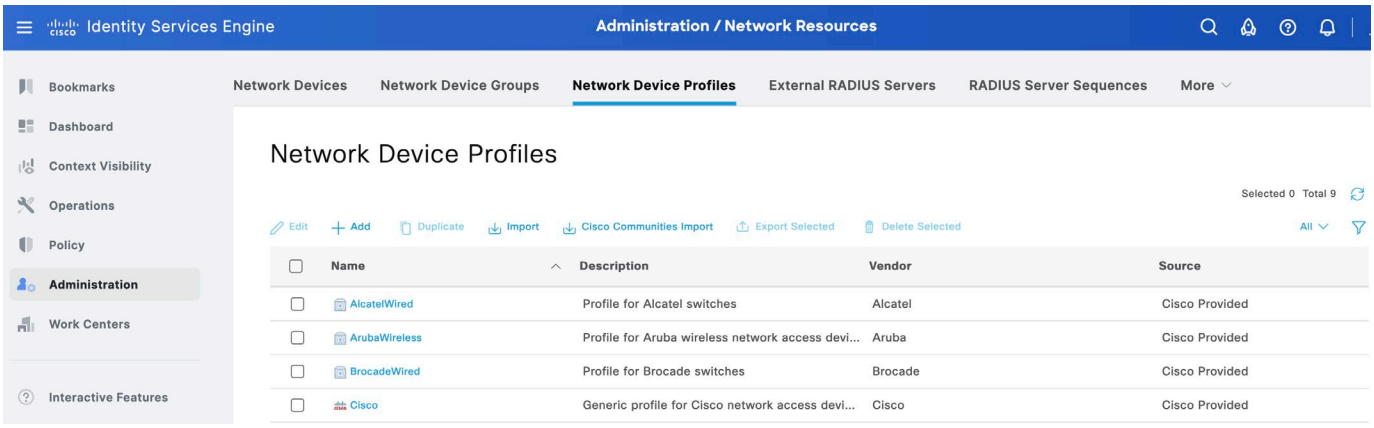


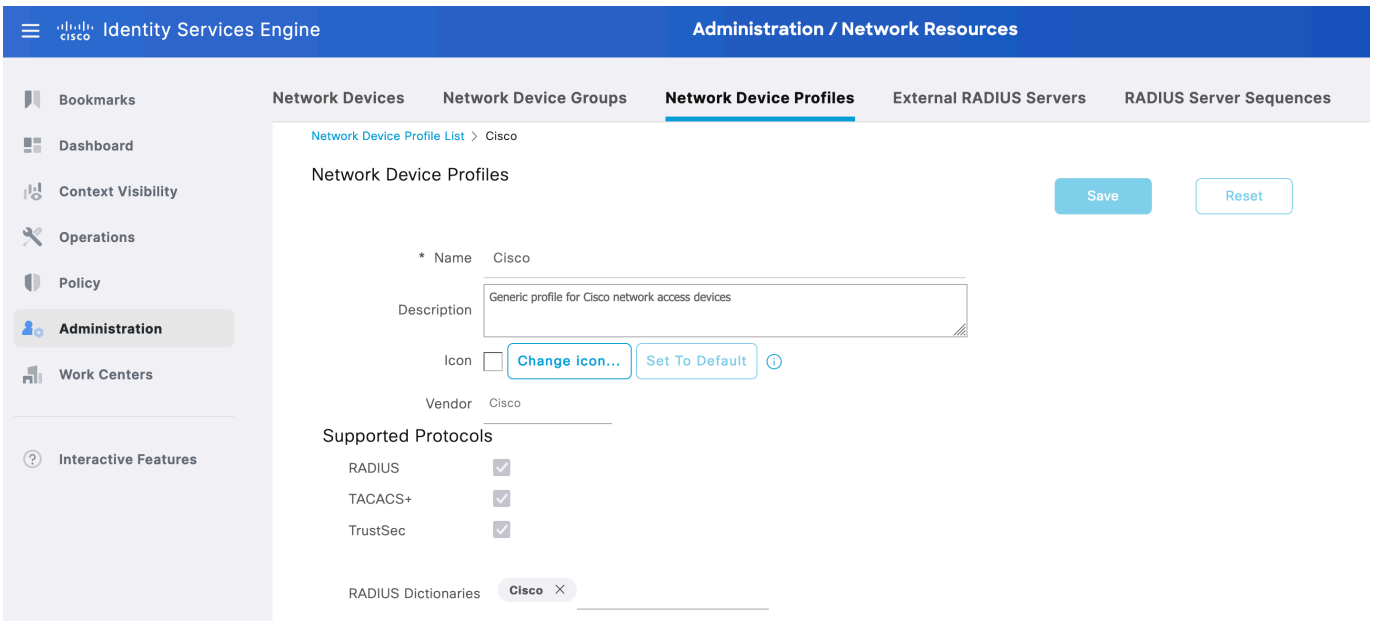
29. Go to **IIS** > **Application Pools** to restart the SCEP service for the new template to take effect.

RADIUS Configuration

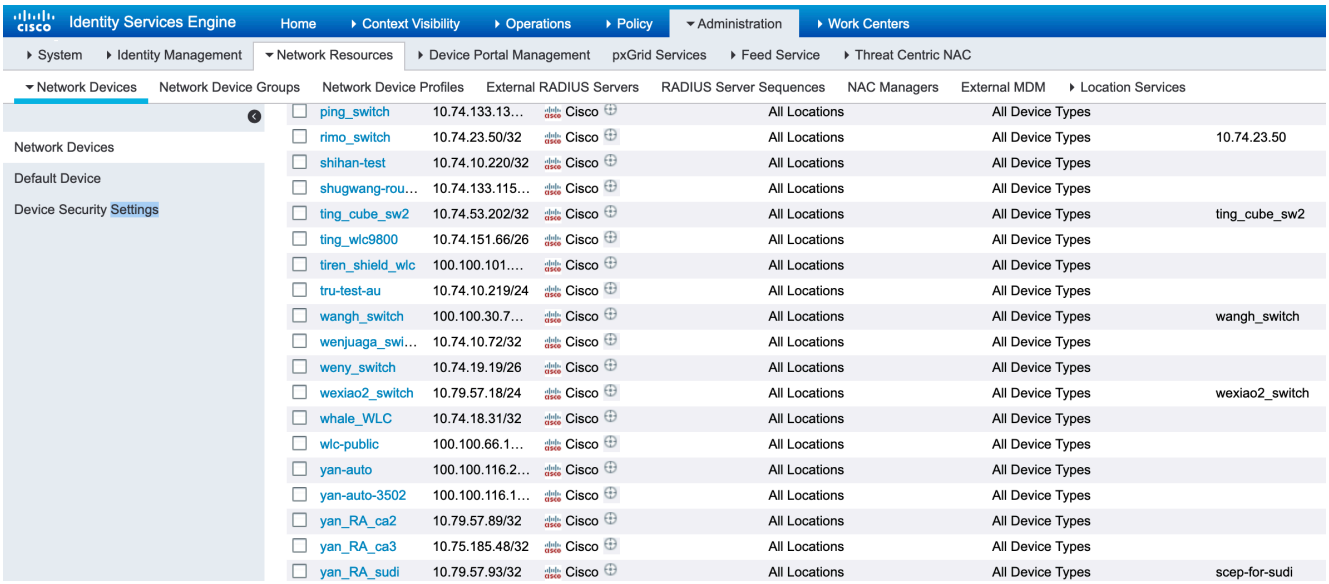
Use the following guidelines to configure the RADIUS server. ISE server plays a role of SCEP device authentication for enrollment, and it can be used for the PKI integration with Cisco IOS RA for SCEP solution.

1. Navigate to **Administration** > **Network Device Profile**s, add a new profile or levering existing profile **Cisco**. When creating a new profile, remember to config **Supported Protocols**, **Authentication/Authorization** and **Permission** properly.

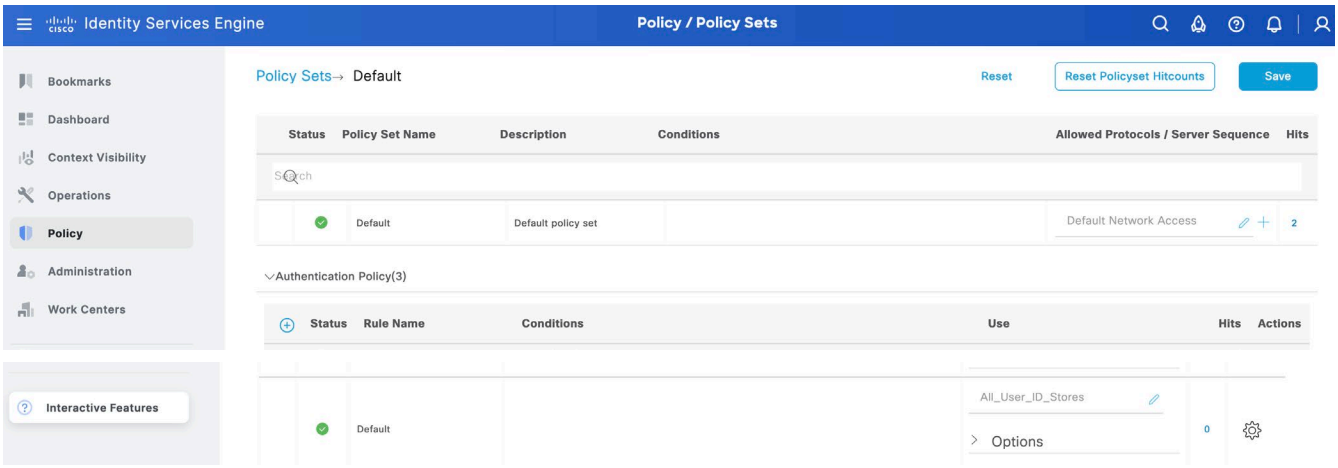




2. Navigate to **Administration** > **Network Resources** > **Network Devices** and then Add a device for Cisco IOS RA. Refer to **yan_RA_sudi** in the following screenshot as an example:



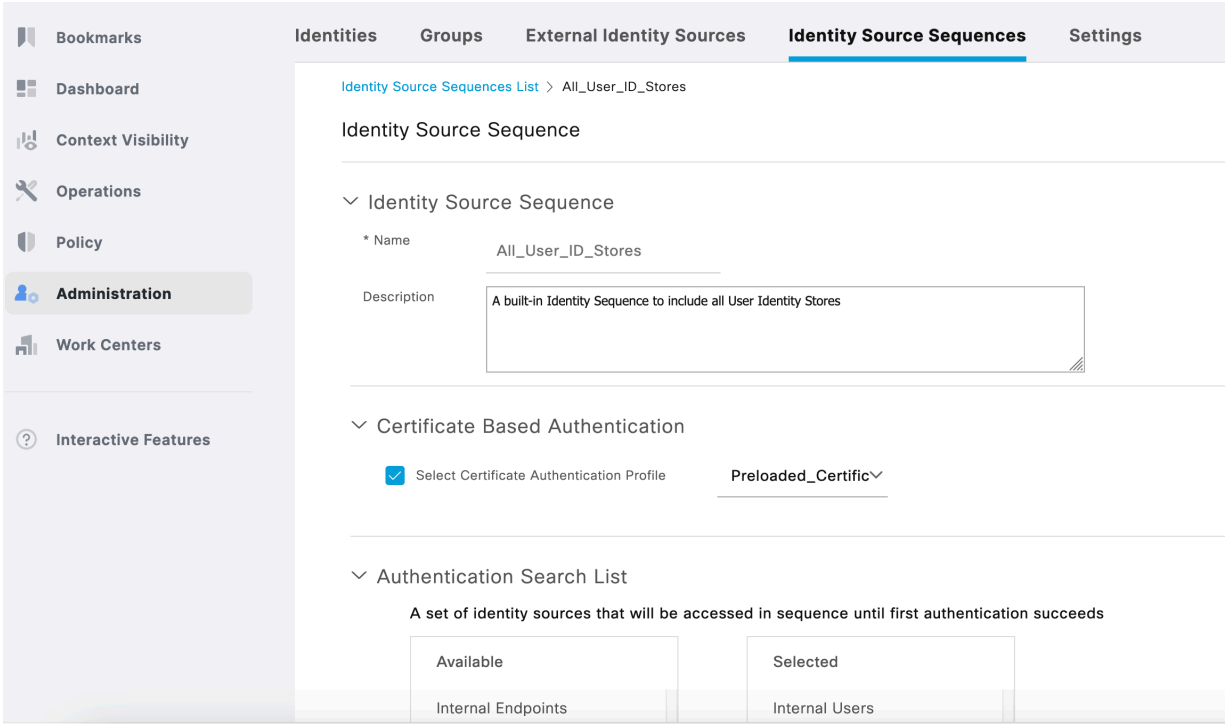
3. Navigate to **Policy** > **Authentication**. Set a **Default** rule to use **Default Network Access** and use **All_Uesr_ID_Stores**.



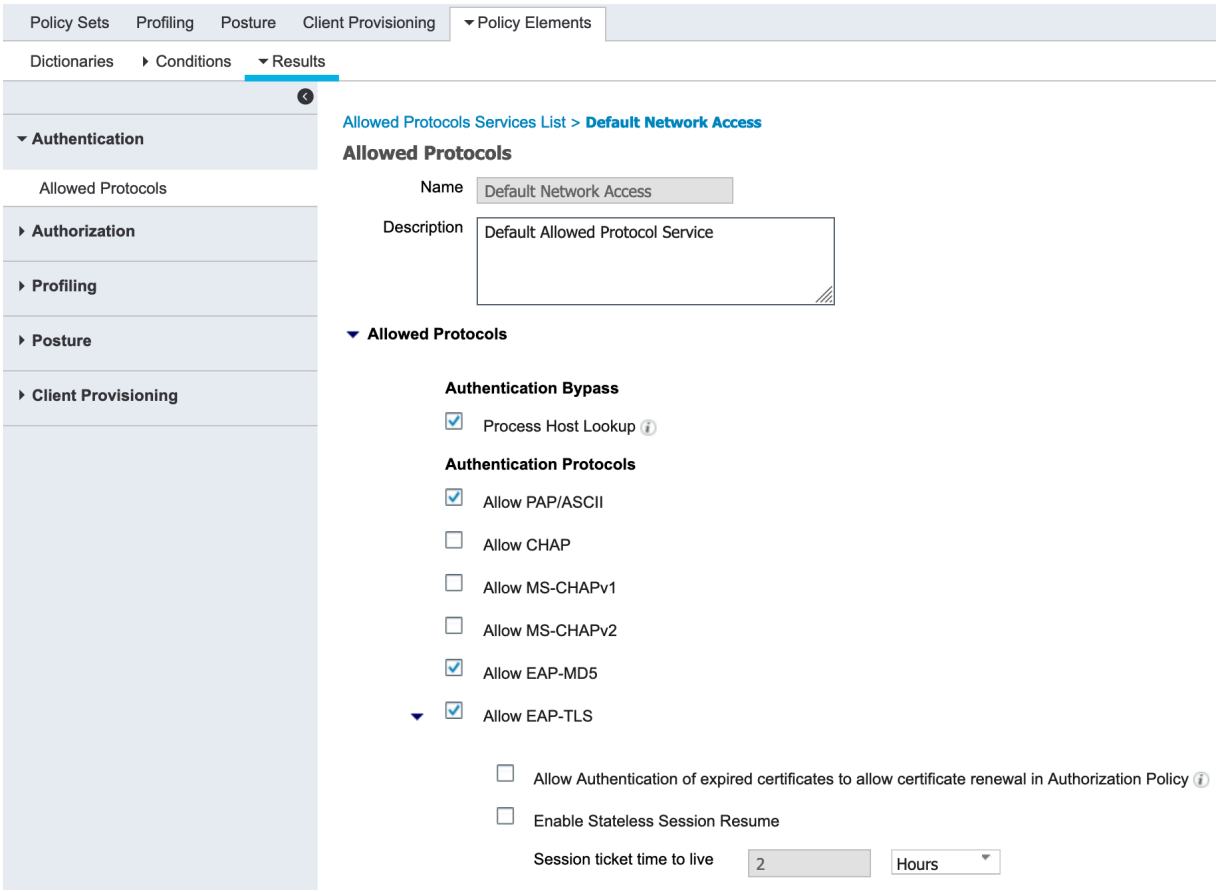
The authentication options can be set to continue for “If authentication failed” or “If user not found” since certificate-based authentication has already been done in Cisco IOS RA.



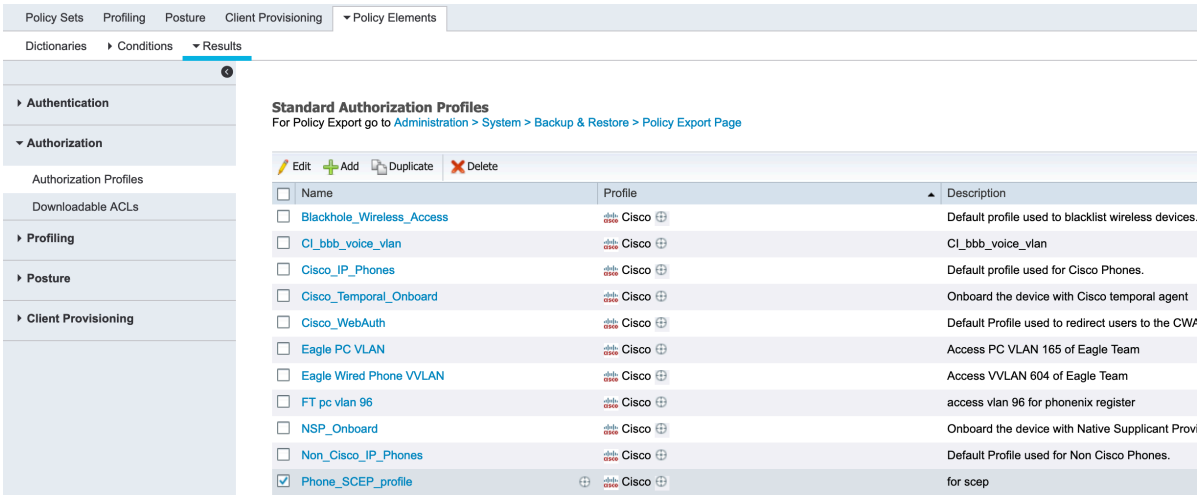
4. Navigate to **Administration** > **Identity Management** > **Identity Source Sequence**.

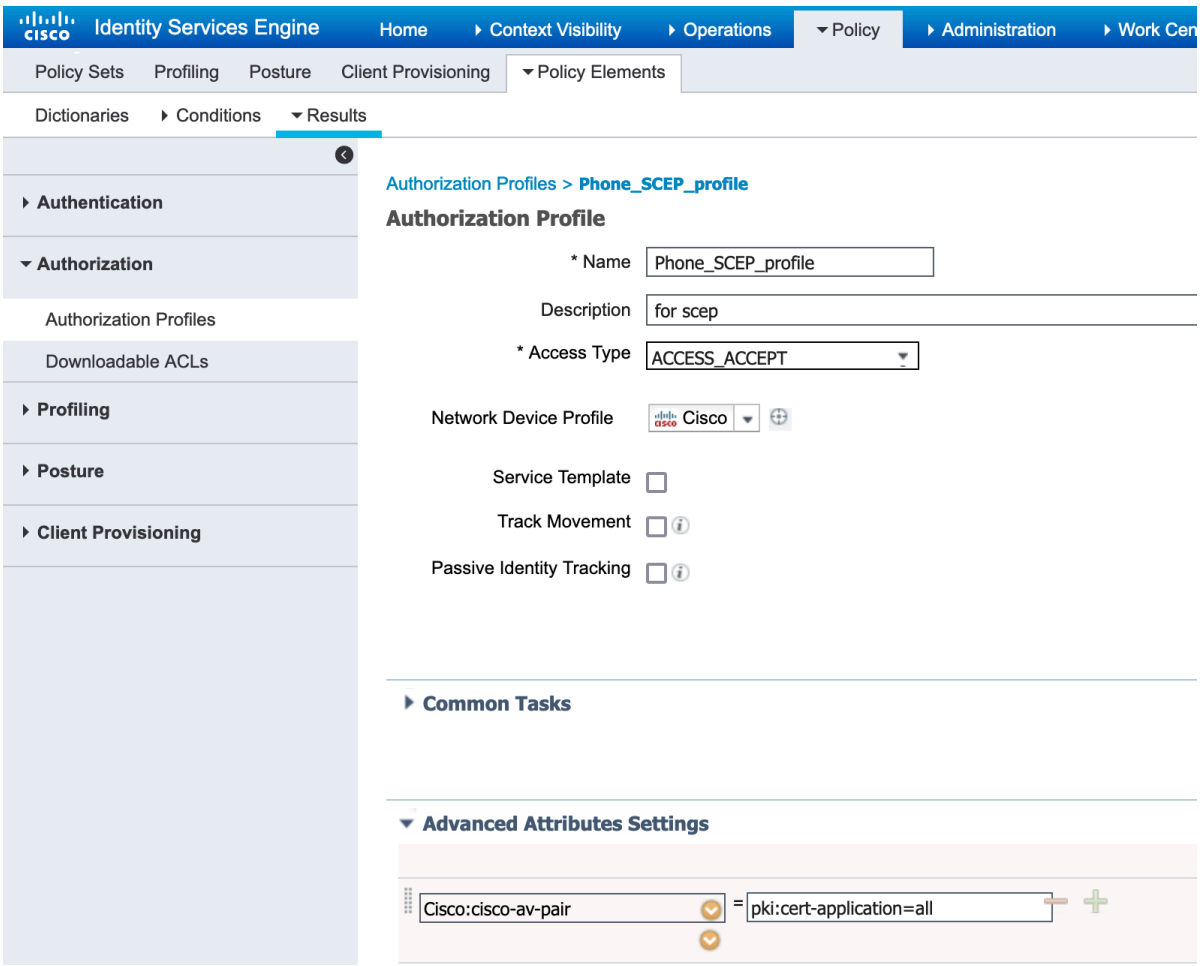


5. Under **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**, edit **Default Network Access** as shown in the following screenshot.

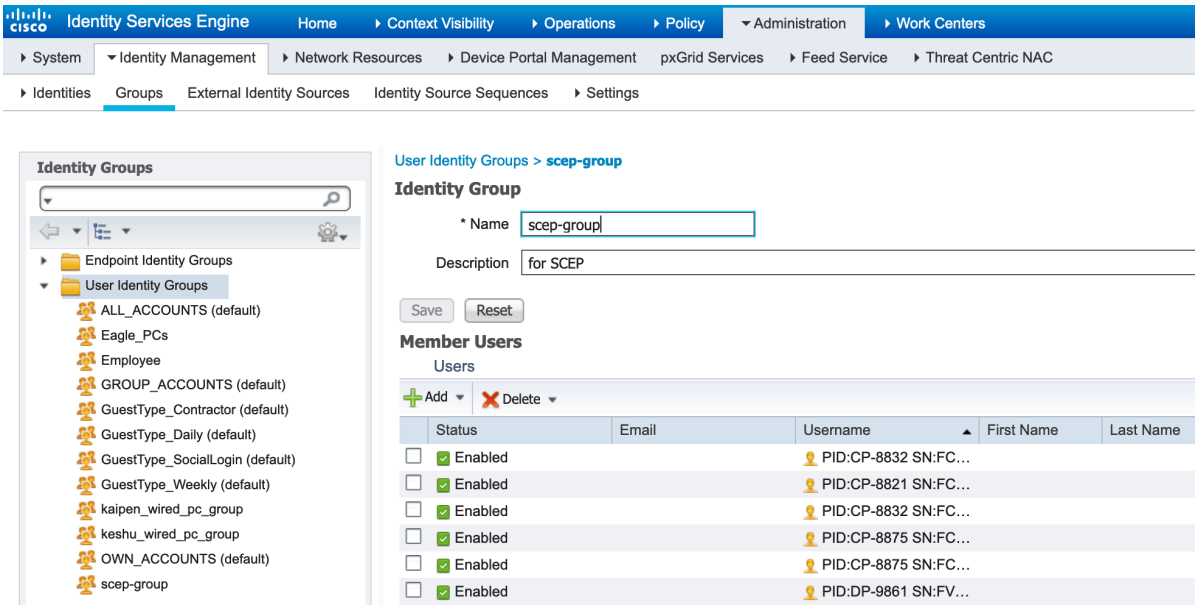


6. Under **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**, add a profile for SCEP. Refer to **Phone_SCEP_profile** in the following screenshot as an example:

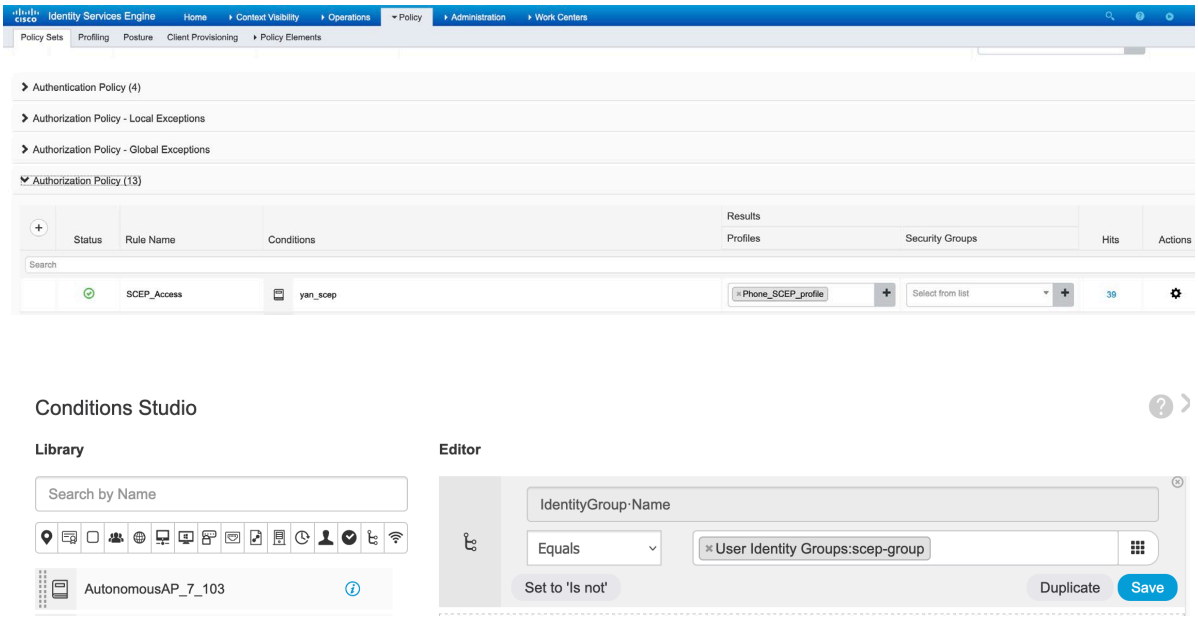




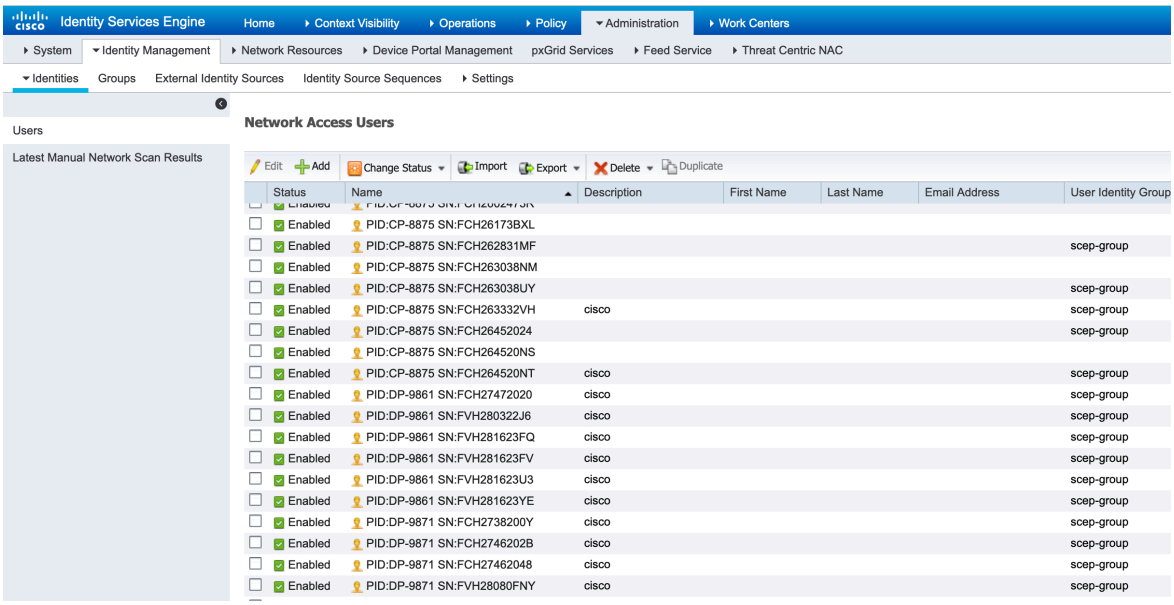
7. Navigate to **Administration** > **Identity Management** > **Group** > **User Identity Groups** and then add a user group for SCEP. Refer to **scep-group** in the following screenshot as an example:

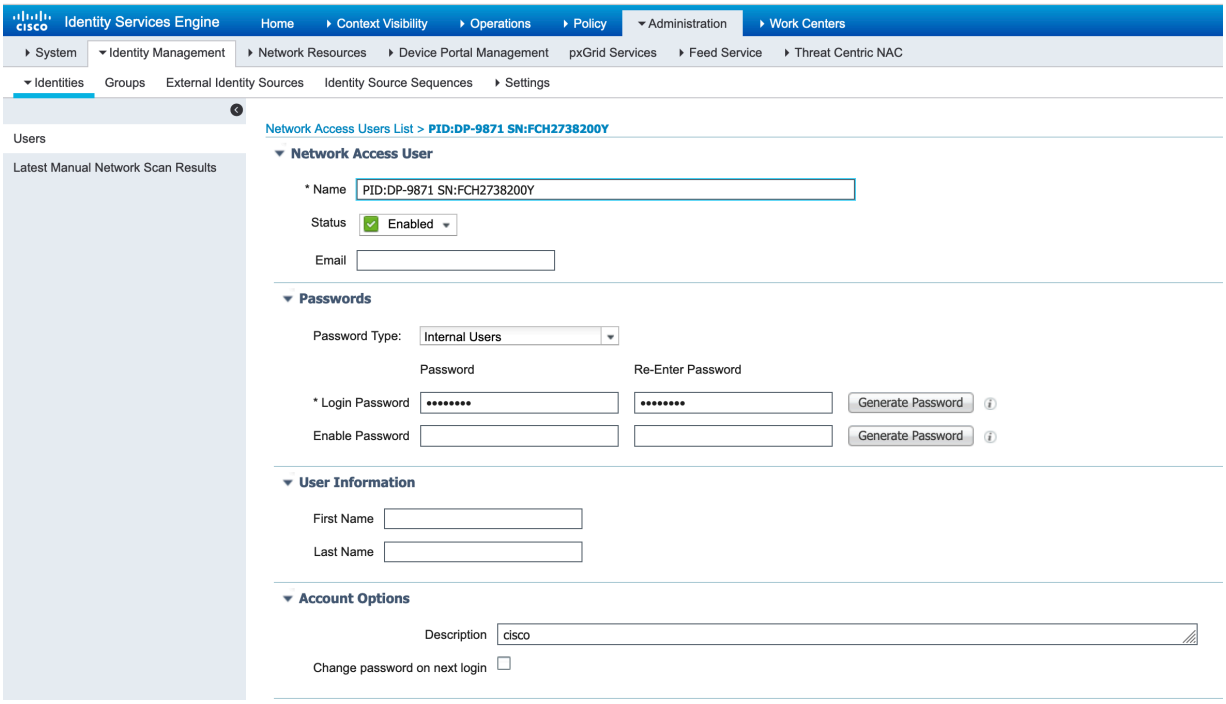


8. Navigate to **Policy** > **Authorization**, and then add a SCEP authorization policy by clicking the down arrow beside **Edit** of an existing policy and select **Insert new rule above**.



9. Navigate to **Administration** > **Identities** > **Users**, and then create user accounts for Cisco Wireless Phone 9821. The username has the format of **serialNumber** (e.g. PID:WP-9821 SN:FCH27472020).





SCEP RA Configuration

Cisco IOS XE/XR is supported as the SCEP RA.

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

Enable HTTP server on the Cisco IOS router.

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

Configure a RADIUS server for device authentication.

ISR_RA# configure terminal

ISR_RA(config)# radius server MyRadius

ISR_RA(config-radius-server)# address ipv4 10.195.19.63 auth-port 1812 acct-port 1813

ISR_RA(config-radius-server)# key <REMOVED>

ISR_RA(config-radius-server)# exit

ISR_RA(config)# aaa authorization network PhoneList group radius

ISR_RA(config)# exit

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

ISR_RA# configure terminal

ISR_RA(config)# crypto pki trustpoint MIC_trustpoint

ISR_RA(ca-trustpoint)# authorization list PhoneList

ISR_RA(ca-trustpoint)# authorization username subjectname commonname

ISR_RA(ca-trustpoint)# exit

ISR_RA(config)# crypto pki trustpoint MIC_trustpoint

ISR_RA(ca-trustpoint)# enrollment terminal

ISR_RA(ca-trustpoint)# revocation-check none

ISR_RA(ca-trustpoint)# exit

ISR_RA(config)# crypto pki authenticate MIC_trustpoint

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

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

MIIEZTCCA02gAwIBAgIBAjANBgkqhkiG9w0BAQsFADArMQ4wDAYDVQQKEwVDaXNj
bzEZMBcGA1UEAxMQQ2lzY28gUm9vdCBDQSBNMjAeFw0xMjExMTIxMzUwNThaFw0z
NzExMTIxMzAwMTdaMDYxDjAMBgNVBAoTBUNpc2NvMSQwIgYDVQQDExtDaXNjbyBN
YW51ZmFjdHVyaW5nIENBIFNIQTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQD0NktCAjJn3kk98hU7wUVp6QlOFrlItEce6CpbfYpeLdUeZduAo+S0otzT
lJwS2BlMhZtacu9vUpfmW9w7nQo9zVT3eyPuhF/6/9TEdVBn75zb5CfV+E6ld+fH
nuPiFyBu+HDDJRd373Op+957IdoWyPvD8hHR1HJGFJ3JJKBg0UScL4JCwleu98Xq
/yPlAqBhExa7a2/fqSmZA0vZIG1bBfWZY8ZtSeTxKg3eWynV+xElabHqTDMYWf+2
obs4YB5lINTbYgHyRETP6T8Xr6TtD0h3654OUHcW+1meBu/jctluMKppeSjVtrof
5vt+pbkCg0iQAAjsL0qczT3yaNXvAgMBAAGjggGHMIIBgzAOBgNVHQ8BAf8EBAMC
AQYwEgYDVR0TAQH/BAgwBgEB/wIBADBcBgNVHSAEVTBTMFEGCisGAQQBCRUBEgAw
QzBBBggrBgEFBQcCARY1aHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtp
L3BvbGljaWVzL2luZGV4Lmh0bWwwHQYDVR0OBBYEFHrXeZXKu0gruFUU/aPAD7yn
D5YZMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jcmwvY3JjYW0yLmNybDB8BggrBgEFBQcBAQRwMG4wPgYIKwYBBQUH
MAKGMmh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9jcmNh
bTIuY2VyMCwGCCsGAQUFBzABhiBodHRwczovL3Rvb2xzLmNpc2NvLmNvbS9wa2kv

b2NzcDAfBgNVHSMEGDAWgBTJAPkfih/CZr2l0m1lDiIuNMMFoDANBgkqhkiG9w0B
AQsFAAOCAQEAc1k2rH6YT4juFxs9q7ObzfcKbNvOyDsaU7av4IHFXmn/JxfnBmUv
YxAI2Hx3xRb0KtG1JGkffQjVAtBboTXynLaQso/jj46ZOubIF8y6Ho3nTAv7Q6VH
kqSCdZClVu91zbHV9FFYQzJxjw1QgB0a4ItS4yhdmgl3oDNEcb3trQezrQ3/857/
ISqBGVLEbKHOu8H6zOLhxAgZ08ae1oQQQJowki0Ibd+LRLGovtEwLg8yyqiTIGve
7VFL2sRa8Z3rK9tlwKVH2kpFKNAeN3rfKFqr0/weR0cyKpmLMrSBTBZcxQcJCYF4
X6FO/32KOqcxJFIOKGVIUjvAvioOqoducw==
-----END CERTIFICATE-----

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

Certificate has the following attributes:

Fingerprint MD5: AC14F08F C3780F8F D9EEE6C9 39111280

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

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

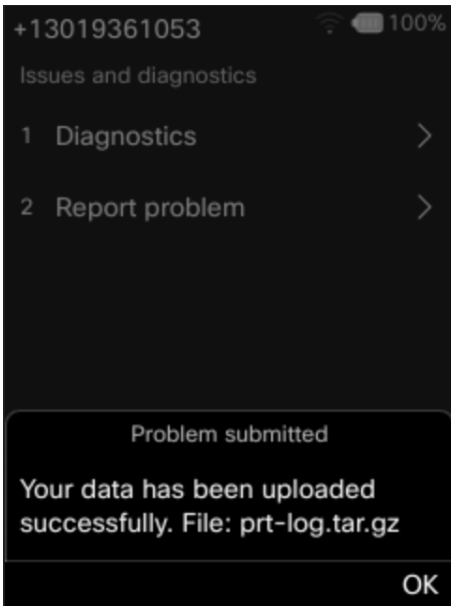
Problem Report Tool

You can create a problem report via the Problem Report Tool in the phone **Settings** menu. Navigate to **Settings** > **Issues and diagnostics** > **Report problem**, enter the date and time information, select a problem description, and then select **Submit** to generate issue report.



The phone then displays the PRT file generating progress. Wait till it completes.

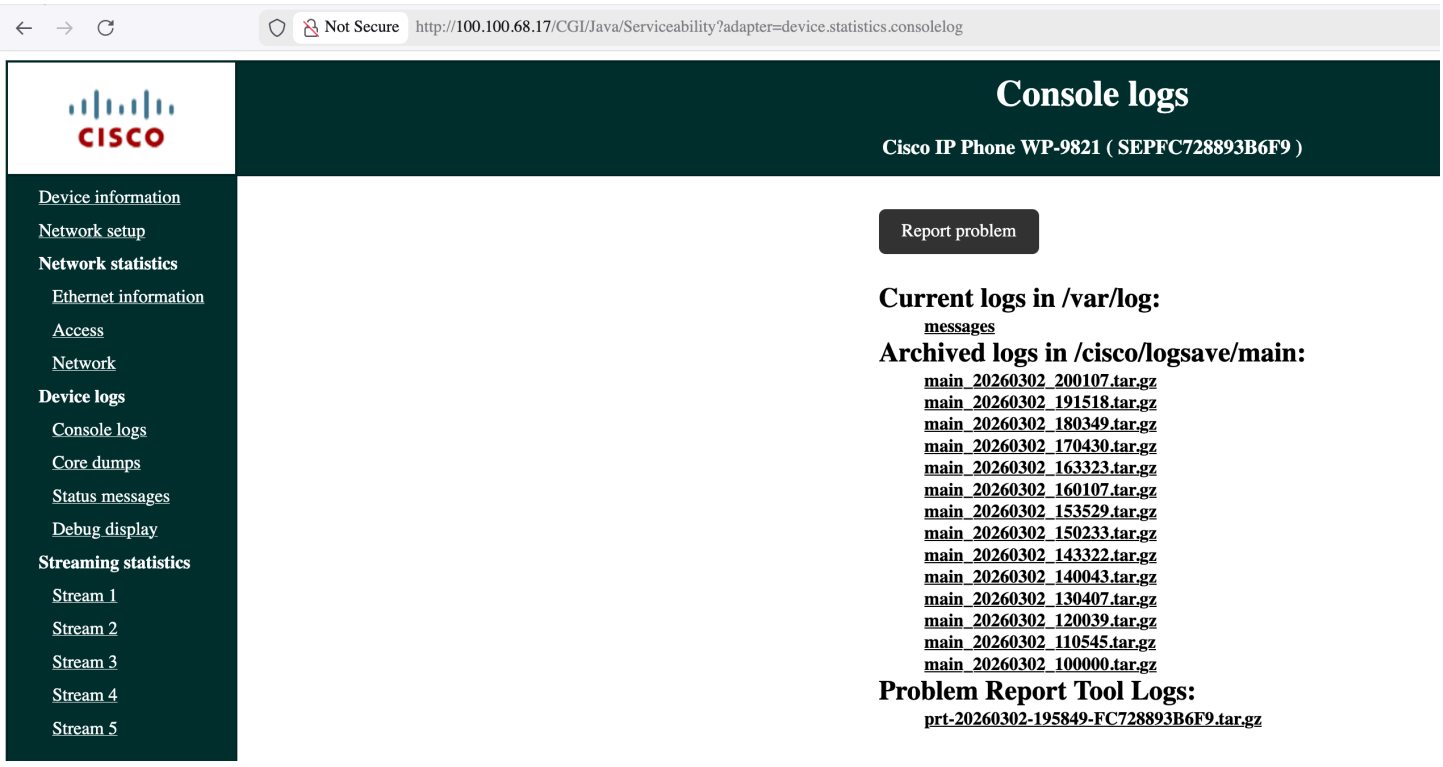




Once the phone shows that the data has been uploaded successfully, a user can access the phone administration web page and download the PRT file.

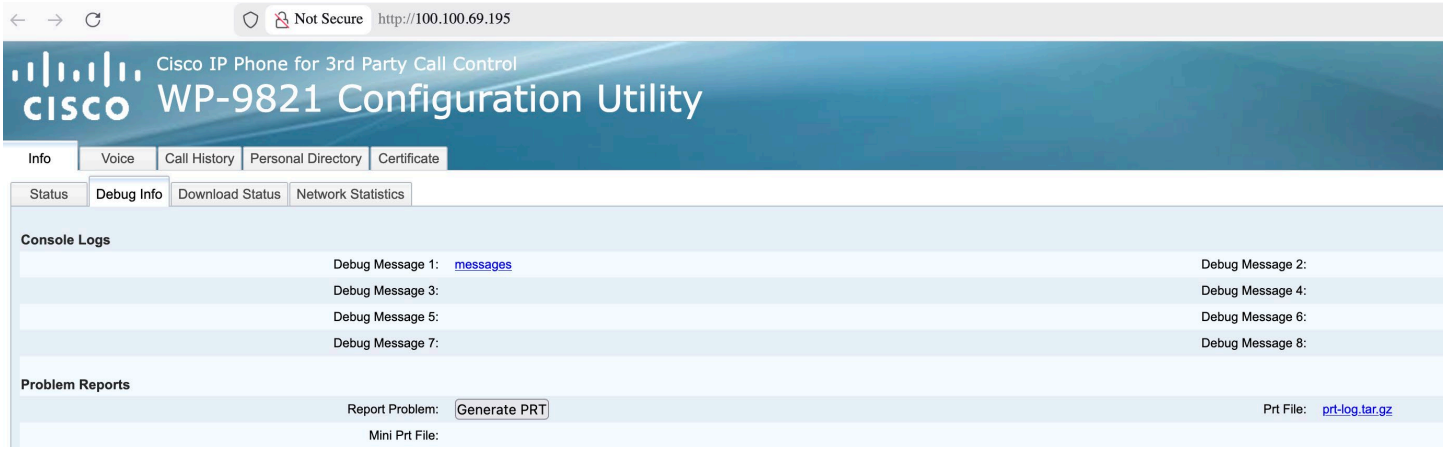
- CUCM phone administration web page

  Access **[web service]://A.B.C.D** and then click **Console logs**. You can find the compressed PRT file download link under **Problem Report Tool Logs**.



- Webex Calling phone administration web page

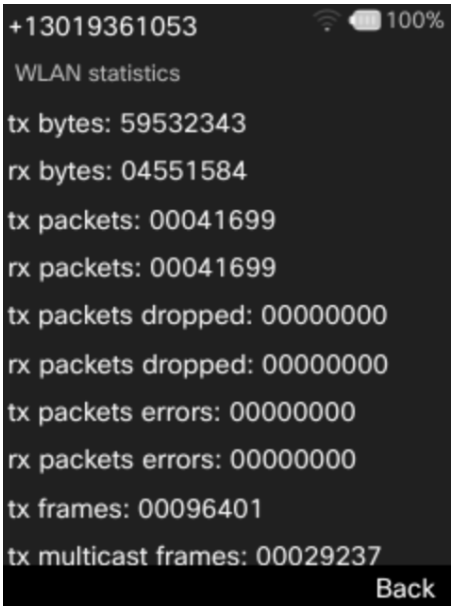
  Access **[web service]://A.B.C.D** and then click **Info** > **Debug Info** to find the generated PRT file.



Administrators can configure a Customer Support Upload rule for Cisco Wireless Phone 9821. When a user initiates a Problem Reporting Tool (PRT) file, the phone automatically uploads it to a remote server for administrative retrieval.

Wi-Fi statistics

Navigate to **Settings** > **Admin settings** > **Status** > **WLAN statistics**.

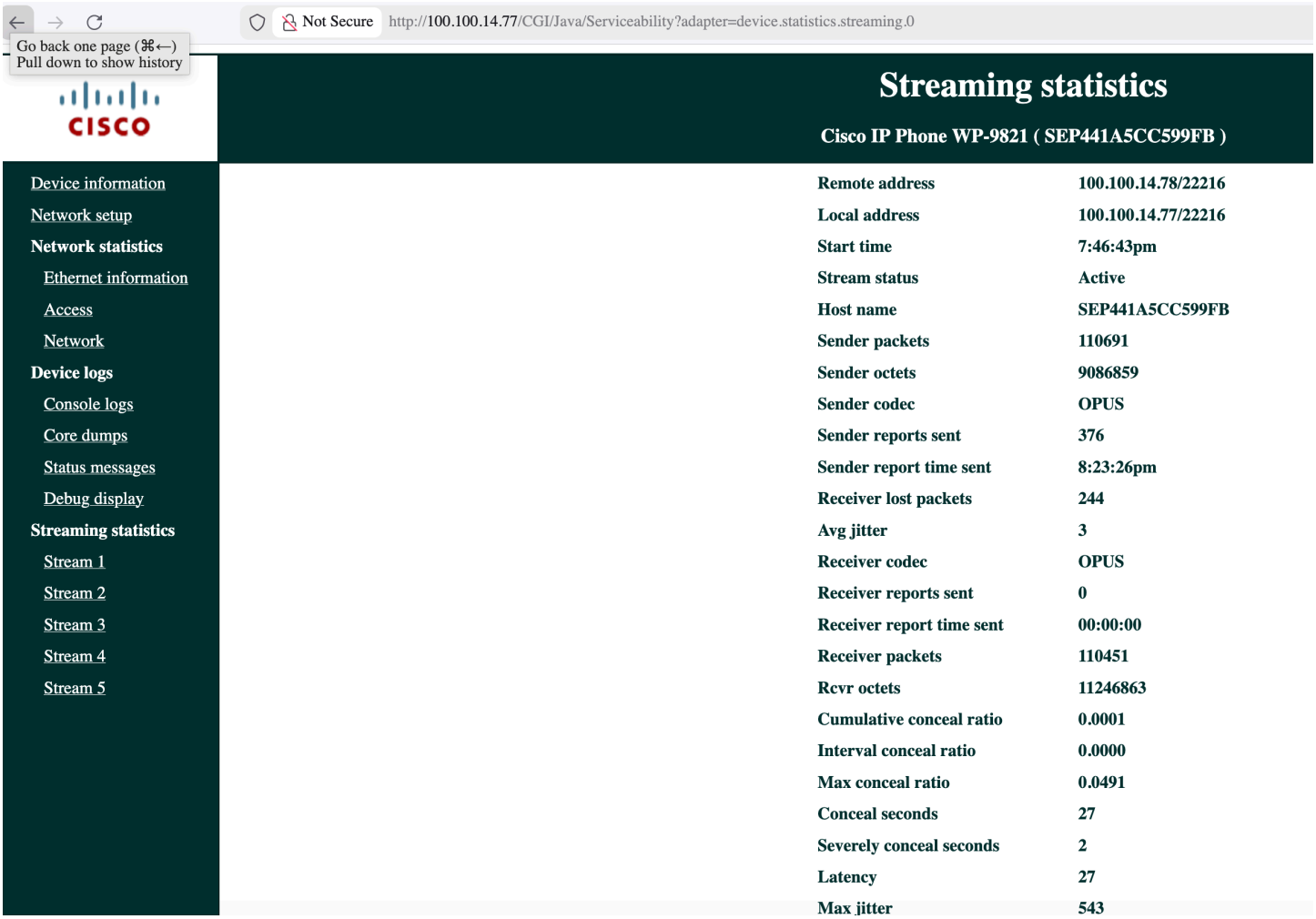


Streaming Statistics

Cisco Wireless Phone 9821 provides call statistic information, where displays codec type, jitter and packet count, and more.

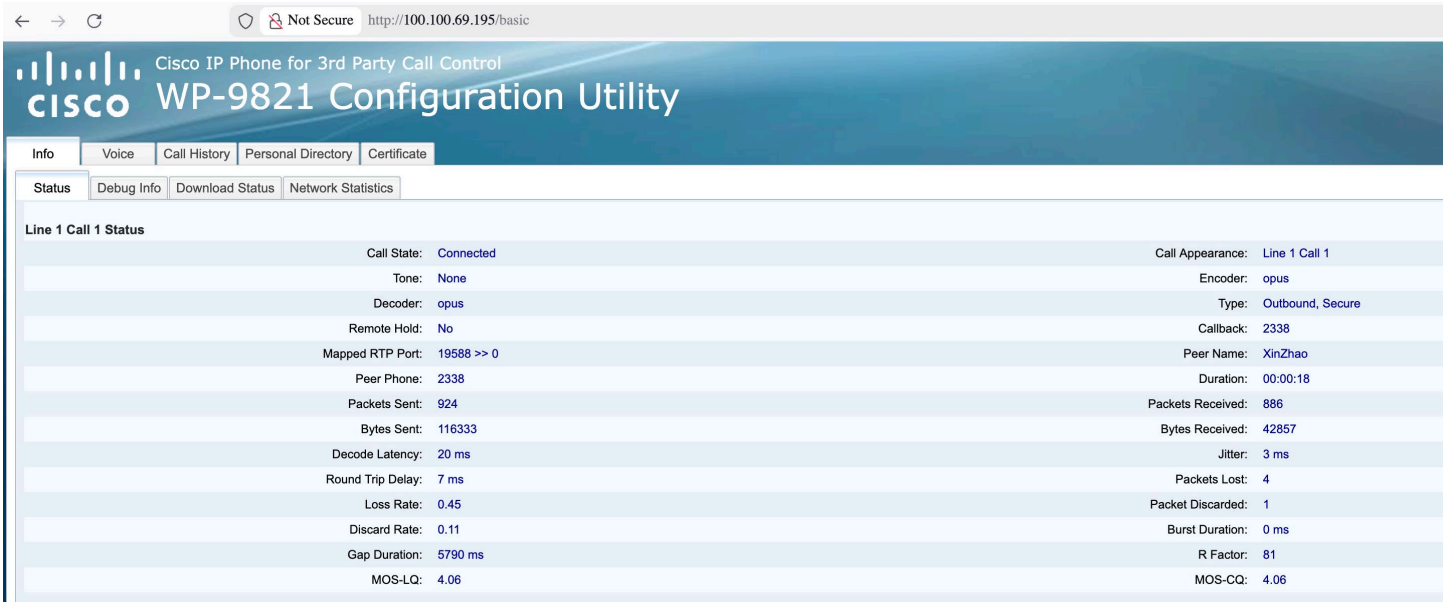
- CUCM phone administration web page

  Select the necessary menu item under **Streaming statistics** to view this information.



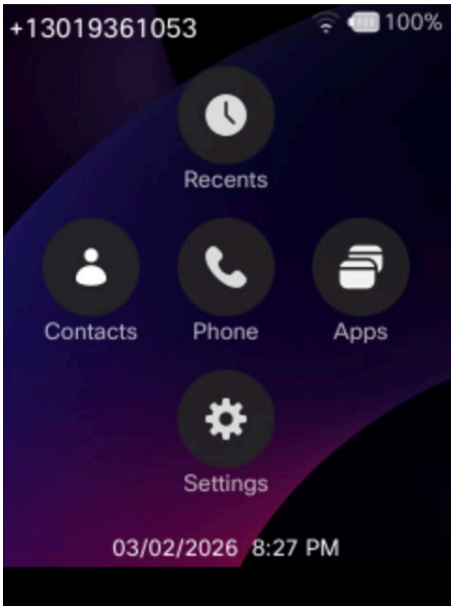
- Webex Calling phone administration web page

  Click **Info** > **Status** to view this information.



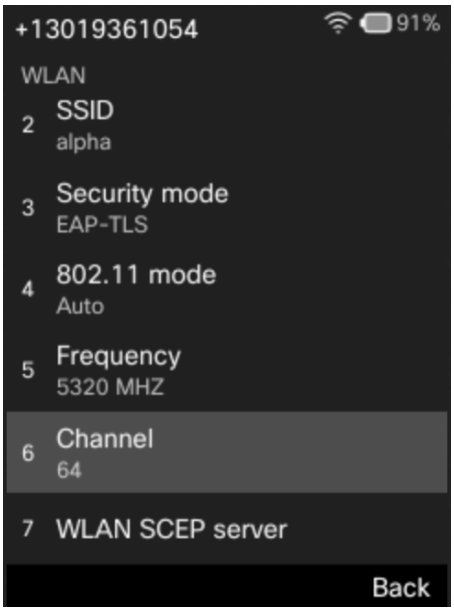
Wi-Fi Signal Indicator

On the Home screen of your phone, Wi-Fi signal is displayed on top-right corner when connected with AP.



Current Access Point

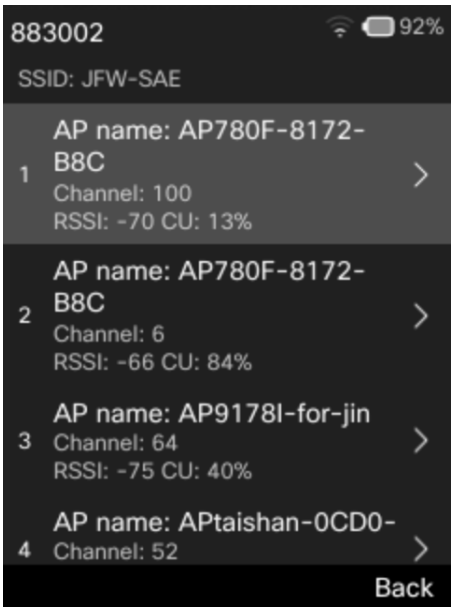
To view the connected AP's channel and BSSID, navigate to **Settings** > **Phone Information** > **Device Information** > **WLAN**.

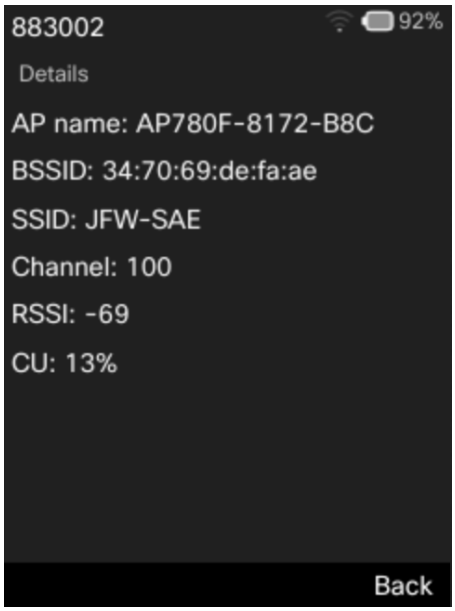


Note: When a user encounters Wi-Fi problem, check the connected AP status, AP parameters, phone side signal strength and phone Wi-Fi statistics. If the configurations are correct and the desired AP is healthy, disable and enable the Wi-Fi profile in the phone menu to recover Wi-Fi connection. If this action fails to recover Wi-Fi connection, place the phone on a desktop charger with a USB-to-Ethernet dongle connected and then generate a PRT from the phone **Settings** menu..

Neighbor list

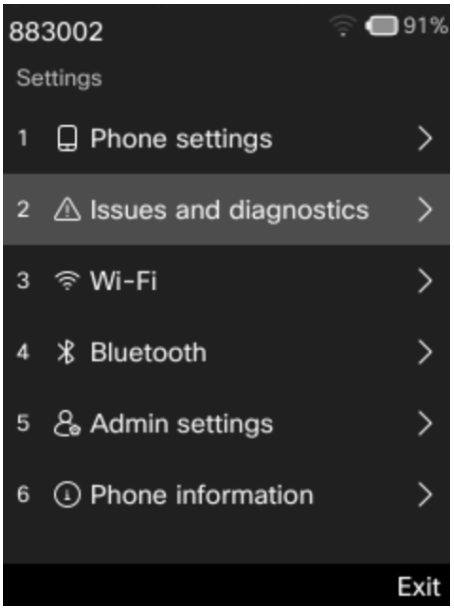
Navigate to **Settings** > **Admin settings** > **Neighbor list** to view the current access point and neighbor access point details.

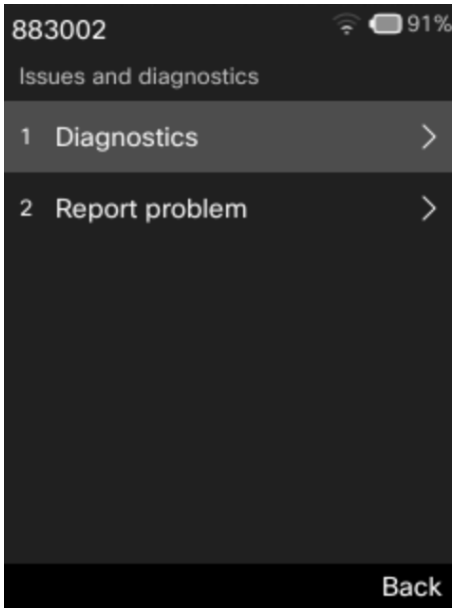


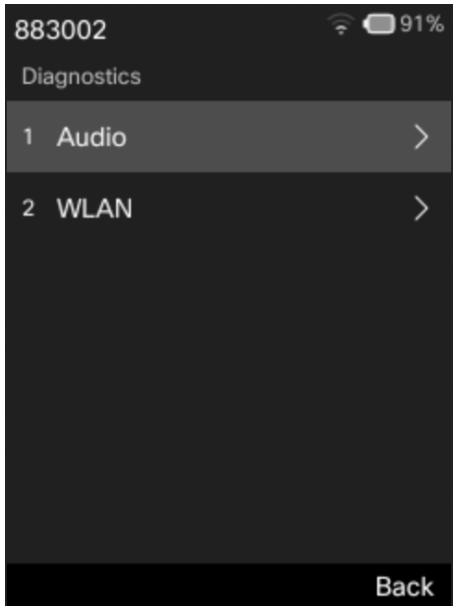


Diagnostics

You can utilize the integrated Audio and WLAN diagnostic tools to help troubleshoot various issues.

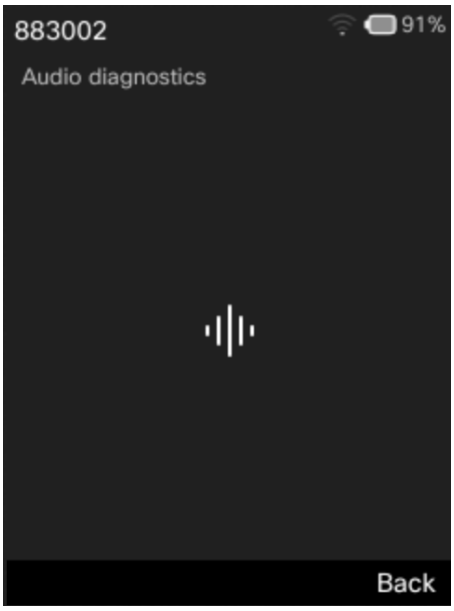






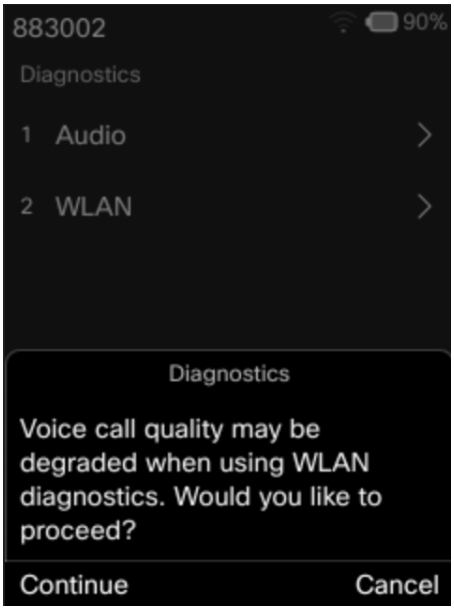
Audio Diagnostics

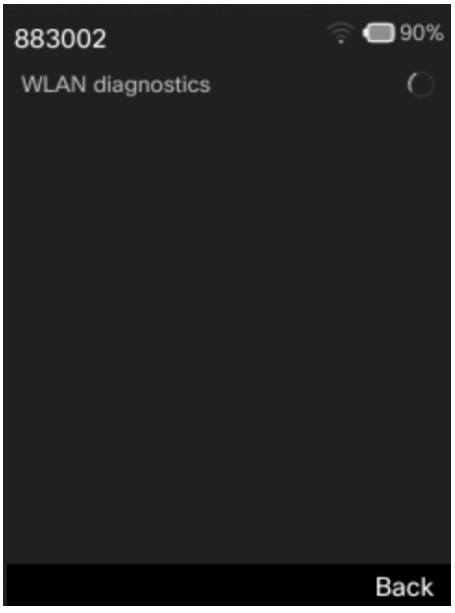
Navigate to **Settings** > **Issues and diagnostics** > **Diagnostics** > **Audio**. Audio Diagnostics can help triage audio hardware components (microphone, speaker, and handset).

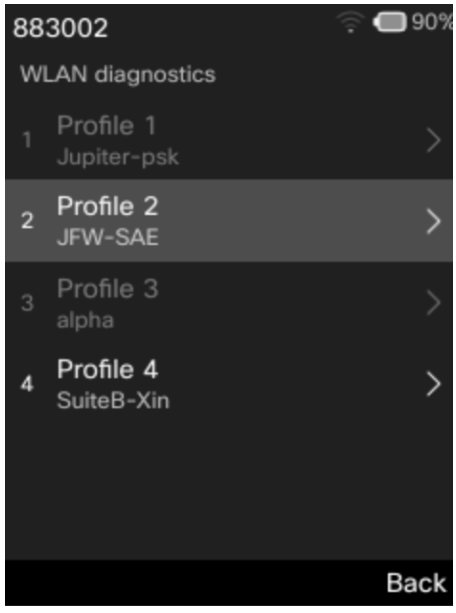


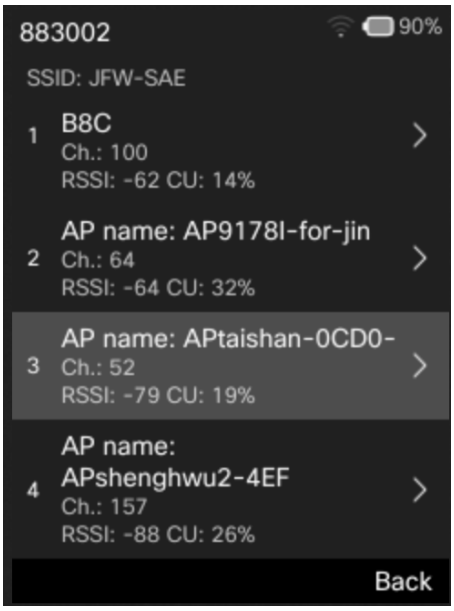
WLAN Diagnostics

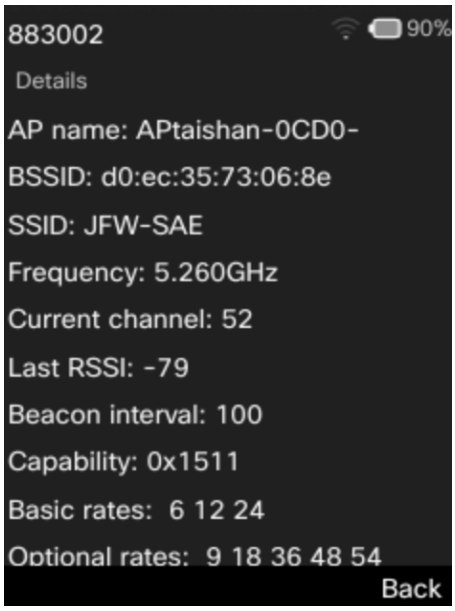
Navigate to **Settings** > **Issues and diagnostics** > **Diagnostics** > **WLAN**. WLAN Diagnostics can display detail for each access point that matches a configured Wi-Fi Profile, including AP name, BSSID, SSID, Frequency, Current channel, Last RSSI, Beacon Interval, Data rate, DTIM, Country code, Power constraint, Power limit, CU, Station count, Admission capacity, WMM, UAPSD, Proxy ARP, and Access category information.











Capturing a Screenshot of the Phone Display

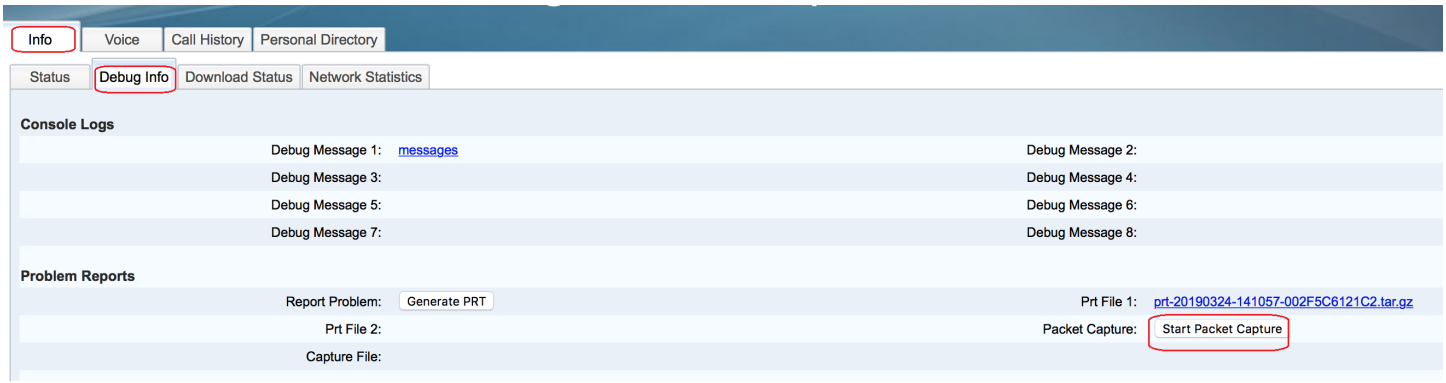
For phones that are registered to Webex Calling, get the IP address of your phone and visit **[web service]://<phone_IP_address>/admin/screendump.bmp** in a web browser. For example, http://192.168.16.43/admin/screendump.bmp. When prompted, enter the password for the admin.

For phones that are registered to Cisco Unified Communications Manager, get the IP address of your phone and visit **[web service]://<phone_IP_address>/CGI/Screenshot**. For example, http192.168.32.124/CGI/Screenshot. When prompted, enter the username and password for the account that your phone is associated with in Cisco Unified Communications Manager.

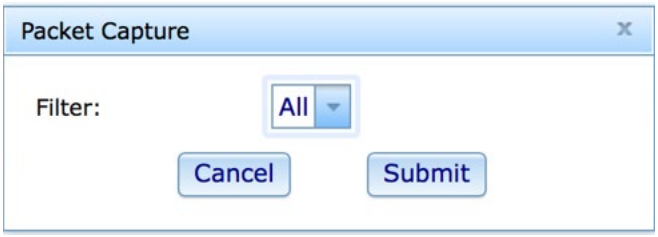
Capturing packets

You can capture the packets for phones that are registered to Webex Calling.

1. Visit **[web service]://A.B.C.D/admin/** in a web browser. When prompted, enter the password for the admin.
2. Access **Info** > **Debug Info**.
3. Click **Start Packet Capture** to start capturing packets.



4. Click **Submit** in the prompt.



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



The captured file is available for downloading.



Additional Documentation

Cisco Wireless Phone 9821 Datasheet

Cisco Wireless Phone 9821 Help Center

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

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

© 2026 Cisco Systems, All rights reserved.