Cisco DX Series
Wireless LAN Deployment Guide

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

The Cisco DX Series introduces a new era in employee productivity, spawning new opportunities to collaboration-enable business processes and workflows, to advance business results.
The Cisco DX Series meets the evolving needs of business, across industries and geographies, at the campus or at home, for both today and tomorrow.

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

Revision History

Date	Comments
05/24/13	10.0(1) Release
08/20/13	10.0(2) Release
04/19/14	10.1(1) Release
09/18/14	10.2(2) Release
06/17/15	10.2(3) Release

Contents

Cisco DX Series Overview

The Cisco DX Series is the platform that provides collaboration within enterprises. It brings together the capabilities of Cisco Unified Communication applications, building upon the solid foundations of Cisco Unified Communications devices, both wired and wireless.
Cisco's implementation of 802.11, employing CCX, permits time sensitive applications such as voice and video to operate efficiently across campus wide wireless LAN (WLAN) deployments. These extensions provide fast roaming capabilities and an almost seamless flow of multimedia traffic, whilst maintaining security as the end user roams between access points.

It should be understood that WLAN uses unlicensed spectrum, and as a result it may experience interference from other devices using the unlicensed spectrum. The proliferation of devices in the 2.4 GHz spectrum, such as Bluetooth headsets, Microwave ovens, cordless consumer phones, means that the 2.4 GHz spectrum may contain more congestion than other spectrums. The 5 GHz spectrum has far fewer devices operating in this spectrum and is the preferred spectrum to operate the Cisco DX Series in order to take advantage of the 802.11a/n data rates available. Despite the optimizations that Cisco have implemented in the Cisco DX Series, the use of unlicensed spectrum means that uninterrupted communication can not be guaranteed, and there may be the possibility of voice or video gaps of up to several seconds during multimedia conversations. Adherence to the deployment guidelines will reduce the likelihood of these voice and video gaps being present, but there is always this possibility. Through the use of unlicensed spectrum, and the inability to guarantee the delivery of messages to a WLAN device, the Cisco DX Series is not intended as a medical device and should not be used to make clinical decisions.

Cisco DX Series Highlights

Cisco DX Series are collaboration devices built for business.

The levels of multimedia performance that have come to be expected from Cisco products are maintained in the Cisco DX Series with the introduction of 802.11n data rates and the inclusion of Cisco Compatible eXtensions (CCX).

- Multi-touch color display
  - DX650 = 7 inch
  - DX70 = 14 inch
  - DX80 = 23 inch
- Android™ OS 4.1.1
- 1.5 GHz dual-core processor
- 8 GB eMMC flash memory
- 2 GB LPDDR2 SDRAM
- Wi-Fi IEEE 802.11 a/b/g/n
- Bluetooth 3.0
- 2 port Gigabit Ethernet switch
  - DX650 = Class 3/4 Power over Ethernet (PoE) for phone port
- HDMI port
  - DX650 = 1 for external monitor support
  - DX70 = 1 for video input and 1 for video output
  - DX80 = 1 for video input and 1 for video output
- Type A USB ports
  - DX650 = 2 USB 2.0 ports
  - DX70 = 3 USB 2.0 ports
  - DX80 = 3 USB 2.0 ports
- 1 micro type B USB port
- 3.5 mm headphone jack
- Micro SD card support
- Full duplex speakerphone and wideband audio
- Forward-facing camera is capable of HD 1080p 30-fps video encoding and decoding
- High-definition video interoperability with Cisco TelePresence™ solution and other H.264 video endpoints
- Full range of Cisco Collaboration and Unified Communication applications

Cisco Quad, Cisco WebEx™, Cisco Unified Presence, Instant Messaging, Email, and Cisco Unified Communications Manager voice and video telephony features

- Virtual desktop client integration (VDI) and cloud computing
- Access to Google Play™
- Expanded Android applications for business, linking Cisco Collaboration APIs through a software developer kit (SDK)

Requirements

The Cisco DX600 Series are IEEE 802.11a/b/g/n collaboration devices that provide voice, video, and data communications.

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

Site Survey

Before deploying the Cisco DX Series into a production environment, a site survey must be completed by a Cisco certified partner with the advanced wireless LAN specialization. During the site survey, the RF (radio frequency) spectrum can be analyzed to determine which channels are usable in the desired band (5 GHz or 2.4 GHz). Typically there is less interference in the 5 GHz band as well as more non-overlapping channels, so 5 GHz is the preferred band for operation and even more highly recommended when the Cisco DX Series is to be used in a mission critical environment. The site survey will include heatmaps showing the intended coverage plan for the location. The site survey will also determine the access point platform type, antenna type, and access point configuration (channel and transmit power) to use at the location. It is recommended to select an access point with integrated antennas for non-rugged environments (e.g. office, healthcare, education, hospitality) and an access point platform requiring external antennas for rugged environments (e.g. manufacturing, warehouse, retail).
See the Designing the Wireless LAN for Voice section for more information.

RF Validation

In order to determine if VoWLAN can be deployed, the environment must be evaluated to ensure the following items meet Cisco guidelines.

Signal

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

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

Also need to ensure that the upstream signal from the Cisco DX Series meets the access point's receiver sensitivity for the transmitted data rate. Rule of thumb is to ensure that the received signal at the access point is -67 dBm or higher.

It is recommended to design the cell size to ensure that the Cisco DX Series can hold a signal for at least 5 seconds.

Channel Utilization

Channel Utilization levels should be kept under 40%.

The Cisco DX Series converts the 0-255 scale value to a percentage, so 105 would equate to around 40% in the Cisco DX Series neighbor list menu.

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 DX Series meets the access point's signal to noise ratio for the transmitted data rate.

Packet Loss / Delay

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

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

Retries

802.11 retransmissions should be less than 20%.

Multipath

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

Many different tools and applications can be used to evaluate these items in order to certify the deployment.

- Cisco Prime Network Control System (NCS) for Unified Wireless LAN Management

  http://www.cisco.com/c/en/us/products/collateral/wireless/prime-network-control-system-series-appliances/data_sheet_c78-650051.html

- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management

  http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product_data_sheet0900aecd802570d0.html

- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management

  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/ciscoworks-wireless-lan-solution-engine-software-2-13/product_data_sheet0900aecd80410b92.html

- Cisco Spectrum Expert

  http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert/product_data_sheet0900aecd807033c3.html

- Cisco Unified Operations Manager

  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-unified-operations-manager/data_sheet_c78-636705.html

Call Control

The Cisco DX Series utilizes Session Initiation Protocol (SIP) for call control with the following communications platforms.

- Cisco Unified Communications Manager (CUCM)

  DX650
  Minimum = 7.1(5)
  Recommended = 8.6(2), 9.1(2), 10.5(2), 11.0(1)

  DX70
  Minimum = 8.5(1)
  Recommended = 8.6(2), 9.1(2), 10.5(2), 11.0(1)

  DX80
  Minimum = 8.5(1)
  Recommended = 8.6(2), 9.1(2), 10.5(2), 11.0(1)

Device Support in Cisco Unified Communications Manager

Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable device support for the Cisco DX Series.

Device packages for Cisco Unified Communications Manager are available at the following location.
http://software.cisco.com/download/navigator.html?mdfid=278875240

Protocols

Supported voice and wireless LAN protocols include the following:

- Wi-Fi MultiMedia (WMM)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
- AAC-LD, G.722, iSAC, G.711, iLBC, G.729
- H.264
- Real Time Control Protocol (RTCP)
- Cisco Discovery Protocol (CDP)

Access Points

The Cisco DX Series is supported on the following Cisco Wireless LAN solutions.

- Cisco Unified Wireless LAN Controller

  Minimum = 7.0.250.0

  Recommended = 7.4.140.0, 7.6.130.0, 8.0.115.0, 8.1.102.0

- Cisco IOS Access Points (Autonomous)

  Minimum = 12.4(21a)JY

  Recommended = 12.4(25d)JA2, 15.2(4)JB6, 15.3(3)JBB

The supported access point models are listed below.

700

700W

1040

1140

1250

1260

1600

1700

2600

2700

3500

3600

3700

1130 AG

1240 AG

600

890

Note: The Cisco DX Series is supported with the Cisco AP3600 when the internal 802.11a/b/g/n radio is utilized, however if the 802.11ac module (AIR-RM3000AC) for the Cisco AP3600 is installed, then Cisco Unified Wireless LAN Controller release 7.6.100.0 or later is required.

The table below lists the modes that are supported by each Cisco Access Point.

Cisco AP Series	802.11a	802.11b	802.11g	802.11n	802.11ac	Unified	Autonomous
600	Yes	Yes	Yes	Yes	No	Yes	No
700	Yes	Yes	Yes	Yes	No	Yes	Yes
700W	Yes	Yes	Yes	Yes	No	Yes	Yes
1040	Yes	Yes	Yes	Yes	No	Yes	Yes
1130	Yes	Yes	Yes	No	No	Yes	Yes
1140	Yes	Yes	Yes	Yes	No	Yes	Yes
1240	Yes	Yes	Yes	No	No	Yes	Yes
1250	Yes	Yes	Yes	Yes	No	Yes	Yes
1260	Yes	Yes	Yes	Yes	No	Yes	Yes
1600	Yes	Yes	Yes	Yes	No	Yes	Yes
1700	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2600	Yes	Yes	Yes	Yes	No	Yes	Yes
2700	Yes	Yes	Yes	Yes	Yes	Yes	Yes

3500	Yes	Yes	Yes	Yes	No	Yes	Yes
3600	Yes	Yes	Yes	Yes	Yes (with AIR-RM3000AC module)	Yes	Yes
3700	Yes	Yes	Yes	Yes	Yes	Yes	Yes
890	Yes	Yes	Yes	Yes	No	Yes	Yes

Note: VoWLAN is not currently supported in conjunction with outdoor MESH technology (1500 series).

Limited support is provided when using 3rd party access points as there are no interoperability tests performed for 3rd party access points.

However the user should have basic functionality when connected to a Wi-Fi compliant access point.

Some of the key features are the following:

- 5 GHz (802.11a/n)
- Wi-Fi Protected Access v2 (WPA2+AES)
- Wi-Fi Multimedia (WMM)
- Differentiated Services Code Point (DSCP)
- Class of Service (802.1p)
- QoS Basic Service Set (QBSS)

The Cisco DX Series can take advantage of Cisco Client Extensions (CCX) enabled access points.

Some of the key features are the following:

- Cisco Centralized Key Management (CCKM)
- Dynamic Transmit Power Control (DTPC)

http://www.cisco.com/c/en/us/products/wireless/compatible-extensions.html

Antennas

Some of the Cisco Access Points require or allow external antennas.

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

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

3rd party antennas are not supported, as there is no interoperability testing performed against 3rd party antennas including Distributed Antenna Systems (DAS) and Leaky Coaxial Systems.

Please refer to the following URL for more info on Cisco Wireless LAN over Distributed Antenna Systems.

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/positioning_statement_c07-565470.html

Note: The Cisco 1040, 1130, 1140, 1602i, 2602i, 3502i, 3602i, and 3702i Series Access Points are to be mounted on the ceiling as they have omni-directional antennas and are not designed to be patches.

Models

The following Cisco DX Series models are available.

Below outlines the modes, frequency ranges and channels supported by each model.

Part Number	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
CP-DX650-K9= CP-DX650-K9-W	2.4 GHz = 4 dBi 5 GHz = 4 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-140 149,153,157,161,165
CP-DX70-W-K9=	2.4 GHz = 2.6 dBi 5 GHz = 4 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-140 149,153,157,161,165
CP-DX80-K9=	2.4 GHz = 4.6 dBi 5 GHz = 7 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-140 149,153,157,161,165

A power cube (CP-PWR-CUBE-4= for Cisco DX650 and CP-PWR-CUBE-5= for DX70 and DX80) is required when utilizing Wi-Fi mode.

Note: Channels 120, 124, 128 are not supported in the Americas, Europe, or Japan, but may be in other regions around the world.

802.11j (channels 34, 38, 42, 46) are not supported.

Channel 14 for Japan is not supported.

World Mode (802.11d)

World Mode allows a client to be used in different regions, where the client can adapt to using the channels and transmit powers advertised by the access point in the local environment.

The Cisco DX Series requires the access point to be 802.11d enabled, where it can then determine which channels and transmit powers to use.

Enable World Mode (802.11d) for the corresponding country where the access point is located.

Some 5 GHz channels are also used by radar technology, which requires that the 802.11 client and access point be 802.11h compliant if utilizing those radar frequencies (DFS channels). 802.11h requires 802.11d to be enabled.

The Cisco DX Series will passively scan DFS channels first before engaging in active scans of those channels.

If using 2.4 GHz (802.11b/g) and 802.11d is not enabled, then the Cisco DX Series can attempt to use channels 1-11 and reduced transmit power.

Note: World Mode is enabled automatically for the Cisco Unified Wireless LAN Controller.

World Mode must be enabled manually for Cisco Autonomous Access Points using the following commands:

```
Interface dot11radio X
 world-mode dot11d country US both
```

Supported Countries

Below are the countries and their 802.11d codes that are supported by the Cisco DX Series.

Australia (AU)
Austria (AT)
Bahrain (BH)
Belgium (BE)
Brazil (BR)
Bulgaria (BG)
Canada (CA)
Chile (CL)
China (CN)
Colombia (CO)
Costa Rica (CR)
Croatia (HR)
Cyprus (CY)
Czech Republic (CZ)
Denmark (DK)
Dominican Republic (DO)
Ecuador (EC)
Egypt (EG)
Estonia (EE)
Finland (FI)
France (FR)
Germany (DE)
Gibraltar (GI)
Greece (GR)
Hong Kong (HK)
Hungary (HU)
Iceland (IS)
India (IN)
Ireland (IE)
Israel (IL)
Italy (IT)
Japan (JP)
Korea (KR)
Latvia (LV)
Liechtenstein (LI)
Lithuania (LT)
Luxembourg (LU)
Macedonia (MK)
Malaysia (MY)
Malta (MT)
Mexico (MX)
Monaco (MC)
Montenegro (ME)
Netherlands (NL)
New Zealand (NZ)
Nigeria (NG)
Norway (NO)
Panama (PA)
Paraguay (PY)
Peru (PE)
Philippines (PH)
Poland (PL)
Portugal (PT)
Puerto Rico (PR)
Romania (RO)
Russian Federation (RU)
Saudi Arabia (SA)
Serbia (RS)
Singapore (SG)
Slovakia (SK)
Slovenia (SI)
South Africa (ZA)
Spain (ES)
Sweden (SE)
Switzerland (CH)
Taiwan (TW)
Thailand (TH)
Turkey (TR)
Ukraine (UA)
United Arab Emirates (AE)
United Kingdom (GB)
United States (US)
Uruguay (UY)
Vietnam (VN)

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

http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

Radio Characteristics

The following table lists the data rates and receiver sensitivity info for the Cisco DX Series.

5 GHz Specifications

5 GHz - 802.11a	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 16 dBm (Depends on model and region)	6 Mbps	OFDM - BPSK	-91 dBm
	9 Mbps	OFDM - BPSK	-91 dBm
	12 Mbps	OFDM - QPSK	-90 dBm
	18 Mbps	OFDM - QPSK	-88 dBm
	24 Mbps	OFDM - 16 QAM	-85 dBm
	36 Mbps	OFDM - 16 QAM	-81 dBm
	48 Mbps	OFDM - 64 QAM	-77 dBm
	54 Mbps	OFDM - 64 QAM	-76 dBm
5 GHz - 802.11n (20)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 15 dBm (Depends on model and region)	7 Mbps (MCS 0)	OFDM - BPSK	-91 dBm
	14 Mbps (MCS 1)	OFDM - QPSK	-89 dBm
	21 Mbps (MCS 2)	OFDM - QPSK	-86 dBm
	29 Mbps (MCS 3)	OFDM - 16 QAM	-84 dBm
	43 Mbps (MCS 4)	OFDM - 16 QAM	-81 dBm
	58 Mbps (MCS 5)	OFDM - 64 QAM	-76 dBm
	65 Mbps (MCS 6)	OFDM - 64 QAM	-74 dBm
	72 Mbps (MCS 7)	OFDM - 64 QAM	-72 dBm
5 GHz - 802.11n (40)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 15 dBm (Depends on model and region)	15 Mbps (MCS 0)	OFDM - BPSK	-90 dBm
	30 Mbps (MCS 1)	OFDM - QPSK	-87 dBm
	45 Mbps (MCS 2)	OFDM - QPSK	-85 dBm
	60 Mbps (MCS 3)	OFDM - 16 QAM	-81 dBm
	90 Mbps (MCS 4)	OFDM - 16 QAM	-78 dBm
	120 Mbps (MCS 5)	OFDM - 64 QAM	-74 dBm
	135 Mbps (MCS 6)	OFDM - 64 QAM	-72 dBm
	150 Mbps (MCS 7)	OFDM - 64 QAM	-70 dBm

2.4 GHz Specifications

2.4 GHz - 802.11b	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 16 dBm (Depends on model and region)	1 Mbps	DSSS - BPSK	-95 dBm
	2 Mbps	DSSS - QPSK	-93 dBm
	5.5 Mbps	DSSS - CCK	-90 dBm

	11 Mbps	DSSS - CCK	-86 dBm
2.4 GHz - 802.11g	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 16 dBm (Depends on model and region)	6 Mbps	OFDM - BPSK	-89 dBm
	9 Mbps	OFDM - BPSK	-89 dBm
	12 Mbps	OFDM - QPSK	-87 dBm
	18 Mbps	OFDM - QPSK	-85 dBm
	24 Mbps	OFDM - 16 QAM	-81 dBm
	36 Mbps	OFDM - 16 QAM	-78 dBm
	48 Mbps	OFDM - 64 QAM	-74 dBm
	54 Mbps	OFDM - 64 QAM	-72 dBm
2.4 GHz - 802.11n (20)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 16 dBm (Depends on model and region)	7 Mbps (MCS 0)	OFDM - BPSK	-88 dBm
	14 Mbps (MCS 1)	OFDM - QPSK	-86 dBm
	21 Mbps (MCS 2)	OFDM - QPSK	-84 dBm
	29 Mbps (MCS 3)	OFDM - 16 QAM	-81 dBm
	43 Mbps (MCS 4)	OFDM - 16 QAM	-78 dBm
	58 Mbps (MCS 5)	OFDM - 64 QAM	-73 dBm
	65 Mbps (MCS 6)	OFDM - 64 QAM	-71 dBm
	72 Mbps (MCS 7)	OFDM - 64 QAM	-69 dBm

Note: Receiver sensitivity is the minimum signal needed to decode a packet at a certain data rate.

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

To achieve 802.11n connectivity, it is recommended that the Cisco DX Series be within 100 feet of the access point.

See the Designing the Wireless LAN for Voice section for more information on signal requirements.

Language Support

The Cisco DX Series supports the following languages.

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

The corresponding locale package must be installed to enable support for that language. English is the default language on the Cisco DX Series.

Download the locale packages from the Localization page at the following URL:

http://software.cisco.com/download/navigator.html?mdfid=278875240

Bluetooth

The Cisco DX Series supports Bluetooth 3.0 technology allowing for wireless headset communications.

Bluetooth enables low bandwidth wireless connections within a range of 30 feet, however it is recommended to keep the Bluetooth device within 10 feet of the Cisco DX Series.

The previously connected device for that Bluetooth profile is given priority.

The Bluetooth device does not need to be within direct line-of-sight of the Cisco DX Series, but barriers, such as walls, doors, etc. can potentially impact the quality.

Bluetooth utilizes the 2.4 GHz frequency just like 802.11b/g/n and many other devices (e.g. microwave ovens, cordless phones, etc.), so the Bluetooth quality can potentially be interfered with due to using this unlicensed frequency.

Bluetooth Profiles

The Cisco DX Series supports the following Bluetooth profiles.

Hands-Free Profile (HFP)

With Bluetooth Hands-Free Profile (HFP) support, the following features can be available if supported by the Bluetooth headset.

- Ring
- Answer a call
- End a call
- Volume Control
- Last Number Redial
- Call Waiting
- Divert / Reject
- 3 way calling (Hold & Accept and Release & Accept)
- Speed Dialing

Advanced Audio Distribution Profile (A2DP)

Bluetooth Advanced Audio Distribution Profile (A2DP) support allows for the transfer of a uni-directional high quality stereo audio stream to a Bluetooth enabled stereo headset, car audio system, etc.

Phone Book Access Profile (PBAP)

Phone Book Access Profile (PBAP) support enables the exchange of phone book objects between devices.

Object Push Profile (OPP)

Object Push Profile (OPP) support enables file sharing between devices.

Objects shared are typically pictures, business cards, meeting details, etc., where the sender initiates the file exchange.

Human Interface Device (HID)

Human Interface Device (HID) provides support for a Bluetooth enabled keyboard or mouse.

For more information, refer to the documentation from the Bluetooth device manufacturer.

Coexistence (802.11b/g/n + Bluetooth)

If using Coexistence where 802.11b/g/n and Bluetooth are used simultaneously, then there are some limitations and deployment requirements to be considered as they both utilize the 2.4 GHz frequency range.

Capacity

When using Coexistence (802.11b/g/n + Bluetooth), call capacity is reduced due to the utilization of the 2.4 GHz for both 802.11b/g/n and Bluetooth transmissions.

Multicast Audio

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

Voice Quality

Depending on the current data rate configuration, CTS may be sent to protect the Bluetooth transmissions when using Coexistence.
In some environments, 6 Mbps may need to be enabled.

Note: It is highly recommended to use 802.11a/n if using Bluetooth due to 802.11b/g/n and Bluetooth both utilizing 2.4 GHz, but also due to the above limitations.

Video Calls

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

The **Video Calling** feature within Cisco Unified Communications Manager must be enabled for each Cisco DX Series if wanting to participate in video calls.

The Cisco DX Series is able to establish video calls with other Cisco DX Series endpoints, Cisco TelePresence Systems, Cisco Unified IP Phone 8900 and 9900 Series, and other video enabled endpoints.

600p or HD 720p is the recommended video format to utilize unless higher-grade video is required when communicating with other capable endpoints.

600p (1024 x 600) is the native default format used for video calls between DX650 endpoints.

For remote users, 600p or HD 720p should be the maximum video resolution enabled in the Cisco DX Series endpoint configuration within Cisco Unified Communications Manager.

A Videoconferencing System with MCU running version 5.7 or later is required to provide videoconferencing capabilities.

A video call can also be established via a VPN session using the Cisco AnyConnect VPN Client.

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

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

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

The following video formats are supported:

- CIF (352 x 288)
- VGA (640 x 480)
- 240p (432 x 240)
- 360p (640 x 360)
- 480p (848 x 480)
- 600p (1024 x 600)
- HD 720p (1280 x 720)
- HD 1080p (1920 x 1080)

For more information about Cisco TelePresence, refer to the following URLs:

http://www.cisco.com/c/en/us/products/collaboration-endpoints/index.html

For more information about Cisco Unified IP Phone 8900 and 9900 Series, refer to the following URLs:

http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8900-series/index.html

http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phones-9900-series/index.html

Security

When deploying a wireless LAN, security is essential.

The Cisco DX Series supports the following wireless security features.

WLAN Authentication

- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2)
- PEAP-GTC (Protected Extensible Authentication Protocol - Generic Token Card)
- CCKM (Cisco Centralized Key Management)
- None

WLAN Encryption

- AES (Advanced Encryption Standard)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
- WEP (Wired Equivalent Protocol) 40/64 and 104/128 bit

Note: Dynamic WEP with 802.1x authentication and Shared Key authentication are not supported.

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

- X.509 Digital Certificates
- Image authentication
- Device authentication
- File authentication
- Signaling authentication
- Secure Cisco Unified SRST
- Media encryption (SRTP)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)
- Secure profiles
- Encrypted configuration files
- Screen Lock
- Remote Lock
- Remote Wipe
- Cisco AnyConnect VPN Client

Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)

Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST) encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the access point and the Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS) or Cisco Identity Services Engine (ISE).

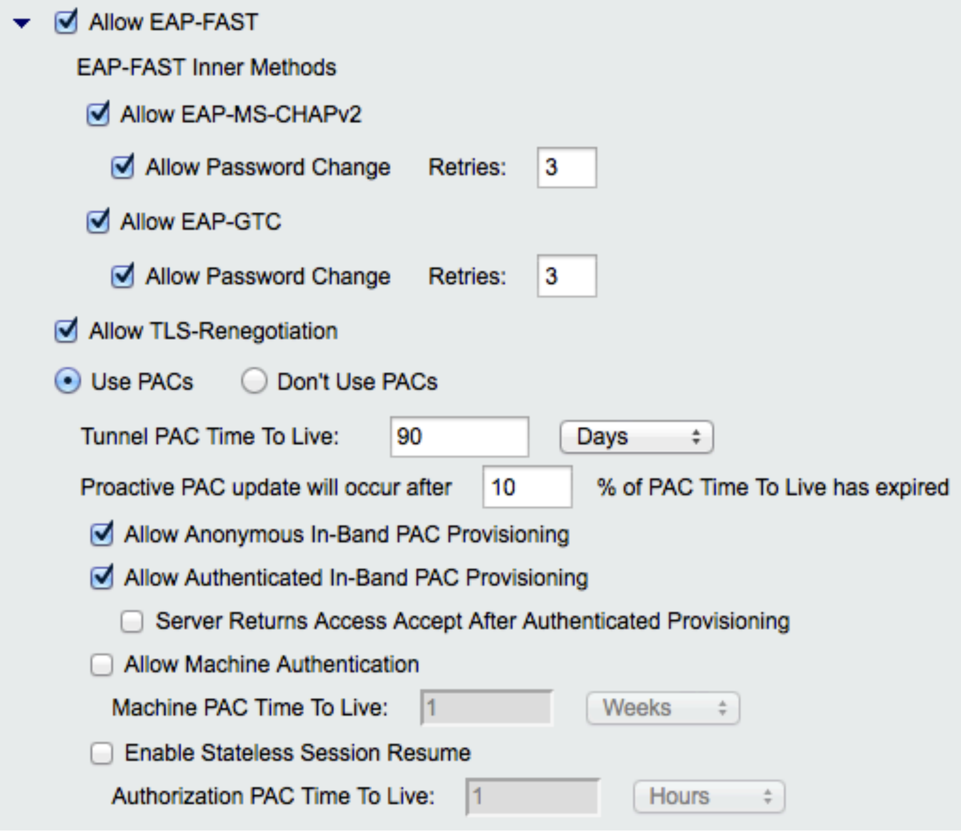
The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (the Cisco DX Series) and the RADIUS server. The server sends an Authority ID (AID) to the client, which in turn selects the appropriate PAC. The client returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both endpoints now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must enable don the RADIUS server.

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

The Cisco DX Series currently supports only automatic provisioning of the PAC, so enable **Allow anonymous in-band PAC provisioning** on the RADIUS server as shown below.

Both EAP-GTC and EAP-MSCHAPv2 must be enabled when **Allow anonymous in-band PAC provisioning** is enabled.

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



☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries: 3

☑ Allow EAP-GTC

☑ Allow Password Change Retries: 3

☑ Allow TLS-Renegotiation

● Use PACs ○ Don't Use PACs

Tunnel PAC Time To Live: 90 Days

Proactive PAC update will occur after 10 % of PAC Time To Live has expired

☑ Allow Anonymous In-Band PAC Provisioning

☑ Allow Authenticated In-Band PAC Provisioning

□ Server Returns Access Accept After Authenticated Provisioning

□ Allow Machine Authentication

Machine PAC Time To Live: 1 Weeks

□ Enable Stateless Session Resume

Authorization PAC Time To Live: 1 Hours

If anonymous PAC provisioning is not allowed in the production wireless LAN environment then a staging RADIUS server can be setup for initial PAC provisioning of the Cisco DX Series.

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

Ensure the production master EAP-FAST RADIUS server is setup to send the EAP-FAST master keys and policies to the staging slave EAP-FAST RADIUS server, which will then allow the Cisco DX Series to use the provisioned PAC in the production environment where **Allow anonymous in-band PAC provisioning** is disabled.

When it is time to renew the PAC, then authenticated in-band PAC provisioning will be used, so ensure that **Allow authenticated in-band PAC provisioning** is enabled.

Ensure that the Cisco DX Series has connected to the network during the grace period to ensure it can use its existing PAC created either using the active or retired master key in order to get issued a new PAC.

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

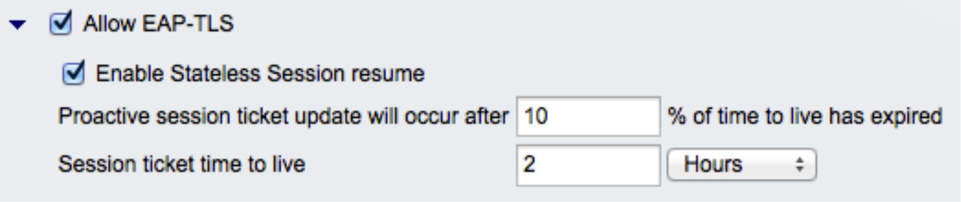
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)

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

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

A certificate is required to be installed.

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



☑ Allow EAP-TLS

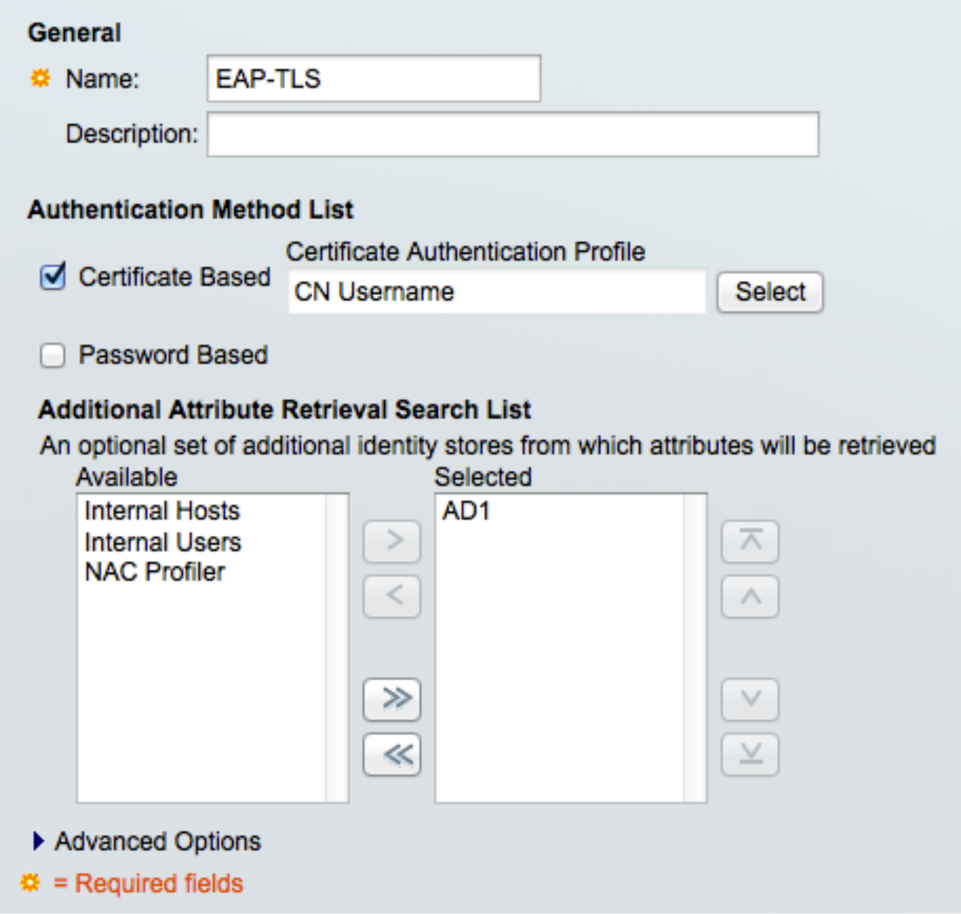
☑ Enable Stateless Session resume

Proactive session ticket update will occur after 10 % of time to live has expired

Session ticket time to live 2 Hours

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

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



General

Name: EAP-TLS

Description:

Authentication Method List

Certificate Authentication Profile

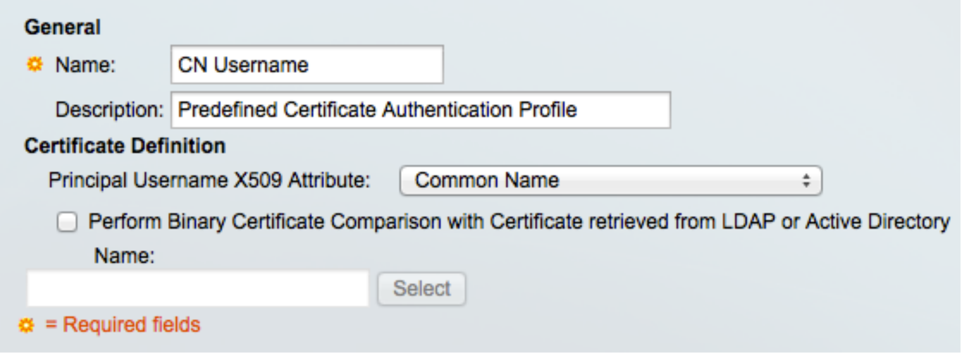
☑ Certificate Based CN Username Select

□ Password Based

Additional Attribute Retrieval Search List

An optional set of additional identity stores from which attributes will be retrieved

Available	Selected
Internal Hosts Internal Users NAC Profiler	AD1



General

Name: CN Username

Description: Predefined Certificate Authentication Profile

Certificate Definition

Principal Username X509 Attribute: Common Name

□ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

Name:

See the Installing Certificates section for more information.

Protected Extensible Authentication Protocol (PEAP)

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

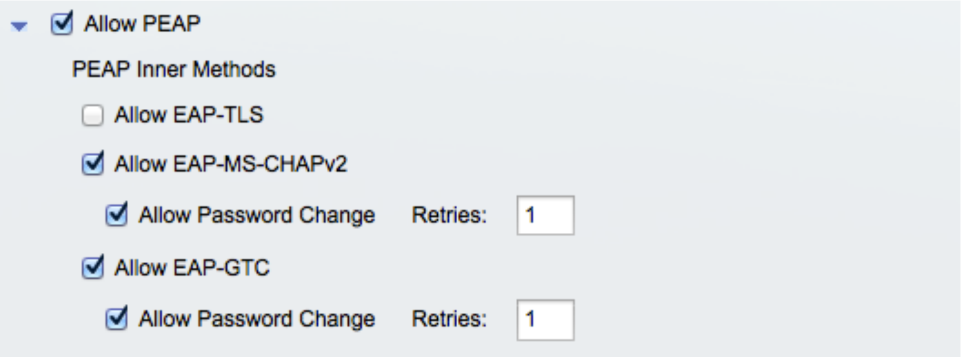
The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping.

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

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

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

See the Installing Certificates section for more information.



- ☑ Allow PEAP
  - PEAP Inner Methods
  - □ Allow EAP-TLS
  - ☑ Allow EAP-MS-CHAPv2
    - ☑ Allow Password Change Retries: 1
  - ☑ Allow EAP-GTC
    - ☑ Allow Password Change Retries: 1

For more information on Cisco Secure Access Control System (ACS) and Cisco Identity Services Engine (ISE), refer to the following links.

http://www.cisco.com/c/en/us/products/security/secure-access-control-system/datasheet-listing.html

http://www.cisco.com/c/en/us/products/security/identity-services-engine/datasheet-listing.html

Fast Secure Roaming (FSR)

CCKM is the recommended deployment model for all environment types where frequent roaming occurs.

CCKM enables fast secure roaming and limits the off-network time to keep audio gaps at a minimum when on call.

802.1x authentication is required in order to utilize CCKM.

802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.

CCKM centralizes the key management and reduces the number of key exchanges.

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

The Cisco DX Series supports CCKM with WPA2 (AES or TKIP) or WPA (TKIP or AES), where WPA2 (AES) with CCKM is recommended.

FSR Type	EAP Type	Key Management	Encryption

CCKM	EAP-FAST	WPA2, WPA	AES, TKIP
CCKM	EAP-TLS	WPA2, WPA	AES, TKIP
CCKM	PEAP-GTC	WPA2, WPA	AES, TKIP
CCKM	PEAP-MSCHAPv2	WPA2, WPA	AES, TKIP

EAP and User Database Compatibility

The following chart displays the EAP and database configurations supported by the Cisco DX Series.

Database Type	**EAP-FAST (Phase Zero)**	**EAP-TLS**	**PEAP-GTC**	**PEAP-MSCHAPv2**
Cisco ACS	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	Yes	Yes
Windows AD	Yes	Yes	Yes	Yes
LDAP	No	Yes	Yes	No
ODBC (ACS for Windows Only)	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	Yes	Yes
All Token Servers	No	No	No	No

Power Management

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

The Cisco DX650 utilizes the CP-PWR-CUBE-4= power supply and the Cisco DX70 and DX80 utilize the CP-PWR-CUBE-5= power supply.

Wireless LAN is automatically disabled when Ethernet is connected and must be re-enabled manually once Ethernet is disconnected.

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

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

Delivery Traffic Indicator Message (DTIM)

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

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

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

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

Quality of Service (QoS)

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

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

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

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384 - 32767
Interactive Video & Audio for Video Calls	AF41 (34)	4	5	UDP 16384 - 32767
TelePresence Calls (Voice & Video)	CS4 (32)	4	5	UDP 16384 - 32767
Call Control	CS3 (24)	3	4	TCP 5060 - 5061

- Be sure that voice, interactive video, and call control packets have the proper QoS markings and other protocols are not using the same QoS markings.
- Select the **Platinum** QoS profile for the WLAN when using Cisco Unified Wireless LAN Controller technology and set the 802.1p tag to **5.**
- Enable Differentiated Services Code Point (DSCP) preservation on the Cisco IOS switch.

Note: Voice and interactive video frames will be marked with DSCP AF41 and WMM UP 5 for standard video calls.

As of the 10.1(1) release for the Cisco DX Series with the Cisco Unified Communications Manager 10.0 release, voice and video frames for TelePresence calls will be marked with DSCP CS4 and WMM UP 5.

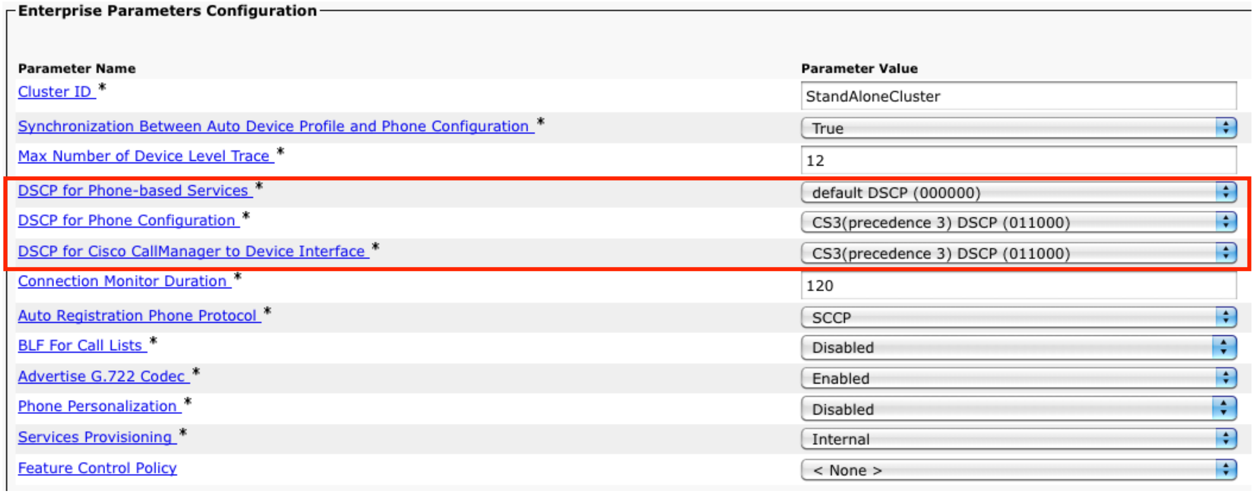
The WMM UP marking could be downgraded if CAC (TSPEC) is enabled for voice or video.

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

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/10_0_1/CUCM_BK_T537717B_00_tcp-port-usage-guide-100.html

Configuring QoS in Cisco Unified Communications Manager

The SIP DSCP values are configured in the Cisco Unified Communications Manager enterprise parameters. Cisco Unified Communications Manager uses the default value of CS3 to have devices set the DSCP marking for SIP packets as shown in the Enterprise Parameters Configuration page.



Enterprise Parameters Configuration

Parameter Name	Parameter Value
Cluster ID *	StandAloneCluster
Synchronization Between Auto Device Profile and Phone Configuration *	True
Max Number of Device Level Trace *	12
DSCP for Phone-based Services *	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120
Auto Registration Phone Protocol *	SCCP
BLF For Call Lists *	Disabled
Advertise G.722 Codec *	Enabled
Phone Personalization *	Disabled
Services Provisioning *	Internal
Feature Control Policy	< None >

Configuring QoS Policies for the Network

Configure QoS policies and settings for the following network devices.

Configuring Cisco Switch Ports

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

Configure the Cisco Unified Wireless LAN Controller for trust COS.

Below is a sample switch configuration for the Cisco Unified Wireless LAN controller:

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

Configure the Cisco Access Point switch ports as well as any uplink switch ports for trust DSCP.

Below is a sample switch configuration for an access point:

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

Note: When using the Cisco Unified Wireless LAN Controller, DSCP trust must be implemented or trust the UDP data ports used by the Cisco Unified Wireless LAN Controller (CAPWAP = 5246 and 5247) on all interfaces where wireless packets will traverse to ensure QoS markings are correctly set.

Configuring Cisco IOS Access Points

Use the following QoS policy on the Cisco IOS Access Point (AP) to enable DSCP to CoS (UP) mapping. This allows packets to be placed into the proper queue as long as those packets are marked correctly when received at the access point level.

```
Class-map match-all Voice
 match ip dscp ef
class-map match-all Video
 match ip dscp af41
class-map match-all TelePresence
 match ip dscp cs4
class-map match-all CallControl
 match ip dscp cs3
!
policy-map DX
 class Voice
  set cos 6
class Video
  set cos 5
class TelePresence
  set cos 5
 class CallControl
  set cos 4
!
interface dot11radioX
 service-policy input DX
 service-policy output DX
```

Configuring Switch Ports for Wired IP Phones

Enable the Cisco wired IP phone switch ports for Cisco phone trust.

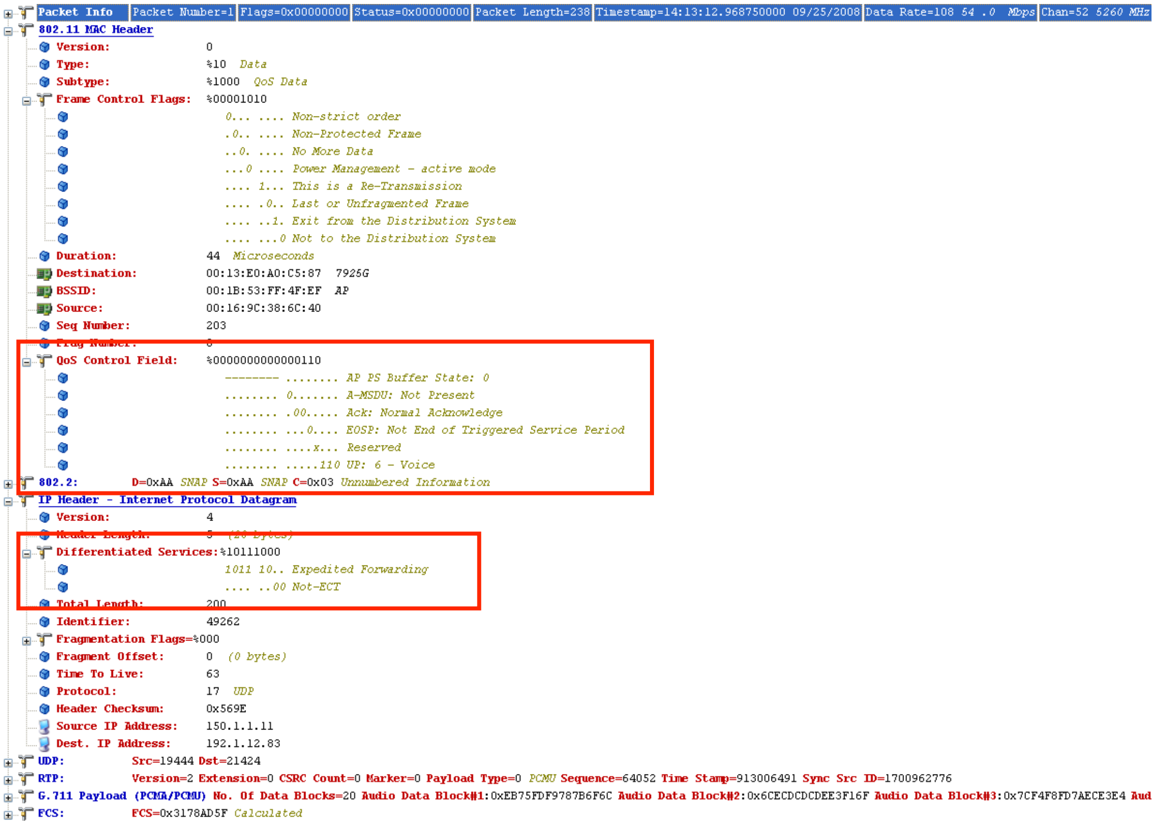
Below is a sample switch configuration:

```
mls qos
!
Interface X
 mls qos trust device cisco-phone
 mls qos trust dscp
```

Sample Voice Packet Capture

The packet capture below displays a voice packet bound for the Cisco DX Series over the air being marked as DSCP = EF and UP = 6.

This would require that admission control mandatory to be disabled for voice, otherwise the voice frame would be downgraded to a lower user priority (UP) since the Cisco DX Series does not currently support TSPEC.



```
Packet Info   Packet Number=1 Flags=0x00000000 Status=0x00000000 Packet Length=238 Timestamp=14:13:12.968750000 09/25/2008 Data Rate=108 54 .0  Mbps Chan=52 5260 MHz
802.11 MAC Header
  Version:              0
  Type:                 %10  Data
  Subtype:              %1000  QoS Data
  Frame Control Flags:  %00001010
                           0... .... Non-strict order
                           .0.. .... Non-Protected Frame
                           ..0. .... No More Data
                           ...0 .... Power Management - active mode
                           .... 1... This is a Re-Transmission
                           .... .0.. Last or Unfragmented Frame
                           .... ..1. Exit from the Distribution System
                           .... ...0 Not to the Distribution System
  Duration:             44  Microseconds
  Destination:          00:13:E0:A0:C5:87  7925G
  BSSID:                00:1B:53:FF:4F:EF  AP
  Source:               00:16:9C:38:6C:40
  Seq Number:           203
  Frag Number:          0
  QoS Control Field:    %0000000000000110
                           -------- ........ AP PS Buffer State: 0
                           ........ 0....... A-MSDU: Not Present
                           ........ .00..... Ack: Normal Acknowledge
                           ........ ...0.... EOSP: Not End of Triggered Service Period
                           ........ ....x... Reserved
                           ........ .....110 UP: 6 - Voice
802.2:          D=0xAA SNAP S=0xAA SNAP C=0x03 Unnumbered Information
IP Header - Internet Protocol Datagram
  Version:              4
  Header Length:        5  (20 bytes)
  Differentiated Services:%10111000
                           1011 10.. Expedited Forwarding
                           .... ..00 Not-ECT
  Total Length:         200
  Identifier:           49262
  Fragmentation Flags=%000
  Fragment Offset:      0  (0 bytes)
  Time To Live:         63
  Protocol:             17  UDP
  Header Checksum:      0x569E
  Source IP Address:    150.1.1.11
  Dest. IP Address:     192.1.12.83
UDP:            Src=19444 Dst=21424
RTP:            Version=2 Extension=0 CSRC Count=0 Marker=0 Payload Type=0 PCMU Sequence=64052 Time Stamp=913006491 Sync Src ID=1700962776
G.711 Payload (PCMA/PCMU) No. Of Data Blocks=20 Audio Data Block#1:0xEB75FDF9787B6F6C Audio Data Block#2:0x6CECDCDCDEE3F16F Audio Data Block#3:0x7CF4F8FD7AECE3E4 Aud
FCS:            FCS=0x3178AD5F Calculated
```

Call Admission Control

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

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

Without TSPEC support, TCLAS is also not supported.

Since TSPEC is not supported at this time, SIP CAC and media session snooping can optionally be enabled on the Cisco Unified Wireless LAN Controller.

See the Configuring the Cisco Unified Wireless LAN Controller and Access Points section for more info including the pros and cons for enabling SIP CAC.

Roaming

The Cisco DX Series defaults to Auto for frequency band mode, which allows the DX Series to connect to either 5 GHz or 2.4 GHz.

As of the 10.2(2) release, the Cisco DX Series gives preference to 5 GHz over 2.4 GHz if configured for Auto frequency band.

When powered on, the DX Series will scan all 5 GHz and 2.4 GHz channels if configured for Auto frequency band mode, then will attempt to associate to a 5 GHz access point with strong signal (>= -67 dBm) if available using the locally configured network settings. If a 5 GHz AP with adequate signal is not available at power on, then the DX Series will attempt to associate to an available access point with the strongest RSSI.

Once connected, then only that frequency band range is scanned (e.g. scan all 5 GHz channels only if connected via 5 GHz) if configured for Auto frequency band, where the other frequency band range can only be scanned if the current connection is lost.

If the DX series frequency band is configured for 5 GHz only or 2.4 GHz only, then just those channels are scanned to discover neighbors.

The Cisco DX Series will list all neighbors within the same frequency band range as the connected access point in order from strongest RSSI to weakest RSSI.

If in the Wi-Fi settings menu and configured for Auto frequency band, both 5 GHz and 2.4 GHz frequency bands are scanned so all available WLANs can be displayed.

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

CCKM is the recommended deployment model for all environment types where frequent roaming occurs.

802.1x authentication is required in order to utilize CCKM.

802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.

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

The Cisco DX Series supports CCKM with WPA2 (AES or TKIP) or WPA (TKIP or AES), where WPA2 (AES) with CCKM is recommended.

Authentication	Roaming Time
WPA/WPA2 Personal	150 ms
WPA/WPA2 Enterprise	300 ms
CCKM	< 100 ms

The Cisco DX Series manages the scanning and roaming events.

Roaming can be triggered for either of the following reasons.

- RSSI Differential
- Max Tx Retransmissions (not receiving 802.11 acknowledgements from the access point)
- Missed Beacons
- AP Disconnect

The roaming trigger for the majority of roams should be due to meeting the required RSSI differential based on the current RSSI, which results in seamless roaming (no voice or video interruptions).

Unexpected roams are triggered either by missing contiguous 802.11 acknowledgements (Max Tx retransmissions) or missing beacons from the access point.

For seamless roaming to occur, the Cisco DX Series must be associated to an access point for at least 3 seconds, otherwise roams can occur based on packet loss (max tx retransmissions or missed beacons).

Roaming based on RSSI may not occur if the current signal has met the strong RSSI threshold.

Note: The Cisco DX Series does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

Multicast

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

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

With multicast, there is no guarantee that the packet will be received the by the client.

The multicast traffic will be sent at the highest mandatory / basic data rate enabled on the access point, so will want to ensure that only the lowest enabled rate is configured as the only mandatory / basic rate.

The client will send the IGMP join request to receive that multicast stream. The client will send the IGMP leave when the session is to be ended.

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

Ensure that IGMP snooping is also enabled on all switches.

It is recommended to enable Multicast Direct in the Cisco Unified Wireless LAN Controller.

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

Designing the Wireless LAN

The following network design guidelines must be followed in order to accommodate for adequate coverage, call capacity and seamless roaming for the Cisco DX Series.

Planning Channel Usage

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

5 GHz (802.11a/n)

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

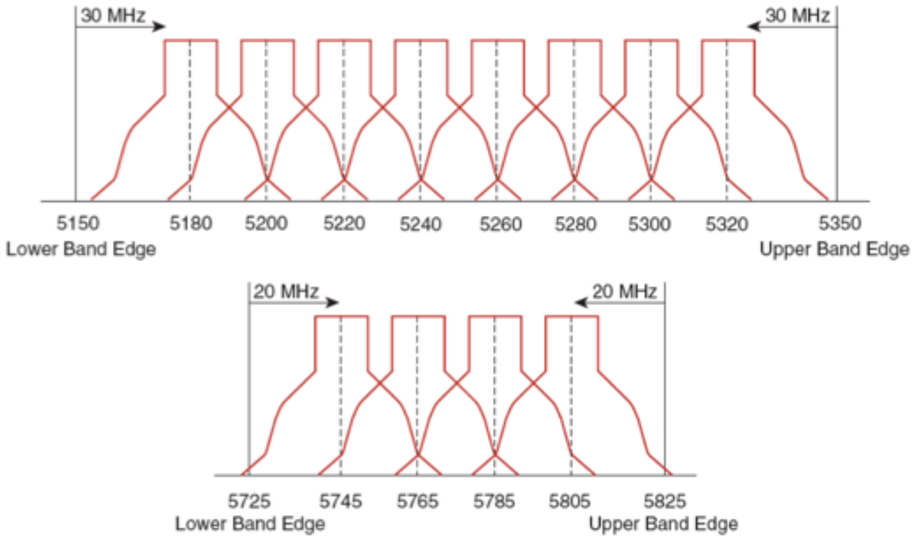
The Cisco DX Series supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.260 - 5.700 GHz, which are 15 of the 24 possible channels.

DFS dynamically instructs a transmitter to switch to another channel whenever radar signal is detected. If the access point detects radar, the radio on the access point goes on hold for at least 60 seconds while the access point passively scans for another usable channel.

TPC allows the client and access point to exchange information, so that the client can dynamically adjust the transmit power. The client uses only enough energy to maintain association to the access point at a given data rate. As a result, the client contributes less to adjacent cell interference, which allows for more densely deployed, high-performance wireless LANs.

5 GHz channels overlap their adjacent channel, so there should be at least 1 channel of separation for adjacent access points.

Need to ensure there is at least 20 percent overlap with adjacent channels when deploying the Cisco DX Series in the 802.11a/n environment, which allows for seamless roaming. For critical areas, it is recommended to increase the overlap (30% or more) to ensure that there can be at least 2 access points available with a signal of-67 dBm or higher, while the Cisco DX Series also meets the access point's receiver sensitivity (required signal level for the current data rate).



Channel ID	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161
Center Freq. MHz	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805
Band	UNII-1				UNII-2															UNNII-3			

Using Dynamic Frequency Selection (DFS) on Access Points

For Cisco Autonomous Access Points, select Dynamic Frequency Selection (DFS) to use auto channel selection.

When DFS is enabled, enable at least one band (bands 1-4).

For Cisco Unified Access Points, enable Auto RF unless there is an intermittent interferer in an area, which select access points can have the channel statically assigned.

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

The presence of an AP on a non-DFS channel can help minimize voice interruptions.

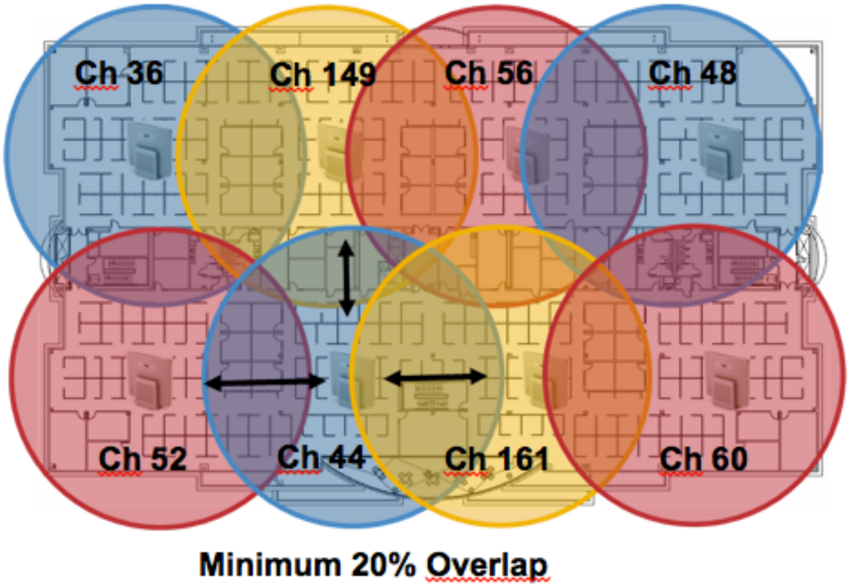
In case of radar activity, have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel is available when an access point's radio is in its hold-off period while scanning for a new usable channel.

For Cisco Autonomous Access Points, enable band 1 only, which allows the access point to use only a UNII-1 channel.

For Cisco Unified Access Points, can manually select a UNII-1 channel (channels 36, 40, 44, 48) for the desired access points.

A UNII-3 channel (5.745 - 5.825 GHz) can optionally be used if available.

In this diagram, 5 GHz cells use a non-DFS channel while other nearby cells use DFS channels to permit maximum call capacity under all conditions.

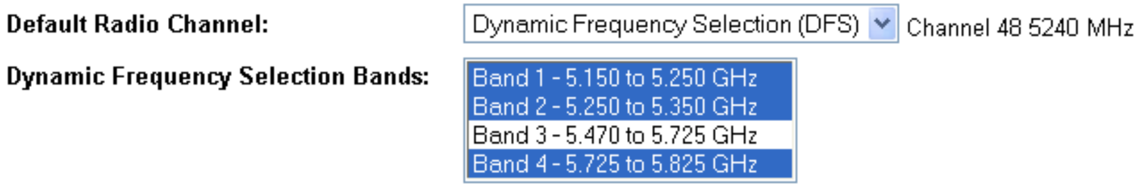


For 5 GHz, 21 channels are available in the Americas and 16 channels in Europe and Japan.

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 - 140), 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.



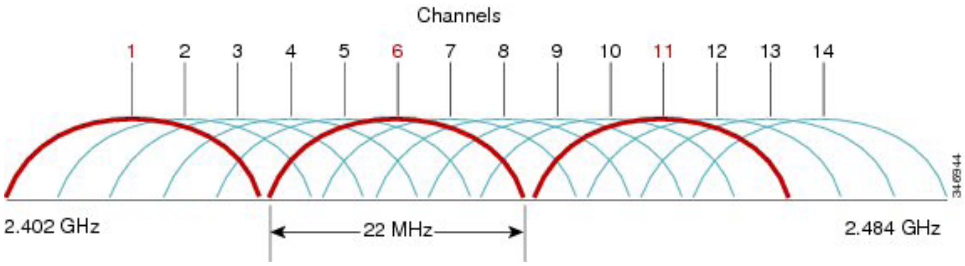
Default Radio Channel: Dynamic Frequency Selection (DFS) Channel 48 5240 MHz

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

2.4 GHz (802.11b/g/n)

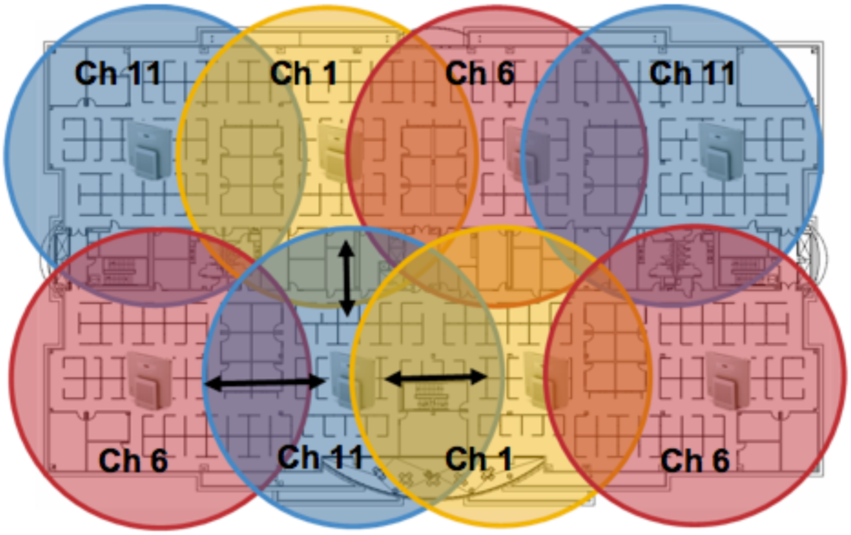
In the 2.4 GHz (802.11b/g/n environment, only non-overlapping channels must be utilized when deploying VoWLAN. Non-overlapping channels have 22 MHz of separation and are at least 5 channels apart.

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



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

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



Minimum 20% Overlap

Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco DX Series should always have a signal of -67 dBm or higher when using 2.4 GHz or 5 GHz, while the Cisco DX Series also meets the access point's receiver sensitivity required signal level for the transmitted data rate.

Ensure the Packet Error Rate (PER) is no higher than 1%.

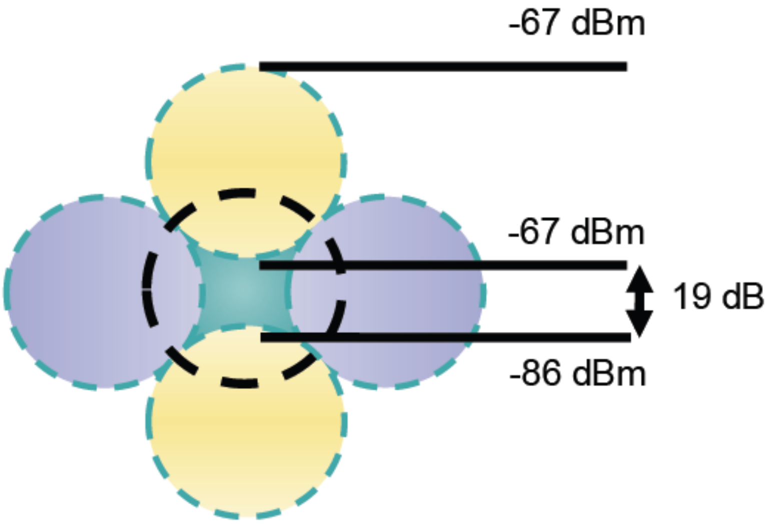
A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal should be maintained.

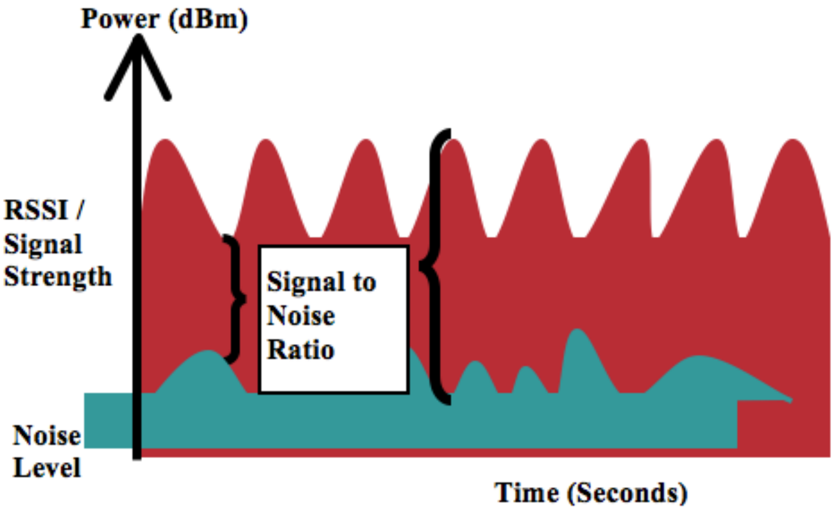
It is recommended to have at least two access points on non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.

To achieve maximum capacity and throughput, the wireless LAN should be designed to 24 Mbps. Higher data rates can optionally be enabled for other applications other than voice only that can take advantage of these higher data rates.

Recommended to set the minimum data rate to 11 Mbps or 12 Mbps for 2.4 GHz (dependent upon 802.11b client support policy) and 12 Mbps for 5 GHz, which should also be the only rate configured as a mandatory / basic rate.
In some environments, 6 Mbps may need to be enabled as a mandatory / basic rate.

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





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

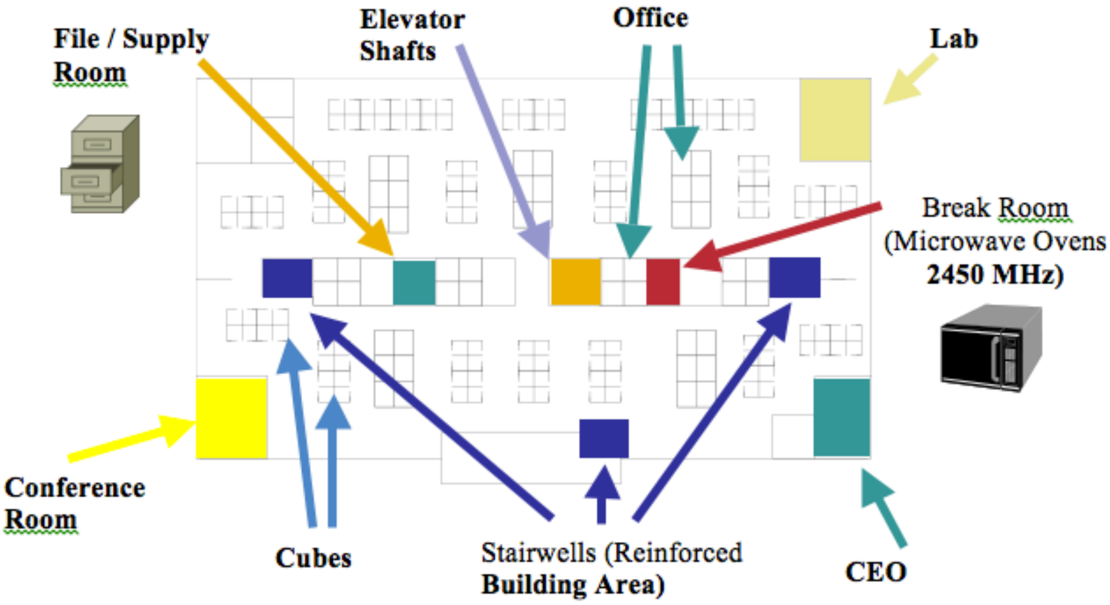
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

Wireless LAN interference is generated by microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or other electronic equipment operating in the 2.4 GHz band.

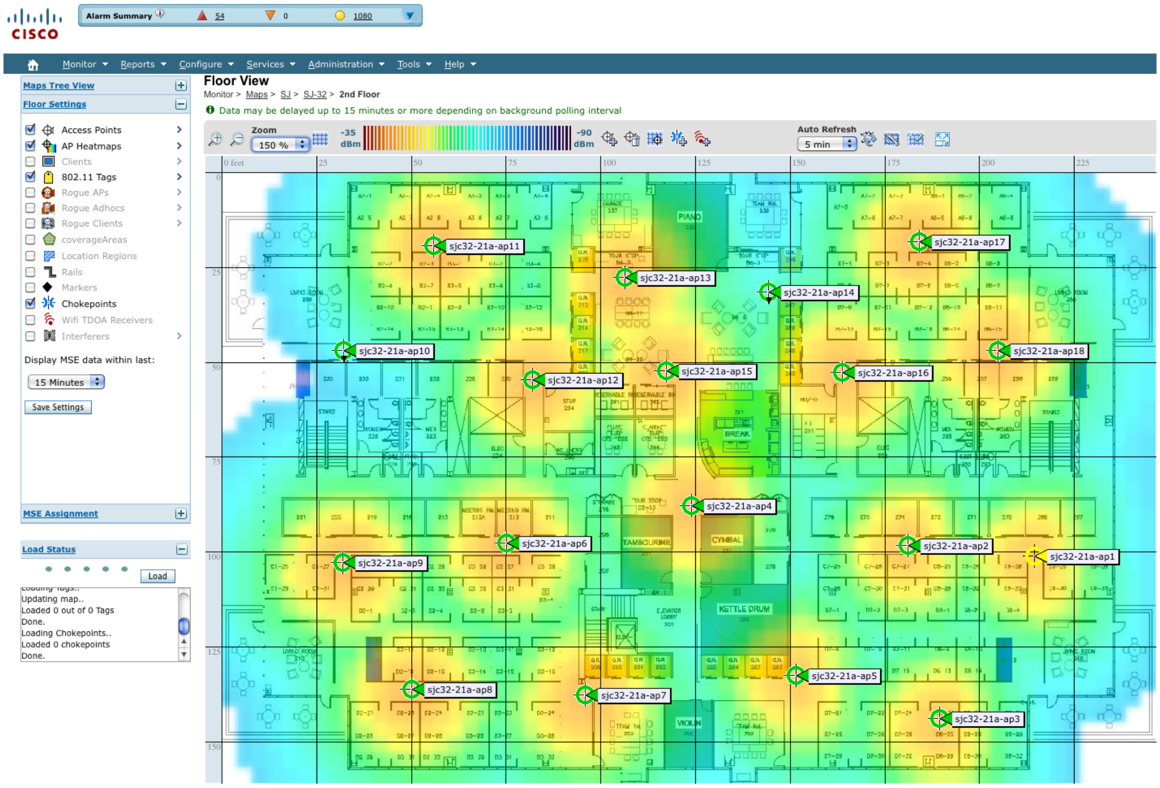
Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g/n. Some microwaves are shielded more than others and that shielding reduces the spread of the energy. Microwave energy can impact channel 11, and some microwaves can affect the entire frequency range (channels 1 through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

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


File / Supply Room
Elevator Shafts
Office
Lab
Break Room (Microwave Ovens 2450 MHz)
Conference Room
Cubes
Stairwells (Reinforced Building Area)
CEO

The Cisco Unified WCS or NCS can be utilized to verify signal strength and coverage.



Floor View

Monitor > Maps > SJ > SJ-32 > 2nd Floor

Data may be delayed up to 15 minutes or more depending on background polling interval

- ☑ Access Points
- ☑ AP Heatmaps
- □ Clients
- ☑ 802.11 Tags
- □ Rogue APs
- □ Rogue Adhocs
- □ Rogue Clients
- □ coverageAreas
- □ Location Regions
- □ Rails
- □ Markers
- ☑ Chokepoints
- □ Wifi TDOA Receivers
- □ Interferers

Display MSE data within last: 15 Minutes

Zoom: 150 %

Auto Refresh: 5 min

```
Updating map..
Loaded 0 out of 0 Tags
Done.
Loading Chokepoints..
Loaded 0 chokepoints
Done.
```

Configuring Data Rates

It is recommended to disable rates below 12 Mbps for 5 GHz deployments and for 2.4 GHz deployments where capacity and range are factored in for best results.

The Cisco DX Series has a single antenna, therefore it supports up to MCS 7 data rates for 802.11n connectivity (up to 50 Mbps).

Higher MCS rates can be left enabled for other 802.11n clients, which are utilizing the same band frequency and utilize MIMO (multiple input / multiple output) antenna technology, which can take advantage of those higher rates.

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

When 802.11b clients exist in the wireless network, then an 802.11b rate must be enabled and only an 802.11b rate can be configured as a mandatory / basic rate. In this case, is suggested to enable the data rates 11 Mbps and higher.

The recommended data rate configurations are the following:

802.11 Mode	Mandatory Data Rates	Supported Data Rates	Disabled Data Rates
802.11a/n	12 Mbps	18-54 Mbps, HT MCS 1 - MCS 7 (HT MCS 8 - MCS 23)	6, 9 Mbps, HT MCS 0
802.11g/n	12 Mbps	18-54 Mbps, HT MCS 1 - MCS 7 (HT MCS 8 - MCS 23)	1, 2, 5.5, 6, 9, 11 Mbps, HT MCS 0
802.11b/g/n	11 Mbps	12-54 Mbps, HT MCS 1 - MCS 7 (HT MCS 8 - MCS 23)	1, 2, 5.5, 6, 9 Mbps, HT MCS 0
802.11a	12 Mbps	18-54 Mbps	6, 9 Mbps
802.11g	12 Mbps	18-54 Mbps	1, 2, 5.5, 6, 9, 11 Mbps
802.11b/g	11 Mbps	12-54 Mbps	1, 2, 5.5, 6, 9 Mbps
802.11b	11 Mbps	None	1, 2, 5.5 Mbps

For a voice only application, data rates higher than 24 Mbps can optionally be enabled or disabled, but there is no advantage from a capacity or throughput perspective and enabling these rates could potentially increase the number of retries for a data frame.

Other applications such as video may be able to benefit from having these higher data rates enabled.

To preserve high capacity and throughput, data rates of 24 Mbps and higher should be enabled.

If deploying in an environment where excessive retries may be a concern, then a limited set of the data rates can be used (e.g. 12, 24, 54, MCS 1, MCS 4, MCS 7), where the lowest enabled rate is the mandatory / basic rate.

For rugged environments or deployments requiring maximum range, it is recommended to enable 6 Mbps as a mandatory / basic rate.

Note: Some environments may require that a lower data rate be enabled due to use of legacy clients, environmental factors or maximum range is required.

Set only the lowest data rate enabled as the single mandatory / basic rate. Multicast packets will be sent at the highest mandatory / basic data rate enabled.

Note that capacity and throughput are reduced when lower rates are enabled.

Call Capacity

Design the network to accommodate the desired call capacity.

The Cisco Access Point can support up to 27 bi-directional voice streams for both 802.11a/n and 802.11g/n at a data rate of 24 Mbps or higher. To achieve this capacity, there must be minimal wireless LAN background traffic and initial radio frequency (RF) utilization.

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

Max # of Streams	Audio Codec	Audio Bit Rate	802.11 Mode	Data Rate
13	G.722 / G.711	64 Kbps	802.11a/n or 802.11g/n + Bluetooth Disabled	6 Mbps
20	G.722 / G.711	64 Kbps	802.11a/n or 802.11g/n + Bluetooth Disabled	12 Mbps
27	G.722 / G.711	64 Kbps	802.11a/n or 802.11g/n + Bluetooth Disabled	24 Mbps or higher

Video Calls

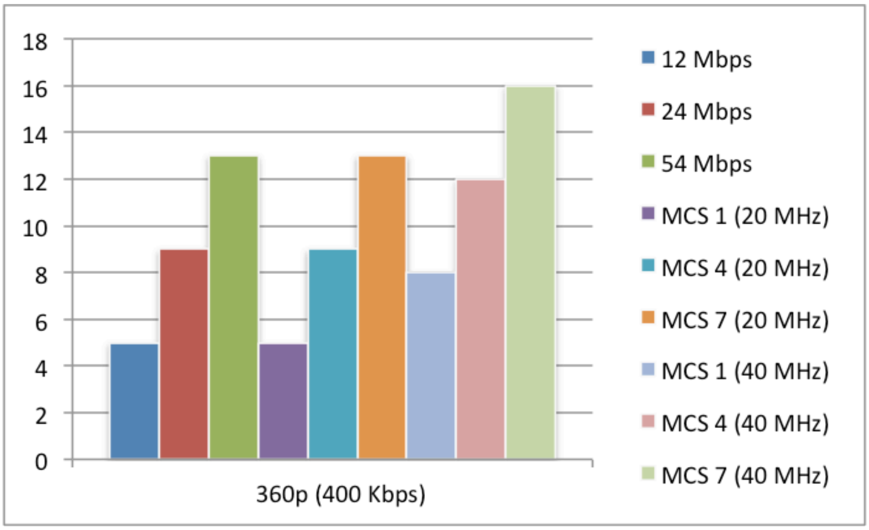
Video calls over Wireless LAN will significantly reduce the potential call capacity.

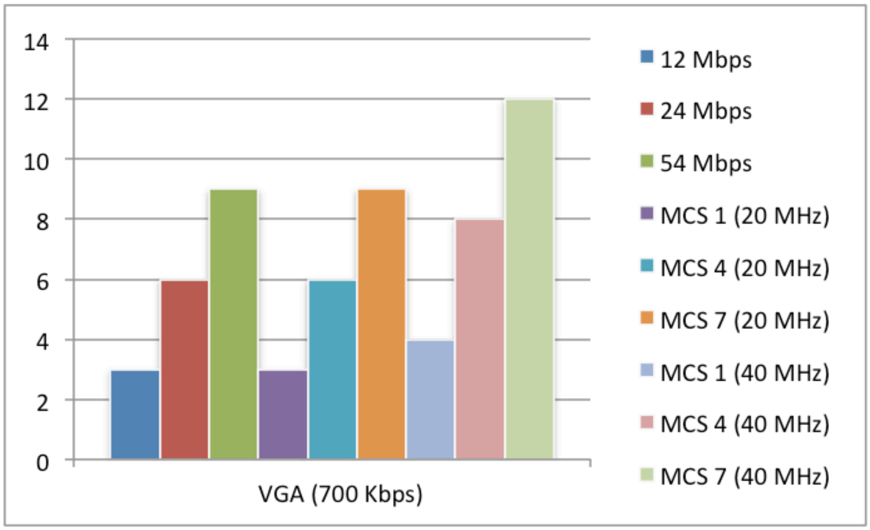
Below lists the maximum number of video calls (single bi-directional voice and video stream) supported per access point / channel for each video bit rate.

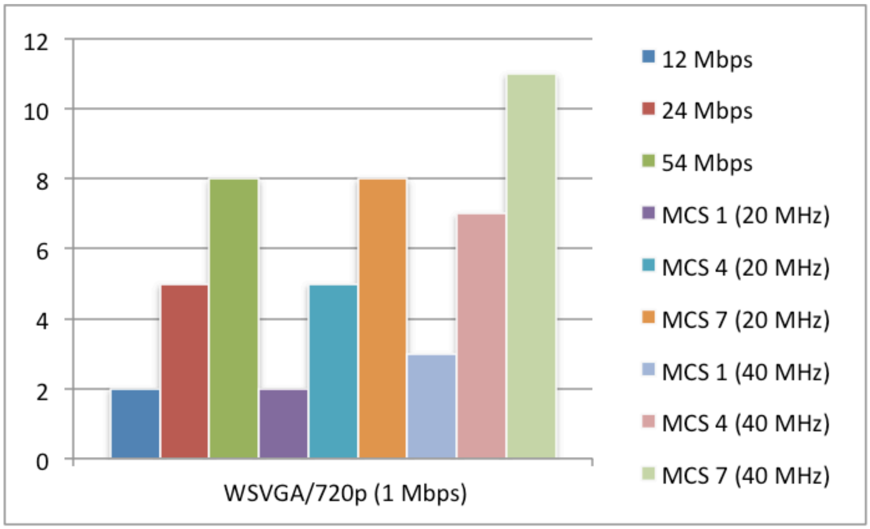
If there are two Cisco DX Series endpoints communicating to each other, then that is two bi-directional voice and video streams.

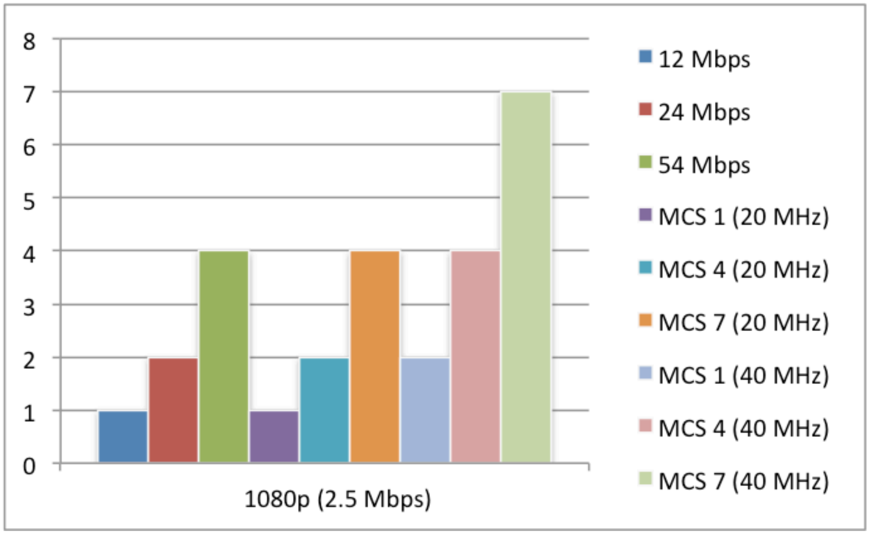
Max # of Video Calls	802.11 Mode	802.11 Data Rate	Audio Codec	Audio Bit Rate	Video Type	Video Resolution	Video Bit Rate
5-13	802.11a or 802.11g + Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	360p	640 x 360	400 Kbps
5-13	802.11a/n or 802.11g/n + Bluetooth Disabled	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	360p	640 x 360	400 Kbps
8-16	802.11a/n or 802.11g/n + Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	360p	640 x 360	400 Kbps
3-9	802.11a or 802.11g + Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	VGA	640 x 480	700 Kbps
3-9	802.11a/n or 802.11g/n +	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	VGA	640 x 480	700 Kbps

	Bluetooth Disabled						
4-12	802.11a/n or 802.11g/n + Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	VGA	640 x 480	700 Kbps
2-8	802.11a or 802.11g + Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 Kbps
2-8	802.11a/n or 802.11g/n + Bluetooth Disabled	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 Kbps
3-11	802.11a/n or 802.11g/n + Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 Kbps
1-4	802.11a or 802.11g + Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	1080p	1920 x 1080	2500 Kbps
1-4	802.11a/n or 802.11g/n + Bluetooth Disabled	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	1080p	1920 x 1080	2500 Kbps
2-7	802.11a/n or 802.11g/n + Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	1080p	1920 x 1080	2500 Kbps









Note: Currently there is no Call Admission Control support for video.

Dynamic Transmit Power Control (DTPC)

To ensure packets are exchanged successfully between the Cisco DX Series and the access point, Dynamic Transmit Power Control (DTPC) should be enabled.

DTPC prevents one-way audio when RF traffic is heard in one direction only.

If the access point does not support DTPC, then the Cisco DX Series will use the highest available transmit power depending on the current channel and data rate.

When using an access point that supports DTPC, set the client power to match the local access point power.

Do not use default setting of **Max** power for client power on Cisco Autonomous Access Points as that will not advertise DTPC to the client.

The access point's radio transmit power should not have a transmit power greater than what the Cisco DX Series can support.

Rugged Environments

When deploying the Cisco DX Series in a rugged environment (e.g. manufacturing, warehouse, retail), additional tuning on top of the standard design recommendations may be necessary.

Below are the key items to focus on when deploying a wireless LAN in a rugged environment.

Access Point and Antenna Selection
For rugged environments, it is recommended to select an access point platform that requires external antennas (e.g. Cisco 1602e, 2602e, 3502e, 3602e, and 3702e Series Access Points). It is also important to ensure an antenna type is selected which can operate well in rugged environments.

Access Point Placement
It is crucial that line of sight to the access point's antennas is maximized by minimizing any obstructions between the Cisco DX Series and the access point. Ensure that the access point and/or antennas are not mounted behind any obstruction or on or near a metal or glass surface.
If access points with integrated antennas (e.g. Cisco 1040, 1130, 1140, 1602i, 2602i, 3502i, 3602i, and 3702i Series Access Points) 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 patches.

Frequency Band
As always, it is recommended to use 5 GHz. Use of 2.4 GHz, especially when 802.11b rates are enabled, may not work well.
For the 5 GHz channel set, it is recommended to use a 8 or 12 channel plan only; disable UNII-2 extended channels if possible.

Data Rates
The standard recommended data rate set may not work well if multipath is present at an elevated level.
Therefore, it is recommended to enable lower data rates (e.g. 6 Mbps) to operate better in such an environment.
If using for voice only, then data rates above 24 Mbps can be disabled to increase first transmission success. If the same band is also used for data, video or other applications, then is suggested to keep the higher data rates enabled.

Transmit Power
Due to the potential of elevated multipath in rugged environments, the transmit power of the access point and the Cisco DX Series should also be restricted. This is more important if planning to deploy 2.4 GHz in a rugged environment.
If using auto transmit power, the access point transmit power can be configured to use a specified range (maximum and minimum power levels) to prevent the access point from transmitting too hot as well as too weak (e.g. 5 GHz maximum of 16 dBm and minimum of 11 dBm).

The Cisco DX Series will utilize the access point's current transmit power setting to determine what transmit power it uses for transmitted frames when DTPC is enabled in the access point's configuration.

Fast Roaming

It is recommended to utilize CCKM for fast roaming. Enabling CCKM also reduces the number of frames in the handshake when roaming to only two frames. Reducing the number of frames during a roam, increases the chances of roam success. When using 802.1x authentication, it is important to use the recommended EAPOL key settings. See the **WLAN Controller Advanced EAP Settings** section in **Configuring the Cisco Unified Wireless LAN Controller and Access Points** for more information.

Quality of Service (QoS)

Need to ensure that DSCP values are preserved throughout the wired network, so that Cisco Unified Wireless LAN Controller and access points can set the WMM UP tag for voice and call control frames correctly.

Beamforming

If using Cisco 802.11n access points, then Beamforming (ClientLink) should be enabled, which can help with client reception.
See the **Beamforming (ClientLink)** section in **Configuring the Cisco Unified Wireless LAN Controller and Access Points** for more information.

Multipath

Multipath occurs when RF signals take multiple paths from a source to a destination.

A part of the signal goes to the destination while another part bounces off an obstruction, then goes on to the destination. As a result, part of the signal encounters delay and travels a longer path to the destination, which creates signal energy loss.

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

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

Below is a list of multipath effects:

Data Corruption

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

Signal Nulling

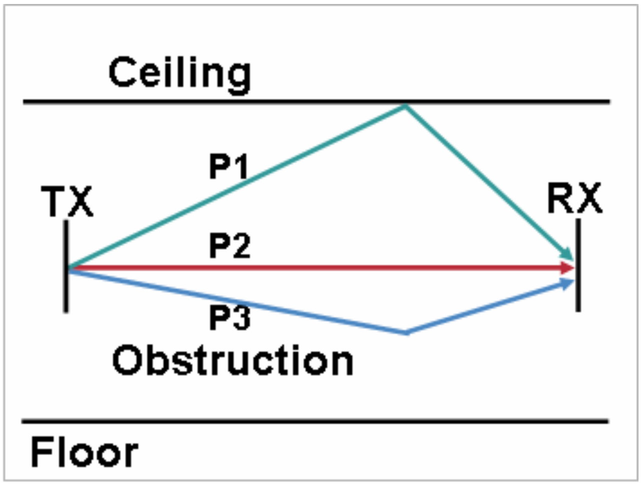
Occurs when the reflected waves arrive exactly out of phase with the main signal and cancel the main signal completely.

Increased Signal Amplitude

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

Decreased Signal Amplitude

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



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

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

Use of antenna diversity can also help in such environments.

Verification with Site Survey Tools

These are many tools and applications that can be utilized to verify coverage, quality and configuration.

- Cisco Prime Network Control System (NCS) for Unified Wireless LAN Management

  http://www.cisco.com/c/en/us/products/collateral/wireless/prime-network-control-system-series-appliances/data_sheet_c78-650051.html

- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management

  http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product_data_sheet0900aecd802570d0.html

- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management

  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/ciscoworks-wireless-lan-solution-engine-software-2-13/product_data_sheet0900aecd80410b92.html

- Cisco Spectrum Expert

  http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert/product_data_sheet0900aecd807033c3.html

- Cisco Unified Operations Manager

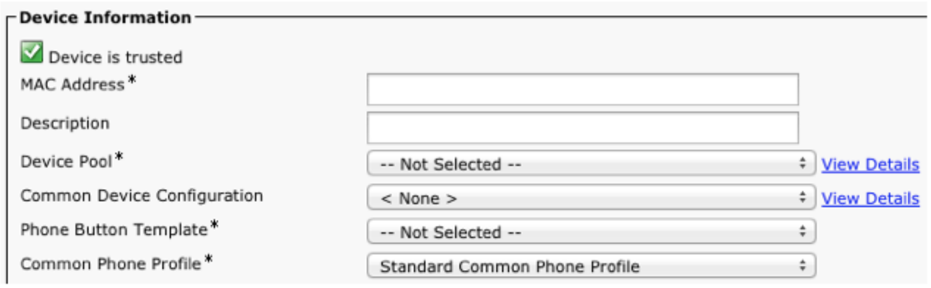
  http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-unified-operations-manager/data_sheet_c78-636705.html

Configuring Cisco Unified Communications Manager

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

When adding the Cisco DX Series to the Cisco Unified Communications Manager it must be provisioned using the Ethernet MAC address as the Wireless LAN MAC is used for Wi-Fi connectivity only.

The Ethernet MAC address can be found by navigating to **Settings** > **About Device** > **Status** on the Cisco DX Series.



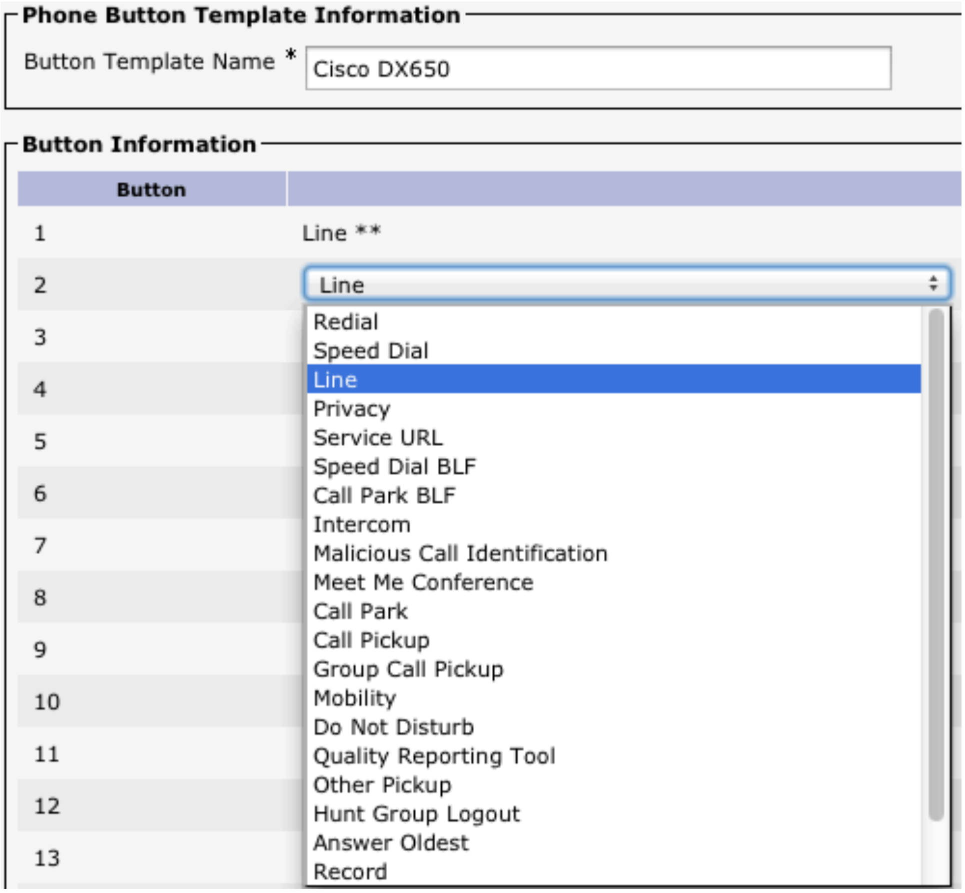
Device Information

☑ Device is trusted

MAC Address*		
Description		
Device Pool*	-- Not Selected --	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	-- Not Selected --	
Common Phone Profile*	Standard Common Phone Profile	

Phone Button Templates

Custom phone button templates can be created with the option for many different features, which can then be applied on a device or group level.



Phone Button Template Information

Button Template Name * Cisco DX650

Button Information

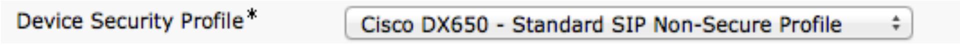
Button	
1	Line **
2	Line
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	

Security Profiles

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

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

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

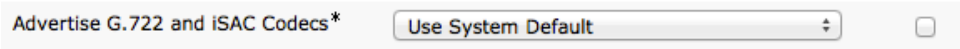


Device Security Profile* Cisco DX650 - Standard SIP Non-Secure Profile

G.722 and iSAC Advertisement

Cisco Unified Communications Manager supports the ability to configure whether G.722 and iSAC are to be a supported codec system wide or not.

G.722 and iSAC codecs can be disabled at the enterprise phone, common phone profile or individual phone level by setting **Advertise G.722 and iSAC Codecs** to **Disabled**.



Advertise G.722 and iSAC Codecs* Use System Default □

For more information, refer to the Cisco Unified Communications Manager documentation.

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

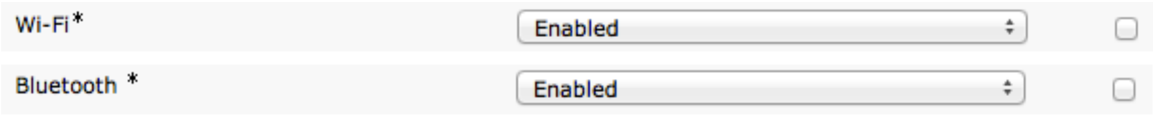
Common Settings

Some settings such as Wireless LAN and Bluetooth can be configured on an enterprise phone, common phone profile or individual phone level.

Wireless LAN and Bluetooth are enabled by default.

Wireless LAN is automatically disabled when Ethernet is connected and must be re-enabled manually once Ethernet is disconnected.

Override common settings can be enabled at either configuration level.



Wi-Fi* Enabled □

Bluetooth * Enabled □

Audio and Video Bit Rates

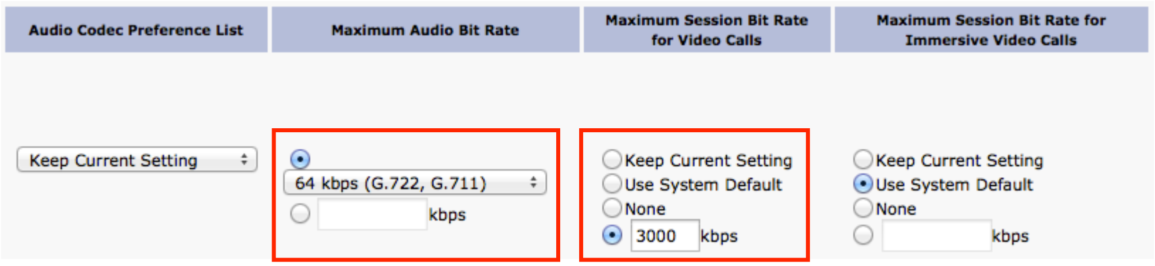
The audio and video bit rate can be configured by creating or editing existing Regions in the Cisco Unified Communications Manager.

It is recommended to select G.722 or G.711 for the audio codec.

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

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

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



Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Keep Current Setting	● 64 kbps (G.722, G.711) ○ kbps	○ Keep Current Setting ○ Use System Default ○ None ● 3000 kbps	○ Keep Current Setting ● Use System Default ○ None ○ kbps

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

Audio Codec	Audio Bit Rate
AAC-LD	128 Kbps
G.722 / G.711	64 Kbps
iSAC	32 Kbps
iLBC	16 Kbps
G.729	8 Kbps

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

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

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

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

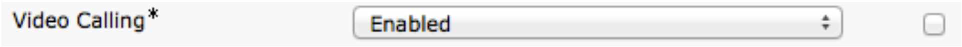
Video Type	Video Resolution	Frames per Second (fps)	Video Bit Rate Range
240p	432 x 240	15 / 30	64-149 Kbps / 150-2999 Kbps
360p	640 x 360	30	300-649 Kbps
480p	848 x 480	30	650-999 Kbps
600p	1024 x 600	30	1100-3000 Kbps
HD 720p	1280 x 720	30	1000-1599 Kbps
HD 1080p	1920 x 1080	30	1600-4000 Kbps
CIF	352 x 288	30	64-159 Kbps

VGA	640 x 480	30	400-1500 Kbps

Video Calling Capabilities

In order for the Cisco DX Series to send and receive video, that capability must be enabled in the Cisco Unified Communications Manager.

Set the **Video Calling** option to **Enabled** in the configuration within the Product Specific Configuration Layout section.

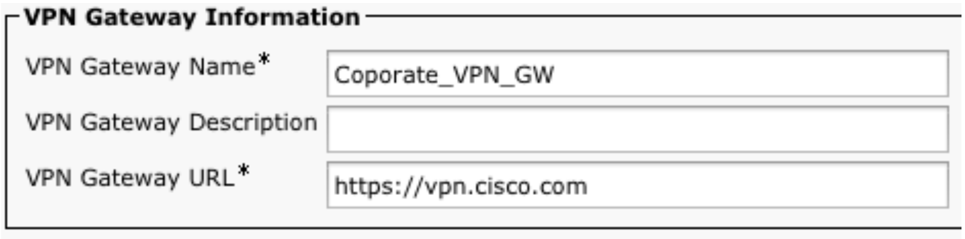


Video Calling* Enabled ☐

VPN Configuration

VPN configuration information can be pushed down from the administrator via Cisco Unified Communications Manager.

A VPN gateway must be created, where the name and VPN gateway URL are defined.



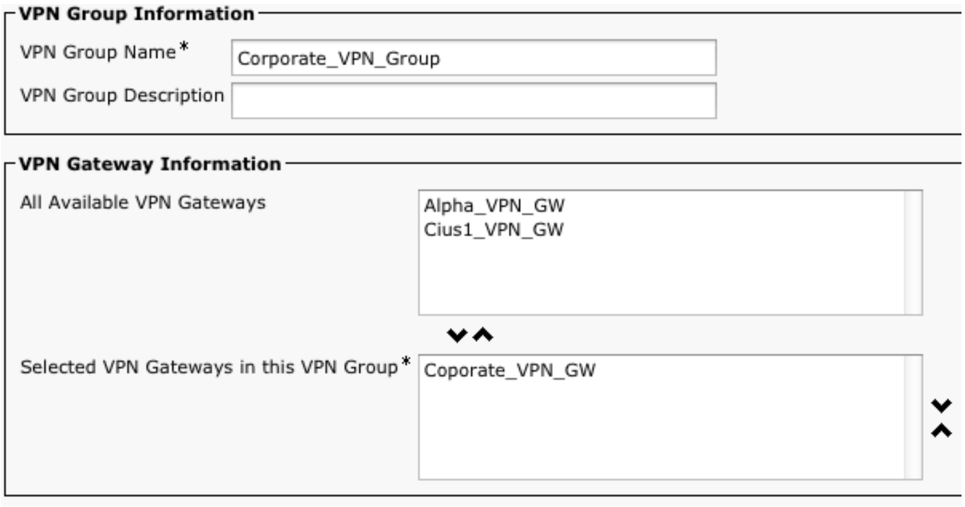
VPN Gateway Information

VPN Gateway Name* Coporate_VPN_GW

VPN Gateway Description

VPN Gateway URL* https://vpn.cisco.com

A VPN group must also be created, which contains information about which VPN gateway will be utilized.



VPN Group Information

VPN Group Name* Corporate_VPN_Group

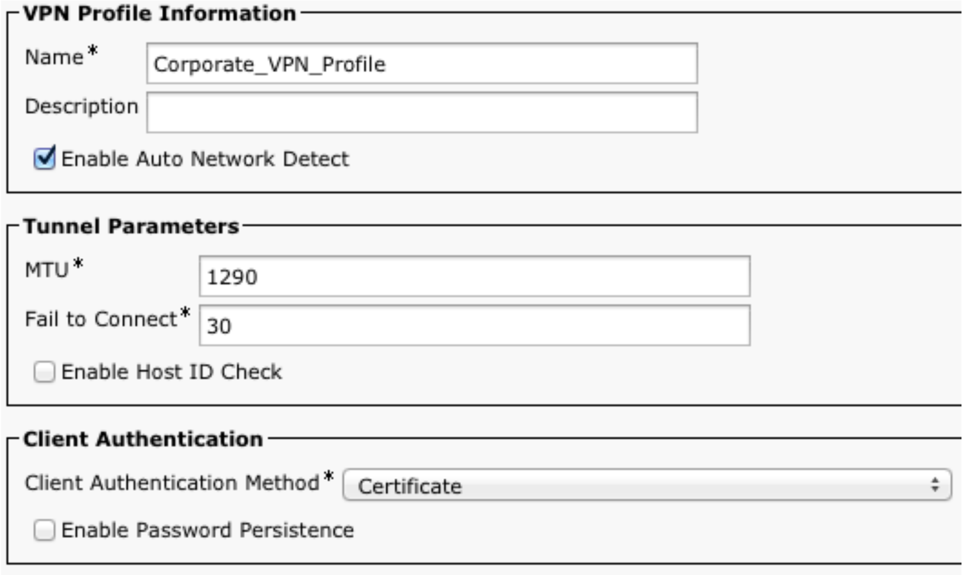
VPN Group Description

VPN Gateway Information

All Available VPN Gateways
Alpha_VPN_GW
Cius1_VPN_GW

Selected VPN Gateways in this VPN Group* Coporate_VPN_GW

A VPN profile must be configured, which specifies which type of client authentication will be utilized as well as other parameters.



VPN Profile Information

Name* Corporate_VPN_Profile

Description

☑ Enable Auto Network Detect

Tunnel Parameters

MTU* 1290

Fail to Connect* 30

☐ Enable Host ID Check

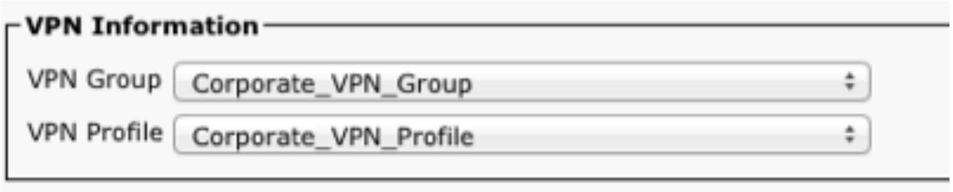
Client Authentication

Client Authentication Method* Certificate

☐ Enable Password Persistence

Once the VPN group and profile have been configured, they can then be applied to a Common Phone Profile, which in turn can be applied to a specific device.

If the Cisco DX Series is currently connected to a network and is unable to connect to the Cisco Unified Communications Manager then it can attempt to establish a VPN session automatically if a VPN profile is configured.



VPN Information

VPN Group Corporate_VPN_Group

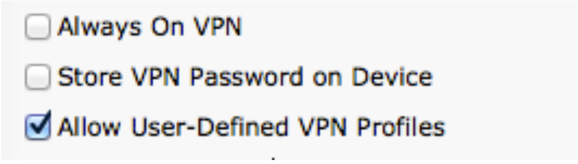
VPN Profile Corporate_VPN_Profile

Always on VPN, **Store VPN Password On Device** and **Allow User-Defined VPN Profiles** can be configured on an enterprise phone, common phone profile or individual phone configuration level.

Always On VPN can help ensure that the Cisco DX Series remains on a secure network and is always connected to Cisco Unified Communications Manager.

Store VPN Password on Device enables a VPN Password to be stored on the device

Allow User-Defined VPN Profiles can enable the user to create their own VPN profiles.



☐ Always On VPN

☐ Store VPN Password on Device

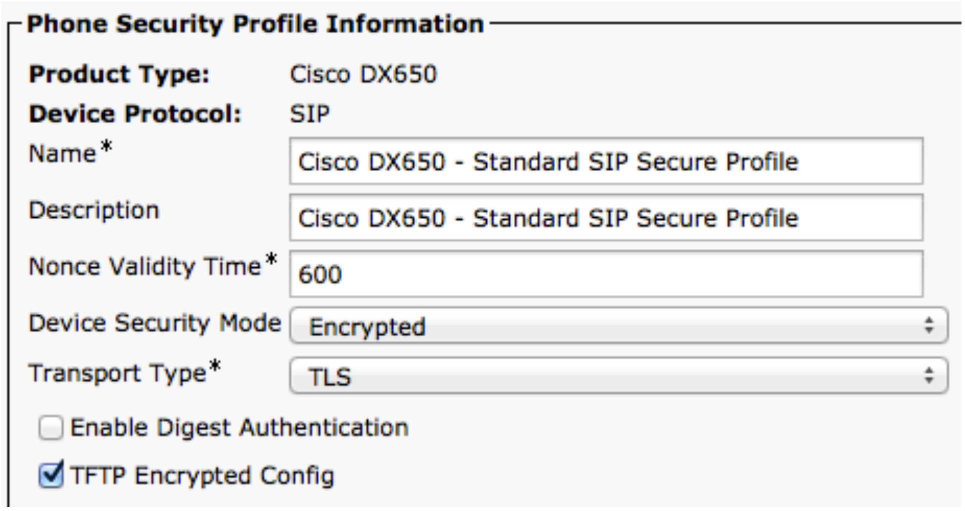
☑ Allow User-Defined VPN Profiles

Wireless LAN Profile Configuration

As of the 10.1(1) release for the Cisco DX Series with the Cisco Unified Communications Manager 10.0 release, the Cisco DX Series can be provisioned with Wireless LAN Profiles via the Cisco Unified Communications Manager.

For initial provisioning, it is recommended to connect the Cisco DX Series to the network via Ethernet.

Prior to creating a Wireless LAN Profile and associating it to a Cisco DX Series, the Cisco DX Series should be configured to utilize a security profile in which TFTP encryption is enabled so Wireless LAN Profile data is not passed down to the Cisco DX Series in clear text via TFTP.



Phone Security Profile Information

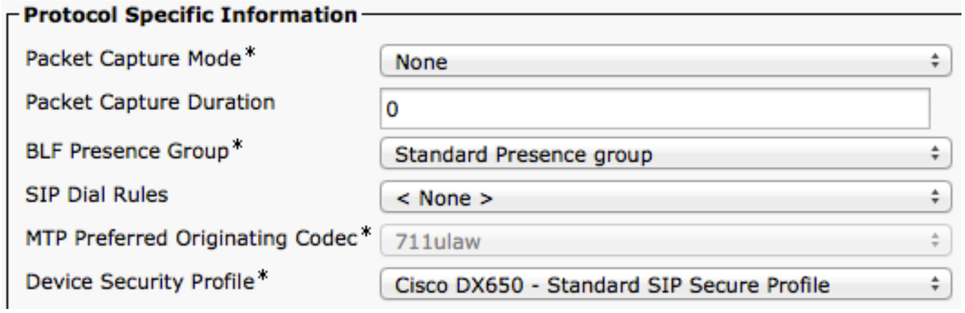
Product Type:	Cisco DX650
Device Protocol:	SIP
Name*	Cisco DX650 - Standard SIP Secure Profile
Description	Cisco DX650 - Standard SIP Secure Profile
Nonce Validity Time*	600
Device Security Mode	Encrypted
Transport Type*	TLS

☐ Enable Digest Authentication

☑ TFTP Encrypted Config

Once the security profile has been created, it then needs to be applied to the Cisco DX Series to enable TFTP encryption for that Cisco DX Series' configuration files.

Select the configured security profile from the **Device Security Profile** drop-down menu.

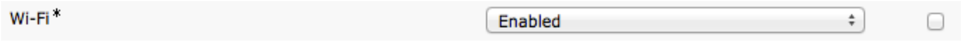


Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco DX650 - Standard SIP Secure Profile

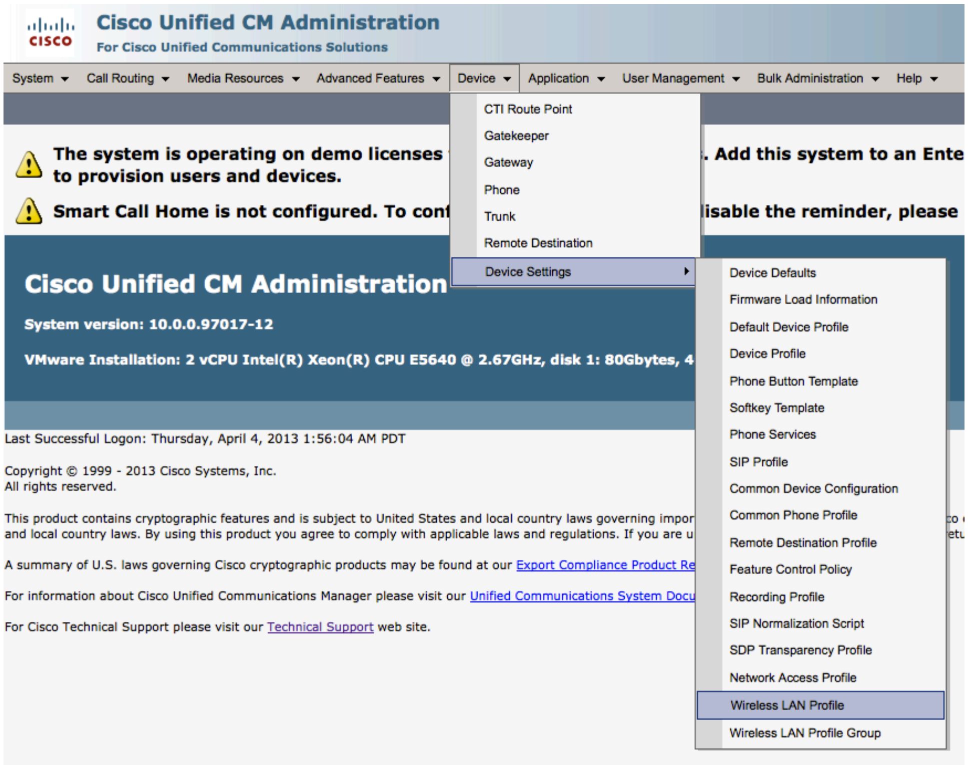
Wi-Fi is enabled by default for the Cisco DX Series, however the Wi-Fi feature can be managed at the Enterprise Phone Configuration, Common Phone Profile or individual phone level.

When using the Wireless LAN Profile feature, **Wi-Fi** must be enabled for the corresponding device otherwise the device will be unable to connect to the Wireless LAN.



Wi-Fi*	Enabled	☐

To create a Wireless LAN Profile, navigate to **Device > Device Settings > Wireless LAN Profile** within the Cisco Unified Communications Manager's Administration interface.



The system is operating on demo licenses . Add this system to an Ente
to provision users and devices.

Smart Call Home is not configured. To conf lisable the reminder, please

Cisco Unified CM Administration

System version: 10.0.0.97017-12

VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5640 @ 2.67GHz, disk 1: 80Gbytes, 4

Last Successful Logon: Thursday, April 4, 2013 1:56:04 AM PDT

Copyright © 1999 - 2013 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing impor co
and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are u etu

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Re

For information about Cisco Unified Communications Manager please visit our Unified Communications System Docu

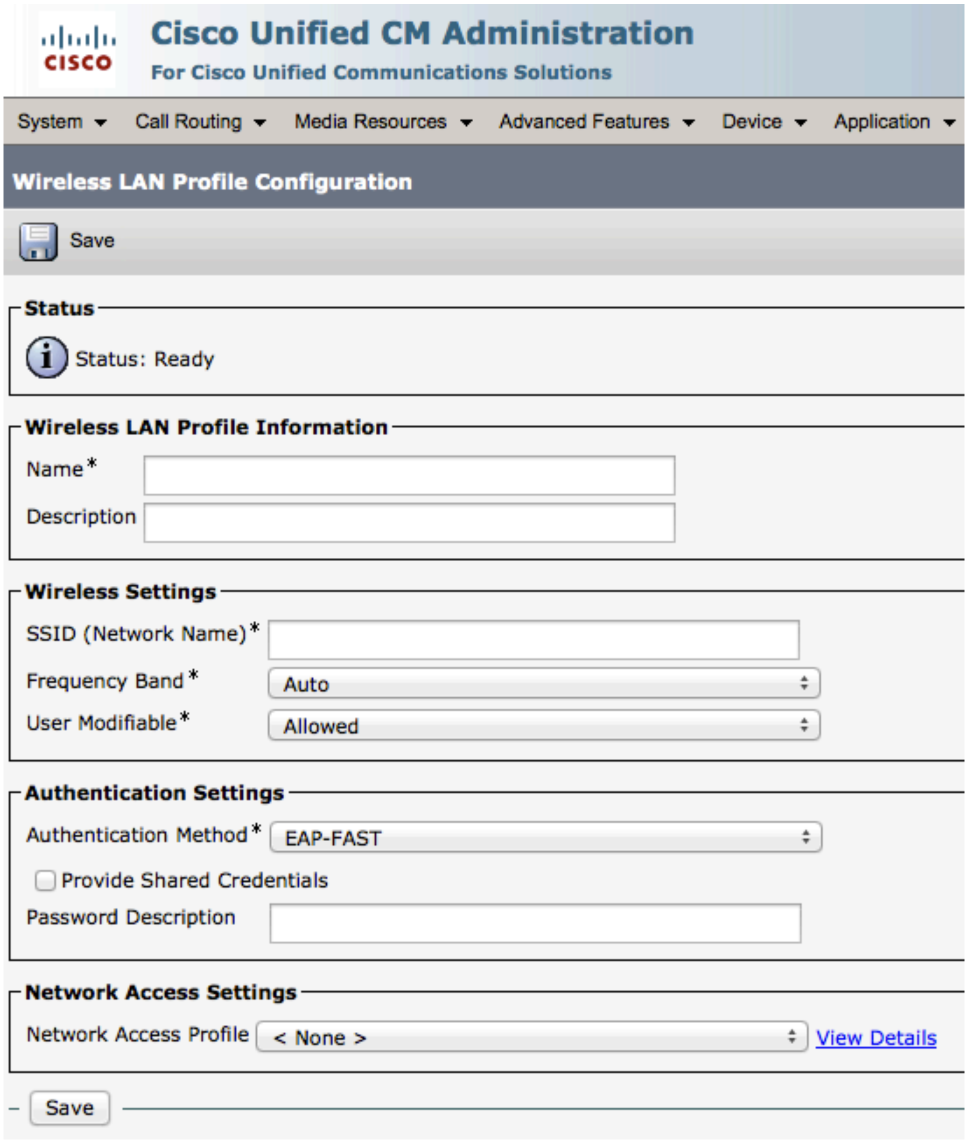
For Cisco Technical Support please visit our Technical Support web site.

From the Wireless LAN Profile page, select **Add New**.

A Wireless LAN Profile can then be created where the Name, Description, Wireless Settings (SSID, Frequency Band, User Modifiable), Authentication Settings, and Network Access Settings are specified.

Below are Wireless LAN Profile defaults:

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



Wireless LAN Profile Configuration

Status

Status: Ready

Wireless LAN Profile Information

Name*

Description

Wireless Settings

SSID (Network Name)*

Frequency Band* Auto

User Modifiable* Allowed

Authentication Settings

Authentication Method* EAP-FAST

□ Provide Shared Credentials

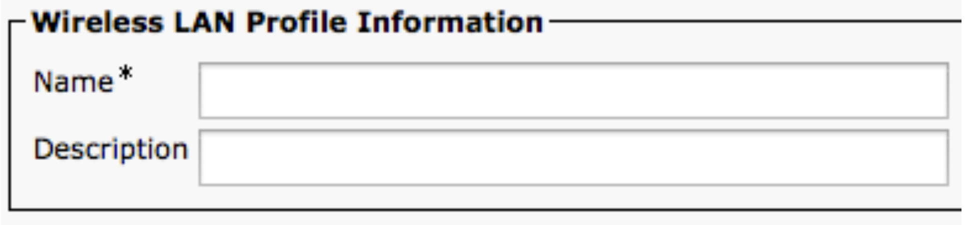
Password Description

Network Access Settings

Network Access Profile < None >

Enter a **Name** for the Wireless LAN Profile containing up to 50 characters.

A **Description** containing up to 63 characters can optionally be configured.

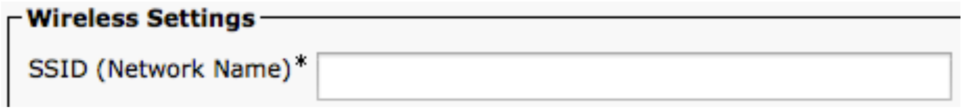


Wireless LAN Profile Information

Name*

Description

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



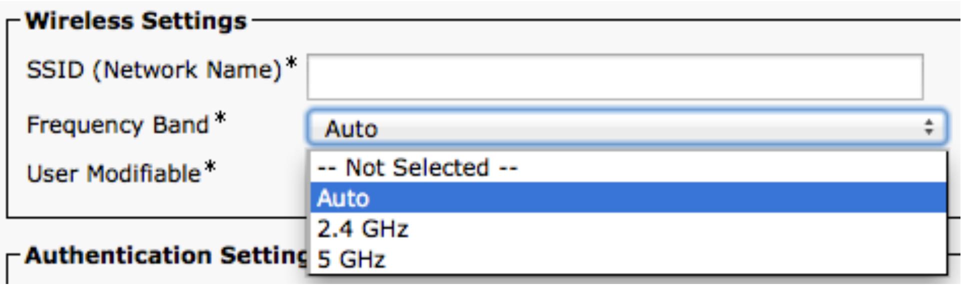
Wireless Settings

SSID (Network Name)*

Select the desired **Frequency Band** option.

Frequency Band is defaulted to Auto, which enables the Cisco DX Series to utilize both 2.4 GHz and 5 GHz frequencies.

If Auto is selected, preference will be given to the 5 GHz frequency band.



Wireless Settings

SSID (Network Name)*

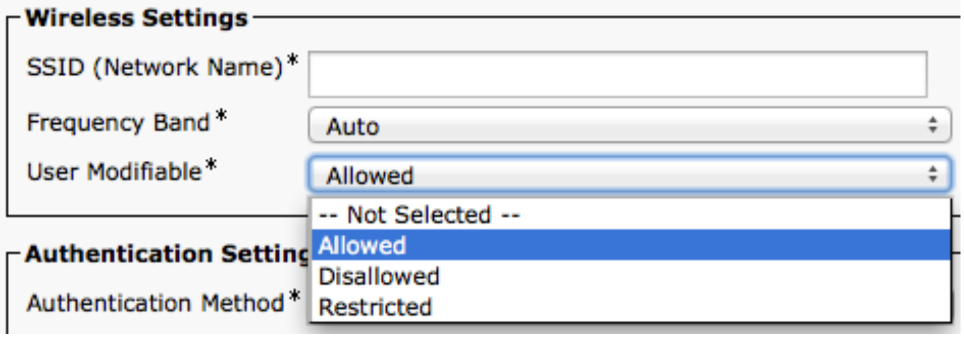
Frequency Band* Auto

User Modifiable*

Authentication Setting

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, WEP Key) locally on the endpoint.
- **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).



Wireless Settings

SSID (Network Name)*

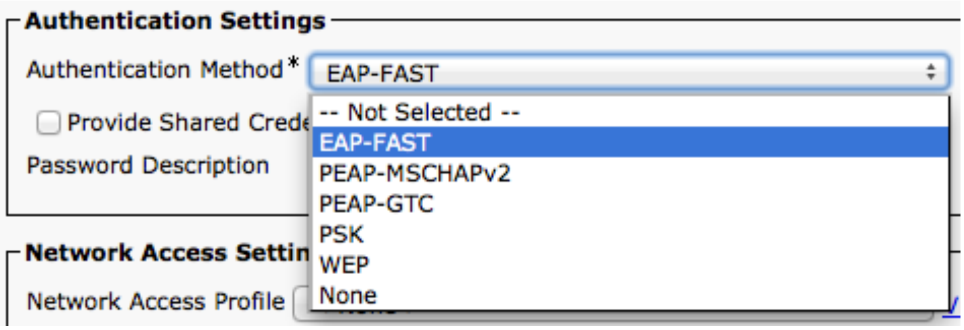
Frequency Band* Auto

User Modifiable* Allowed

Authentication Setting

Authentication Method*

Select the desired **Authentication Method** option.



Authentication Settings

Authentication Method* EAP-FAST

□ Provide Shared Crede

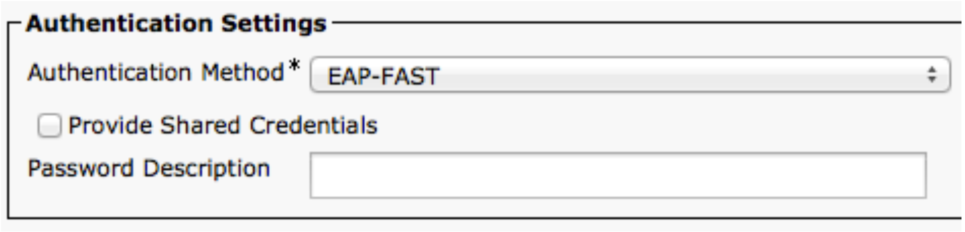
Password Description

Network Access Settin

Network Access Profile

If **EAP-FAST**, **PEAP-MSCHAPv2**, or **PEAP-GTC** is selected then the option to enter shared credentials (Username and Password) is available.

If **Provide Shared Credentials** is not checked, then the Username and Password will need to be configured locally on the Cisco DX Series by the admin or user.



Authentication Settings

Authentication Method* EAP-FAST

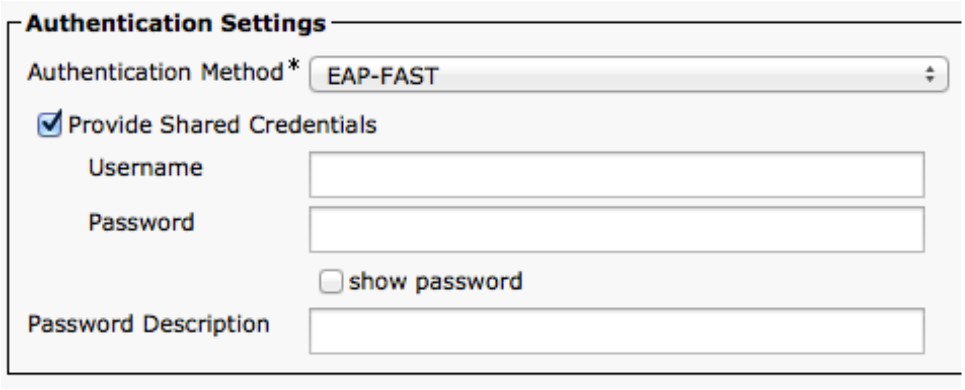
□ Provide Shared Credentials

Password Description

If **Provide Shared Credentials** is checked, then the specified **Username** and **Password** will be utilized for all Cisco DX Series that utilize this Wireless LAN Profile.

Up to 64 characters can be entered for the Username and Password.

A **Password Description** can optionally be entered.



Authentication Settings

Authentication Method* EAP-FAST

☑ Provide Shared Credentials

Username

Password

□ show password

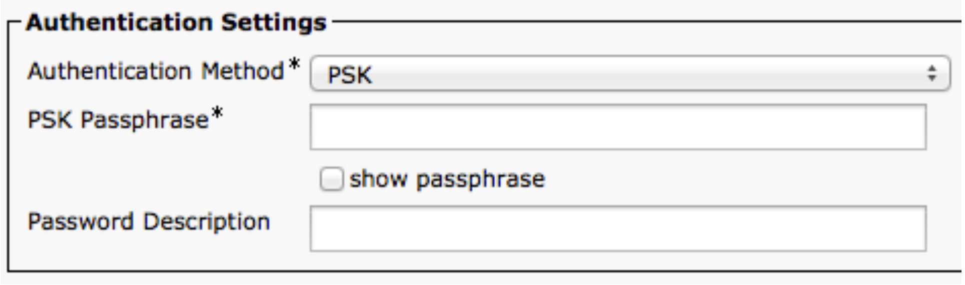
Password Description

If **PSK** is selected to utilize Pre-Shared Key authentication, then a **PSK Passphrase** must be entered.

The **PSK Passphrase** must be in one of the following formats:

- 8-63 ASCII character string
- 64 HEX character string

A **Password Description** can optionally be entered.



Authentication Settings

Authentication Method* PSK

PSK Passphrase*

□ show passphrase

Password Description

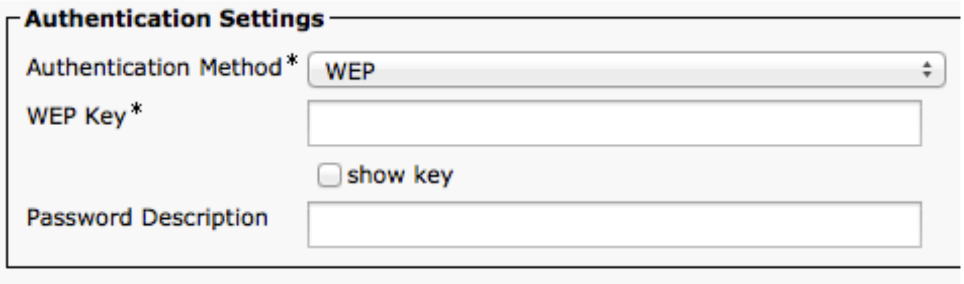
If **WEP** is selected to utilize static WEP (Wired Equivalent Privacy) authentication, then a **WEP Key** must be entered.

Only WEP key 1 is supported, so need to ensure that the entered key matches transmit key on the access point side.

The **WEP Key** must be in one of the following formats:

- **40/64 Bit Key** = 5 digit ASCII or 10 digit HEX character string
- **104/128 Bit Key** = 13 digit ASCII or 26 digit HEX character string

A **Password Description** can optionally be entered.



Authentication Settings

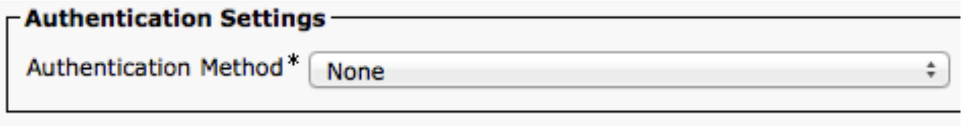
Authentication Method* WEP

WEP Key*

□ show key

Password Description

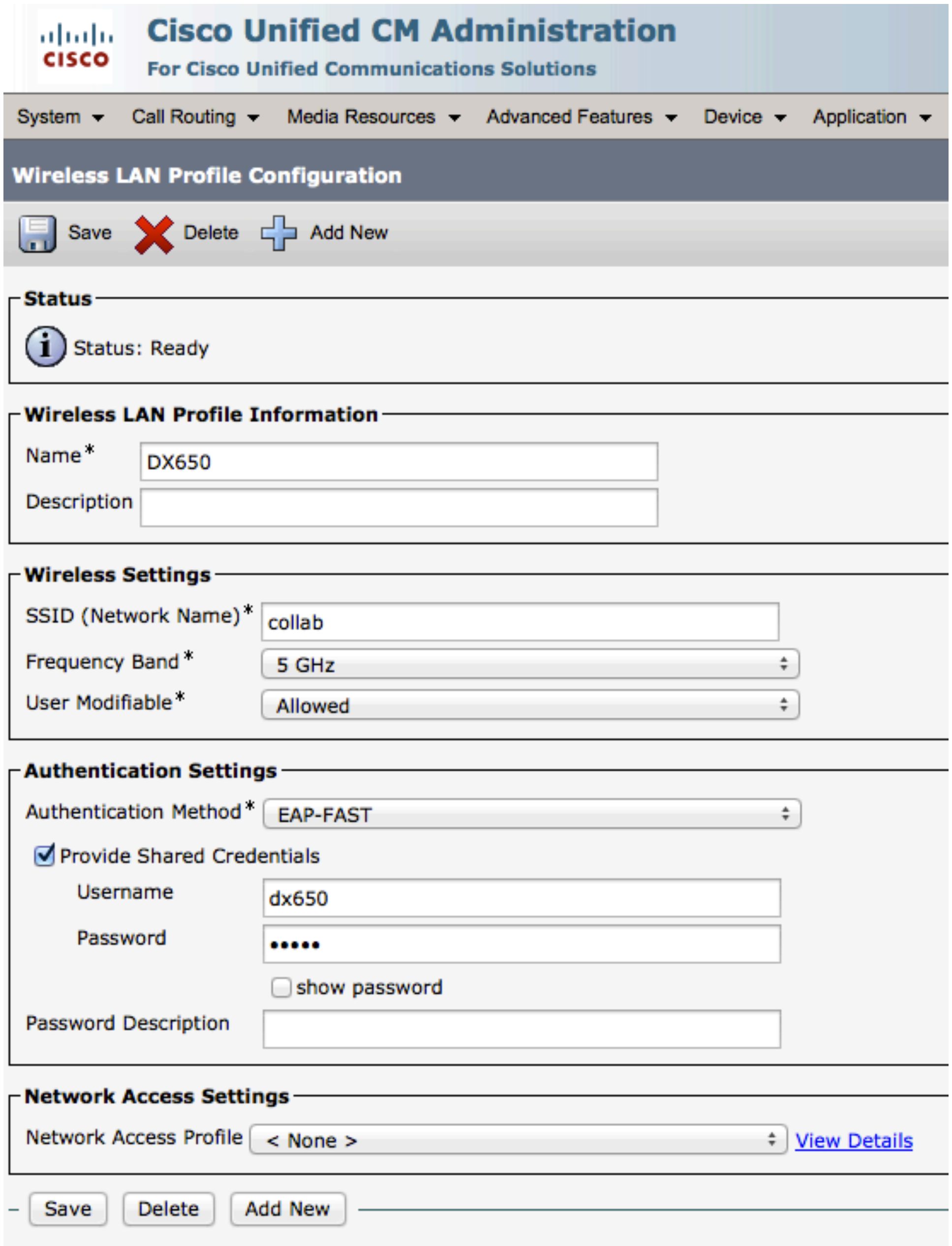
If **None** is selected, then no authentication is required and no encryption will be utilized.



Authentication Settings

Authentication Method* None

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



Wireless LAN Profile Configuration

Status

Status: Ready

Wireless LAN Profile Information

Name*	DX650
Description	

Wireless Settings

SSID (Network Name)*	collab
Frequency Band*	5 GHz
User Modifiable*	Allowed

Authentication Settings

Authentication Method*	EAP-FAST

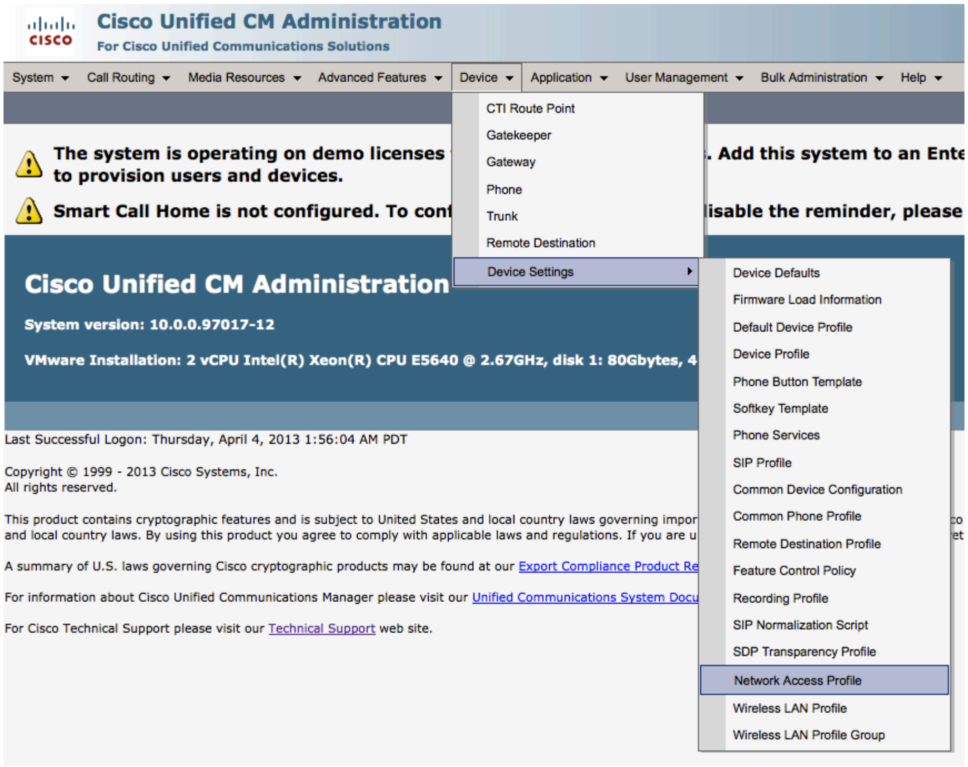
☑ Provide Shared Credentials

Username	dx650
Password	•••••
	□ show password
Password Description	

Network Access Settings

Network Access Profile	< None > View Details

To create a Network Access Profile, navigate to **Device** > **Device Settings** > **Network Access Profile** within the Cisco Unified Communications Manager's Administration interface.



The system is operating on demo licenses . Add this system to an Ente
to provision users and devices.

Smart Call Home is not configured. To conf lisable the reminder, please

Cisco Unified CM Administration

System version: 10.0.0.97017-12

VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5640 @ 2.67GHz, disk 1: 80Gbytes, 4

Last Successful Logon: Thursday, April 4, 2013 1:56:04 AM PDT

Copyright © 1999 - 2013 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing impor co
and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are u et

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Re

For information about Cisco Unified Communications Manager please visit our Unified Communications System Docu

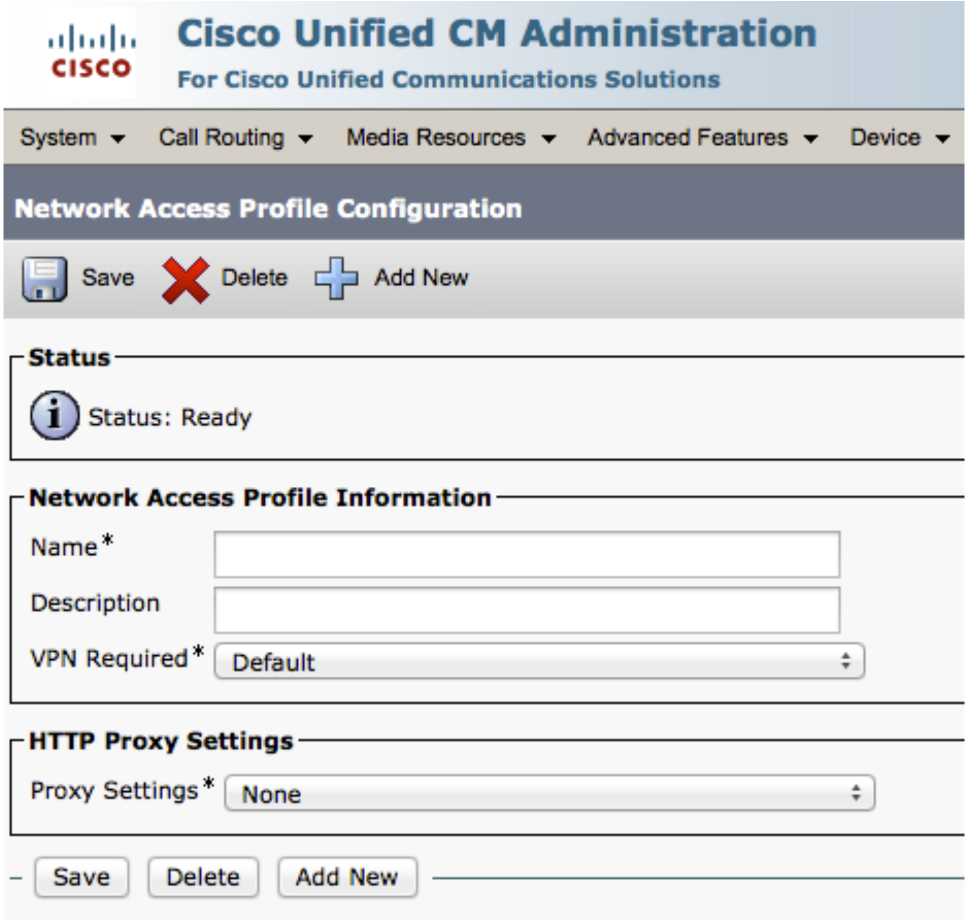
For Cisco Technical Support please visit our Technical Support web site.

From the Network Access Profile page, select **Add New**.

A Network Access Profile can then be created where the Name, Description, VPN Required, and Proxy Settings are specified.

Below are Network Access Profile defaults:

- **VPN Required** = Default
- **Proxy Settings** = None



Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Device
Save
Delete
Add New

Network Access Profile Configuration

Status

Status: Ready

Network Access Profile Information

Name*

Description

VPN Required* Default

HTTP Proxy Settings

Proxy Settings* None

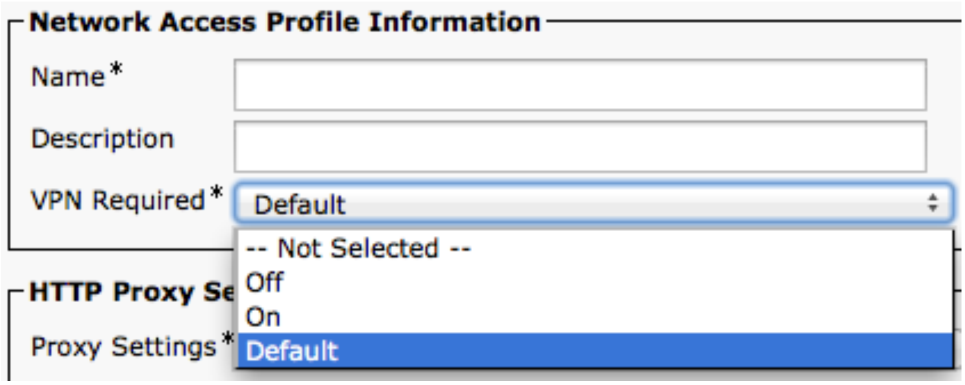
Enter a **Name** for the Network Access Profile containing up to 50 characters.

A **Description** containing up to 63 characters can optionally be configured.

Select the desired **VPN Required** option.

If On is selected, then VPN will always be utilized when this Network Access Profile is utilized.

If Default is selected, then the system default will be used.



Network Access Profile Information

Name*

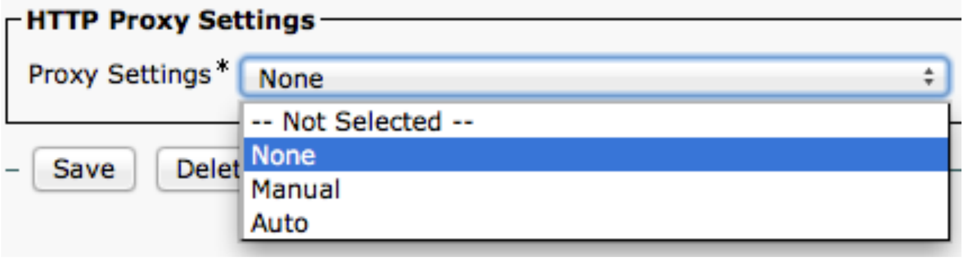
Description

VPN Required* Default

HTTP Proxy Se

Proxy Settings*

Select the desired **Proxy Settings** option.



HTTP Proxy Settings

Proxy Settings* None

If Manual is selected, then **Proxy Hostname** and **Proxy Port** must be configured.

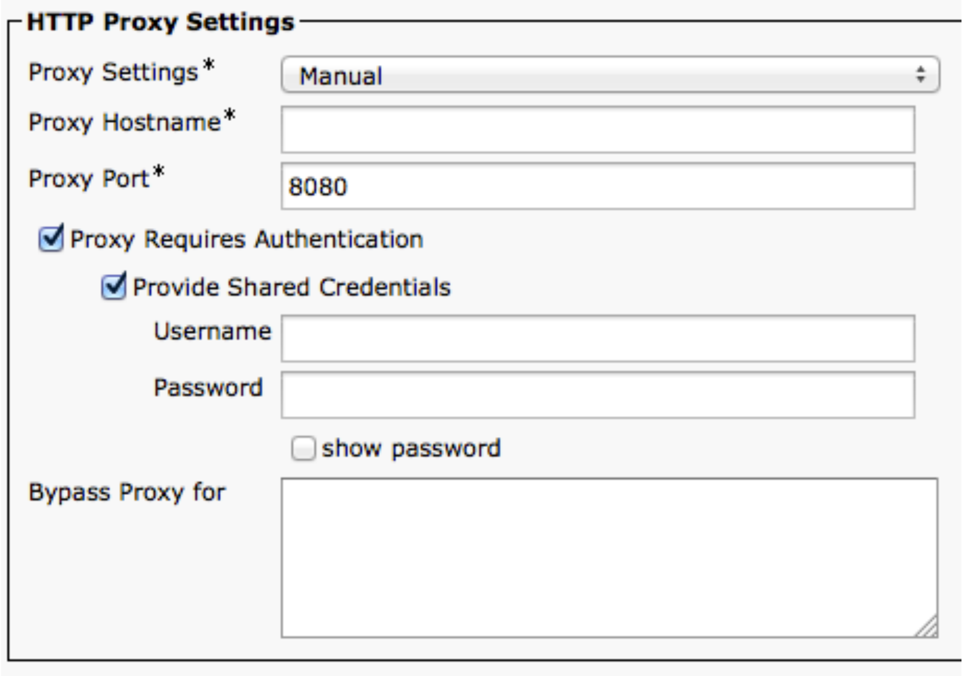
The Proxy Hostname can be up to 255 characters.

The Proxy Port is defaulted to port 8080, but can be configured for 1-65535.

Proxy Authentication can optionally be enabled by selecting **Proxy Requires Authentication** then **Provide Shared Credentials**.

Up to 64 characters can be entered for the Username and Password.

Enter the domain names as necessary in the **Bypass Proxy for** box.



HTTP Proxy Settings

Proxy Settings* Manual

Proxy Hostname*

Proxy Port* 8080

☑ Proxy Requires Authentication

☑ Provide Shared Credentials

Username

Password

□ show password

Bypass Proxy for

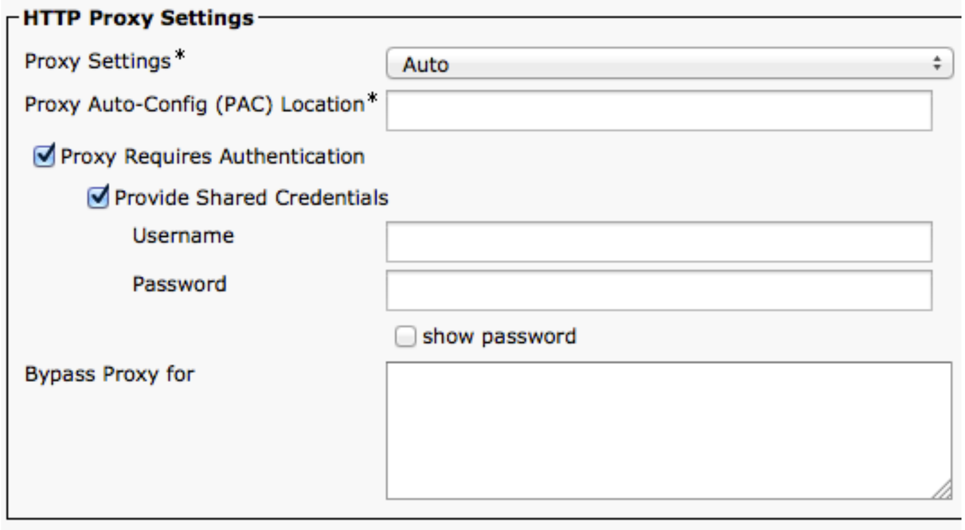
If Auto is selected, then **Proxy Auto-Config (PAC) Location** must be configured.

The Proxy Auto-Config (PAC) Location can be up to 255 characters.

Proxy Authentication can optionally be enabled by selecting **Proxy Requires Authentication** then **Provide Shared Credentials**.

Up to 64 characters can be entered for the Username and Password.

Enter the domain names as necessary in the **Bypass Proxy for** box.



HTTP Proxy Settings

Proxy Settings* Auto

Proxy Auto-Config (PAC) Location*

☑ Proxy Requires Authentication

☑ Provide Shared Credentials

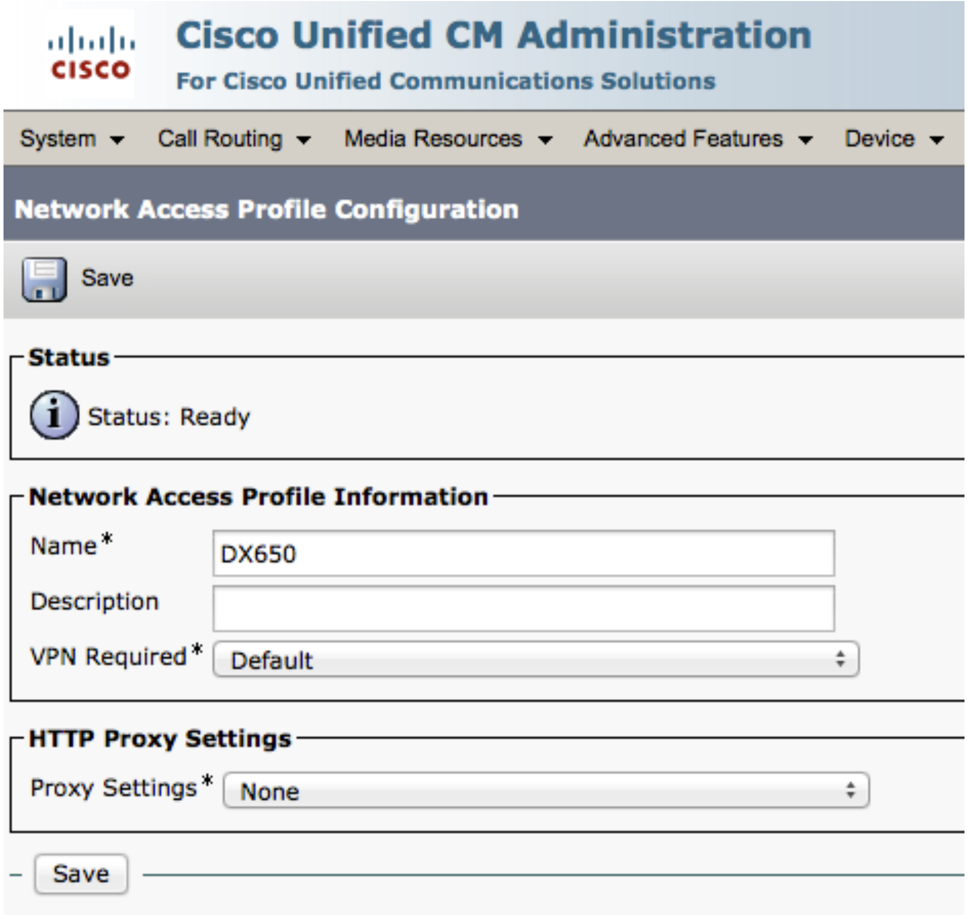
Username

Password

☐ show password

Bypass Proxy for

Select **Save** once the Network Access Profile configuration is complete.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Device
Save

Network Access Profile Configuration

Status

Status: Ready

Network Access Profile Information

Name* DX650

Description

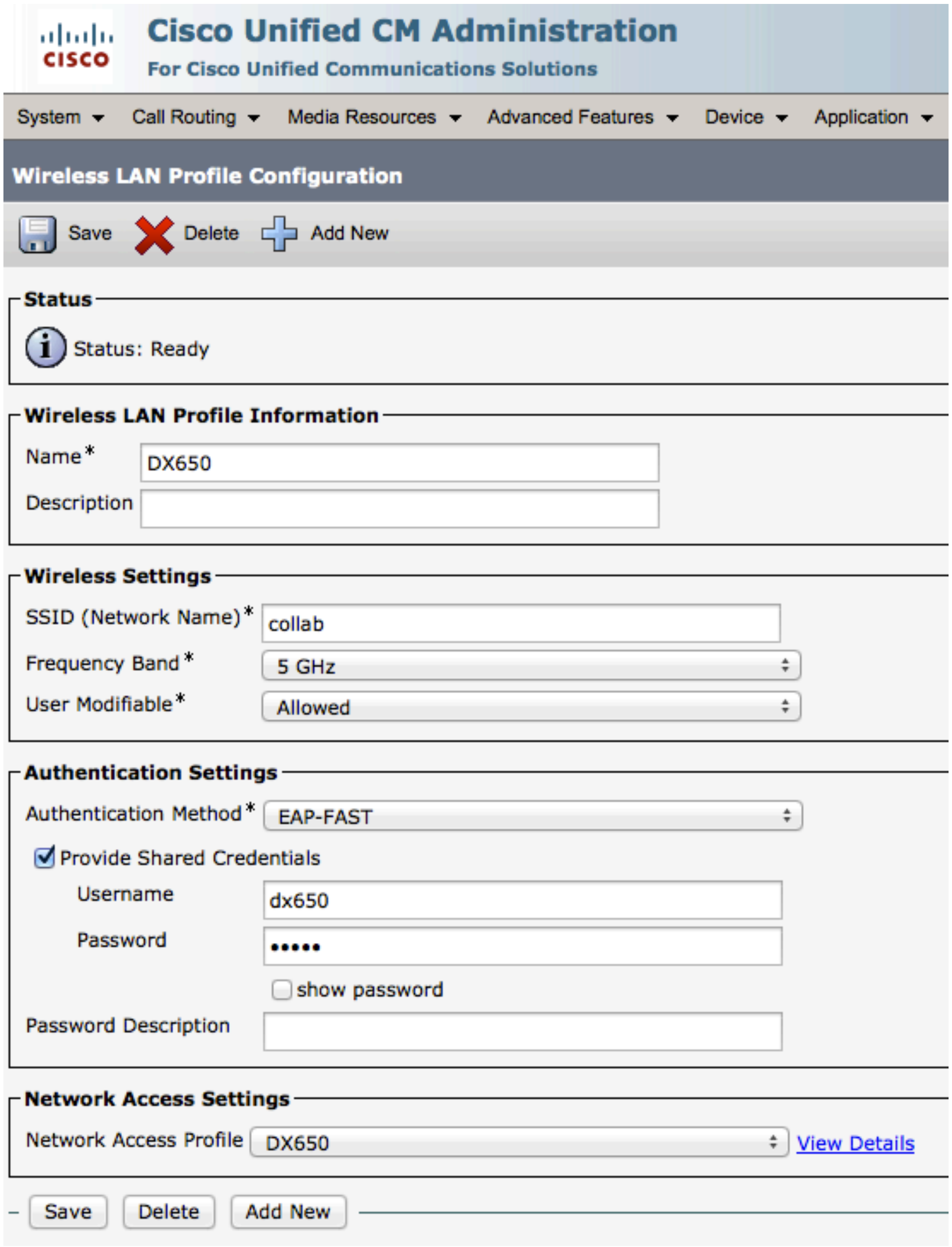
VPN Required* Default

HTTP Proxy Settings

Proxy Settings* None

Once the Network Access Profile has been created, it can be applied to a Wireless LAN Profile.

Select **Save** once the Network Access Profile has been applied to the Wireless LAN Profile.



Wireless LAN Profile Configuration

Status

Status: Ready

Wireless LAN Profile Information

Name* DX650

Description

Wireless Settings

SSID (Network Name)* collab

Frequency Band* 5 GHz

User Modifiable* Allowed

Authentication Settings

Authentication Method* EAP-FAST

☑ Provide Shared Credentials

Username dx650

Password •••••

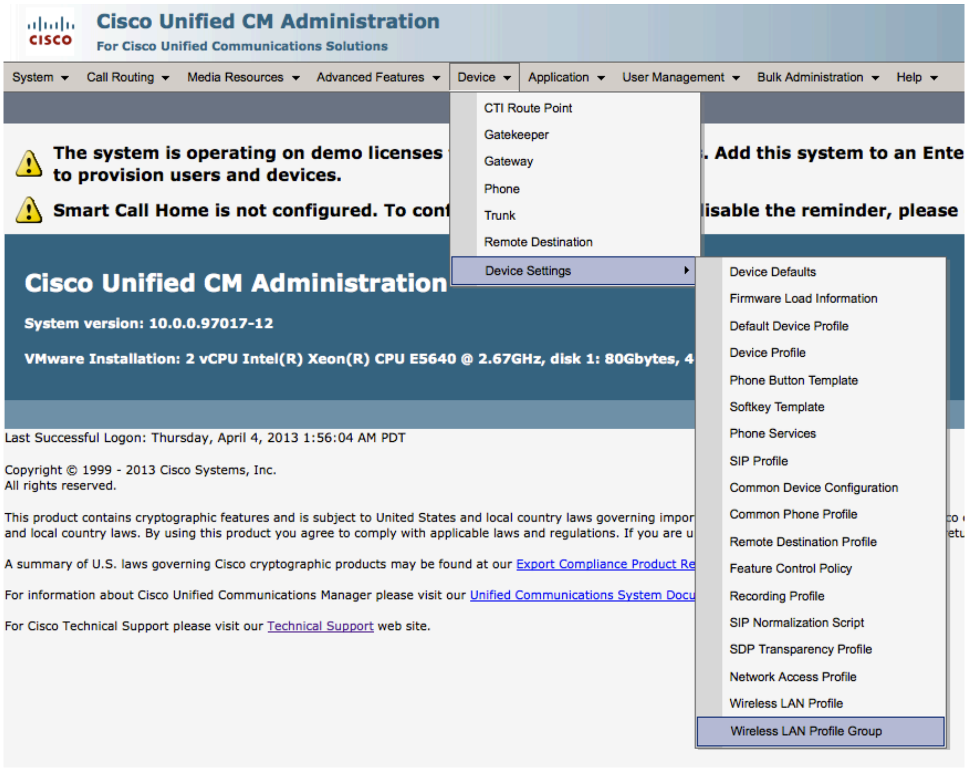
□ show password

Password Description

Network Access Settings

Network Access Profile DX650 View Details

To create a Wireless LAN Profile Group, navigate to **Device > Device Settings > Wireless LAN Profile Group** within the Cisco Unified Communications Manager's Administration interface.



The system is operating on demo licenses . Add this system to an Ente
to provision users and devices.

Smart Call Home is not configured. To conf lisable the reminder, please

Cisco Unified CM Administration

System version: 10.0.0.97017-12

VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5640 @ 2.67GHz, disk 1: 80Gbytes, 4

Last Successful Logon: Thursday, April 4, 2013 1:56:04 AM PDT

Copyright © 1999 - 2013 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing impor co
and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are u etu

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Re

For information about Cisco Unified Communications Manager please visit our Unified Communications System Docu

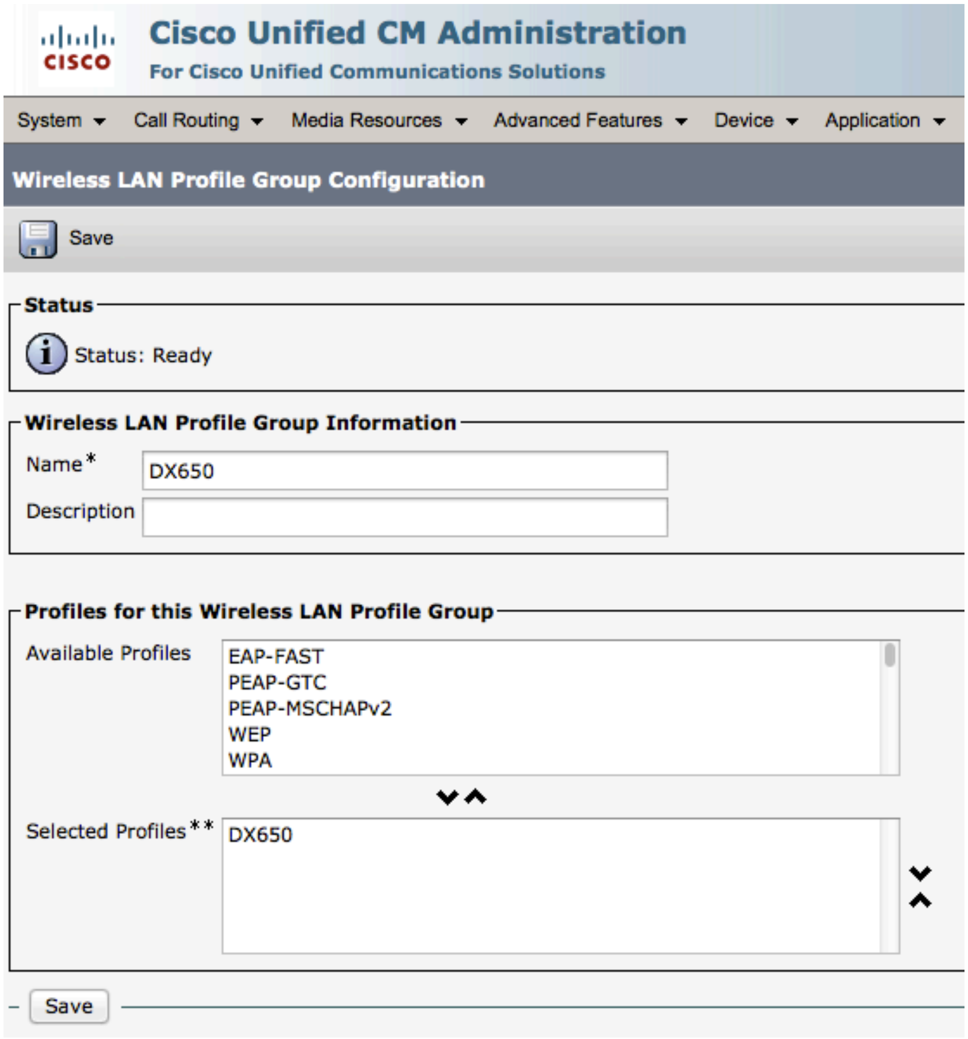
For Cisco Technical Support please visit our Technical Support web site.

From the Wireless LAN Profile Group page, select **Add New**.

A Wireless LAN Profile Group can then be created where the Name, Description, and Wireless LAN Profiles are specified.

Up to **4** Wireless LAN Profiles can be added to a Wireless LAN Profile Group.

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


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Device
Application
Save

Wireless LAN Profile Group Configuration

Status

Status: Ready

Wireless LAN Profile Group Information

Name* DX650

Description

Profiles for this Wireless LAN Profile Group

Available Profiles: EAP-FAST, PEAP-GTC, PEAP-MSCHAPv2, WEP, WPA

Selected Profiles** DX650

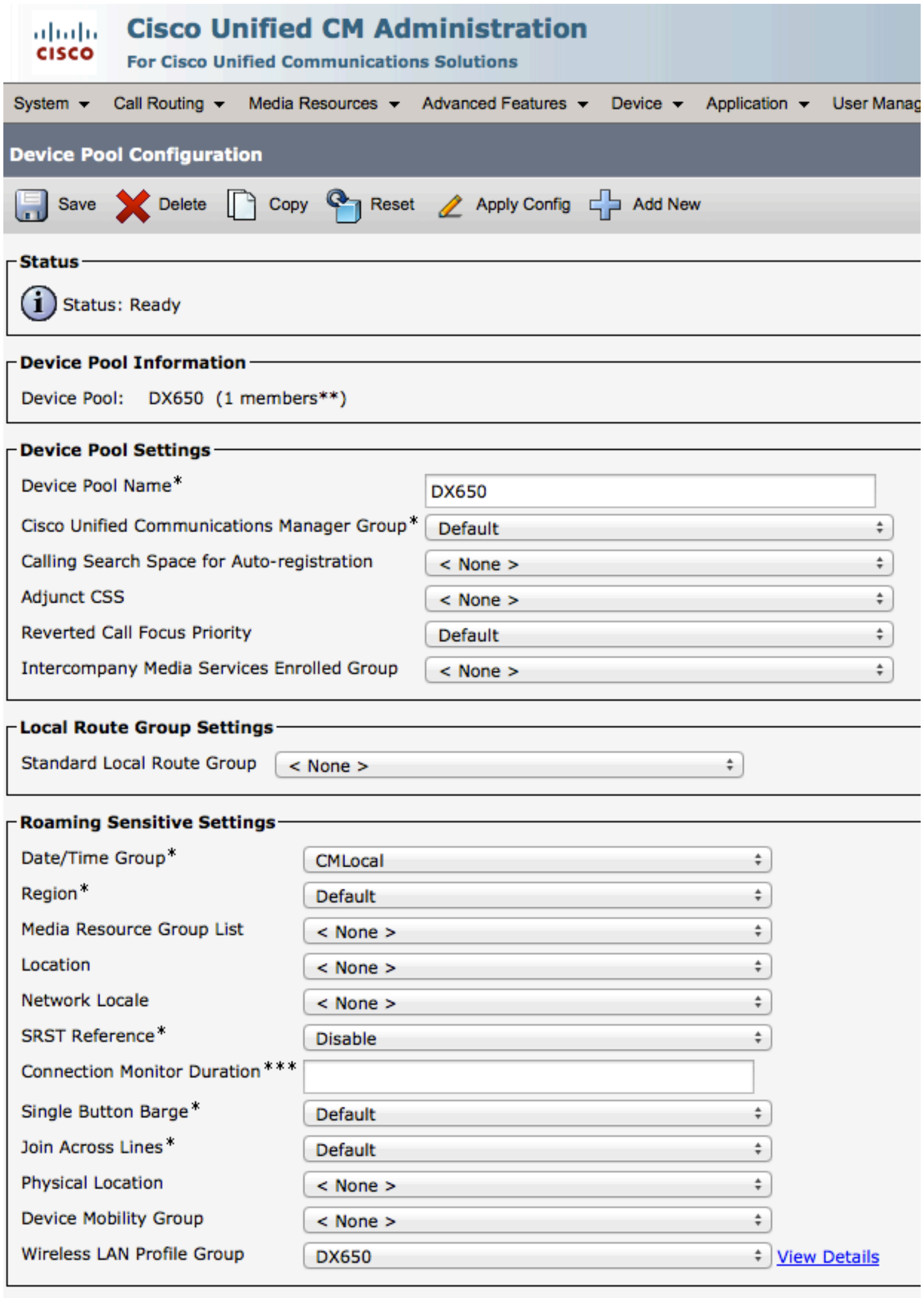
Once the Wireless LAN Profile Group has been created, it can be applied to a Device Pool or an individual Cisco DX Series.

To apply a Wireless LAN Profile Group to a device pool, navigate to **System > Device Pool** within the Cisco Unified Communications Manager's Administration interface.

Create a Device Pool as necessary and put the desired Cisco DX Series into this Device Pool.

Once the Device Pool has been created, configure the Wireless LAN Profile Group then select **Save**.

Once the Wireless LAN Profile Group has been applied to the Device Pool, select **Apply Config** for the Cisco DX Series to download the Wireless LAN Profile Group configuration.



Device Pool Configuration

Status

Status: Ready

Device Pool Information

Device Pool: DX650 (1 members**)

Device Pool Settings

Device Pool Name*	DX650
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >

Local Route Group Settings

Standard Local Route Group	< None >

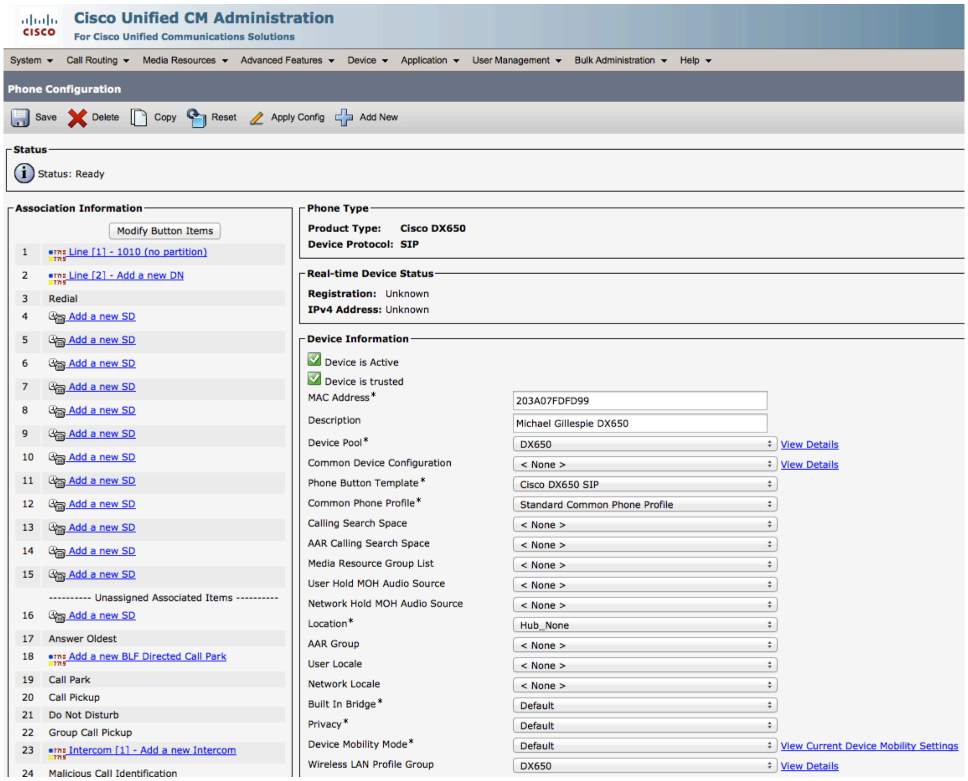
Roaming Sensitive Settings

Date/Time Group*	CMLocal
Region*	Default
Media Resource Group List	< None >
Location	< None >
Network Locale	< None >
SRST Reference*	Disable
Connection Monitor Duration***	
Single Button Barge*	Default
Join Across Lines*	Default
Physical Location	< None >
Device Mobility Group	< None >
Wireless LAN Profile Group	DX650

To apply a Wireless LAN Profile Group to an individual Cisco DX Series, navigate to **Device > Phone** within the Cisco Unified Communications Manager's Administration interface.

Navigate to the desired Cisco DX Series, configure the Wireless LAN Profile Group then select **Save**.

Once the Wireless LAN Profile Group has been applied to the individual Cisco DX Series, select **Apply Config** for the Cisco DX Series to download the Wireless LAN Profile Group configuration.



Phone Configuration

Status

Status: Ready

Association Information

1	Line [1] - 1010 (no partition)
2	Line [2] - Add a new DN
3	Redial
4	Add a new SD
5	Add a new SD
6	Add a new SD
7	Add a new SD
8	Add a new SD
9	Add a new SD
10	Add a new SD
11	Add a new SD
12	Add a new SD
13	Add a new SD
14	Add a new SD
15	Add a new SD
	--------- Unassigned Associated Items ---------
16	Add a new SD
17	Answer Oldest
18	Add a new BLF Directed Call Park
19	Call Park
20	Call Pickup
21	Do Not Disturb
22	Group Call Pickup
23	Intercom [1] - Add a new Intercom
24	Malicious Call Identification

Phone Type

Product Type: Cisco DX650
Device Protocol: SIP

Real-time Device Status

Registration: Unknown
IPv4 Address: Unknown

Device Information

☑ Device is Active
☑ Device is trusted

MAC Address*	203A07FDFD99	
Description	Michael Gillespie DX650	
Device Pool*	DX650	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Cisco DX650 SIP	
Common Phone Profile*	Standard Common Phone Profile	
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Media Resource Group List	< None >	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Location*	Hub_None	
AAR Group	< None >	
User Locale	< None >	
Network Locale	< None >	
Built In Bridge*	Default	
Privacy*	Default	
Device Mobility Mode*	Default	View Current Device Mobility Settings
Wireless LAN Profile Group	DX650	View Details

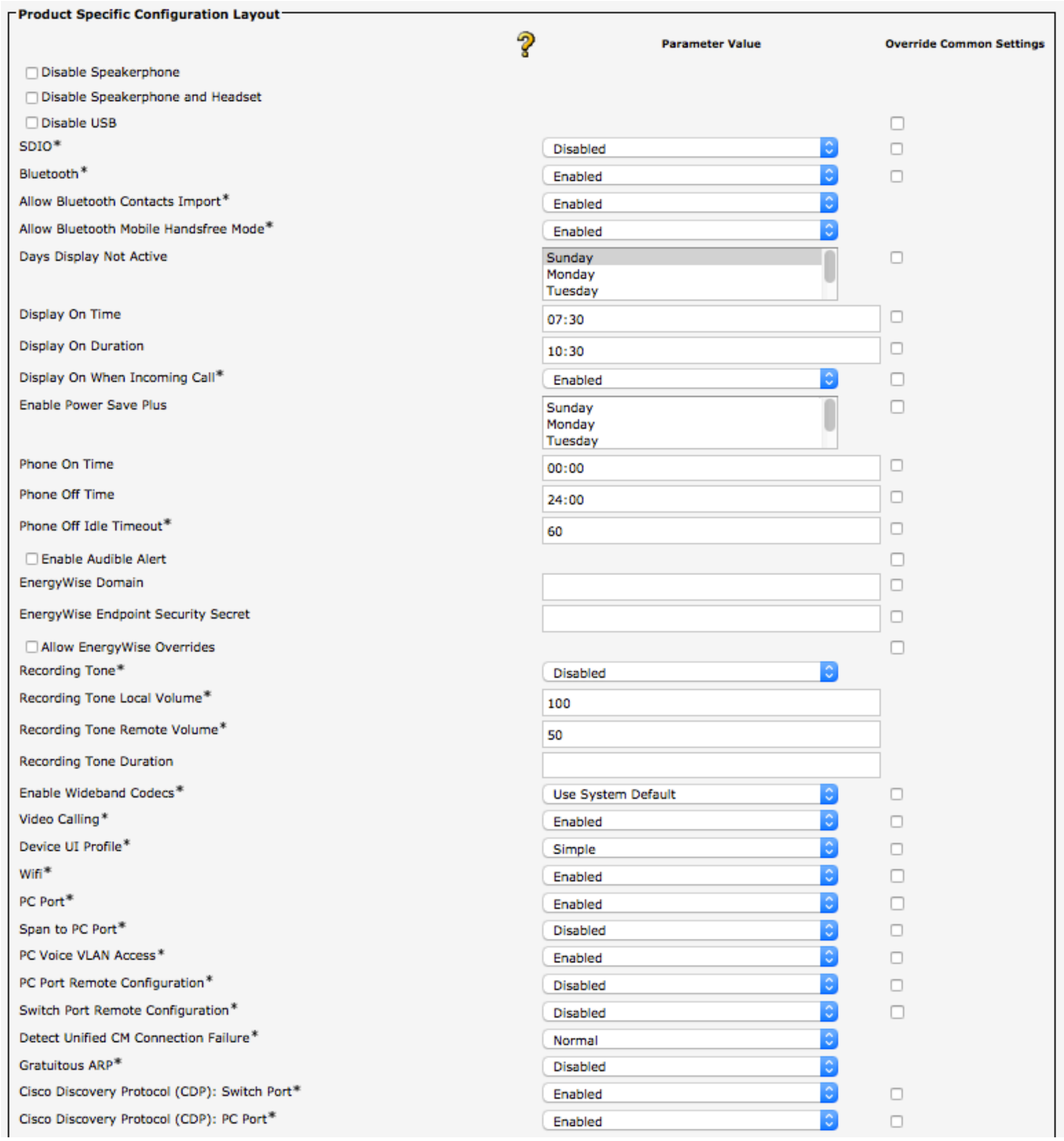
Product Specific Configuration Options

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

For a description of these options, click **?** at the top of the configuration page.

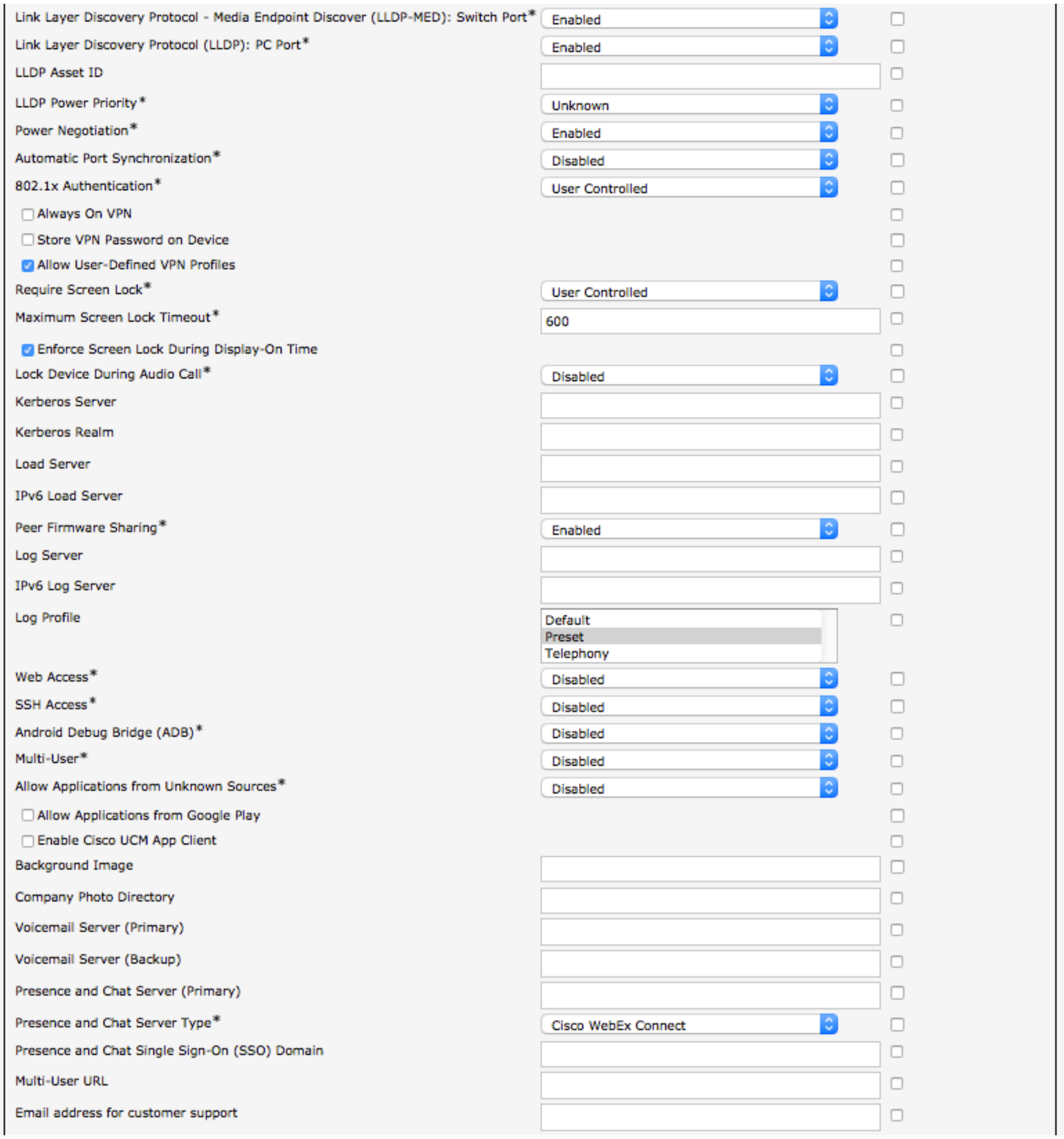
Product specific configuration options can be configured in bulk via the Bulk Admin Tool if using Cisco Unified Communications Manager.

Some of the product specific configuration options can be configured on an enterprise phone, common phone profile or individual phone configuration level.



Product Specific Configuration Layout

	Parameter Value	Override Common Settings
□ Disable Speakerphone		
□ Disable Speakerphone and Headset		
□ Disable USB		□
SDIO*	Disabled	□
Bluetooth*	Enabled	□
Allow Bluetooth Contacts Import*	Enabled	
Allow Bluetooth Mobile Handsfree Mode*	Enabled	
Days Display Not Active	Sunday Monday Tuesday	□
Display On Time	07:30	□
Display On Duration	10:30	□
Display On When Incoming Call*	Enabled	□
Enable Power Save Plus	Sunday Monday Tuesday	□
Phone On Time	00:00	□
Phone Off Time	24:00	□
Phone Off Idle Timeout*	60	□
□ Enable Audible Alert		□
EnergyWise Domain		□
EnergyWise Endpoint Security Secret		□
□ Allow EnergyWise Overrides		□
Recording Tone*	Disabled	
Recording Tone Local Volume*	100	
Recording Tone Remote Volume*	50	
Recording Tone Duration		
Enable Wideband Codecs*	Use System Default	□
Video Calling*	Enabled	□
Device UI Profile*	Simple	□
Wifi*	Enabled	□
PC Port*	Enabled	□
Span to PC Port*	Disabled	□
PC Voice VLAN Access*	Enabled	□
PC Port Remote Configuration*	Disabled	□
Switch Port Remote Configuration*	Disabled	□
Detect Unified CM Connection Failure*	Normal	
Gratuitous ARP*	Disabled	
Cisco Discovery Protocol (CDP): Switch Port*	Enabled	□
Cisco Discovery Protocol (CDP): PC Port*	Enabled	□



Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*	Enabled	□
Link Layer Discovery Protocol (LLDP): PC Port*	Enabled	□
LLDP Asset ID		□
LLDP Power Priority*	Unknown	□
Power Negotiation*	Enabled	□
Automatic Port Synchronization*	Disabled	□
802.1x Authentication*	User Controlled	□
□ Always On VPN		□
□ Store VPN Password on Device		□
☑ Allow User-Defined VPN Profiles		□
Require Screen Lock*	User Controlled	□
Maximum Screen Lock Timeout*	600	□
☑ Enforce Screen Lock During Display-On Time		□
Lock Device During Audio Call*	Disabled	□
Kerberos Server		□
Kerberos Realm		□
Load Server		□
IPv6 Load Server		□
Peer Firmware Sharing*	Enabled	□
Log Server		□
IPv6 Log Server		□
Log Profile	Default Preset Telephony	□
Web Access*	Disabled	□
SSH Access*	Disabled	□
Android Debug Bridge (ADB)*	Disabled	□
Multi-User*	Disabled	□
Allow Applications from Unknown Sources*	Disabled	□
□ Allow Applications from Google Play		□
□ Enable Cisco UCM App Client		□
Background Image		□
Company Photo Directory		□
Voicemail Server (Primary)		□
Voicemail Server (Backup)		□
Presence and Chat Server (Primary)		□
Presence and Chat Server Type*	Cisco WebEx Connect	□
Presence and Chat Single Sign-On (SSO) Domain		□
Multi-User URL		□
Email address for customer support		□

Field Name	**Description**
Disable Speakerphone	Disable only the speakerphone functionality. Disabling speakerphone functionality will not affect the headset. You can use lines and speed dials with headset/handset.
Disable Speakerphone and Headset	Disable all speakerphone functions and headset microphone.
Disable USB	Disable the USB ports on the device.
SDIO	Indicates whether the SDIO device on the device is enabled or disabled.
Bluetooth	Indicates whether the Bluetooth device on the device is enabled or disabled.
Allow Bluetooth Contacts Import	This parameter allows the user to import and sync contacts and call history from their Bluetooth device.

Allow Bluetooth Mobile Handsfree Mode	This parameter allows the user to use their mobile phone line on the desk phone.
Days Display Not Active	This field allows the user to specify the days that the backlight is to remain off by default. Typically this would be Saturday and Sunday for US corporate customers. Saturday and Sunday should be the default. The list contains all of the days of the week. To turn off backlight on Saturday and Sunday the User would hold down Control and select Saturday and Sunday.
Display On Time	This field indicates the time of day the display is to automatically turn itself on for days listed in the off schedule. The value should be in a 24 hour format. Where 0:00 is the beginning of the day and 23:59 is the end of the day. Leaving this field blank will activate the display at the default time of the day (e.g. - "7:30"). To set the display to turn on at 7:00AM the user would enter "07:00" without the quotes. If they wanted the display to turn on at 2:00PM they would enter "14:00" without the quotes.
Display On Duration	This field indicates the amount of time the display is to be active for when it is turned on by the programmed schedule. Leaving this field blank will make the phone use a pre-determined default value of "10:30". Maximum value is 24 hours. This value is in free form hours and minutes. "1:30" would activate the display for one hour and 30 minutes.
Display On When Incoming Call	When the device is in screen saver mode, this will turn the display on when a call is ringing.
Enable Audible Alert	This checkbox, when enabled, instructs the phone to play an audible alert ten minutes prior to the time specified in the field, Phone Off Time. The select key on the phone will quickly flash to visually alert the user to the impending phone state change (powering off as a result of the Power Save Plus feature). To also audibly alert the user, enable this checkbox. The default is disabled. This checkbox only applies if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	This field defines the EnergyWise domain in which the phone is participating. An EnergyWise domain is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, you must also provide an EnergyWise domain. The default is blank.
EnergyWise Endpoint Security Secret	This field defines the password (shared secret) used to communicate within the EnergyWise domain. An EnergyWise domain and secret is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, you must also provide an EnergyWise domain and secret. The default is blank.
Allow EnergyWise Overrides	This checkbox determines whether you will allow the EnergyWise domain controller policy to send power level updates to the phones. A few conditions apply; first, one or more days must be selected in the Enable Power Save Plus field. If the Enable Power Save Plus list box does not have any days selected, the phone will ignore the EnergyWise directive to turn off the phone. Second, the settings in Unified CM Administration will take effect on schedule even if EnergyWise sends an override. For example, assume the Display Off Time is set to 22:00 (10 p.m.), the value in the Display On Time field is 06:00 (6 a.m.), and the Enable Power Save Plus has one or more days selected. If EnergyWise directs the phone to turn off at 20:00 (8 p.m.), that directive will remain in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6 a.m. At 6 a.m., the phone will turn on and resume receiving its power level changes from the settings in Unified CM Administration. To change the

	power level on the phone again, EnergyWise must reissue a new power level change command. Also, any user interaction will take effect so if a user presses the select softkey after EnergyWise has directed the phone to power off, the phone will power on as a result of the user action. The default is unchecked.
Recording Tone	This can be used to configure whether the recording tone is enabled or disabled on the phone. If enabled, the phone mixes the recording tone into both directions for every call.
Recording Tone Local Volume	This can be used to configure the loudness setting of the recording tone that the local party hears. This loudness setting applies regardless of the actual device used for hearing (handset, speakerphone, headset). The loudness setting should be in the range of 0% to 100%, with 0% being no tone and 100% being at the same level as the current volume setting. The default value is 100%.
Recording Tone Remote Volume	This can be used to configure the loudness setting of the recording tone that the remote party hears. The loudness setting should be in the range of 0% to 100%, with 0% being less than -66dBM and 100% being -4dBM. The default value is -10dBM or 50%.
Recording Tone Duration	Indicates the length of time in milliseconds for which the recording tone is inserted in the audio stream. The default for this parameter is set to the value in the Network locale file for this field. The valid range for this parameter is a value between 1 and 3000 milliseconds.
Enable Wideband Codecs	Indicates whether the phone application will advertise the wideband codecs to the Cisco Unified Communications Manager. Codec negotiation involves two steps: first, the phone application must advertise the supported codec(s) to the Cisco Unified Communications Manager (not all endpoints support the same set of codecs). Second, when the Cisco Unified Communications Manager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. Valid values specify Use System Default (this phone application will defer to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (this phone application will not advertise the wideband codecs to the Cisco Unified Communications Manager) or Enabled (this phone application will advertise the wideband codecs to the Cisco Unified Communications Manager).
Video Calling	When enabled, indicates that the device will participate in video calls.
Device UI Profile	Changes the device's user interface characteristics to optimize for specific user personas such as basic video callers (Simple), public space phone (Public) or general collaboration users (Enhanced).
Wifi	Indicates whether the Wi-Fi on the device is enabled or disabled.
PC Port	Indicates whether the PC port on the device is enabled or disabled. The port labeled “COMPUTER” on the back of the device connects a PC or workstation to the device so they can share a single network connection.
Span to PC Port	Indicates whether the device will forward packets transmitted and received on the device’s network port to the PC port. Select Enabled if an application is being run on the PC port that requires monitoring of the device’s traffic such as monitoring and recording applications (common in call center environments) or network packet capture tools used for diagnostic purposes. To use this feature PC Voice VLAN access must be enabled.
PC Voice VLAN Access	Indicates whether a device attached to the PC port on the device is allowed access

	to the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the device. Set this setting to Enabled if an application is being run on the PC that requires monitoring of the device traffic. These could include monitoring and recording applications and use of network monitoring software for analysis purposes.
PC Port Remote Configuration	Allows remote configuration of the PC port speed and duplex of the device. This overrides any manual configuration on the device.
Switch Port Remote Configuration	Allows remote configuration of the switch port speed and duplex of the device. This overrides any manual configuration on the device. Be aware that configuring this port may cause the device to lose network connectivity.
Detect Unified CM Connection Failure	This field determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. Note that the precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing. This only applies to the wired Ethernet connection. Default = Normal
Gratuitous ARP	Indicates whether the device will learn MAC addresses from Gratuitous ARP responses. Disabling the device ability to accept Gratuitous ARP will prevent applications, which use this mechanism for monitoring and recording of voice streams from working. If monitoring capability is not desired, change this setting to Disabled.
Cisco Discover Protocol (CDP): Switch Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the device's switch port.
Cisco Discover Protocol (CDP): PC Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the device's PC port.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the device's switch port.
Link Layer Discovery Protocol – (LLDP): PC Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the device's PC port.
LLDP Asset ID	Allows administrator to set Asset ID for Link Layer Discovery Protocol.
LLDP Power Priority	Allows administrator to set Power Priority for Link Layer Discovery Protocol.
Power Negotiation	Allows administrator to enable or disable Power Negotiation. Enable the Power Negotiation feature when the device is connected to a switch that supports power negotiation. However, if a switch does not support power negotiation, then you should disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the device can power up accessories up to 12.9W.
Automatic Port Synchronization	Enables the phone to synchronize the PC and SW ports to the same speed and to

	duplex. Only ports configured for auto negotiate change speeds.
802.1x Authentication	Specifies the 802.1x authentication feature status.
Always On VPN	Indicates whether the device will always start the VPN AnyConnect client and establish a connection with the configured VPN profile from the Cisco Unified Communications Manager.
Store VPN Password on Device	This parameter controls whether VPN password can be stored on the device. Its value is used only when Password Persistence is set to true. If disabled, the user's VPN password is stored in memory and is automatically re-submitted upon subsequent connects. However, when the device reboots, the user will have to re-enter their VPN password again. If enabled, the user's VPN password is stored on the device and will persist across reboots.
Allow User-Defined VPN Profiles	This parameter controls whether the user can use the AnyConnect VPN client to create VPN profiles. If disabled, the user cannot create VPN profiles.
Require Screen Lock	This parameter indicates whether screen lock is required on the device. If "User Controlled" is selected, the device will not prompt for a PIN or password. The "PIN" and "Password" options require the user to enter a password to unlock the screen. A "PIN" is a numeric password that is at least four digits long. A "Password" is an alphanumeric password, consisting of at least 4 alphanumeric characters, one of which must be a non-numeric number, and one must be a capital letter.
Maximum Screen Lock Timeout	Maximum idle time in seconds before the device automatically locks the screen. After the screen is locked, the user password is required to unlock it.
Enforce Screen Lock During Display-On Time	This parameter provides an unobtrusive lock policy that allows users to work freely with their device throughout the workday, without the device locking after the interval that is set in Cisco Unified Communications Manager. After work, the device locks as defined in the policy, to prevent unauthorized users from accessing it. The device always supports the user-controlled manual lock option (power button), for meetings or lunch breaks. The device remains locked until the user enters the PIN/password on next use. ON - Device locks during the workday or during display-on time (default setting). OFF - Device locks only during display-off time or after work hours, based on day/time settings listed above.
Lock Device During Audio Call	When an active voice call is in progress, an administrator can override the screen lock PIN enforcement timer to keep the screen active during an audio call. Screen lock timer takes effect after audio call is completed and timer is exceeded.
Kerberos Server	Authentication server for web proxy Kerberos.
Kerberos Realm	Realm for web proxy Kerberos.
Load Server	Indicates that the device will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IP address (using standard IP addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The device will not be redirected to the TFTP server. If this field is left blank, the device will use the designated TFTP server to obtain its load files and upgrades.
IPv6 Load Server	Indicates that the phone will use an alternative IPv6 server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you

	to indicate a local IPv6 server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IPv6 address (using standard IPv6 addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades.
Peer Firmware Sharing	PPID. Enables or disables Peer to Peer image distribution in order to allow a single device in a subnet to retrieve an image firmware file then distribute it to its peers - thus reducing TFTP bandwidth and providing for a faster firmware upgrade time.
Log Server	Specifies an IP address and port of a remote system where log messages are sent.
IPv6 Log Server	Specifies an IPv6 address and port of a remote system where log messages are sent. The format is: [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]:ppppp@@options. Options will be format as base=x;pfs=y; base value range is 0~7,pfs value range is 0~1.And the two parameters are optional. Absence of pfs or base,pfs will be set to the default value 0 and base will be set to the default value 7.
Log Profile	Run the pre-defined debug command remotely.
Web Access	This parameter indicates whether the device will accept connections from a web browser or other HTTP client. Disabling the web server functionality of the device will block access to the device's internal web pages. These pages provide statistics and configuration information. Features, such as QRT (Quality Report Tool), will not function properly without access to the device's web pages. This setting will also affect any serviceability application such as CiscoWorks 2000 that relies on web access.
SSH Access	This parameter indicates whether the device will accept SSH connections. Disabling the SSH server functionality of the device will block access to the device.
Android Debug Bridge (ADB)	This parameter enables or disables the Android Debug Bridge (ADB) on the device.
Multi-User	This parameter indicates whether multi-user is enabled or disabled on the device.
Allow Applications from Unknown Sources	This parameter controls whether the user can install Android applications on the device from a URL or from Android packages (APK) that are received through email, instant message (IM), or from a Secure Digital (SD) card.
Allow Applications from Google Play	This parameter controls whether the user can install Android applications from the Google's Android Market.
Enable Cisco UCM App Client	This parameter controls whether the Application Client runs on the device. When the Application Client is enabled, users can select the applications they would like to install from the Cisco Unified Communications Manager.
Background Image	This parameter specifies the default wallpaper file. Only the administrator disables end user access to phone wallpaper list, could this parameter take effect.
Company Photo Directory	This parameter specifies the URL, which the device can query for a user and get the image associated with that user.

Voicemail Server (Primary)	Hostname or IP address of the primary visual voicemail server.
Voicemail Server (Backup)	Hostname or IP address of the backup visual voicemail server.
Presence and Chat Server (Primary)	Hostname or IP address of the primary presence server.
Presence and Chat Server Type	This parameter indicates the type of server specified in the "Presence and Chat Server" field.
Presence and Chat Single Sign-On (SSO) Domain	The enterprise domain used by Cisco WebEx Connect Cloud to perform Single-Sign-On (SSO) authentication against an enterprise.
Multi-User URL	This parameter specifies the URL of the extension mobility server.
Email address for customer support	This sets an email address to which the user can send problem report files from the 'Problem Reporting Tool' on the endpoint.

Below are DX650 specific options.

Enable Power Save Plus	To enable the Power Save Plus feature, select the day(s) that you want the phone to power off on schedule. You can select multiple days by pressing and holding the Control key while clicking on the days that you want Power Save Plus to operate. The default is disabled (no days selected). In Power Save Plus mode, enough power is maintained to illuminate one key. All other functions of the phone are turned off in Power Save Plus mode. Power Save Plus mode turns off the phone for the time period specified in the Phone On Time and Phone Off Time fields. This time period is usually outside of your organization's regular operating hours. The illuminated key allows a user to press it to restore full power to the phone. After pressing the illuminated key, the phone power-cycles and reregisters with Unified CM before it becomes fully operational. Power Save Plus is disabled by default. When you select day(s) in this field, the following notice displays to indicate e911 concerns. By enabling Power Save Plus, you are agreeing to the terms specified in this Notice. : While Power Save Plus Mode (The "Mode") is in effect, endpoints configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (I) You are taking full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (II) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (III) You will fully inform users of the effects of the mode on calls, calling and otherwise.
Phone On Time	This field determines the time that the phone turns on automatically on the days that are selected in the Enable Power Save Plus list box. Enter the time in 24 hour format, where 00:00 represents midnight. For example, to automatically turn the phone on at 7:00 a.m., (0700), enter 07:00. To turn the phone on at 2:00 p.m. (1400), enter 14:00.If this field is blank, the phone automatically turns on at 00:00.
Phone Off Time	This field determines the time of day that the phone will turn itself off on the days that are selected in the Enable Power Save Plus list box. Enter the time in the following format hours:minutes. If this field is blank, the phone automatically turns off at midnight (00:00). Note: If Phone On Time is blank (or 00:00) and Phone Off Time is blank (or 24:00), the phone will remain on continuously, effectively disabling the Power Save Plus feature unless you allow EnergyWise

	to send overrides.
Phone Off Idle Timeout	This field represents the number of minutes that the device must be idle before the device will request the power sourcing equipment (PSE) to power down the device. The value in this field takes effect: - When the device was in Power Save Plus mode as scheduled and was taken out of Power Save Plus mode because the phone user pressed the select key - When the phone is repowered by the attached switch - When the Phone Off Time is met but the phone is in use. The unit is minutes. The default is 60. The range is 20 to 1440.

For more information on these features, see the Cisco DX Series Administration Guide or the Cisco DX Series Release Notes.

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

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html

Configuring the Cisco Unified Wireless LAN Controller and Access Points

When configuring the Cisco Unified Wireless LAN Controller and Access Points, use the following guidelines:

- Ensure **CCKM** is **Enabled** if utilizing 802.1x authentication
- Set **Quality of Service (QoS)** to **Platinum**
- Set the **WMM Policy** to **Required**
- Ensure **Session Timeout** is enabled and configured correctly
- Ensure **Aironet IE** is **Enabled**
- Set **DTPC Support** to **Enabled**
- Disable **P2P (Peer to Peer) Blocking Action** / **Public Secure Packet Forwarding (PSPF)**
- Ensure **Client Exclusion** is configured correctly
- Disable **DHCP Address Assignment Required**
- Set **MFP Client Protection** to **Optional** or **Disabled**
- Set the **DTIM Period** to **2**
- Set **Client Load Balancing** to **Disabled**
- Set **Client Band Select** to **Disabled**
- Set **IGMP Snooping** to **Enabled**
- Enable **Symmetric Mobile Tunneling Mode** if Layer 3 mobility is utilized
- Enable **Short Preamble** if using 2.4 GHz
- Enable **ClientLink** if utilizing Cisco 802.11n Access Points
- Configure the **Data Rates** as necessary
- Enable **CCX Location Measurement**
- Configure **Auto RF** as necessary
- Configure **SIP CAC Support** for **Voice** as necessary

- Enable **Traffic Stream Metrics** for **Voice**
- Set **Admission Control Mandatory** to **Disabled** for **Video**
- Set **EDCA Profile** to **Voice and Video Optimized**
- Set **Enable Low Latency MAC** to **Disabled**
- Ensure that **Power Constraint** is **Disabled**
- Enable **Channel Announcement** and **Channel Quiet Mode**
- Configure the **High Throughput Data Rates** as necessary
- Configure the **Frame Aggregation** settings
- Enable **CleanAir** if utilizing Cisco Access Points with CleanAir technology
- Configure **Multicast Direct Feature** as necessary
- Set the **802.1p tag** to **5** for the **Platinum** QoS profile

Note: If clients from other regions are present and will attempt to associate with the wireless LAN, then ensure that World Mode (802.11d) is enabled.

When using 802.1x authentication, it is recommended to implement CCKM to offer fast secure roaming.

WLAN Settings

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

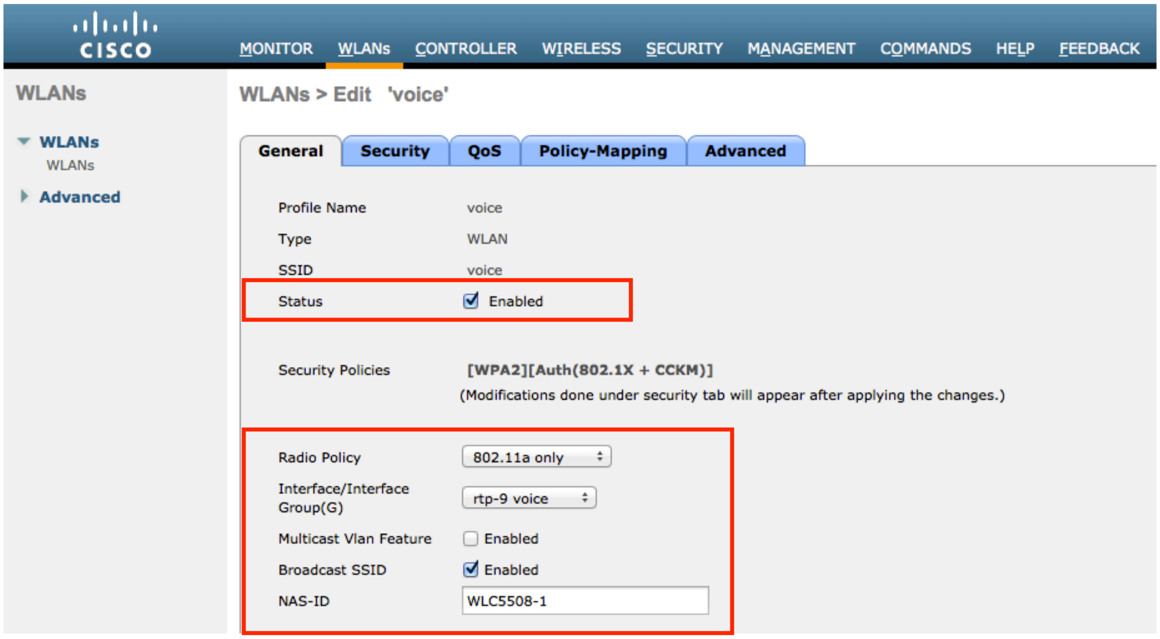
However, if there is an existing SSID configured to support voice and/or video capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

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

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

Enabling **Broadcast SSID** can help with deployment of the Cisco DX Series where the network can simply be selected from the list and additional parameters (e.g. security credentials, frequency band) can then be configured instead of having to manually configure all parameters.

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



WLANs > Edit 'voice'

Profile Name voice

Type WLAN

SSID voice

Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X + CCKM)]

(Modifications done under security tab will appear after applying the changes.)

Radio Policy 802.11a only

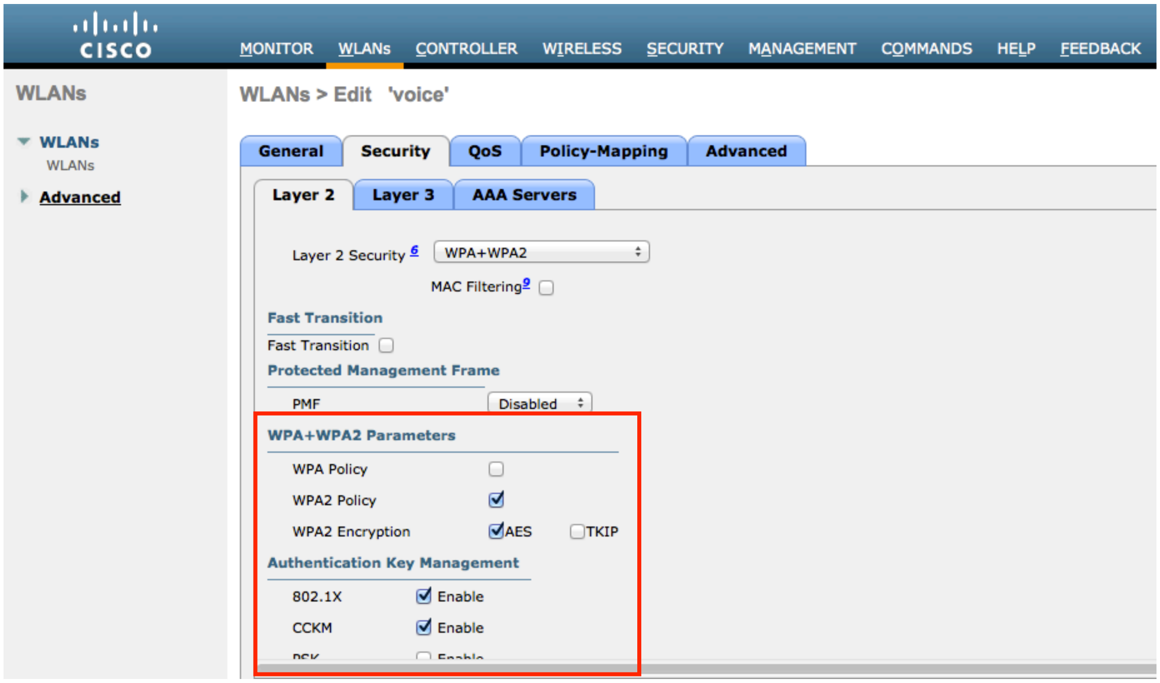
Interface/Interface Group(G) rtp-9 voice

Multicast Vlan Feature □ Enabled

Broadcast SSID ☑ Enabled

NAS-ID WLC5508-1

To utilize CCKM for fast secure roaming, enable WPA2 policy with AES encryption and 802.1x + CCKM for authenticated key management type in order to enable fast secure roaming.



WLANs > Edit 'voice'

Layer 2 Security 6 WPA+WPA2

MAC Filtering9 □

Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑AES □TKIP

Authentication Key Management

802.1X ☑ Enable

CCKM ☑ Enable

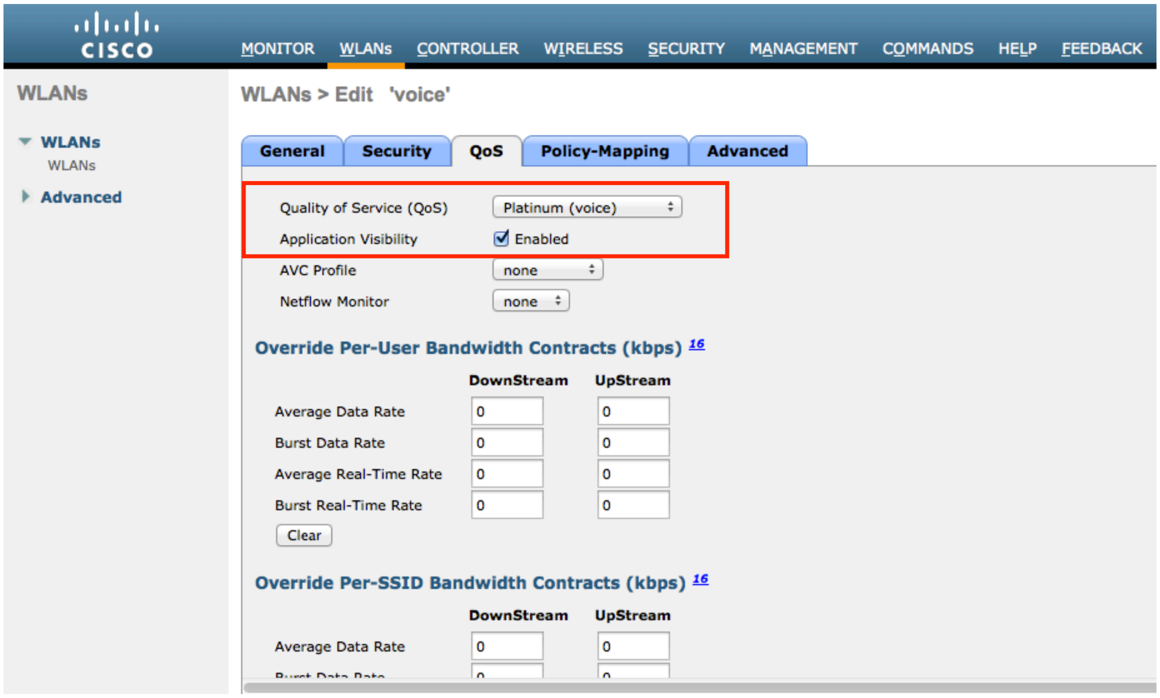
PSK □ Enable

The WMM policy should be set to **Required** only if the Cisco DX Series or other WMM enabled voice and/or video capable endpoints will be using this SSID.

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

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

Enable **7920 AP CAC** to advertise Qos Basic Service Set (QBSS) to the client.



WLANs > Edit 'voice'

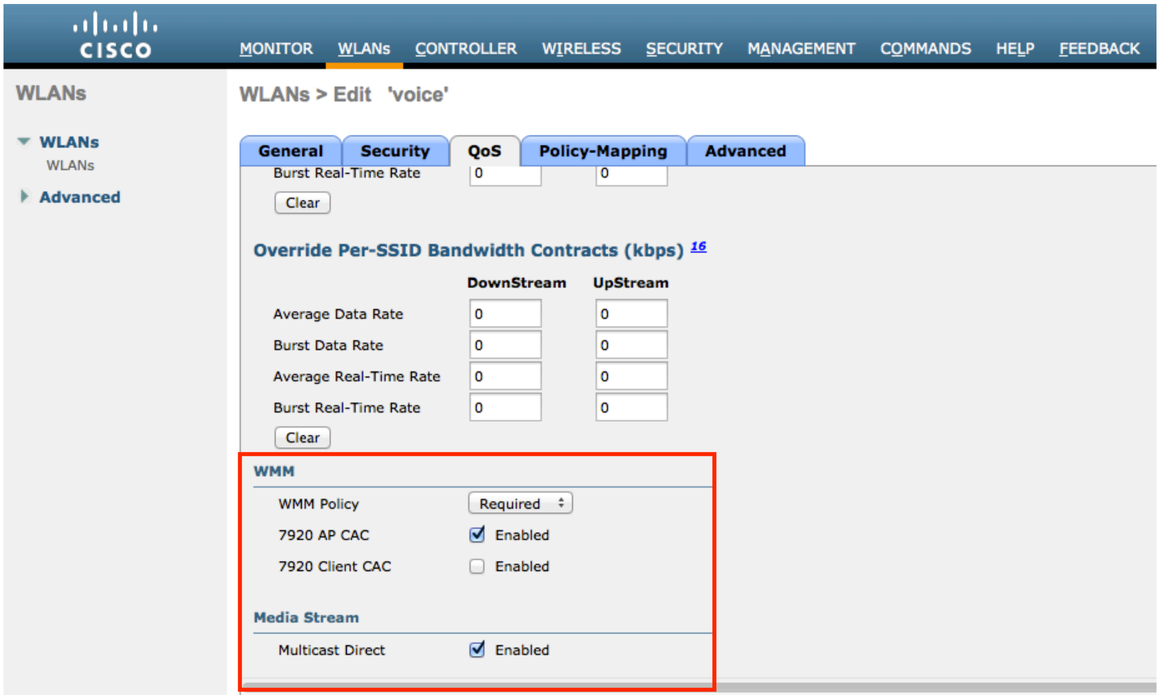
Quality of Service (QoS): Platinum (voice)
Application Visibility: ☑ Enabled
AVC Profile: none
Netflow Monitor: none

Override Per-User Bandwidth Contracts (kbps) [16]

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

Override Per-SSID Bandwidth Contracts (kbps) [16]

	DownStream	UpStream
Average Data Rate	0	0



WLANs > Edit 'voice'

Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) [16]

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

WMM

WMM Policy: Required
7920 AP CAC: ☑ Enabled
7920 Client CAC: □ Enabled

Media Stream

Multicast Direct: ☑ Enabled

Configure **Enable Session Timeout** as necessary per your requirements. It is recommended to either disable the session timeout or extend the timeout (e.g. 24 hours / 86400 seconds) to avoid possible interruptions during audio or video calls. If disabled it will avoid any potential interruptions altogether, but enabling session timeout can help to re-validate client credentials periodically to ensure that the client is using valid credentials.

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

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

Configure **Client Exclusion** as necessary.

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

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

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

DHCP Address Assignment Required should be disabled.

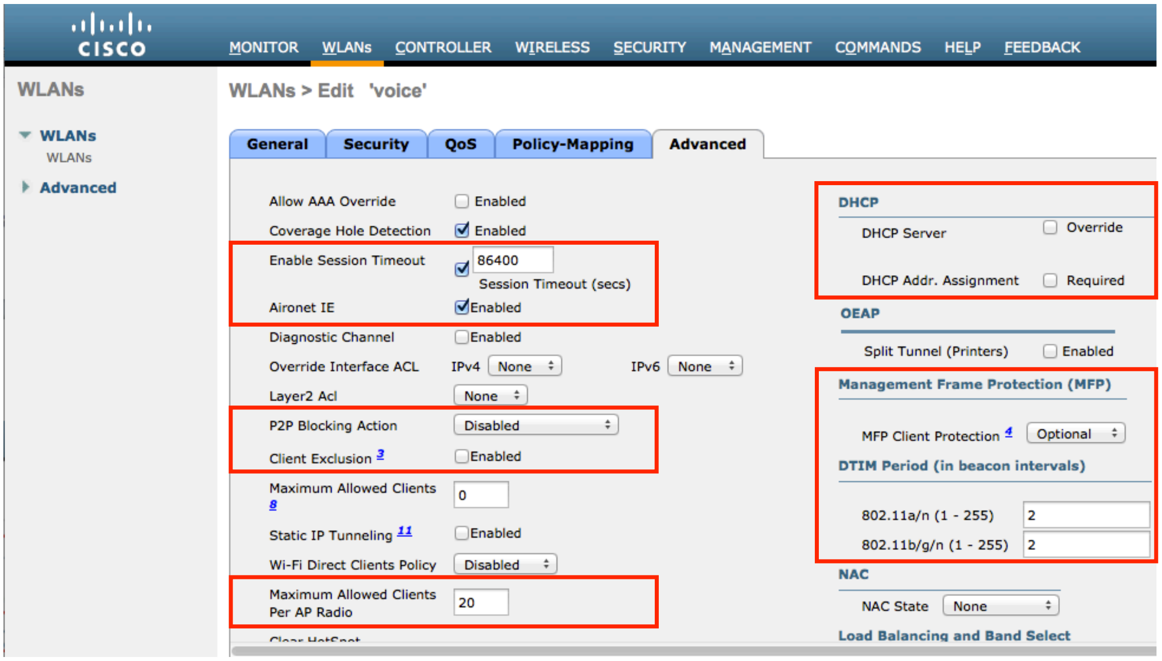
Management Frame Protection should be set to **Optional** or **Disabled.**

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

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

Media Session Snooping can optionally be enabled to utilize SIP CAC.

It is recommended to set **Re-anchor Roamed Voice Clients** to disabled as this can cause brief interruptions with wireless LAN connectivity when a call is terminated after performing an inter-controller roaming.



WLANs > Edit 'voice'

Allow AAA Override ☐ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 86400 Session Timeout (secs)

Aironet IE ☑Enabled

Diagnostic Channel ☐Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

P2P Blocking Action Disabled

Client Exclusion [3] ☐Enabled

Maximum Allowed Clients [8] 0

Static IP Tunneling [11] ☐Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 20

Clear HotSpot

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☐ Required

OEAP

Split Tunnel (Printers) ☐ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)

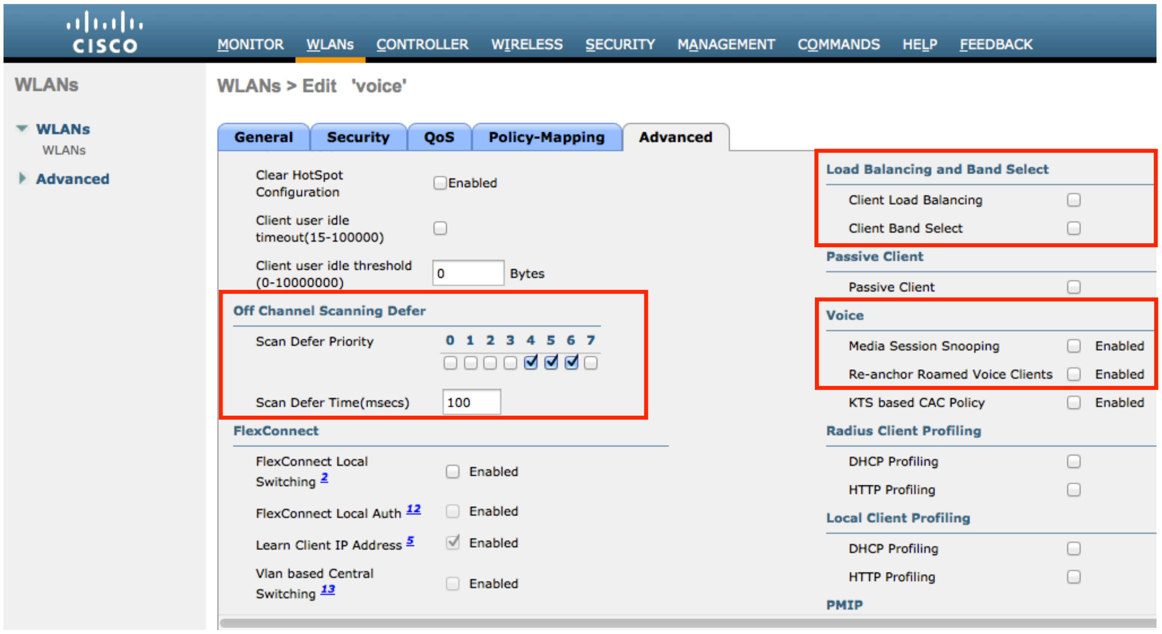
802.11a/n (1 - 255) 2

802.11b/g/n (1 - 255) 2

NAC

NAC State None

Load Balancing and Band Select



WLANs > Edit 'voice'

Clear HotSpot Configuration ☐Enabled

Client user idle timeout(15-100000) ☐

Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7
☐ ☐ ☐ ☐ ☑ ☑ ☑ ☐

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching [2] ☐ Enabled

FlexConnect Local Auth [12] ☐ Enabled

Learn Client IP Address [5] ☑ Enabled

Vlan based Central Switching [13] ☐ Enabled

Load Balancing and Band Select

Client Load Balancing ☐

Client Band Select ☐

Passive Client

Passive Client ☐

Voice

Media Session Snooping ☐ Enabled

Re-anchor Roamed Voice Clients ☐ Enabled

KTS based CAC Policy ☐ Enabled

Radius Client Profiling

DHCP Profiling ☐

HTTP Profiling ☐

Local Client Profiling

DHCP Profiling ☐

HTTP Profiling ☐

PMIP

For the Cisco Autonomous Access Point, ensure that the SSID is configured for open + eap as and network-eap when using 802.1x authentication.

```
dot11 ssid voice
   vlan 21
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa cckm
   admit-traffic
```

If the Cisco Autonomous Access Point is registered to a WDS (Wireless Domain Services) server, ensure both types of authentication are enabled in the WDS configuration.

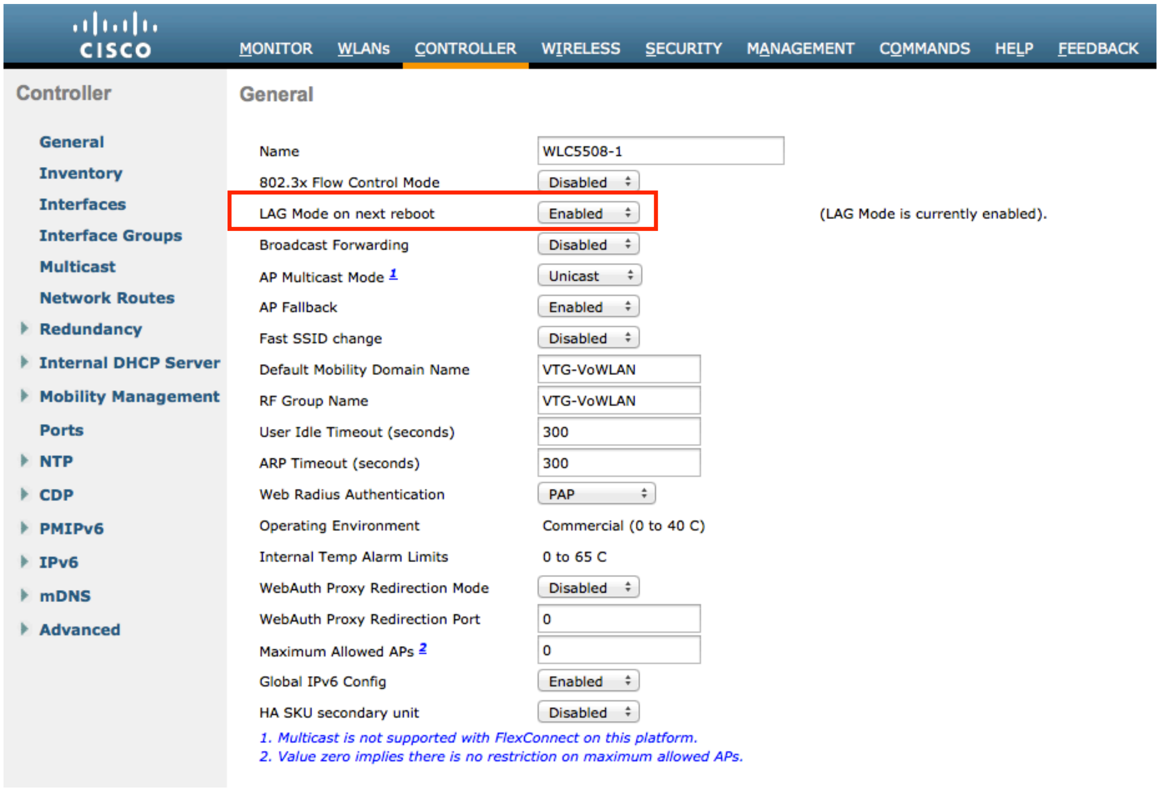
```
wlccp authentication-server infrastructure method_Infrastructure

wlccp authentication-server client mac method_Clients

wlccp authentication-server client eap method_Clients

wlccp authentication-server client leap method_Clients

wlccp wds priority 255 interface BVI1
```

Controller Settings

Ensure the Cisco Unified Wireless LAN Controller hostname is configured correctly.

Enable Link Aggregation (LAG) if utilizing multiple ports on the Cisco Unified Wireless LAN Controller.

Configure the desired AP multicast mode.

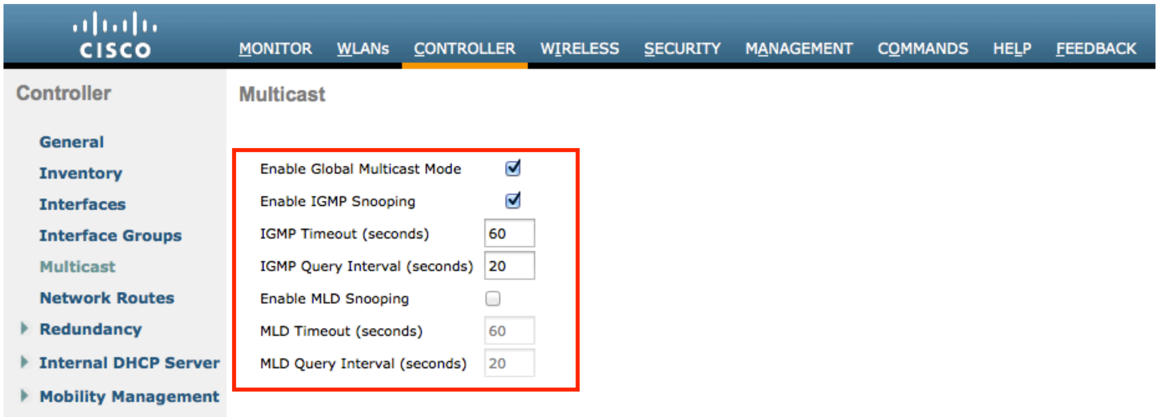


General

Name	WLC5508-1
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled (LAG Mode is currently enabled).
Broadcast Forwarding	Disabled
AP Multicast Mode [1]	Unicast
AP Fallback	Enabled
Fast SSID change	Disabled
Default Mobility Domain Name	VTG-VoWLAN
RF Group Name	VTG-VoWLAN
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C
WebAuth Proxy Redirection Mode	Disabled
WebAuth Proxy Redirection Port	0
Maximum Allowed APs [2]	0
Global IPv6 Config	Enabled
HA SKU secondary unit	Disabled

1. Multicast is not supported with FlexConnect on this platform.
2. Value zero implies there is no restriction on maximum allowed APs.

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

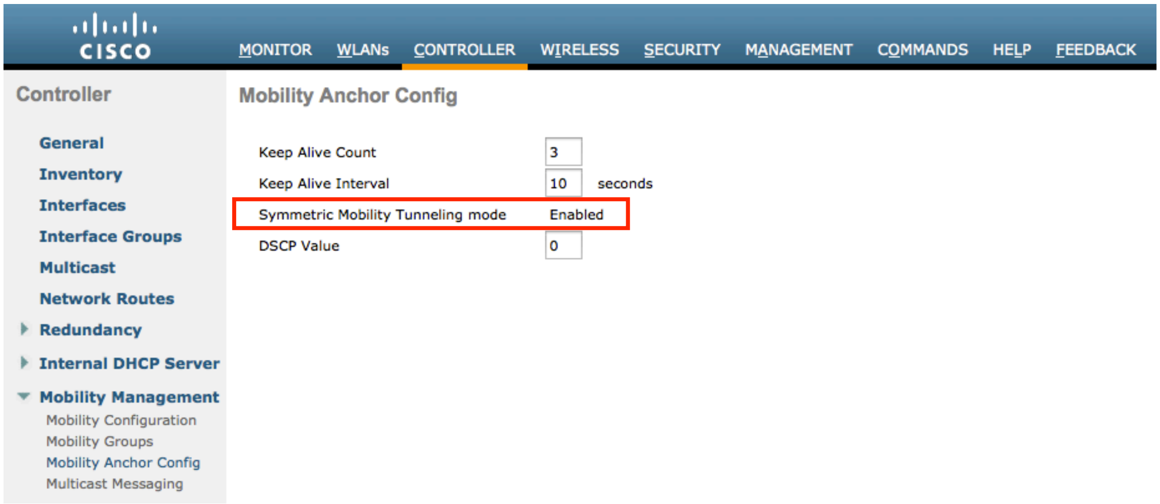


Multicast

Enable Global Multicast Mode	☑
Enable IGMP Snooping	☑
IGMP Timeout (seconds)	60
IGMP Query Interval (seconds)	20
Enable MLD Snooping	□
MLD Timeout (seconds)	60
MLD Query Interval (seconds)	20

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

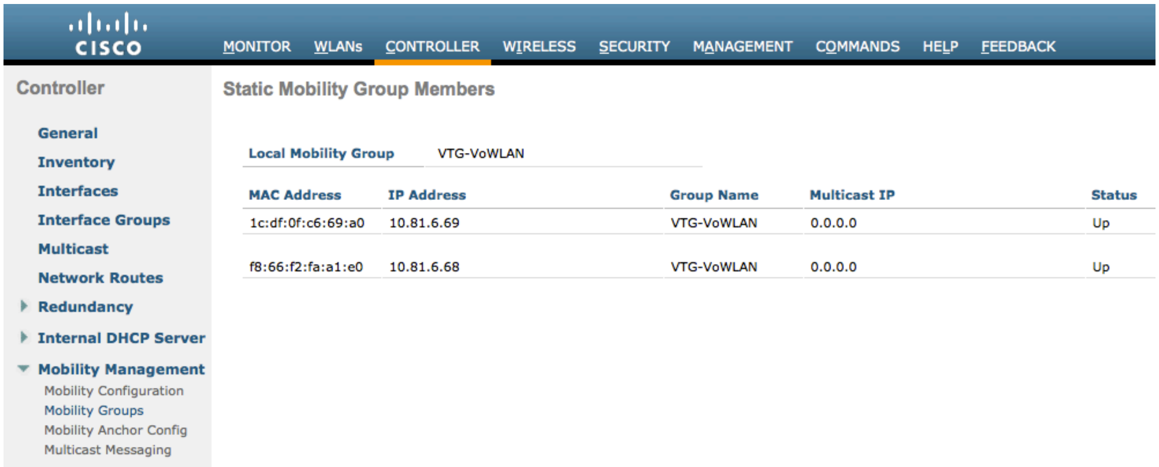
In the recent versions, Symmetric Mobility Tunneling is enabled by default and non-configurable.



Mobility Anchor Config

Keep Alive Count	3
Keep Alive Interval	10 seconds
Symmetric Mobility Tunneling mode	Enabled
DSCP Value	0

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



Static Mobility Group Members

Local Mobility Group VTG-VoWLAN

MAC Address	IP Address	Group Name	Multicast IP	Status
1c:df:0f:c6:69:a0	10.81.6.69	VTG-VoWLAN	0.0.0.0	Up
f8:66:f2:fa:a1:e0	10.81.6.68	VTG-VoWLAN	0.0.0.0	Up

802.11 Network Settings

If using 5 GHz, ensure the 802.11a network status is **Enabled**.

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

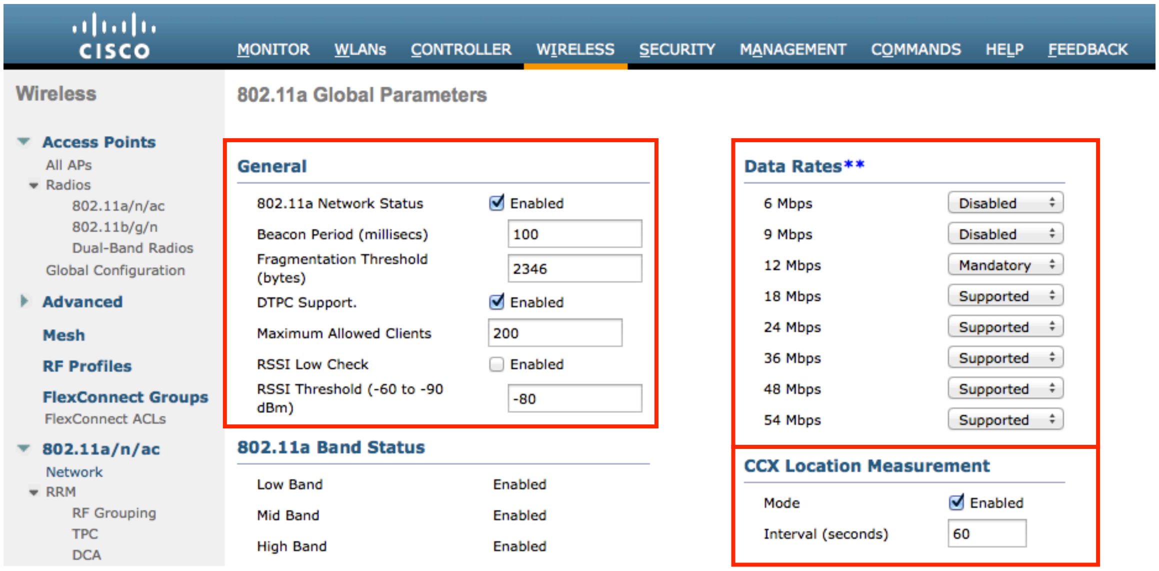
Ensure **DTPC Support** is enabled.

If using Cisco 802.11n Access Points, ensure **ClientLink** is enabled.

With the current releases, **Maximum Allowed Clients** can be configured.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

Enable **CCX Location Measurement**.



802.11a Global Parameters

General

802.11a Network Status	☑ Enabled
Beacon Period (millisecs)	100
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200
RSSI Low Check	□ Enabled
RSSI Threshold (-60 to -90 dBm)	-80

802.11a Band Status

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

CCX Location Measurement

Mode	☑ Enabled
Interval (seconds)	60

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

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

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

Ensure **DTPC Support** is enabled.

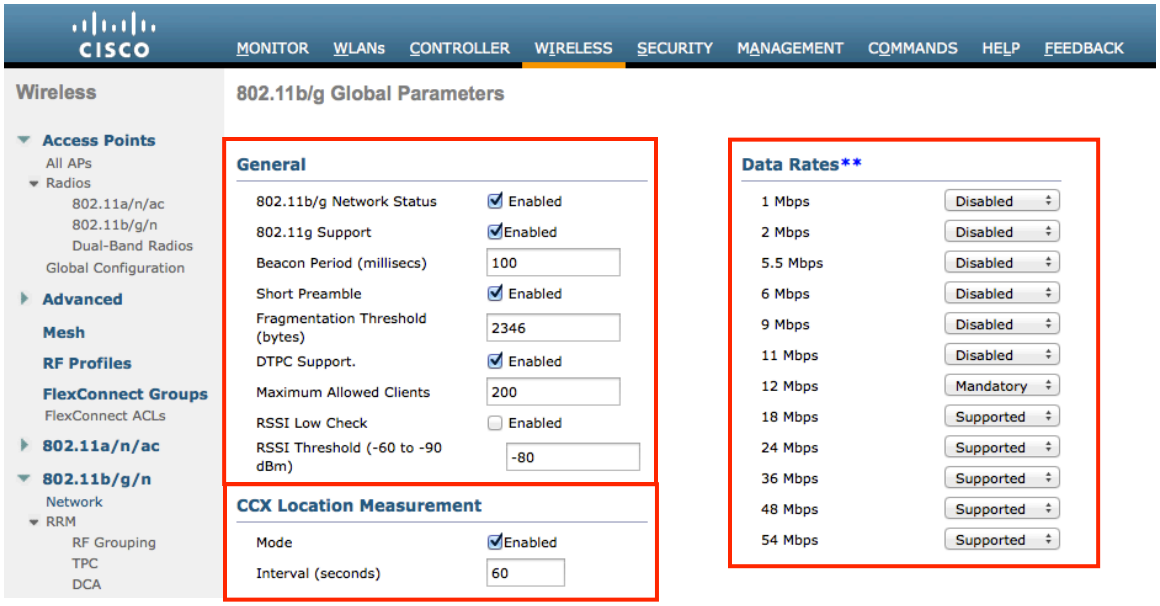
If using Cisco 802.11n Access Points, ensure **ClientLink** is enabled.

With the current releases, **Maximum Allowed Clients** can be configured.

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

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

Enable **CCX Location Measurement**.



802.11b/g Global Parameters

General

802.11b/g Network Status	☑ Enabled
802.11g Support	☑ Enabled
Beacon Period (millisecs)	100
Short Preamble	☑ Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200
RSSI Low Check	□ Enabled
RSSI Threshold (-60 to -90 dBm)	-80

CCX Location Measurement

Mode	☑ Enabled
Interval (seconds)	60

Data Rates**

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

Beamforming (ClientLink)

Enable **ClientLink** if using Cisco 802.11n Access Points.

Beamforming is not supported with data rates 1, 2, 5.5, and 11 Mbps.

For releases prior to 7.2.103.0, **ClientLink** can be enabled globally via the 802.11 Global Parameters section or on individual access points via the access point's 802.11 radio configuration page.

As of release 7.2.103.0, **ClientLink** is no longer configurable via the Cisco Unified Wireless LAN Controller's web interface and is only configurable via command line.

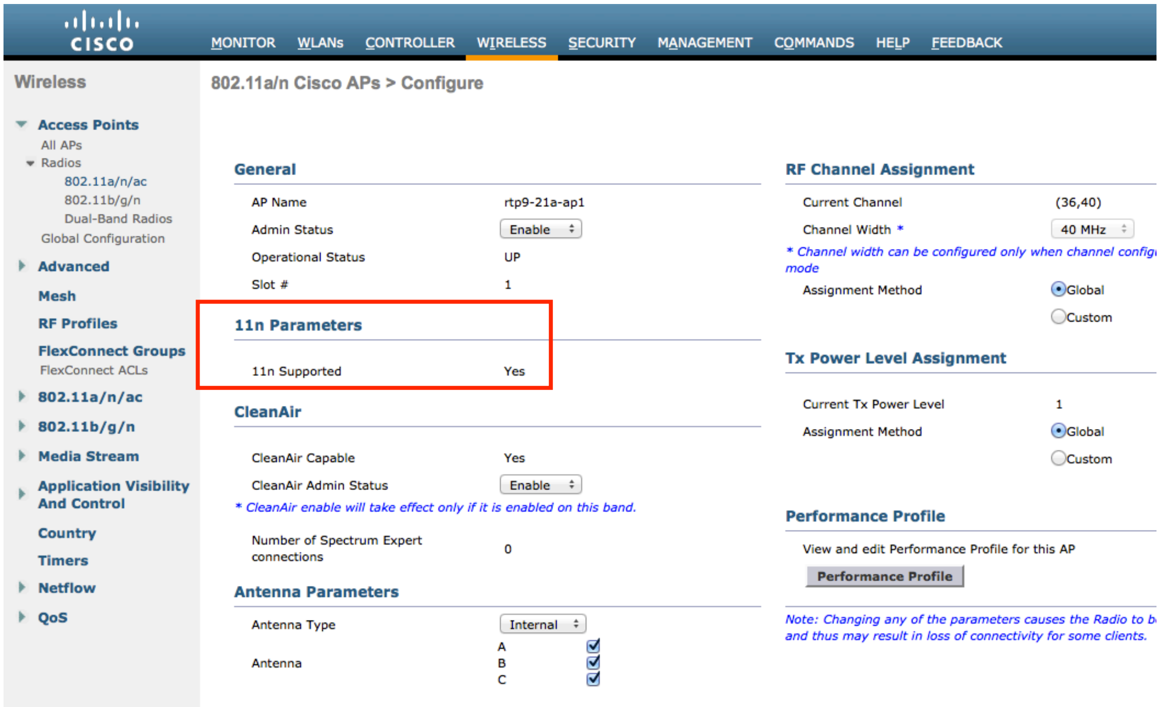
With releases 7.2.103.0 and later use the following commands to enable the beamforming feature globally for all access points or for individual access point radios.

```
(Cisco Controller) >config 802.11a beamforming global enable
(Cisco Controller) >config 802.11a beamforming ap <ap_name> enable
(Cisco Controller) >config 802.11b beamforming global enable
(Cisco Controller) >config 802.11b beamforming ap <ap_name> enable
```

The current status of the beamforming feature can be displayed by using the following command.

```
(Cisco Controller) >show 802.11a
(Cisco Controller) >show 802.11b
```

Legacy Tx Beamforming setting.................... **Enabled**



802.11a/n Cisco APs > Configure

General

AP Name	rtp9-21a-ap1
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	(36,40)
Channel Width *	40 MHz

* Channel width can be configured only when channel configi mode

Assignment Method	● Global ○ Custom

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	● Global ○ Custom

Performance Profile

View and edit Performance Profile for this AP

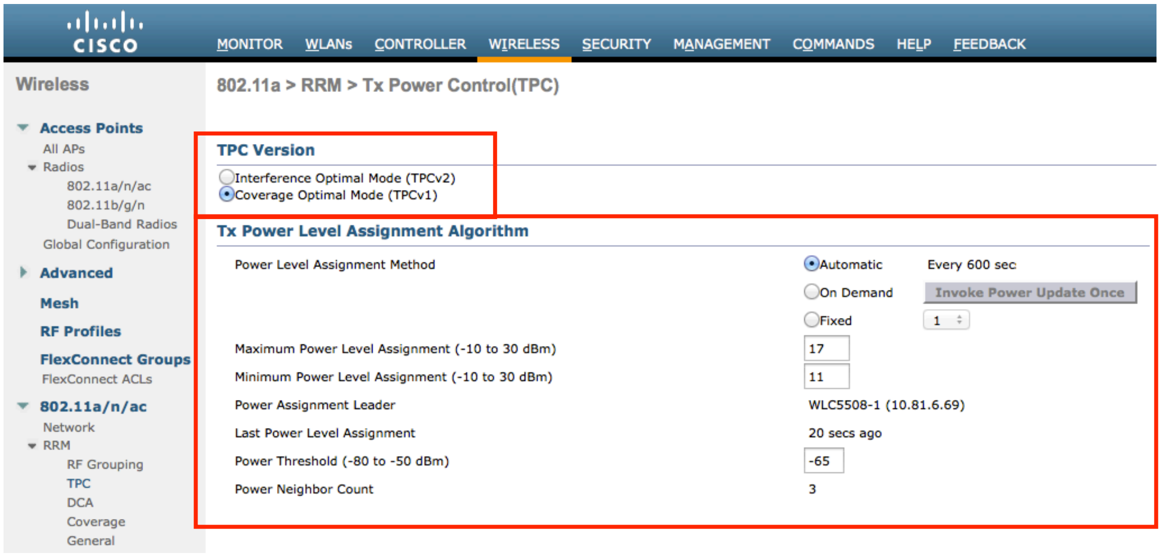
Note: Changing any of the parameters causes the Radio to b and thus may result in loss of connectivity for some clients.

Auto RF (RRM)

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

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

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



802.11a > RRM > Tx Power Control(TPC)

TPC Version

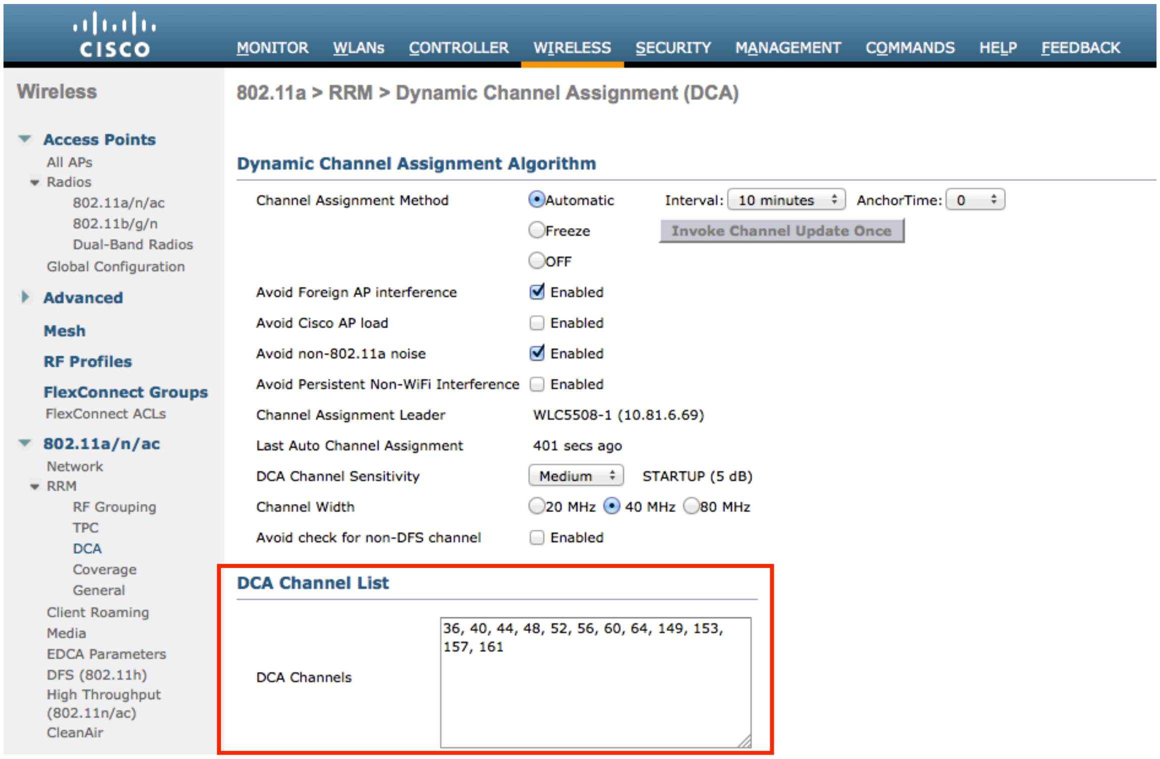
○ Interference Optimal Mode (TPCv2)
● Coverage Optimal Mode (TPCv1)

Tx Power Level Assignment Algorithm

Power Level Assignment Method	● Automatic	Every 600 sec
	○ On Demand	Invoke Power Update Once
	○ Fixed	1
Maximum Power Level Assignment (-10 to 30 dBm)	17	
Minimum Power Level Assignment (-10 to 30 dBm)	11	
Power Assignment Leader	WLC5508-1 (10.81.6.69)	
Last Power Level Assignment	20 secs ago	
Power Threshold (-80 to -50 dBm)	-65	
Power Neighbor Count	3	

If using 5 GHz, it is recommended to enable up to 12 channels only to avoid any potential delay of access point discovery due to having to scan many channels.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points.



802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

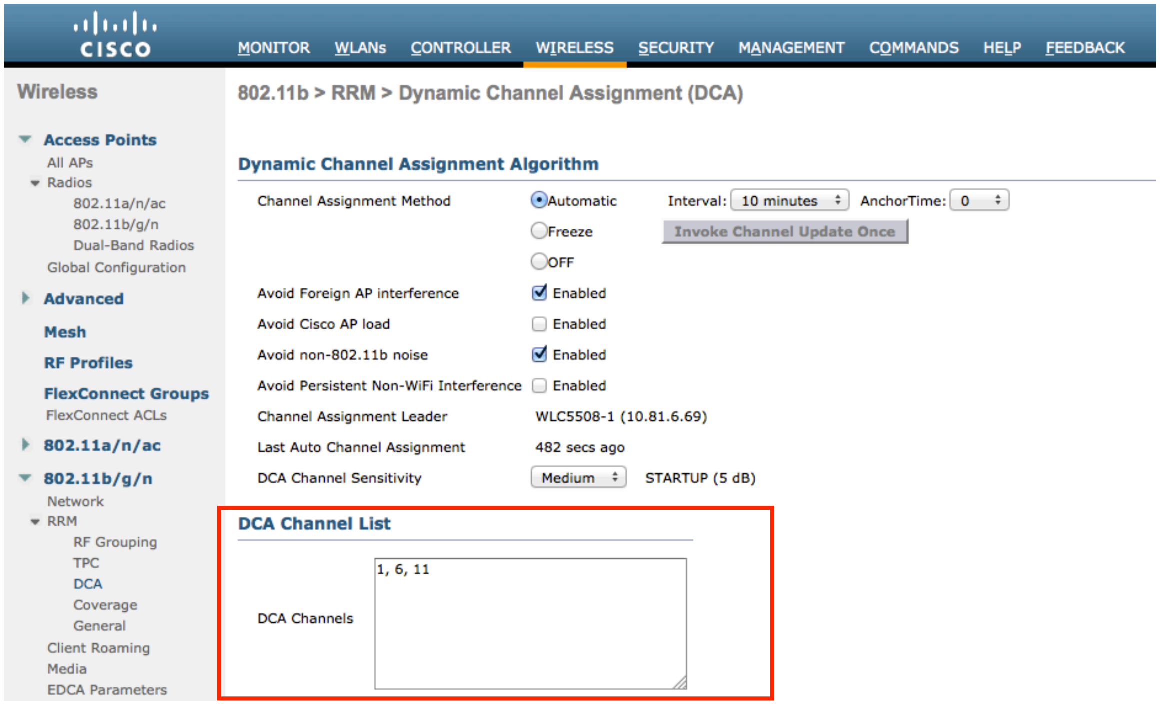
Channel Assignment Method	● Automatic	Interval: 10 minutes AnchorTime: 0
	○ Freeze	Invoke Channel Update Once
	○ OFF	
Avoid Foreign AP interference	☑ Enabled	
Avoid Cisco AP load	□ Enabled	
Avoid non-802.11a noise	☑ Enabled	
Avoid Persistent Non-WiFi Interference	□ Enabled	
Channel Assignment Leader	WLC5508-1 (10.81.6.69)	
Last Auto Channel Assignment	401 secs ago	
DCA Channel Sensitivity	Medium	STARTUP (5 dB)
Channel Width	○ 20 MHz ● 40 MHz ○ 80 MHz	
Avoid check for non-DFS channel	□ Enabled	

DCA Channel List

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

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

It is recommended to configure the 2.4 GHz channel for 20 MHz even if using Cisco 802.11n Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.



802.11b > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method ● Automatic Interval: 10 minutes AnchorTime: 0
○ Freeze
○ OFF

Avoid Foreign AP interference ☑ Enabled

Avoid Cisco AP load □ Enabled

Avoid non-802.11b noise ☑ Enabled

Avoid Persistent Non-WiFi Interference □ Enabled

Channel Assignment Leader WLC5508-1 (10.81.6.69)

Last Auto Channel Assignment 482 secs ago

DCA Channel Sensitivity Medium STARTUP (5 dB)

DCA Channel List

DCA Channels 1, 6, 11

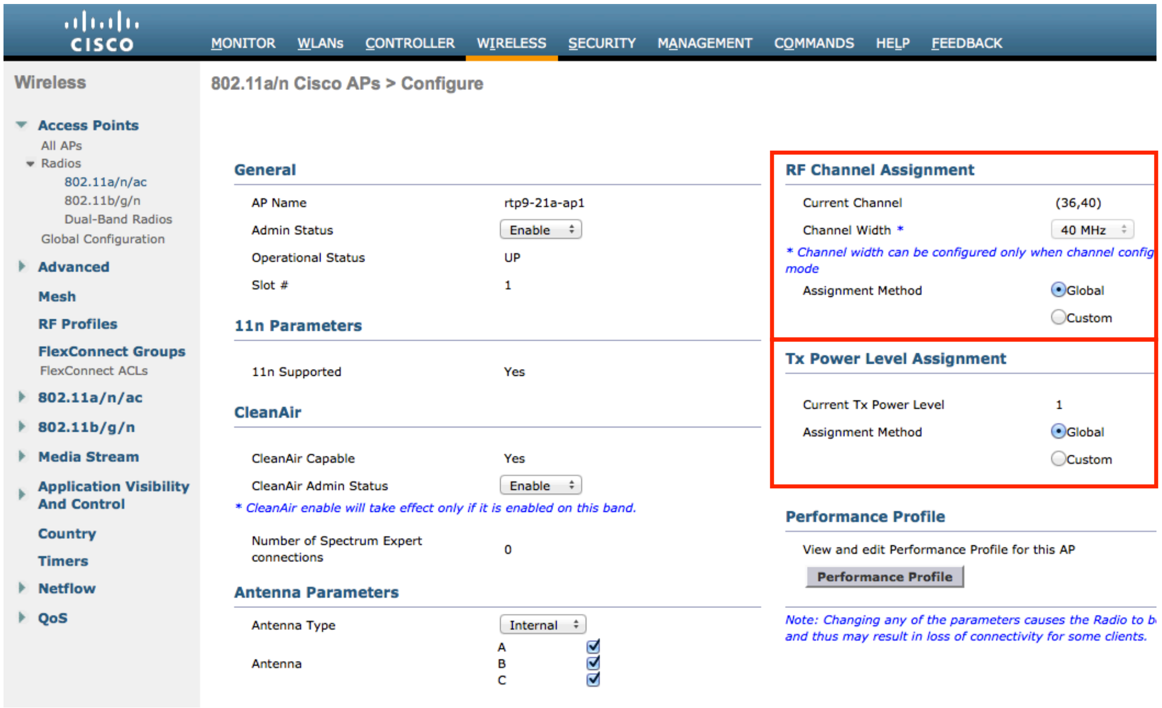
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which band is to be utilized.

Other access points enabled can be enabled for Auto RF and workaround the access points that are statically configured.

This may be necessary if there is an intermittent interferer present in an area.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points.

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



802.11a/n Cisco APs > Configure

General

AP Name rtp9-21a-ap1

Admin Status Enable

Operational Status UP

Slot # 1

11n Parameters

11n Supported Yes

CleanAir

CleanAir Capable Yes

CleanAir Admin Status Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections 0

Antenna Parameters

Antenna Type Internal

Antenna A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel (36,40)

Channel Width * 40 MHz

** Channel width can be configured only when channel config mode*

Assignment Method ● Global
○ Custom

Tx Power Level Assignment

Current Tx Power Level 1

Assignment Method ● Global
○ Custom

Performance Profile

View and edit Performance Profile for this AP

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

Client Roaming

The Cisco DX Series does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

Call Admission Control

The Cisco DX Series currently does not support TSPEC (Call Admission Control).

Call Admission Control (TSPEC) for voice should only be enabled if other TSPEC capable clients are using the same band frequency; TSPEC for video should not be enabled.

If **Admission Control Mandatory (ACM)** is enabled for **Voice**, the Cisco DX Series will be required to downgrade the priority of the audio packets sent upstream from UP6 (voice) to a lower priority (UP5 video) for an audio only call.

If Call Admission Control for voice is to be enabled, then configure maximum bandwidth and reserved roaming bandwidth percentages for either 5 or 2.4 GHz depending on which band is to be utilized.

The maximum bandwidth default setting for voice is **75%** where **6%** of that bandwidth is reserved for roaming clients.

Roaming clients are not limited to using the reserved roaming bandwidth, but roaming bandwidth is to reserve some bandwidth for roaming clients in case all other bandwidth is utilized.

If CAC is to be enabled, will want to ensure **Load-based CAC** is enabled, which is available for the Cisco Unified Wireless LAN Controller, but not currently available on the Cisco Autonomous Access Point platform.

Load-based CAC will account for all energy on the channel.

Since TSPEC is not supported currently, **SIP CAC** can be utilized, which will require media session snooping to be enabled on the WLAN.

Traffic Stream Metrics (TSM) is not supported as this feature requires TSPEC support, but can be enabled if other capable clients are utilizing the same band frequency.

SIP CAC is to help ensure that downstream voice frames are prioritized correctly.

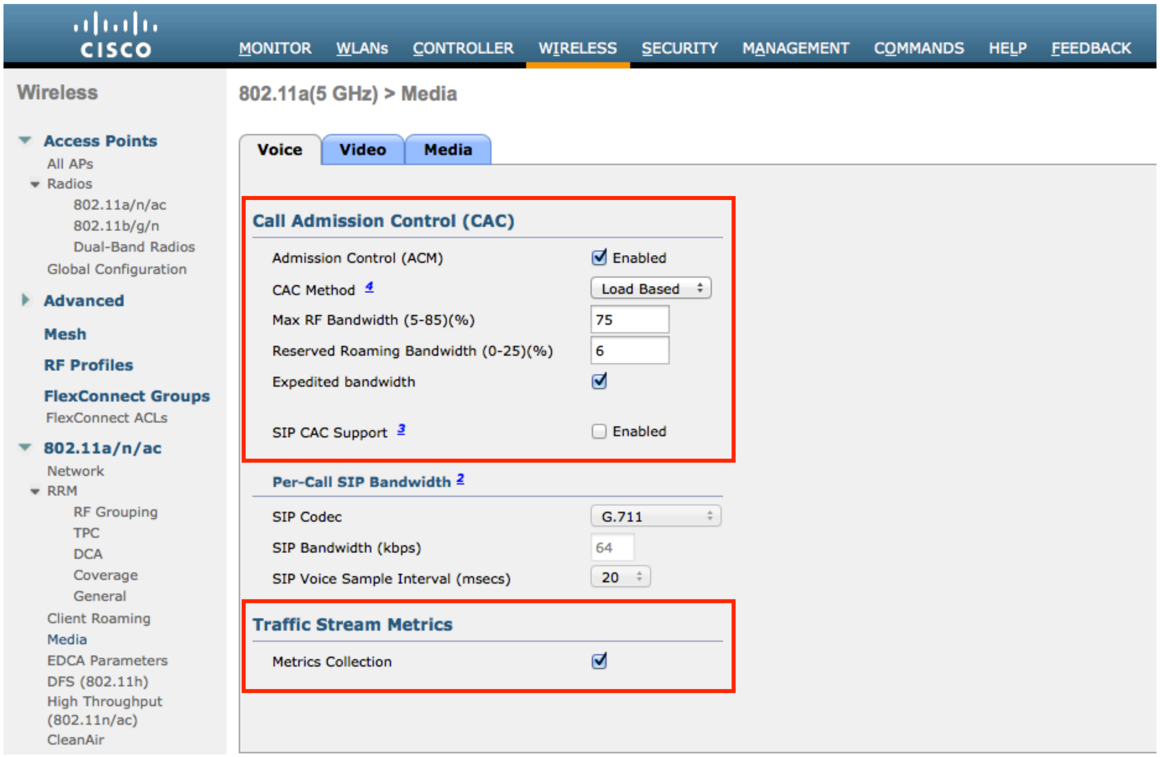
Load based CAC logic is utilized with SIP CAC, so all 802.11 traffic and energy on the channel is accounted for to determine available bandwidth.

The access point has different methods for call admission control when using SIP CAC depending on whether the client uses TCP or UDP for SIP communications.

If the client uses TCP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN and will not forward the SIP frames upstream or downstream if there is not bandwidth available for the new voice stream. This could potentially result in loss of registration to the Cisco Unified Communications Manager.

If the client uses UDP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN and will sent a 486 busy message to the client, which in turn can be interpreted as a **Network Busy** message and the client could either roam to another access point or simply terminate the call setup for that session.

The Cisco DX Series uses TCP for SIP communications, therefore if the channel is busy where another call can not be allowed, then the Cisco DX Series could potentially lose registration to the Cisco Unified Communications Manager.



802.11a(5 GHz) > Media

Call Admission Control (CAC)

Admission Control (ACM)	☑ Enabled
CAC Method [4]	Load Based
Max RF Bandwidth (5-85)(%)	75
Reserved Roaming Bandwidth (0-25)(%)	6
Expedited bandwidth	☑
SIP CAC Support [3]	□ Enabled

Per-Call SIP Bandwidth [2]

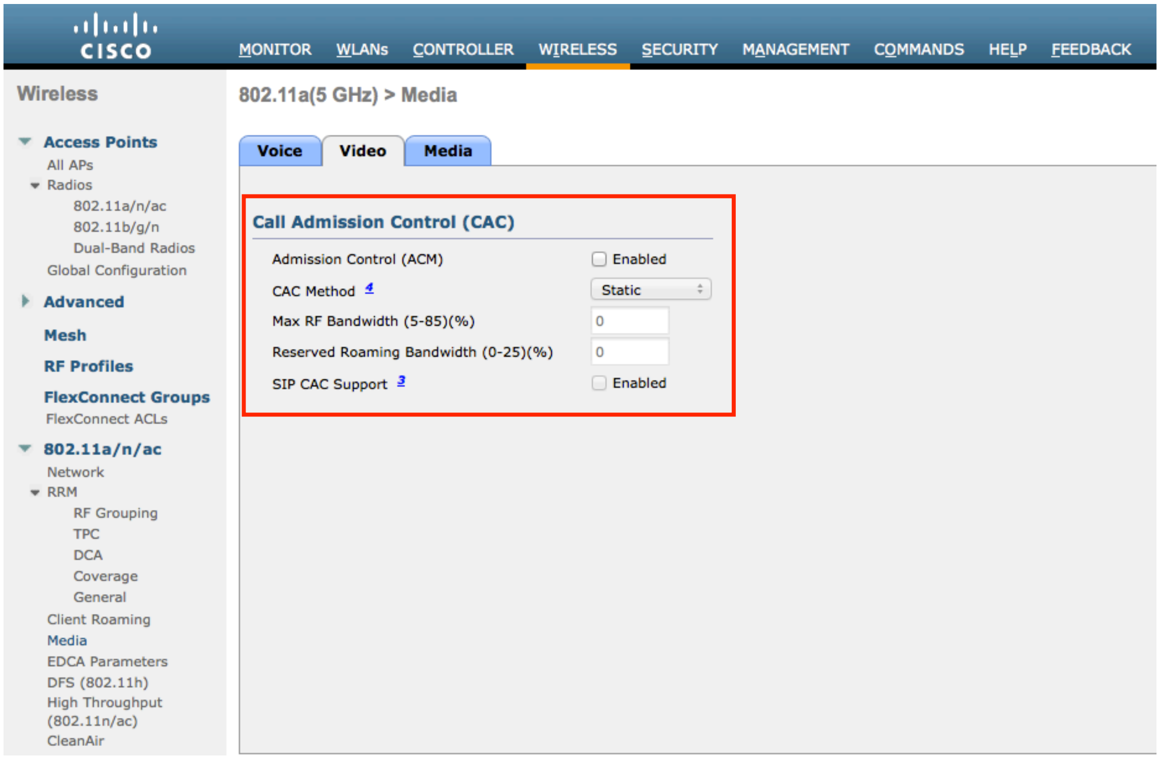
SIP Codec	G.711
SIP Bandwidth (kbps)	64
SIP Voice Sample Interval (msecs)	20

Traffic Stream Metrics

Metrics Collection	☑

Admission Control Mandatory for **Video** should be disabled.

If enabled, priority of video frames will be downgraded to best effort.



802.11a(5 GHz) > Media

Call Admission Control (CAC)

Admission Control (ACM)	□ Enabled
CAC Method [4]	Static
Max RF Bandwidth (5-85)(%)	0
Reserved Roaming Bandwidth (0-25)(%)	0
SIP CAC Support [3]	□ Enabled

If Call Admission Control for voice is enabled, then the following configuration should be active, which can be displayed in the **show run-config**.

```
Call Admission Control (CAC) configuration
Voice AC - Admission control (ACM)............ Enabled
Voice max RF bandwidth........................ 75
Voice reserved roaming bandwidth.............. 6
Voice load-based CAC mode..................... Enabled
Voice tspec inactivity timeout................ Disabled
Video AC - Admission control (ACM)............ Disabled
Voice Stream-Size............................. 84000
Voice Max-Streams............................. 2
Video max RF bandwidth........................ 25
Video reserved roaming bandwidth.............. 6
```

The voice stream-size and voice max-streams values can be adjusted as necessary by using the following command.

```
(Cisco Controller) >config 802.11a cac voice stream-size 84000 max-streams 2
```

Ensure QoS is setup correctly under the WLAN configuration, which can be displayed by using the following command.

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

```
Quality of Service............................... Platinum (voice)
WMM............................................. Allowed
Dot11-Phone Mode (7920)......................... ap-cac-limit
Wired Protocol.................................. 802.1P (Tag=5)
```

When enabling Call Admission Control on the Cisco Autonomous Access Point, the admission must be unblocked on the SSID as well.

Load-based CAC and support for multiple streams are not present on the Cisco Autonomous Access Points therefore it is not recommended to enable CAC on Cisco Autonomous Access Points.

The Cisco Autonomous Access Point only allows for 1 stream and the stream size is not customizable, therefore SRTP and barge will not work if CAC is enabled.

```
dot11 ssid voice
  vlan 21
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa cckm
  admit-traffic
```

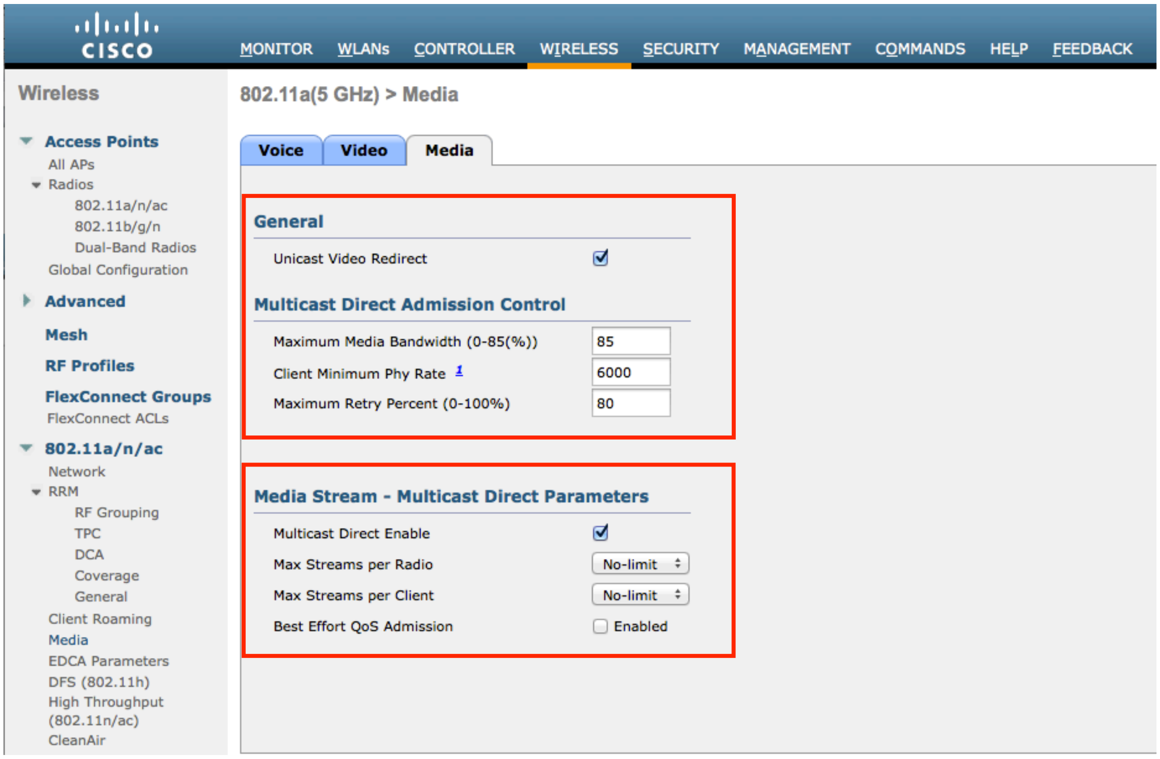
It is recommended to use the defaults, where 5.5, 6, 11, 12 and 24 Mbps are enabled as nominal rates for 802.11b/g, 6, 12, and 24 Mbps enabled for 802.11a and 6.5, 13, and 26 Mbps enabled for 802.11n.

If enabling the STREAM feature either directly or via selecting **Optimized Voice** for the radio access category in the QoS configuration section, ensure that only voice packets are being put into the voice queue. Signaling packets (SIP) should be put into a separate queue. This can be ensured by setting up a QoS policy mapping the DSCP to the correct queue.

For more information about Call Admission Control and QoS, refer to the **Configuring QoS** chapter in the Cisco IOS Software Configuration Guide for Cisco Aironet Access Points at this URL:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4-25d-JA/Configuration/guide/cg_12_4_25d_JA.html

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



802.11a(5 GHz) > Media

General

Unicast Video Redirect ☑

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%))	85
Client Minimum Phy Rate [1]	6000
Maximum Retry Percent (0-100%)	80

Media Stream - Multicast Direct Parameters

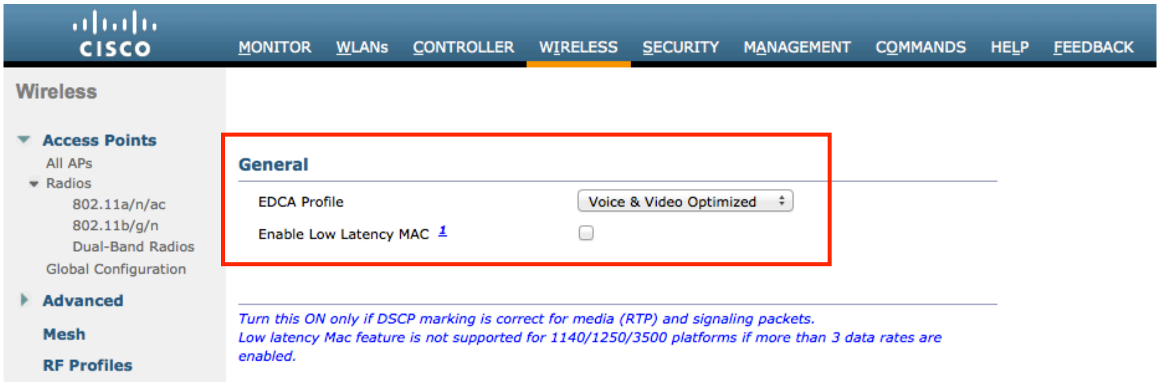
Multicast Direct Enable	☑
Max Streams per Radio	No-limit
Max Streams per Client	No-limit
Best Effort QoS Admission	□ Enabled

EDCA Parameters

Set the EDCA profile for **Voice and Video Optimized** and disable **Low Latency MAC** for either 5 or 2.4 GHz depending on which band is to be utilized.

Low Latency MAC (LLM) reduces the number of retransmissions to 2-3 per packet depending on the access point platform, so it can cause issues if multiple data rates are enabled.

LLM is not supported on the Cisco 802.11n Access Points.



General

EDCA Profile	Voice & Video Optimized
Enable Low Latency MAC [1]	□

Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets.
Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled.

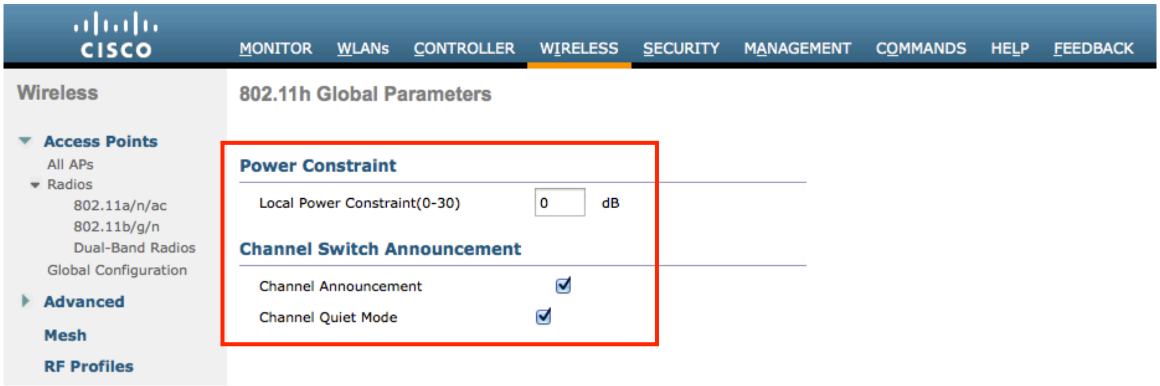
DFS (802.11h)

In the DFS (802.11h) configuration, channel announcement and quiet mode should be enabled.

Power Constraint should be left un-configured or set to 0 dB as DTPC will be used by the Cisco DX Series to control the transmission power.

In later versions of the Cisco Unified Wireless LAN Controller it does not allow both TPC (Power Constraint) and DTPC (Dynamic Transmit Power Control) to be enabled simultaneously.

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



802.11h Global Parameters

Power Constraint

Local Power Constraint(0-30) 0 dB

Channel Switch Announcement

Channel Announcement ☑

Channel Quiet Mode ☑

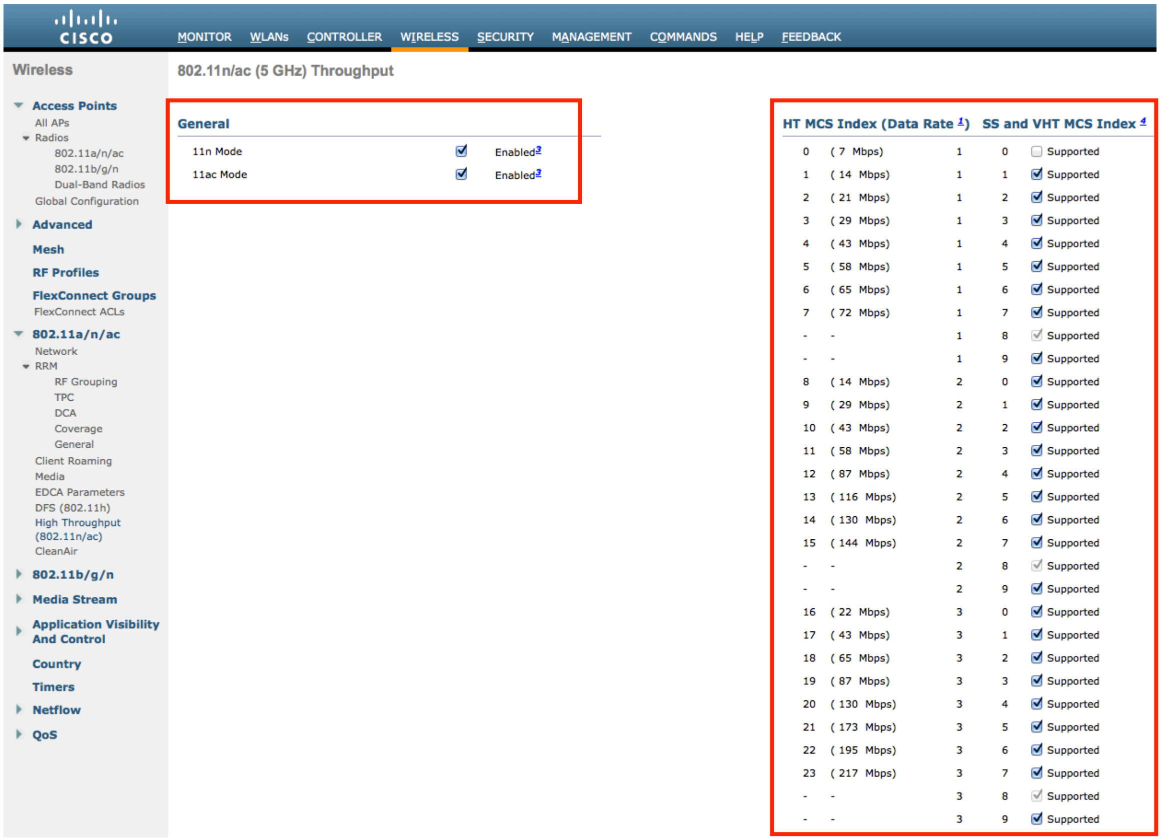
High Throughput (802.11n)

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

Ensure that **WMM** is enabled and **WPA2(AES)** is configured in order to utilize 802.11n data rates.

The Cisco DX Series supports MCS 0 - MCS 7 data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of the those higher data rates.

It is recommended to disable MCS 0.



802.11n/ac (5 GHz) Throughput

General

11n Mode	☑	Enabled[2]
11ac Mode	☑	Enabled[3]

HT MCS Index (Data Rate [1])		SS and VHT MCS Index [4]		
0	(7 Mbps)	1	0	☐ Supported
1	(14 Mbps)	1	1	☑ Supported
2	(21 Mbps)	1	2	☑ Supported
3	(29 Mbps)	1	3	☑ Supported
4	(43 Mbps)	1	4	☑ Supported
5	(58 Mbps)	1	5	☑ Supported
6	(65 Mbps)	1	6	☑ Supported
7	(72 Mbps)	1	7	☑ Supported
-	-	1	8	☑ Supported
-	-	1	9	☑ Supported
8	(14 Mbps)	2	0	☑ Supported
9	(29 Mbps)	2	1	☑ Supported
10	(43 Mbps)	2	2	☑ Supported
11	(58 Mbps)	2	3	☑ Supported
12	(87 Mbps)	2	4	☑ Supported
13	(116 Mbps)	2	5	☑ Supported
14	(130 Mbps)	2	6	☑ Supported
15	(144 Mbps)	2	7	☑ Supported
-	-	2	8	☑ Supported
-	-	2	9	☑ Supported
16	(22 Mbps)	3	0	☑ Supported
17	(43 Mbps)	3	1	☑ Supported
18	(65 Mbps)	3	2	☑ Supported
19	(87 Mbps)	3	3	☑ Supported
20	(130 Mbps)	3	4	☑ Supported
21	(173 Mbps)	3	5	☑ Supported
22	(195 Mbps)	3	6	☑ Supported
23	(217 Mbps)	3	7	☑ Supported
-	-	3	8	☑ Supported
-	-	3	9	☑ Supported

Frame Aggregation

Frame aggregation is a process of packaging multiple MAC Protocol Data Units (MPDUs) or MAC Service Data Units (MSDUs) together to reduce the overheads where in turn throughput and capacity can be optimized.
Aggregation of MAC Protocol Data Unit (A-MPDU) requires the use of block acknowledgements.

It is recommended to adjust the A-MPDU and A-MSDU settings to the following to optimize the experience with the Cisco DX Series.

A-MPDU
User Priority 0, 3, 4, 5 = Enabled
User Priority 1, 2, 6, 7 = Disabled

A-MSDU
User Priority 1, 2 = Enabled
User Priority 0, 3, 4, 5, 6, 7 = Disabled

In the 7.0.116.0 release for the Cisco Unified Wireless LAN Controller, the default A-MPDU and A-MSDU configuration is the following.

A-MPDU
User Priority 0, 4, 5 = Enabled
User Priority 1, 2, 3, 6, 7 = Disabled

A-MSDU
User Priority 0, 1, 2, 3, 4, 5 = Enabled
User Priority 6, 7 = Disabled

Use the following commands to configure the A-MPDU and A-MSDU settings per the Cisco DX Series recommendations.

In order to configure the 5 GHz settings, the 802.11a network will need to be disabled first, then re-enabled after the changes are complete.

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

In order to configure the 2.4 GHz settings, the 802.11b/g network will need to be disabled first, then re-enabled after the changes are complete.

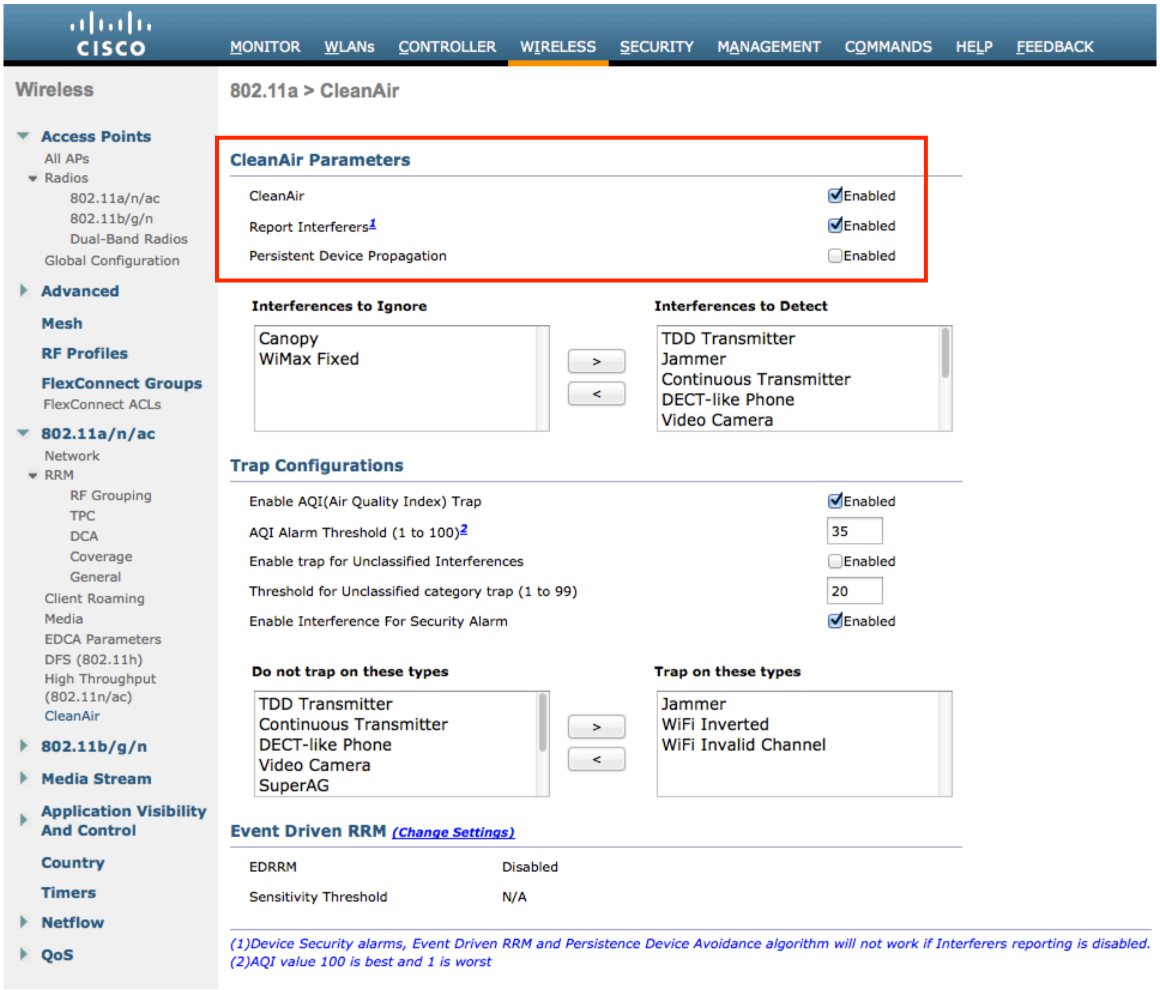
```
config 802.11b 11nSupport a-mpdu tx priority 0 enable
config 802.11b 11nSupport a-mpdu tx priority 3 enable
config 802.11b 11nSupport a-mpdu tx priority 4 enable
config 802.11b 11nSupport a-mpdu tx priority 5 enable
config 802.11b 11nSupport a-mpdu tx priority 1 disable
config 802.11b 11nSupport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

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

```
802.11n Status:
  A-MPDU Tx:
    Priority 0............................... Enabled
    Priority 1............................... Disabled
    Priority 2............................... Disabled
    Priority 3............................... Enabled
    Priority 4............................... Enabled
    Priority 5............................... Enabled
    Priority 6............................... Disabled
    Priority 7.............................. Disabled
  A-MSDU Tx:
    Priority 0.............................. Disabled
    Priority 1.............................. Enabled
    Priority 2.............................. Enabled
    Priority 3.............................. Disabled
    Priority 4.............................. Disabled
    Priority 5.............................. Disabled
    Priority 6.............................. Disabled
    Priority 7.............................. Disabled
```

CleanAir

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



802.11a > CleanAir

CleanAir Parameters

CleanAir	☑Enabled
Report Interferers[1]	☑Enabled
Persistent Device Propagation	□Enabled

Interferences to Ignore	Interferences to Detect
Canopy WiMax Fixed	TDD Transmitter Jammer Continuous Transmitter DECT-like Phone Video Camera

Trap Configurations

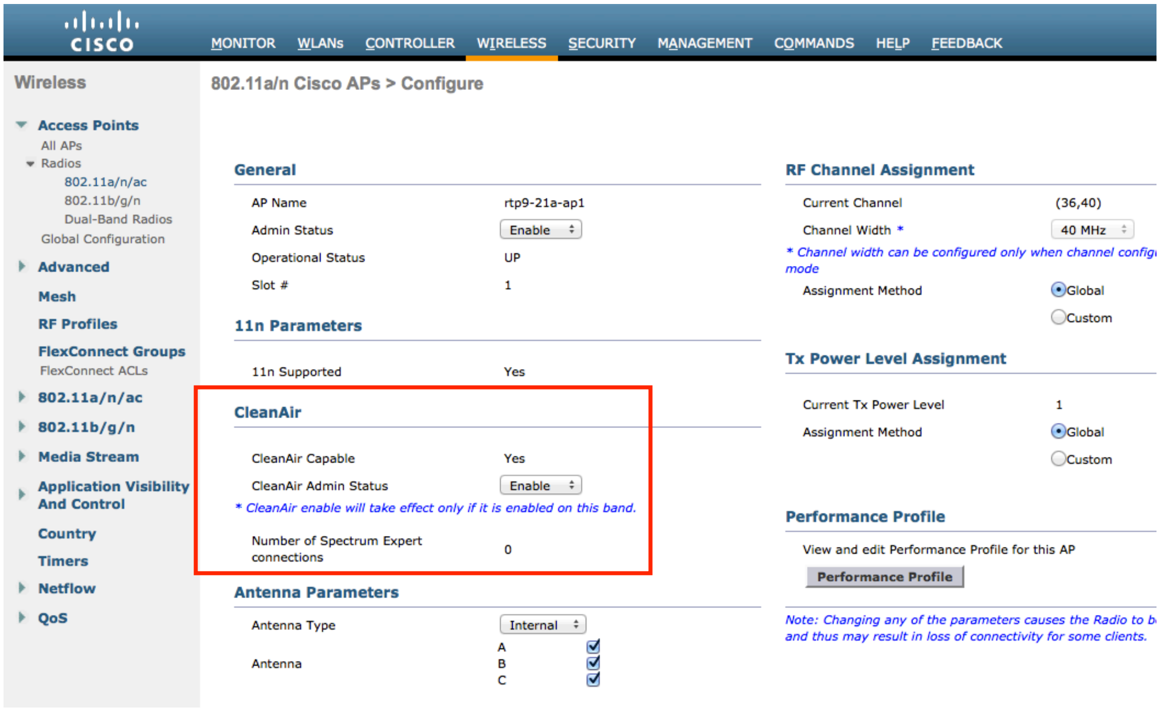
Enable AQI(Air Quality Index) Trap	☑Enabled
AQI Alarm Threshold (1 to 100)[2]	35
Enable trap for Unclassified Interferences	□Enabled
Threshold for Unclassified category trap (1 to 99)	20
Enable Interference For Security Alarm	☑Enabled

Do not trap on these types	Trap on these types
TDD Transmitter Continuous Transmitter DECT-like Phone Video Camera SuperAG	Jammer WiFi Inverted WiFi Invalid Channel

Event Driven RRM *(Change Settings)*

EDRRM	Disabled
Sensitivity Threshold	N/A

(1)Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled.
(2)AQI value 100 is best and 1 is worst



802.11a/n Cisco APs > Configure

General

AP Name	rtp9-21a-ap1
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	(36,40)
Channel Width *	40 MHz

* Channel width can be configured only when channel configu
mode

Assignment Method	● Global ○ Custom

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	● Global ○ Custom

Performance Profile

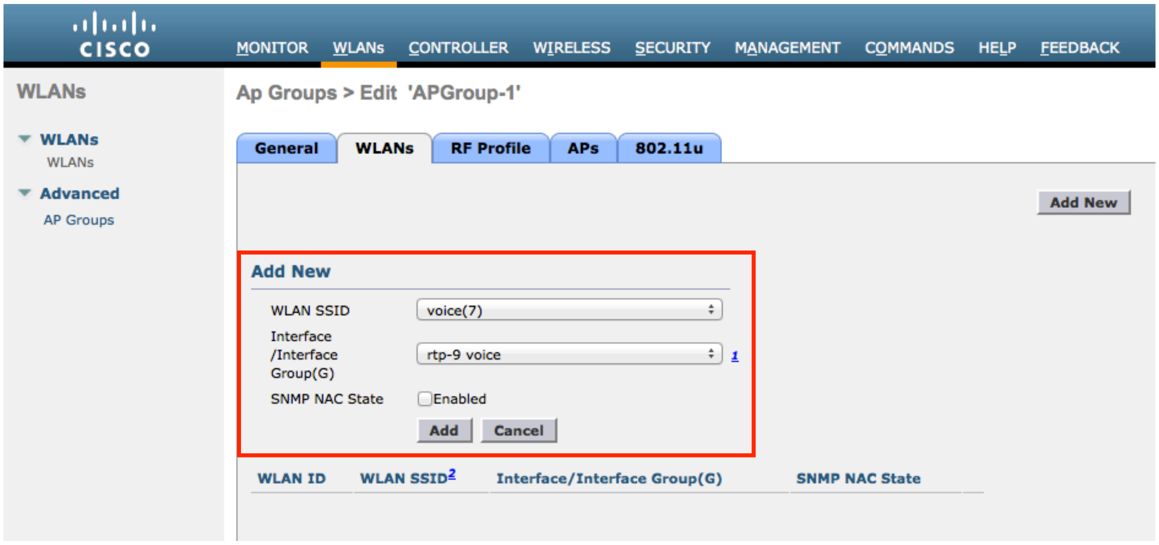
View and edit Performance Profile for this AP

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

AP Groups

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

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



Ap Groups > Edit 'APGroup-1'

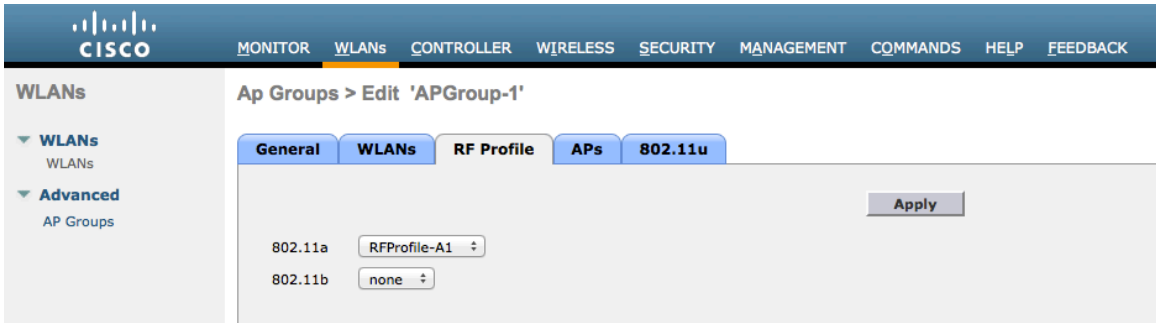
Add New

WLAN SSID	voice(7)
Interface /Interface Group(G)	rtp-9 voice
SNMP NAC State	□ Enabled

WLAN ID	WLAN SSID[2]	Interface/Interface Group(G)	SNMP NAC State

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

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



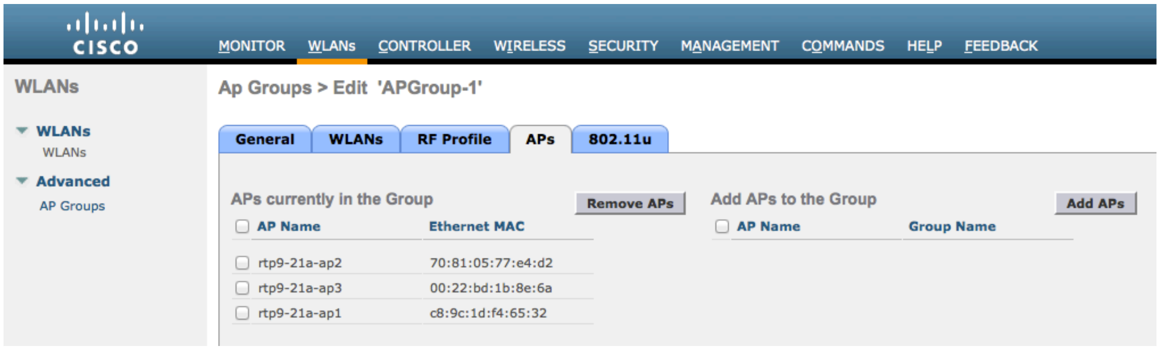
Ap Groups > Edit 'APGroup-1'

802.11a RFProfile-A1

802.11b none

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

Those access points will then reboot.



Ap Groups > Edit 'APGroup-1'

APs currently in the Group

□ AP Name	Ethernet MAC
□ rtp9-21a-ap2	70:81:05:77:e4:d2
□ rtp9-21a-ap3	00:22:bd:1b:8e:6a
□ rtp9-21a-ap1	c8:9c:1d:f4:65:32

Add APs to the Group

□ AP Name	Group Name

RF Profiles

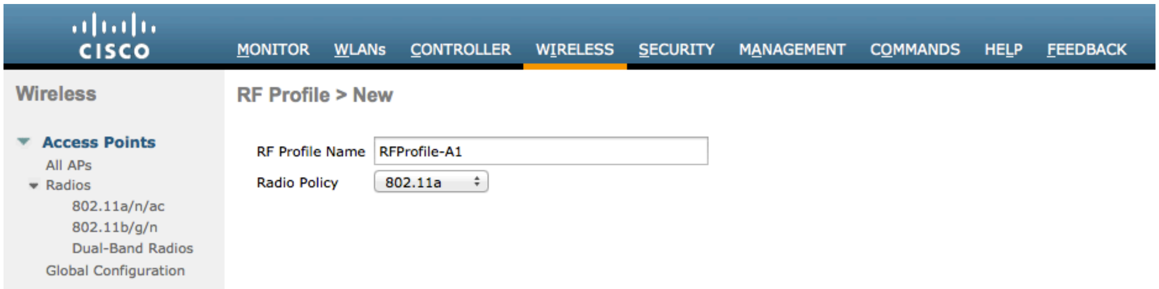
RF Profiles can be created to specify which frequency bands, data rates, RRM settings, etc. a group of access points should use.

It is highly recommended to enable the SSID used by the Cisco DX Series to be applied to 5 GHz radios only.

RF Profiles are applied to an AP group once created. See the AP Groups section for more info on AP Group configuration.

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

Select 802.11a or 802.11b/g for the **Radio Policy**.



RF Profile > New

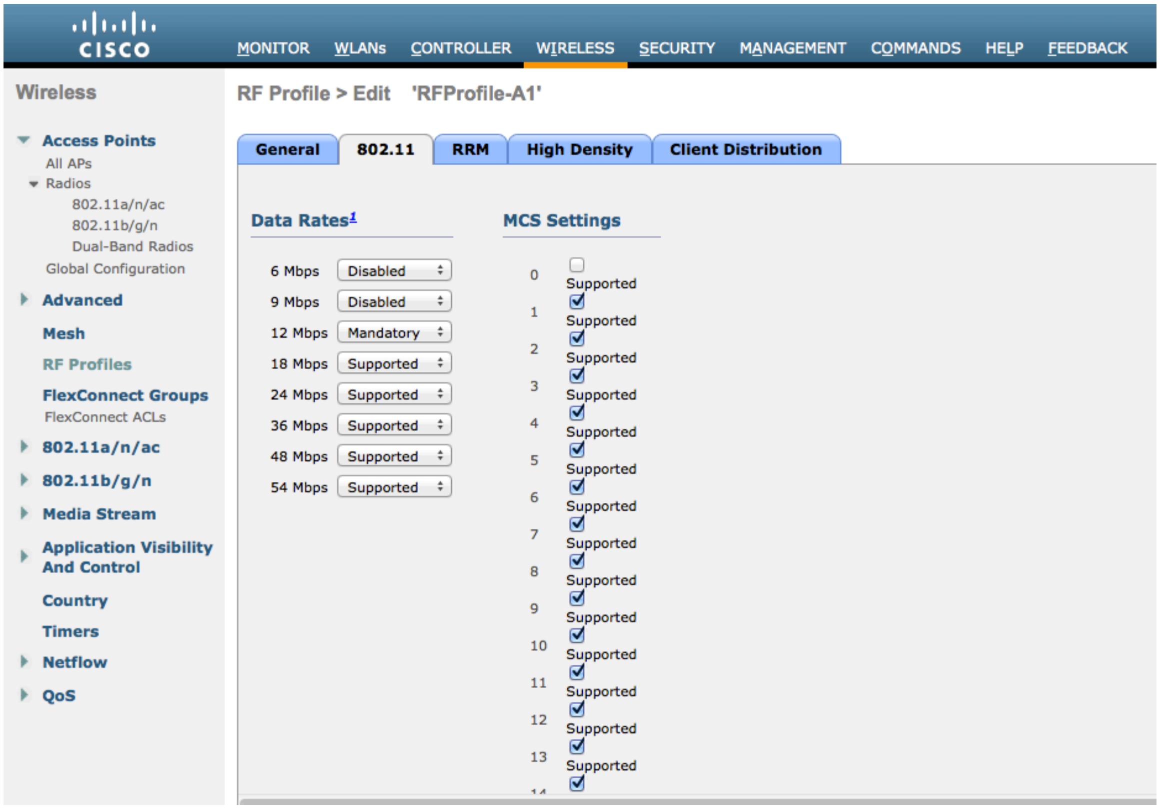
RF Profile Name RFProfile-A1

Radio Policy 802.11a

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

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

MCS 0 should be disabled unless 6 Mbps is also enabled.



RF Profile > Edit 'RFProfile-A1'

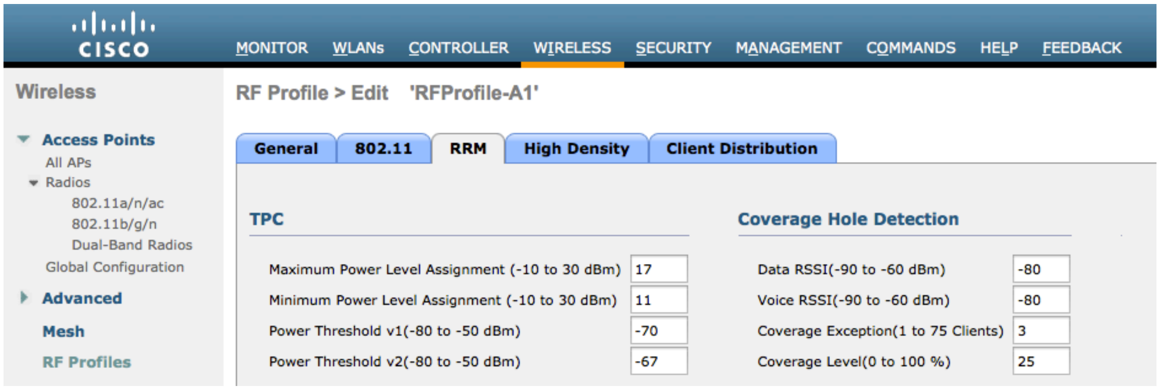
Data Rates[1]

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

MCS Settings

0	□ Supported
1	☑ Supported
2	☑ Supported
3	☑ Supported
4	☑ Supported
5	☑ Supported
6	☑ Supported
7	☑ Supported
8	☑ Supported
9	☑ Supported
10	☑ Supported
11	☑ Supported
12	☑ Supported
13	☑ Supported
14	☑

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



RF Profile > Edit 'RFProfile-A1'

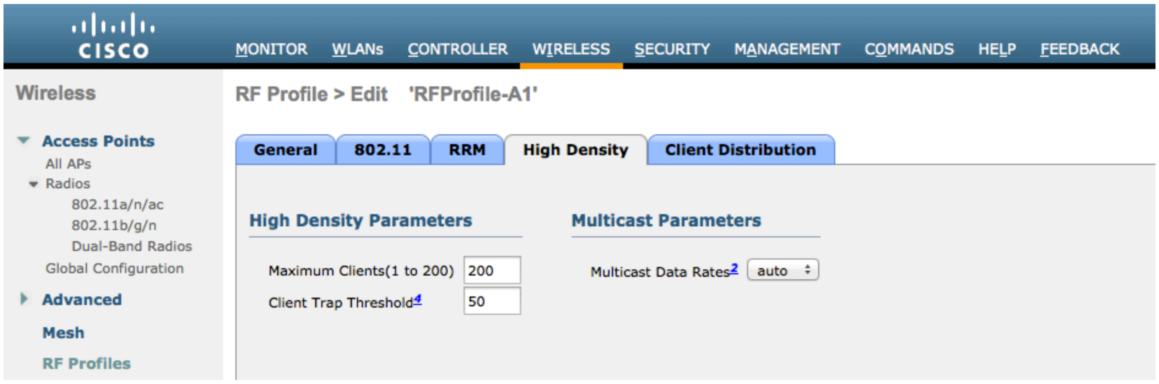
TPC

Maximum Power Level Assignment (-10 to 30 dBm)	17
Minimum Power Level Assignment (-10 to 30 dBm)	11
Power Threshold v1(-80 to -50 dBm)	-70
Power Threshold v2(-80 to -50 dBm)	-67

Coverage Hole Detection

Data RSSI(-90 to -60 dBm)	-80
Voice RSSI(-90 to -60 dBm)	-80
Coverage Exception(1 to 75 Clients)	3
Coverage Level(0 to 100 %)	25

On the High Density tab, Maximum Clients and Multicast Data Rates can be configured.



RF Profile > Edit 'RFProfile-A1'

High Density Parameters

Maximum Clients(1 to 200)	200
Client Trap Threshold[4]	50

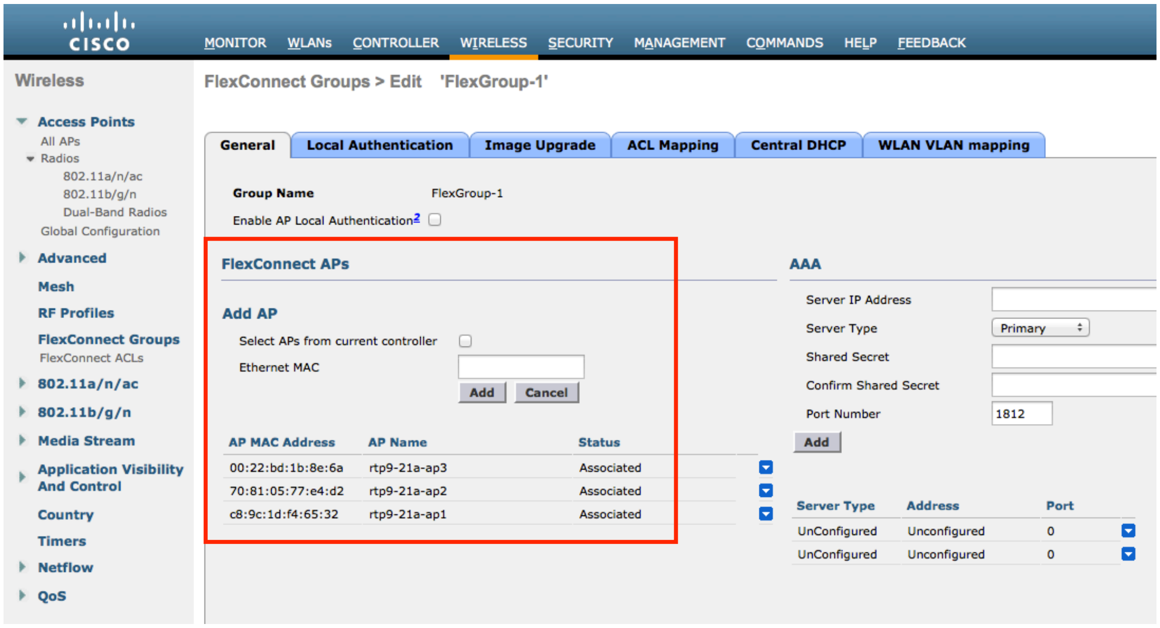
Multicast Parameters

Multicast Data Rates[2]	auto

FlexConnect Groups

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

If utilizing CCKM, then seamless roams can only occur when roaming to access points within the same FlexConnect Group.



FlexConnect Groups > Edit 'FlexGroup-1'

Group Name	FlexGroup-1
Enable AP Local Authentication[2]	☐

FlexConnect APs

Add AP

Select APs from current controller	☐
Ethernet MAC	

AP MAC Address	AP Name	Status
00:22:bd:1b:8e:6a	rtp9-21a-ap3	Associated
70:81:05:77:e4:d2	rtp9-21a-ap2	Associated
c8:9c:1d:f4:65:32	rtp9-21a-ap1	Associated

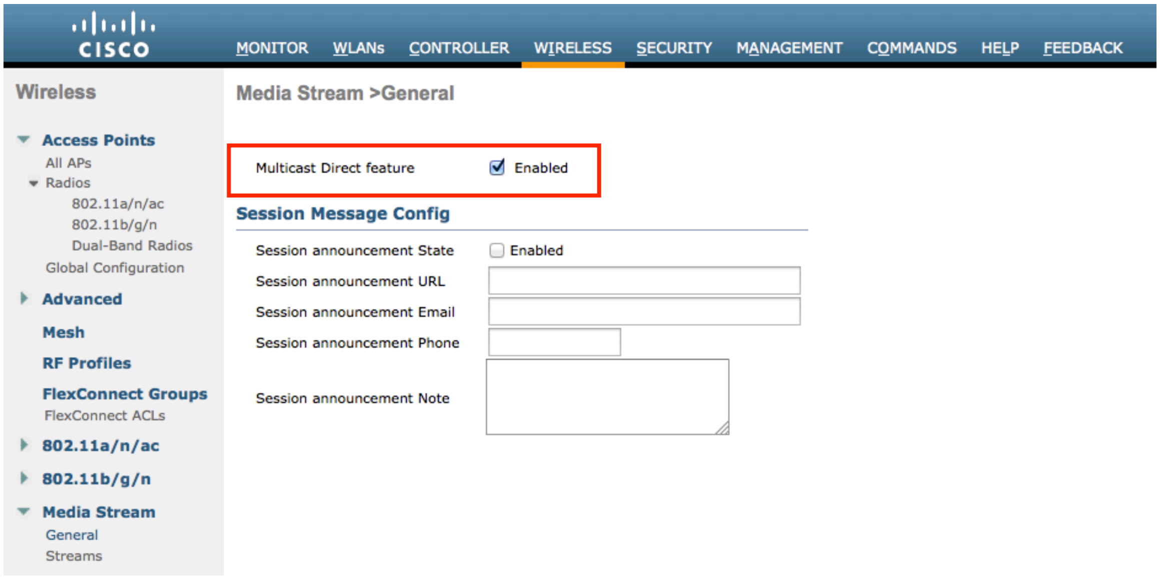
AAA

Server IP Address	
Server Type	Primary
Shared Secret	
Confirm Shared Secret	
Port Number	1812

Server Type	Address	Port
UnConfigured	Unconfigured	0
UnConfigured	Unconfigured	0

Multicast Direct

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



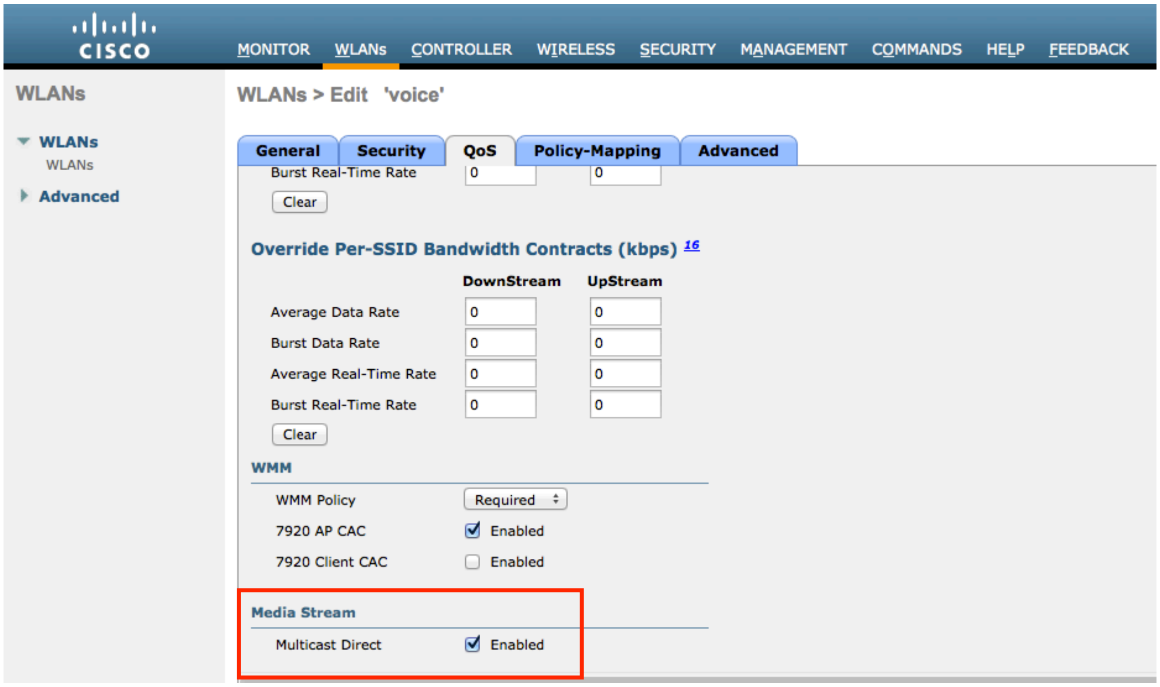
Media Stream >General

Multicast Direct feature ☑ Enabled

Session Message Config

Session announcement State	□ Enabled
Session announcement URL	
Session announcement Email	
Session announcement Phone	
Session announcement Note	

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



WLANs > Edit 'voice'

Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) [16]

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

WMM

WMM Policy	Required
7920 AP CAC	☑ Enabled
7920 Client CAC	□ Enabled

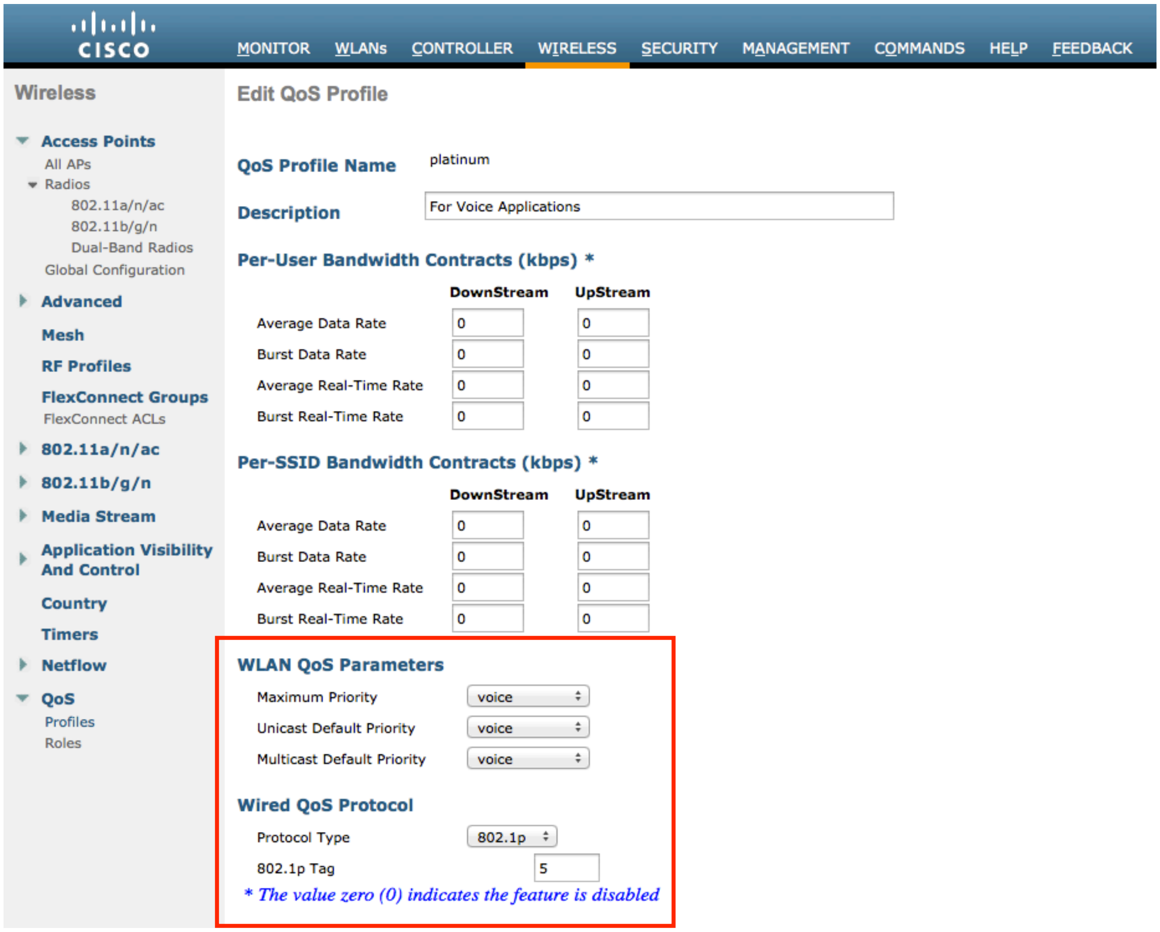
Media Stream

Multicast Direct ☑ Enabled

QoS Profiles

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

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



Edit QoS Profile

QoS Profile Name platinum

Description For Voice Applications

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority voice

Unicast Default Priority voice

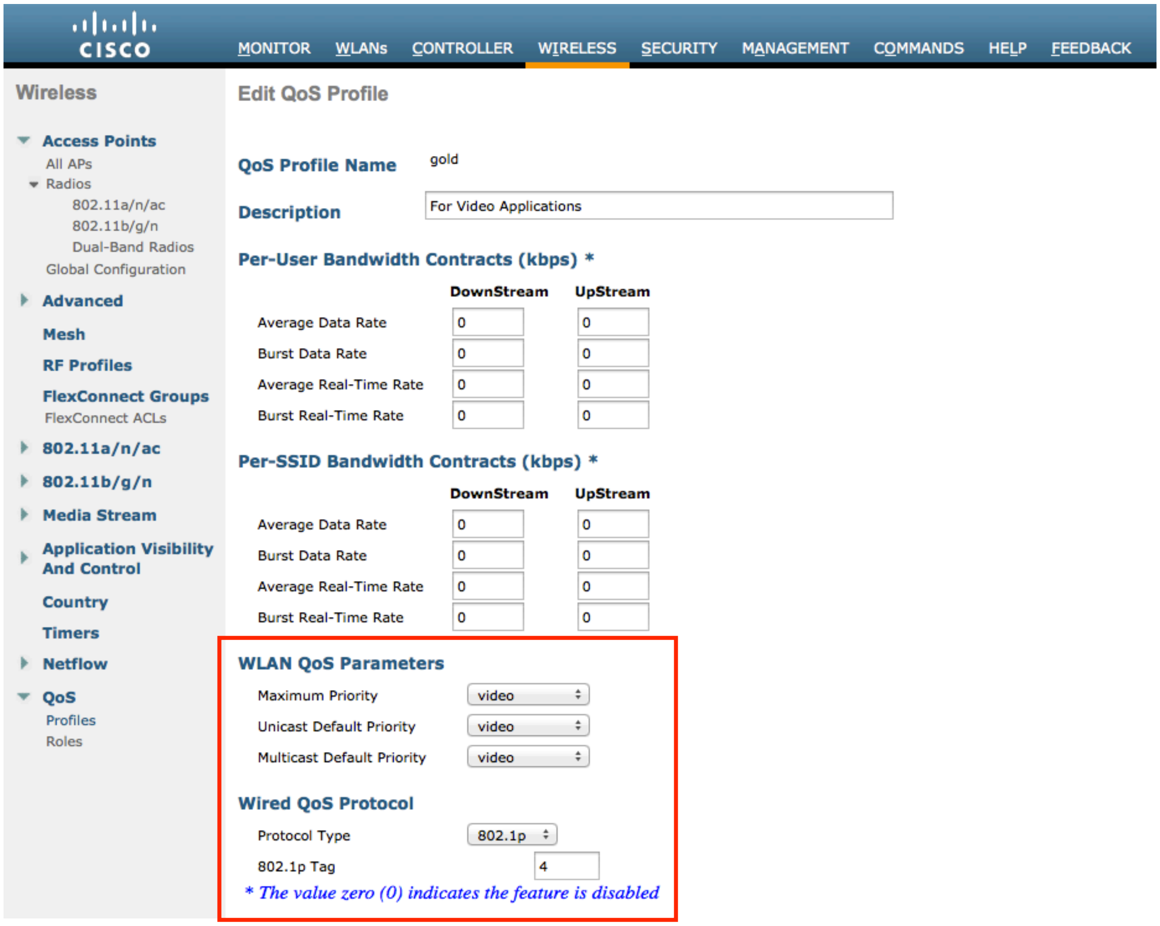
Multicast Default Priority voice

Wired QoS Protocol

Protocol Type 802.1p

802.1p Tag 5

** The value zero (0) indicates the feature is disabled*



Edit QoS Profile

QoS Profile Name: gold

Description: For Video Applications

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority: video

Unicast Default Priority: video

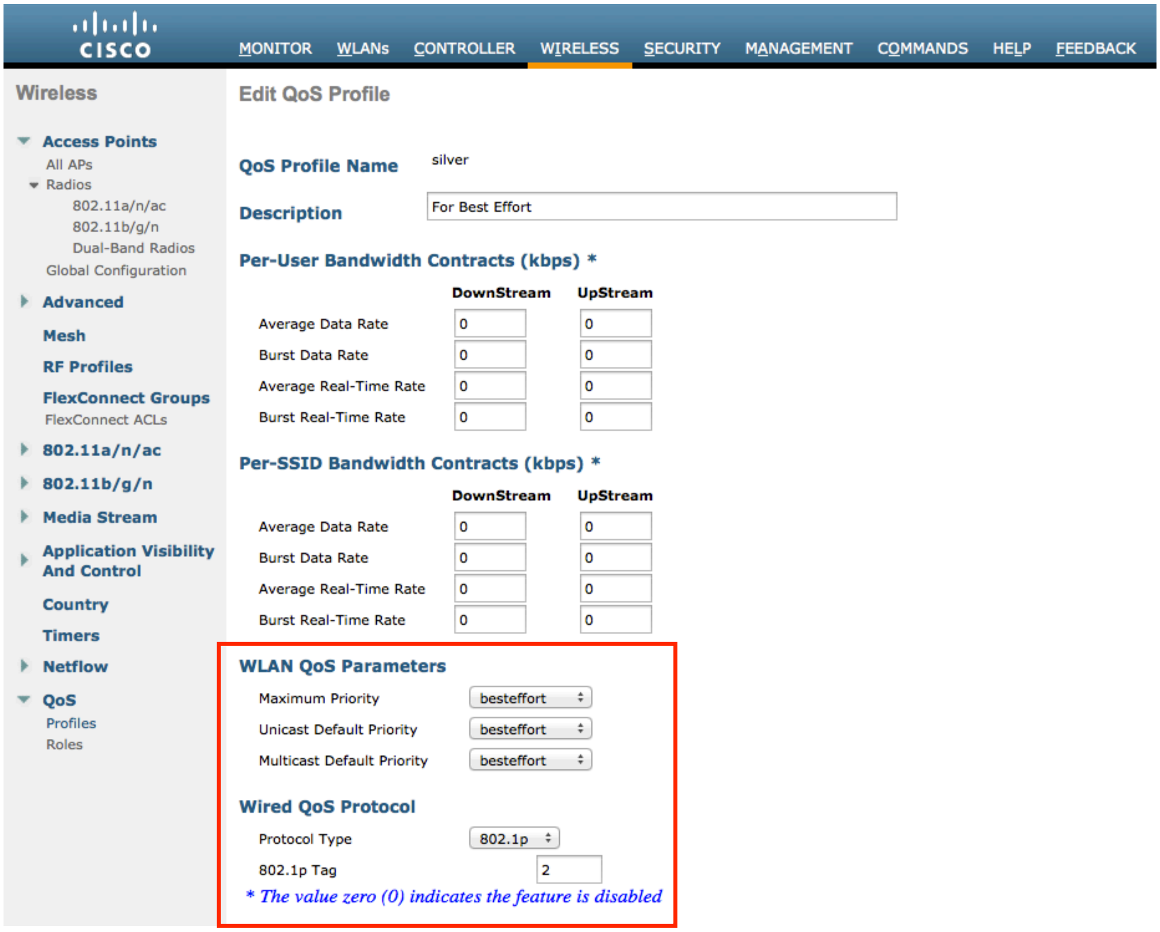
Multicast Default Priority: video

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 4

** The value zero (0) indicates the feature is disabled*



Edit QoS Profile

QoS Profile Name silver

Description For Best Effort

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority besteffort

Unicast Default Priority besteffort

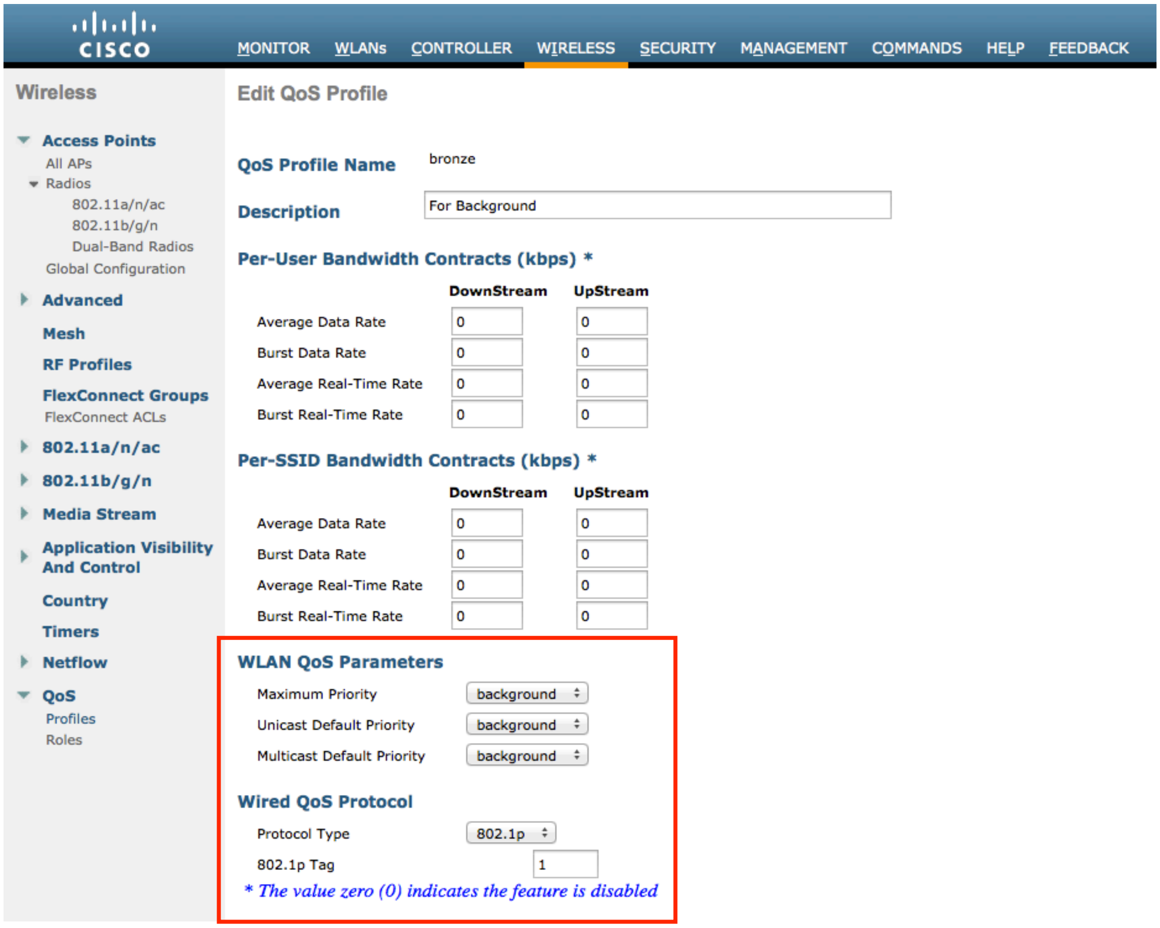
Multicast Default Priority besteffort

Wired QoS Protocol

Protocol Type 802.1p

802.1p Tag 2

** The value zero (0) indicates the feature is disabled*



Edit QoS Profile

QoS Profile Name: bronze

Description: For Background

Per-User Bandwidth Contracts (kbps) *

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

Per-SSID Bandwidth Contracts (kbps) *

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

WLAN QoS Parameters

Maximum Priority: background

Unicast Default Priority: background

Multicast Default Priority: background

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 1

** The value zero (0) indicates the feature is disabled*

Note: The 802.1p tag mappings were changed with the 7.5.102.0 release.

Prior to the 7.5.102.0 release, Platinum = 6, Gold = 5, Silver = 3, Bronze = 1.

QoS Basic Service Set (QBSS)

There are three different versions of QoS Basic Service Set (QBSS) that the Cisco DX Series supports.

The first version from Cisco was on a 0-100 scale and was not based on clear channel assessment (CCA), so it does not account for channel utilization, but only the 802.11 traffic traversing that individual access point's radio. So it does not account for other 802.11 energy or interferers using the same frequencies.

QBSS is also a part of 802.11e, which is on a 0-255 scale and is CCA based. So this gives a true representation on how busy the channel is. The max threshold is also defined on the client side, which is set to 105.

The Cisco DX Series converts the QBSS info to a percentage format (0-255 to 0-100%), which is displayed as the Channel Utilization value in the neighbor list menu.

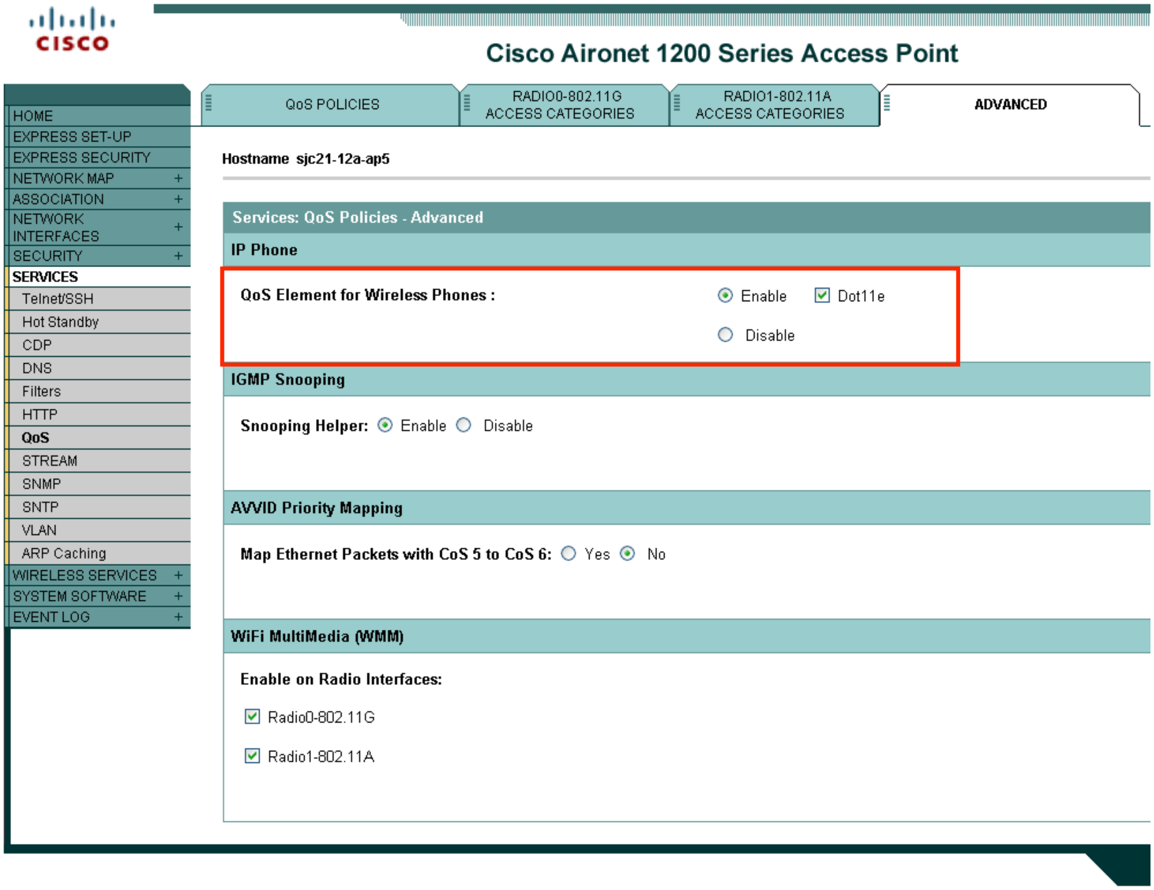
The second version from Cisco is based on the 802.11e version, but allows the default max threshold of 105 to be optionally configured.

Each version of QBSS can be optionally be configured on the access point.

For the Cisco Unified Wireless LAN Controller, enabling WMM will enable the 802.11e version of QBSS. There are also the **7920 Client CAC** and **7920 AP CAC** options, where **7920 Client CAC** will enable Cisco version 1 and **7920 AP CAC** enables Cisco version 2. See the WLAN QoS Settings section for more info.

For the Cisco Autonomous Access Point, **dot11 phone** or **dot11 phone dot11e** will enable QBSS.

Dot11 phone will enable the 2 Cisco versions, where **dot11 phone dot11e** will enable both CCA versions (802.11e and Cisco version 2). It is recommended to enable **dot11 phone dot11e**.



Hostname sjc21-12a-ap5

Services: QoS Policies - Advanced

IP Phone

QoS Element for Wireless Phones : ● Enable ☑ Dot11e ○ Disable

IGMP Snooping

Snooping Helper: ● Enable ○ Disable

AVVID Priority Mapping

Map Ethernet Packets with CoS 5 to CoS 6: ○ Yes ● No

WiFi MultiMedia (WMM)

Enable on Radio Interfaces:

☑ Radio0-802.11G

☑ Radio1-802.11A

CCKM Timestamp Tolerance

The default CCKM timestamp tolerance is set to 1000 ms.

It is recommended to adjust the CCKM timestamp tolerance to 5000 ms to optimize the Cisco DX Series roaming experience.

```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance ?
 <tolerance>    Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds; Default tolerance 1000 msecs
```

Use the following command to configure the CCKM timestamp tolerance per Cisco recommendations.

```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id >
```

To confirm the change, enter **show wlan <WLAN id>**, where the following will be displayed.

```
CCKM tsf Tolerance............................... 5000
```

Auto-Immune

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

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

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

```
(Cisco Controller) >show wps summary

Auto-Immune
  Auto-Immune.................................. Disabled

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

Signature Policy
  Signature Processing.......................... Enabled
```

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

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

WLAN Controller Advanced EAP Settings

Need to ensure that the advanced EAP settings in the Cisco Unified Wireless LAN Controller are configured per the information below.

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

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

```
EAP-Request Max Retries......................... 2
EAPOL-Key Timeout (milliseconds)...................... 400
EAPOL-Key Max Retries............................ 4
```

If using 802.1x or WPA/WPA2, the EAP-Request Timeout on the Cisco Unified Wireless LAN Controller should be set to at least 20 seconds.

In later versions of Cisco Unified Wireless LAN Controller software, the default EAP-Request Timeout was changed from 2 to 30 seconds.

To change the EAP-Request Timeout on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >config advanced eap request-timeout 30
```

If using WPA/WPA2 PSK then it is recommended to reduce the EAPOL-Key Timeout to 400 milliseconds from the default of 1000 milliseconds with EAPOL-Key Max Retries set to 4 from the default of 2.

If using WPA/WPA2, then using the default values where the EAPOL-Key Timeout is set to 1000 milliseconds and EAPOL-Key Max Retries are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.

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

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

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

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

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

TKIP Countermeasure Holdoff Time

TKIP countermeasure mode can occur if the access point receives two Message Integrity Check (MIC) errors within a 60 second period. When this occurs, the access point will de-authenticate all TKIP clients associated to that 802.11 radio and holdoff any clients for the countermeasure holdoff time (default = 60 seconds).

To change the TKIP countermeasure holdoff time on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command:

```
(Cisco Controller) >config wlan security tkip hold-down <nseconds> <WLAN id>
```

To confirm the change, enter **show wlan <WLAN id>**, where the following will be displayed.

```
Tkip MIC Countermeasure Hold-down Timer....... 60
```

For the Cisco Autonomous Access Point, enter the time in seconds to holdoff clients if a TKIP countermeasure event occurs.

```
Interface dot11radio X
 countermeasure tkip hold-time <nseconds>
```

VLANs and Cisco Autonomous Access Points

Segment wireless voice and data into separate VLANs.

A subnet for wireless clients should not exceed 1,000 hosts.

When using Cisco Autonomous Access Points, use a dedicated native VLAN. The Cisco Autonomous Access Points utilize Inter-Access Point Protocol (IAPP), which is a multicast protocol.

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

Ensure that Public Secure Packet Forwarding (PSPF) is not enabled for the voice VLAN as this will prevent clients from communicating directly when associated to the same access point. If PSPF is enabled, then the result will be no way audio.

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

The network ID in the SSID configuration with the Cisco Autonomous Access Point should only be disabled if Layer 3 mobility is enabled where the Wireless LAN Services Module (WLSM) is deployed.

Configuring the Cisco DX Series

To configure the Wi-Fi settings on the Cisco DX Series, use the keypad and touch screen to navigate to **Settings > Wireless & networks > Wi-Fi settings.**

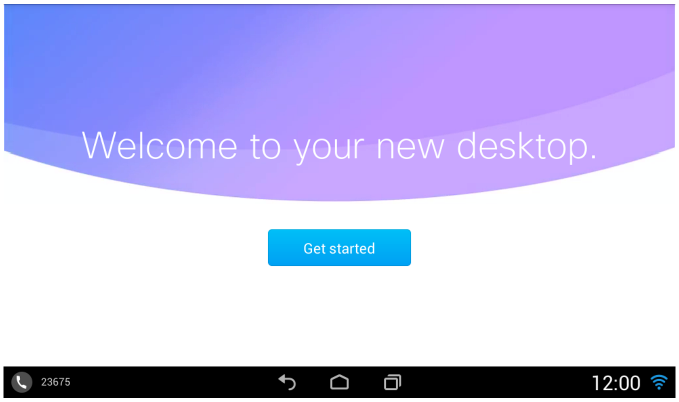
The power supply is required to enable the Cisco DX Series for wireless LAN mode.

Setup Assistant

When first powering on the Cisco DX Series, the Setup Assistant will be launched to guide the user through the setup process.

Select the service to start the configuration process.

- WebEx
- Jabber
- Voicemail
- Email
- Contacts
- Calendar



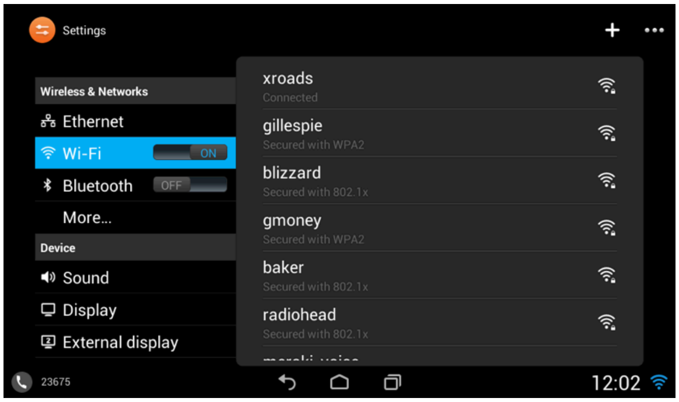
Welcome to your new desktop.

Wireless LAN Settings

Use the following guidelines to configure the wireless LAN profile.

- Navigate to **Settings** > **Wireless & Networks** > **Wi-Fi**.
- Ensure that **Wi-Fi** is set to **On.**

  Ensure **Wi-Fi** is enabled in the Cisco Unified Communications Manager; otherwise the option will not be visible in the settings menu.
  If there is an active Ethernet connection, then **Wi-Fi** will be disabled and Ethernet must be disconnected before **Wi-Fi** can be enabled.
- Either select the broadcasted Wi-Fi network from the list or add the Wi-Fi network manually.
- If adding the Wi-Fi network manually, select Add network then enter the **SSID** (case sensitive).



Wi-Fi ON
Bluetooth OFF

xroads
Connected
gillespie
Secured with WPA2
blizzard
Secured with 802.1x
gmoney
Secured with WPA2
baker
Secured with 802.1x
radiohead
Secured with 802.1x

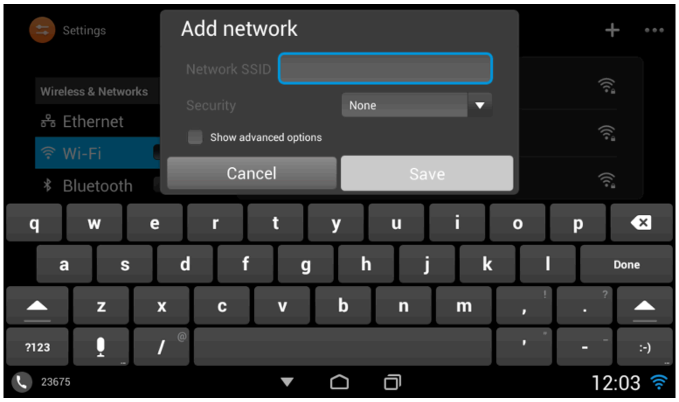
- Below lists the available security modes supported and the key management and encryption types that can be used for each mode.

  The key management and encryption type (cipher) will be auto-configured based on the access point's current configuration, where precedence is giving to the strongest key management type enabled (e.g. WPA2) then the strongest cipher enabled (e.g. AES).

Security Mode	802.1x Type	Key Management	Encryption
None	N/A	None	None

WEP	N/A	Static	WEP (40/64 or 104/128 bit)
WPA/WPA2 PSK	N/A	WPA2, WPA	AES, TKIP
802.1x EAP	EAP-FAST, PEAP-MSCHAPv2, PEAP-GTC, TLS	WPA2, WPA	AES, TKIP

- If wanting to configure a wireless network profile without security (open security), then simply enter the **SSID** and select **None** for the security type.


Add network

Network SSID

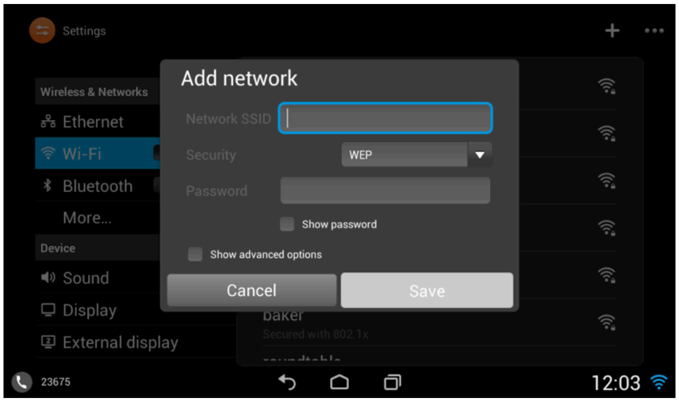
Security None

□ Show advanced options

- **WEP** security mode requires that the static WEP key (password) be entered.

  Only key index 1 is supported, so will want to ensure that only key index 1 is configured on the access point.

Key Style	Key Size	Characters
ASCII	40/64 bit	5
ASCII	104/128 bit	13
HEX	40/64 bit	10 (0-9, A-F)
HEX	104/128 bit	26 (0-9, A-F)


Add network

Network SSID

Security WEP

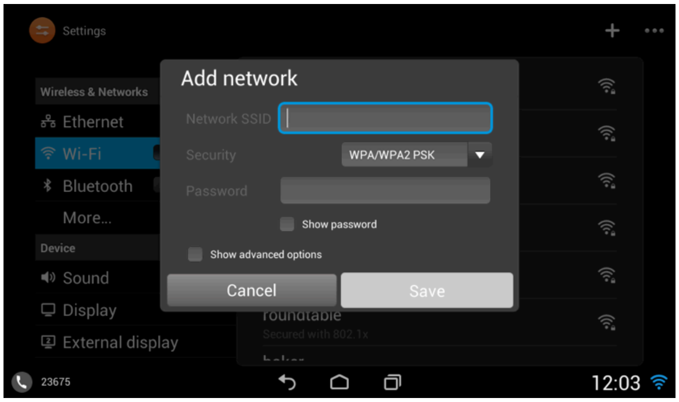
Password

□ Show password

□ Show advanced options

- If selecting **WPA/WPA2 PSK** as the security mode, then a Pre-Shared Key (password) must be configured. Enter the ASCII or hexadecimal formatted password.

Key Style	Characters
ASCII	8-63
HEX	64 (0-9,A-F)



Add network

Network SSID

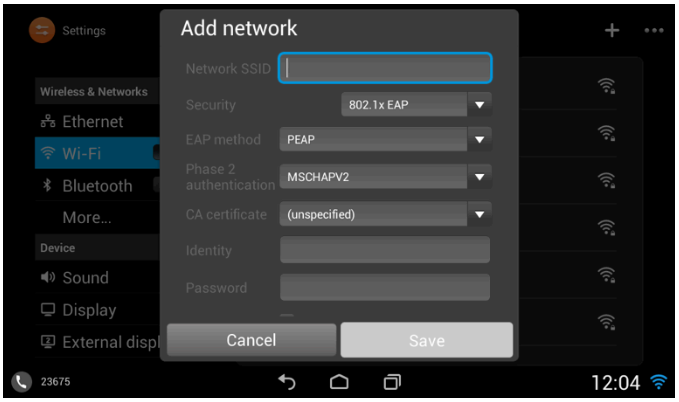
Security: WPA/WPA2 PSK

Password

□ Show password

□ Show advanced options

- If selecting **802.1x EAP** as the security mode, then a username (identity) and password must be configured if using EAP-FAST (FAST) or PEAP.
- If selecting PEAP, then the Phase 2 authentication type must be specified (MSCHAPv2 or GTC).
- A CA certificate can optionally be imported and configured if wanting to use PEAP with server validation.
- If using EAP-TLS (TLS), then a user certificate and CA certificate are required to be imported and configured.



Add network

Network SSID

Security: 802.1x EAP

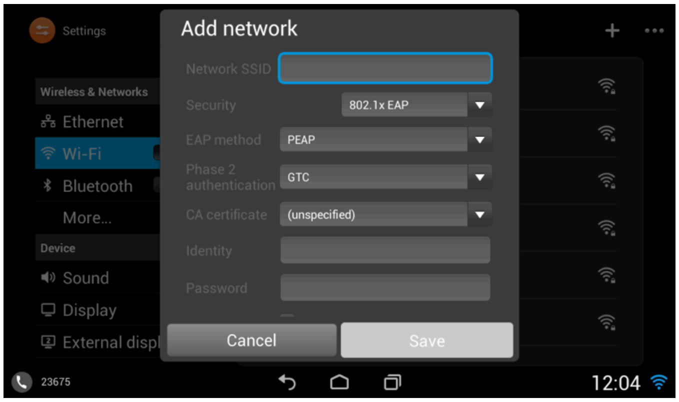
EAP method: PEAP

Phase 2 authentication: MSCHAPV2

CA certificate: (unspecified)

Identity

Password



Add network

Network SSID

Security: 802.1x EAP

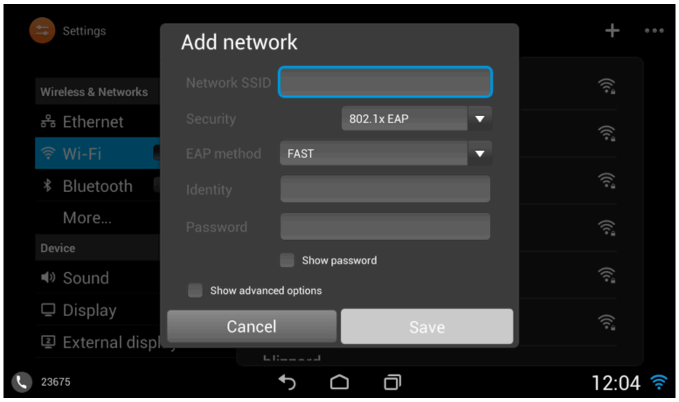
EAP method: PEAP

Phase 2 authentication: GTC

CA certificate: (unspecified)

Identity

Password



Add network

Network SSID

Security: 802.1x EAP

EAP method: FAST

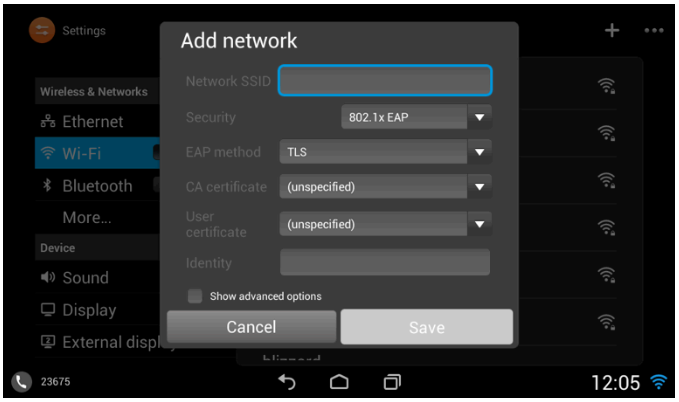
Identity

Password

□ Show password

□ Show advanced options

Cancel Save



Add network

Network SSID

Security: 802.1x EAP

EAP method: TLS

CA certificate: (unspecified)

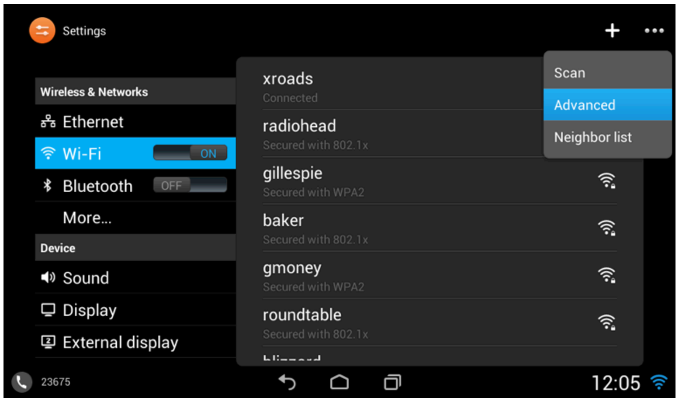
User certificate: (unspecified)

Identity

□ Show advanced options

Cancel Save

- To set the frequency band to be used, select **Wi-Fi frequency band** when in **Settings** > **Wireless & Networks** > **Wi-Fi** > **Advanced**. Select **…** in the upper right corner to display the **Advanced** menu.



xroads
Connected

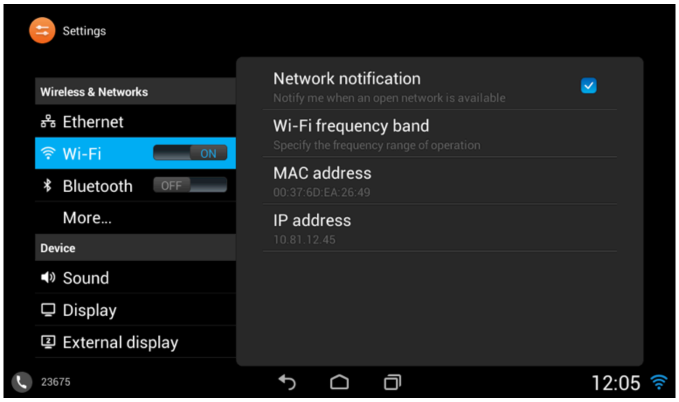
radiohead
Secured with 802.1x

gillespie
Secured with WPA2

baker
Secured with 802.1x

gmoney
Secured with WPA2

roundtable
Secured with 802.1x



Network notification ☑
Notify me when an open network is available

Wi-Fi frequency band
Specify the frequency range of operation

MAC address
00:37:6D:EA:26:49

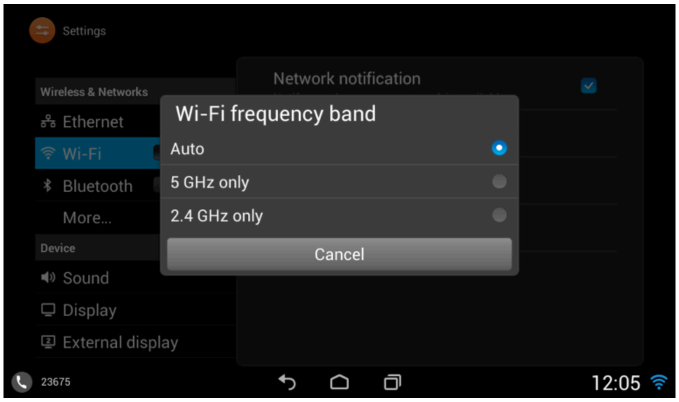
IP address
10.81.12.45

- Select one of the following 802.11 modes to set the frequency band.
  - Auto
  - 5 GHz
  - 2.4 GHz

Auto mode will scan both 5 GHz and 2.4 GHz channels at power on or if disconnected then will attempt to associate to a 5 GHz access point with strong signal (>= -67 dBm) if available; otherwise will attempt to associate to an available access point with the strongest RSSI.
5 GHz Only mode will only scan 5 GHz channels, and then will attempt to associate to an available 5 GHz access point.

2.4 GHz Only mode will only scan 2.4 GHz channels, and then will attempt to associate to an available 2.4 GHz access point.

It is highly recommended to set the frequency band on the Cisco DX Series to 5 GHz only when wanting to utilize the 5 GHz frequency band only, which prevents scanning and potentially roaming to the 2.4 GHz frequency band.



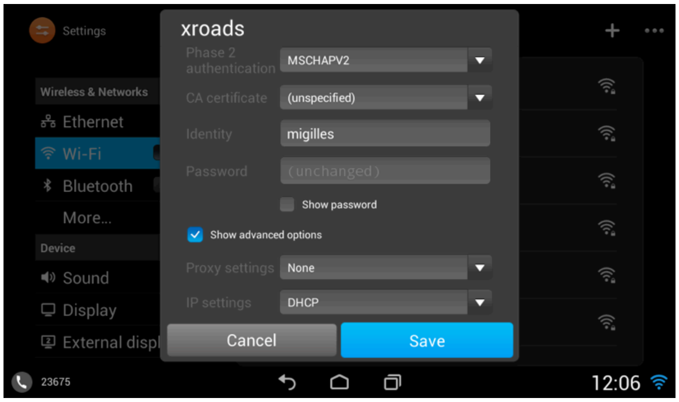
Wi-Fi frequency band

● Auto

○ 5 GHz only

○ 2.4 GHz only

- Dynamic Host Configuration Protocol (DHCP) or static IP settings can be configured via the **IP settings** option in the wireless LAN profile configuration after checking **Show advanced options.**



xroads

Phase 2 authentication: MSCHAPV2

CA certificate: (unspecified)

Identity: migilles

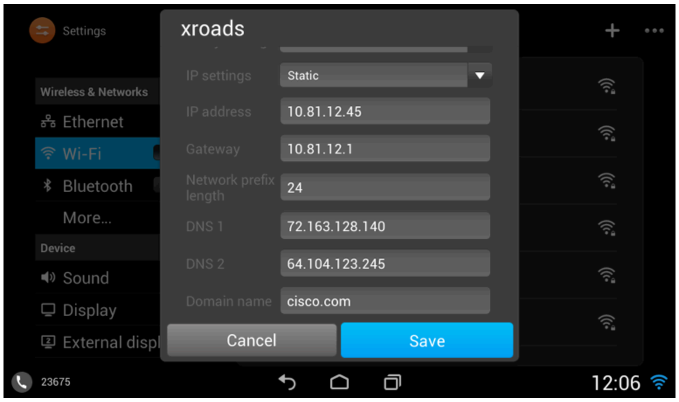
Password: (unchanged)

□ Show password

☑ Show advanced options

Proxy settings: None

IP settings: DHCP



xroads

IP settings: Static

IP address: 10.81.12.45

Gateway: 10.81.12.1

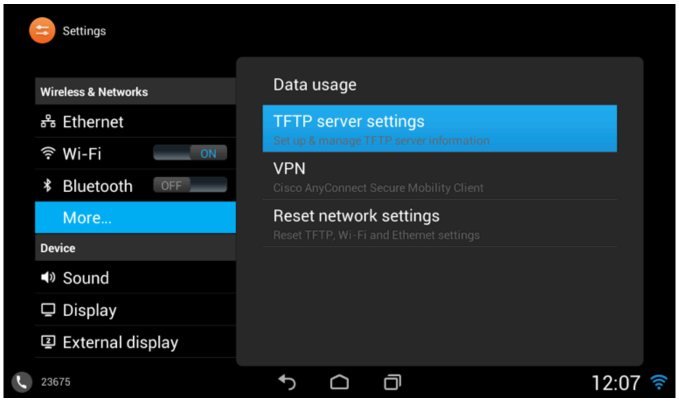
Network prefix length: 24

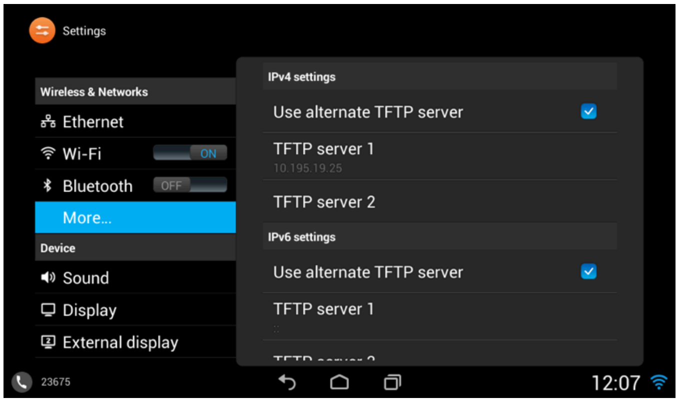
DNS 1: 72.163.128.140

DNS 2: 64.104.123.245

Domain name: cisco.com

- If DHCP option 150 or 66 is not configured to provide the TFTP server IP address via the network's DHCP scope, then navigate to **Settings > Wireless & Networks > More… > TFTP server settings**, enable **Use alternate TFTP** server, and enter the IP address of the TFTP servers.





IPv4 settings

Use alternate TFTP server ☑

TFTP server 1: 10.195.19.25

TFTP server 2

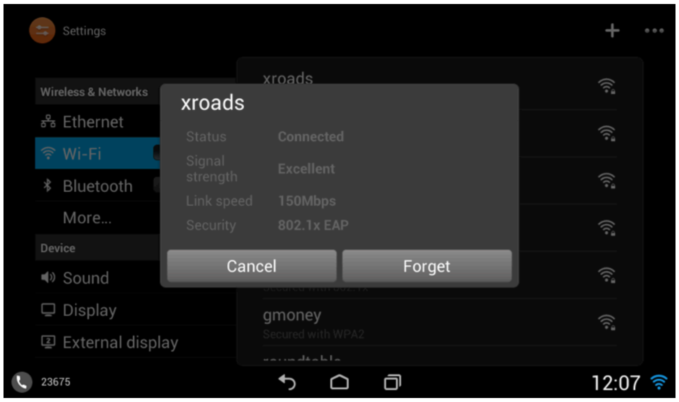
IPv6 settings

Use alternate TFTP server ☑

TFTP server 1: ::

TFTP server 2

- Network profiles can be removed by tapping on the wireless LAN selection then selecting **Forget** or by selecting and holding the wireless LAN selection, where **Forget network** will be displayed.
- Wireless LAN profile parameters can be modified after selecting and holding the wireless LAN selection, then selecting **Modify network**.



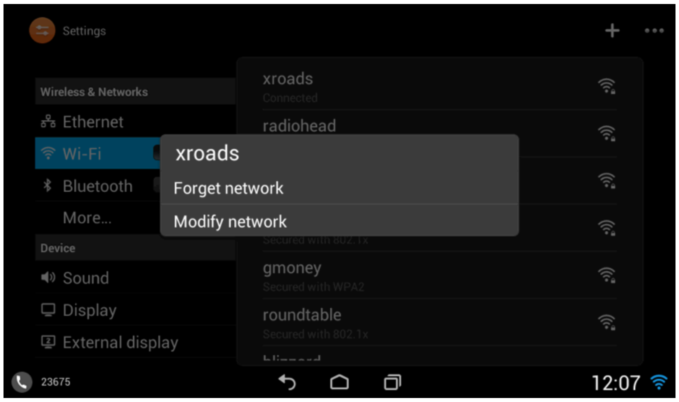
xroads

Status Connected

Signal strength Excellent

Link speed 150Mbps

Security 802.1x EAP



Note: CCKM will be negotiated if enabled on the access point when using EAP-FAST, EAP-TLS or PEAP.

WEP128 is listed as WEP104 on the Cisco Unified Wireless LAN Controllers.

Shared Key authentication and 802.1x + Dynamic WEP are not supported.

The Cisco DX Series can remember up to 8 wireless LANs profiles.

If unable to add a network, check to see if the max number of wireless LAN profiles has been met already, where one of those wireless LAN profiles may need to be deleted manually in order to add a new network.

For more information, refer to the Cisco DX Series Administration Guide at this URL:

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

Installing Certificates

The Cisco DX Series supports X.509 digital certificates, which can be utilized with EAP-TLS or for authentication server validation when using PEAP.

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.

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

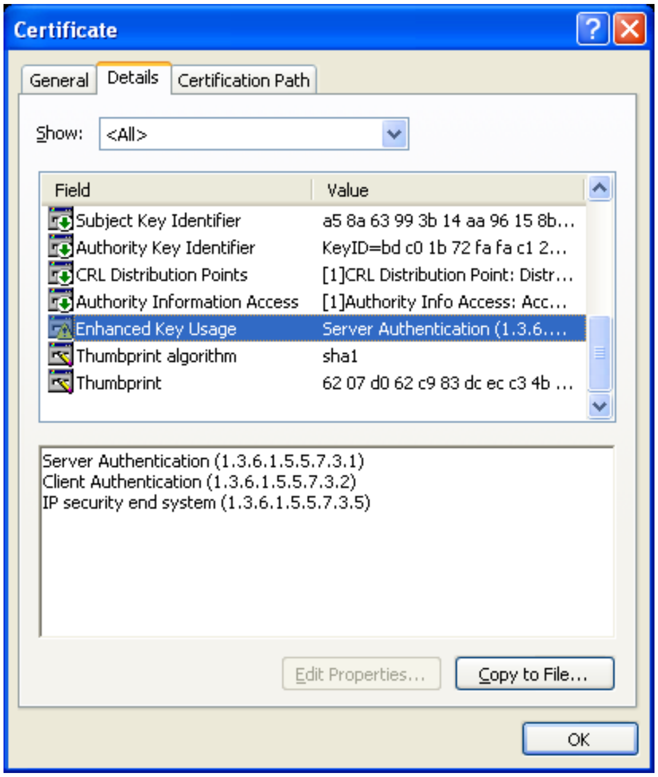
Microsoft® Certificate Authority (CA) servers are recommended as we have certified interoperability only with those CA types. Other CA server types may not be completely interoperable with the Cisco DX Series.

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

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

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

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



Field	Value
Subject Key Identifier	a5 8a 63 99 3b 14 aa 96 15 8b...
Authority Key Identifier	KeyID=bd c0 1b 72 fa fa c1 2...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Enhanced Key Usage	Server Authentication (1.3.6....
Thumbprint algorithm	sha1
Thumbprint	62 07 d0 62 c9 83 dc ec c3 4b ...

```
Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)
IP security end system (1.3.6.1.5.5.7.3.5)
```

X.509 digital certificates are required to be installed if utilizing EAP-TLS or PEAP with server validation for WLAN authentication.

The user certificate must be in **PKCS #12** format (**.p12** or **.pfx** extension), which contains the certificate and private key.

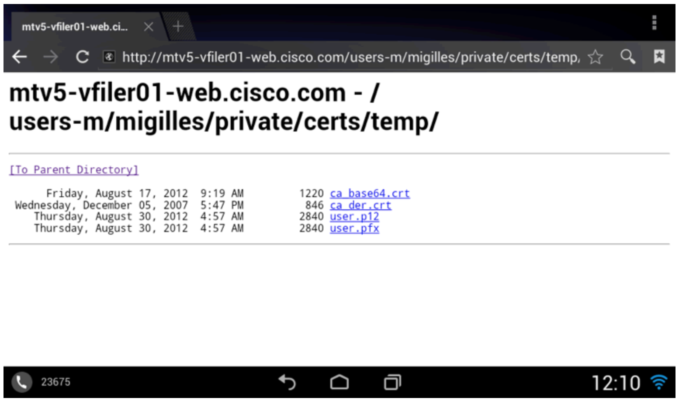
The CA certificate must use **DER** or **Base-64 (PEM)** encoding (**.crt** extension as the .cer format is not supported).

Once a certificate is installed, then it is deemed a secure device and a CA certificate is then required if utilizing PEAP.

Certificates can be installed via a web browser download or via ADB push (**adb push *cert_name* /sdcard/*cert_name***)

Use the following guidelines for installing certificates on the Cisco DX Series.

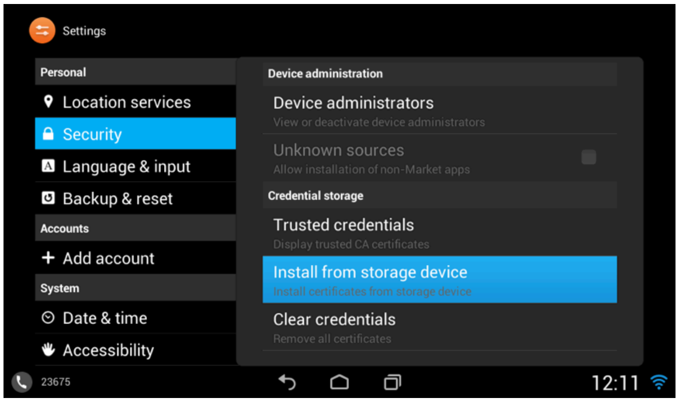
- To install a certificate via the web browser, simply navigate to the certificate then select it.
- If a certificate is copied to the Cisco DX Series via ADB push, then select the **Install from storage device** option.


mtv5-vfiler01-web.ci...
http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp,
23675
12:10

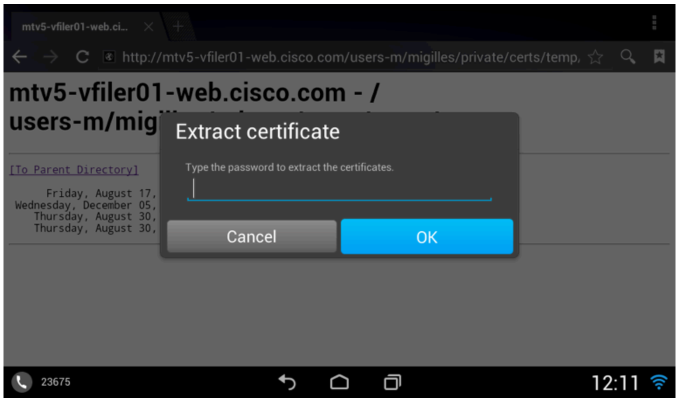
mtv5-vfiler01-web.cisco.com - / users-m/migilles/private/certs/temp/

[To Parent Directory]

```
     Friday, August 17, 2012  9:19 AM        1220 ca_base64.crt
Wednesday, December 05, 2007  5:47 PM         846 ca_der.crt
    Thursday, August 30, 2012  4:57 AM        2840 user.p12
    Thursday, August 30, 2012  4:57 AM        2840 user.pfx
```



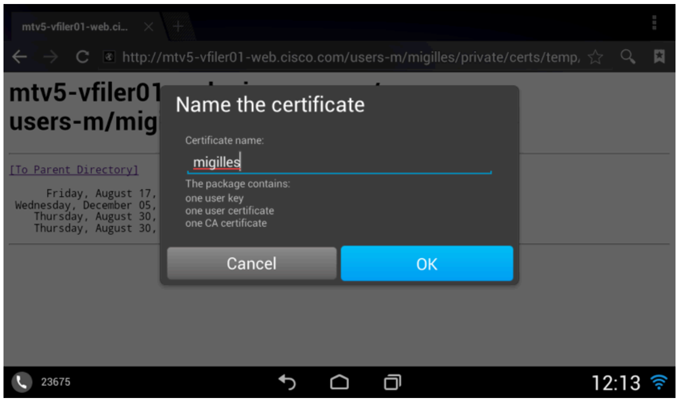
- For the user certificate install, the password will need to be entered to extract the certificates and keys from the imported PKCS #12 file.
- After the password is entered, a prompt will be displayed to name the certificate during.



http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp,

Extract certificate

Type the password to extract the certificates.



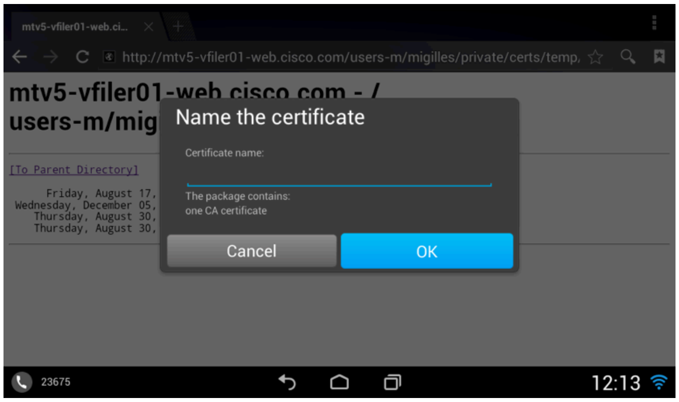
http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp,

Name the certificate

Certificate name: migilles

The package contains:
one user key
one user certificate
one CA certificate

- For the CA certificate, simply name the certificate.



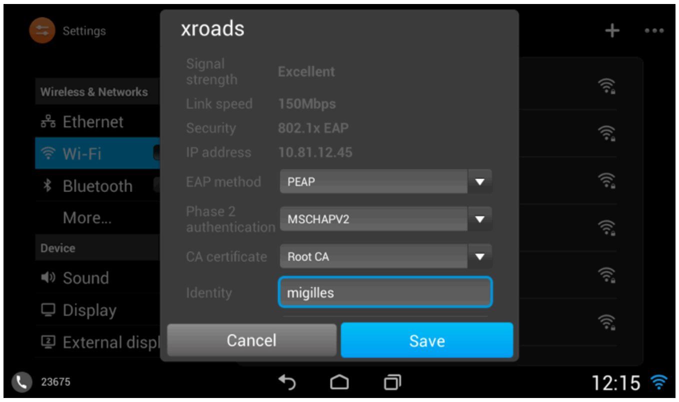
http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp,

Name the certificate

Certificate name:

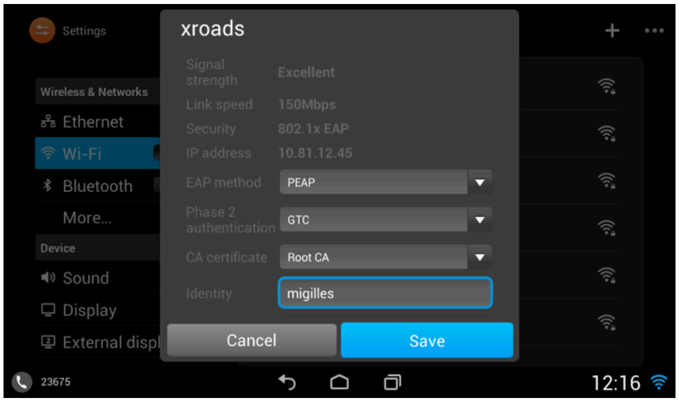
The package contains:
one CA certificate

- Once the certificates are installed, they can then be utilized for PEAP with server validation or EAP-TLS.
- For PEAP with server validation, the **CA certificate** needs to be configured.
- For EAP-TLS, the **User certificate** and **CA certificate** need to be configured.



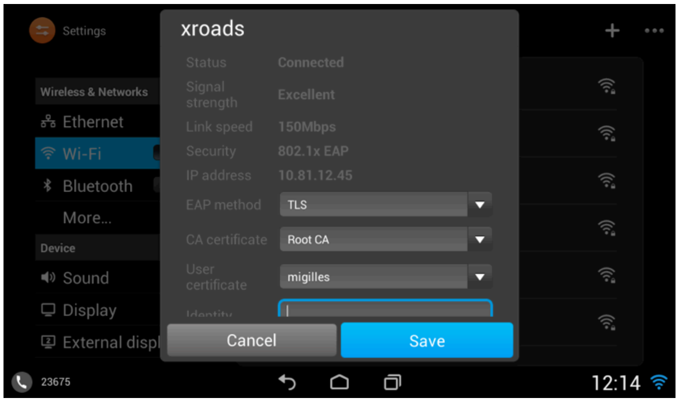
xroads

Signal strength: Excellent
Link speed: 150Mbps
Security: 802.1x EAP
IP address: 10.81.12.45
EAP method: PEAP
Phase 2 authentication: MSCHAPV2
CA certificate: Root CA
Identity: migilles



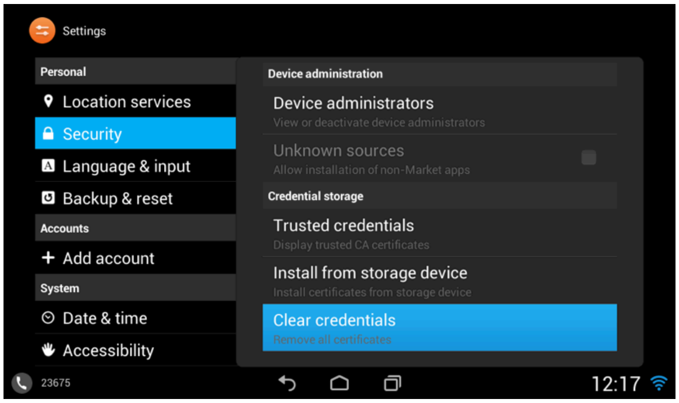
xroads

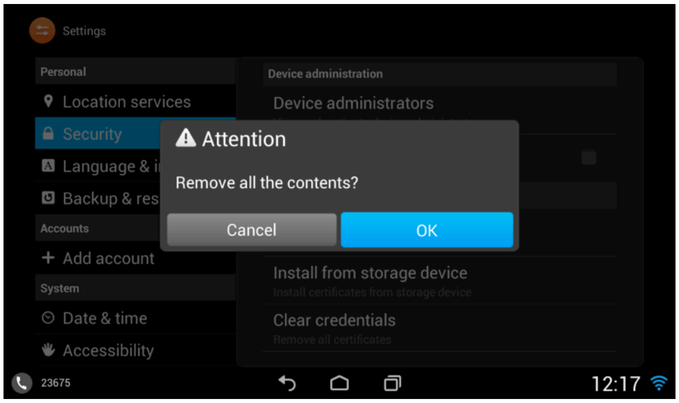
Signal strength: Excellent
Link speed: 150Mbps
Security: 802.1x EAP
IP address: 10.81.12.45
EAP method: PEAP
Phase 2 authentication: GTC
CA certificate: Root CA
Identity: migilles


xroads

Status: Connected
Signal strength: Excellent
Link speed: 150Mbps
Security: 802.1x EAP
IP address: 10.81.12.45
EAP method: TLS
CA certificate: Root CA
User certificate: migilles

- To remove all certificates, select **Clear credentials** in the Security menu.




Attention

Remove all the contents?

Bluetooth Settings

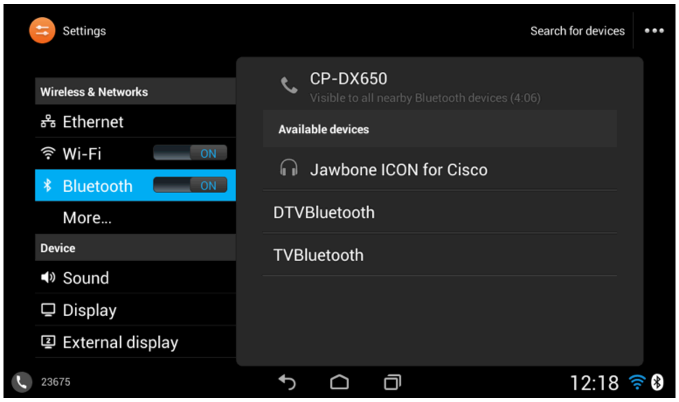
The Cisco DX Series has Bluetooth 3.0 support, which enables hands-free communications.

To pair a Bluetooth device to the Cisco DX Series, follow the instructions below.

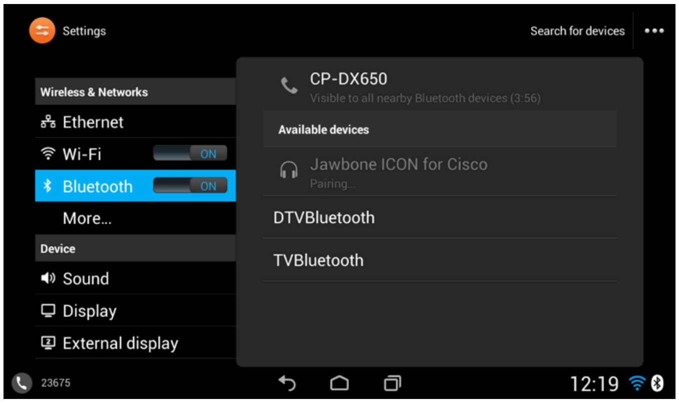
- Navigate to **Settings** > **Wireless & Networks** > **Bluetooth**.
- Ensure that **Bluetooth** is set to **On**.

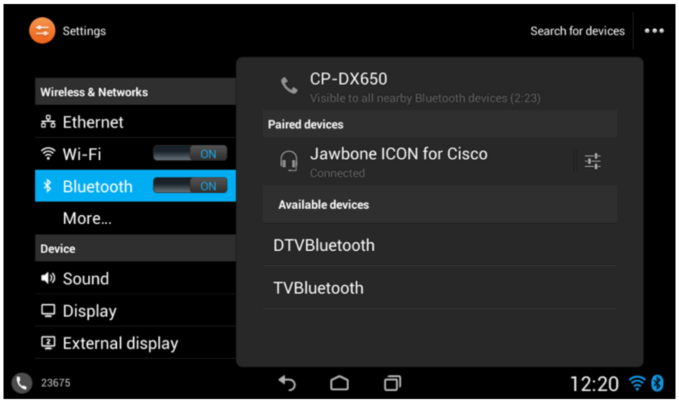
  Ensure **Bluetooth** is enabled in the Cisco Unified Communications Manager; otherwise the option will not be visible in the settings menu.
- Select **Search for devices**.

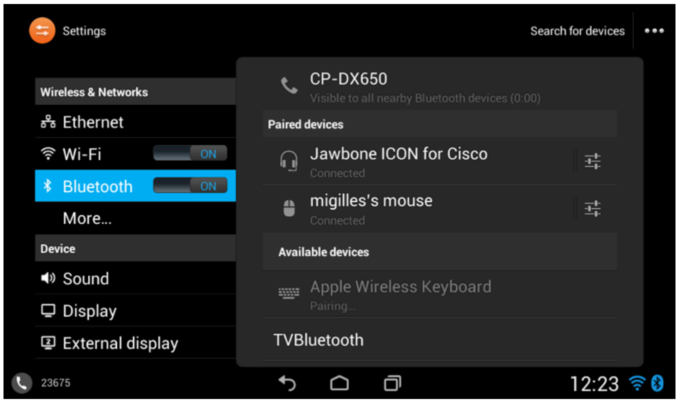
  Ensure the Bluetooth device is in pairing mode
- Select the Bluetooth device after it is displayed in the list.
- Configure the Bluetooth device name for the Cisco DX Series as necessary by selecting **…** in the upper right corner then **Rename Device**.
- The Cisco DX Series visibility via Bluetooth can optionally be enabled temporarily (max of 2 minutes).

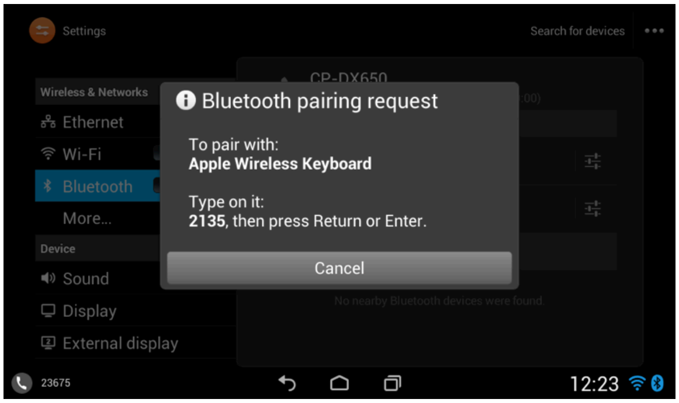


- The Cisco DX Series will then attempt to pair will attempt to use the pin code **0000**. If unsuccessful, enter the pin code when prompted.
- Once paired, then the Cisco DX Series will attempt to connect to the Bluetooth device.



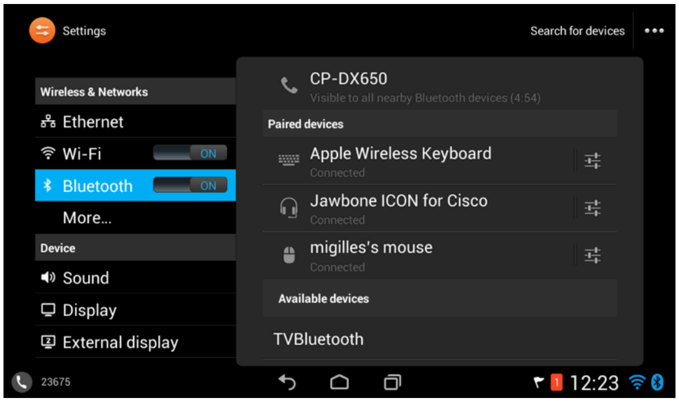




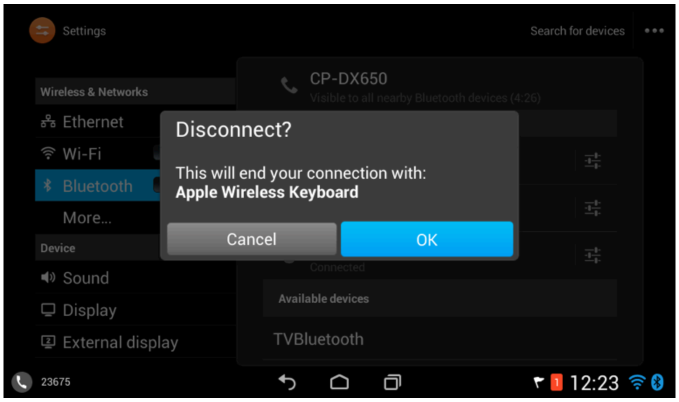

Bluetooth pairing request

To pair with:
Apple Wireless Keyboard

Type on it:
2135, then press Return or Enter.



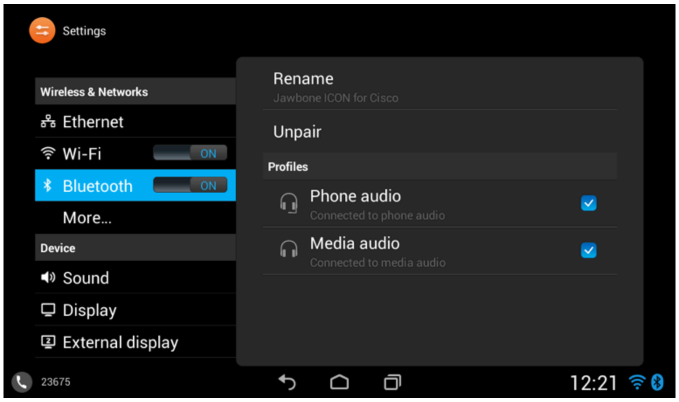
- Selecting the Bluetooth device then selecting **OK** will disconnect that currently connected Bluetooth device.

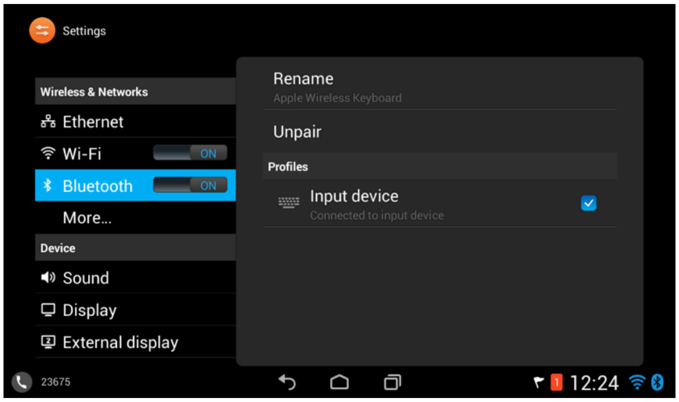


Disconnect?

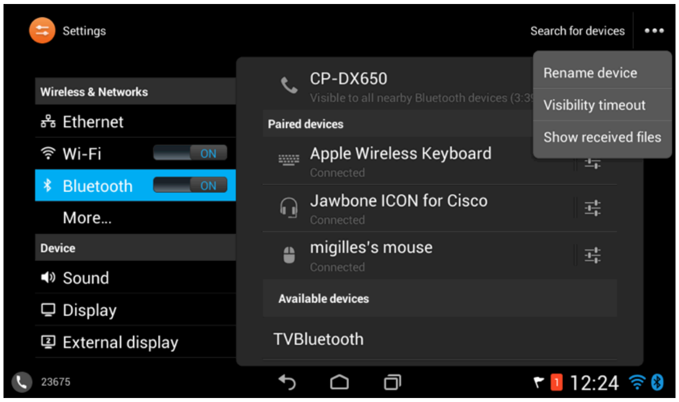
This will end your connection with:
Apple Wireless Keyboard

- The Bluetooth device name can be renamed as necessary by selecting the settings icon associated to the paired device then selecting **Rename**.
- Select **Unpair** to unpair the selected Bluetooth device.





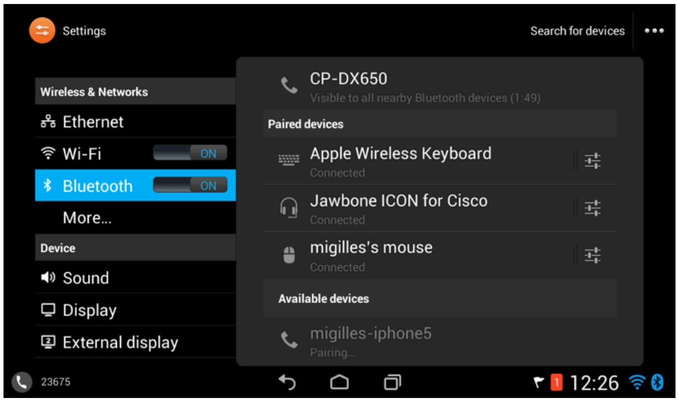
- Additional Bluetooth settings and menus can be accessed by selecting **…** in the upper right corner.

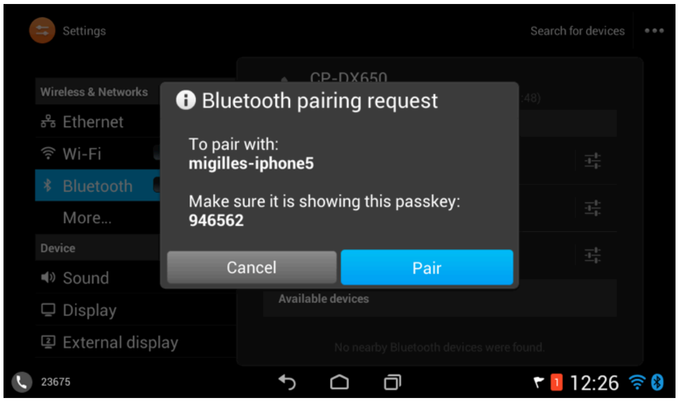


Mobile Phone Sharing

As of the 10.1(1) release for the Cisco DX Series, a mobile phone can be paired to the Cisco DX Series to enable Mobile Phone Sharing.

- Ensure the Bluetooth enabled mobile phone is in pairing mode, then select the device in the list.
- A security prompt will then be displayed to authorize and initiate pairing.
- Select **Pair** once the passkey has been confirmed.



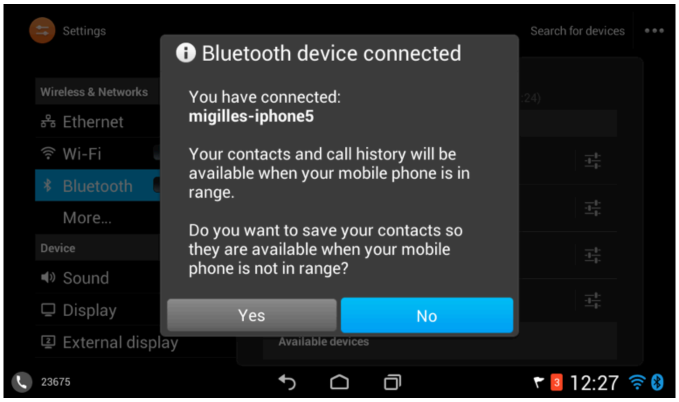

Bluetooth pairing request

To pair with:
migilles-iphone5

Make sure it is showing this passkey:
946562

- Once paired, then the Cisco DX Series will attempt to connect to the Bluetooth enabled mobile phone.
- A prompt then will be displayed to select whether the contacts and call history from the Bluetooth enabled mobile phone should always be available or only when the Bluetooth enabled mobile phone is connected.

  Need to ensure that **Allow Bluetooth Contacts Import** is enabled in the Cisco Unified Communications Manager.



Bluetooth device connected

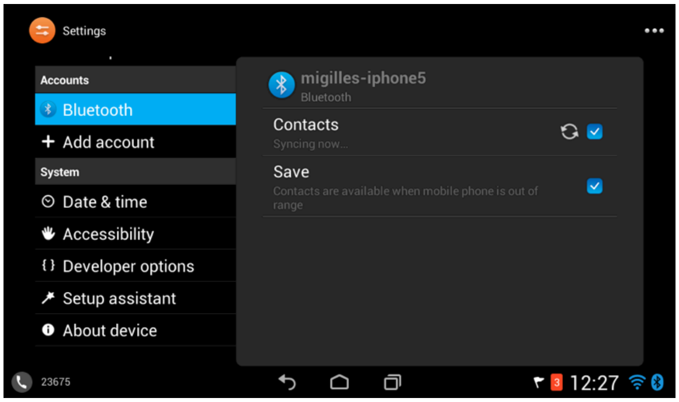
You have connected:
migilles-iphone5

Your contacts and call history will be available when your mobile phone is in range.

Do you want to save your contacts so they are available when your mobile phone is not in range?

Yes | No

- A Bluetooth account will be created for the paired Bluetooth enabled mobile phone.

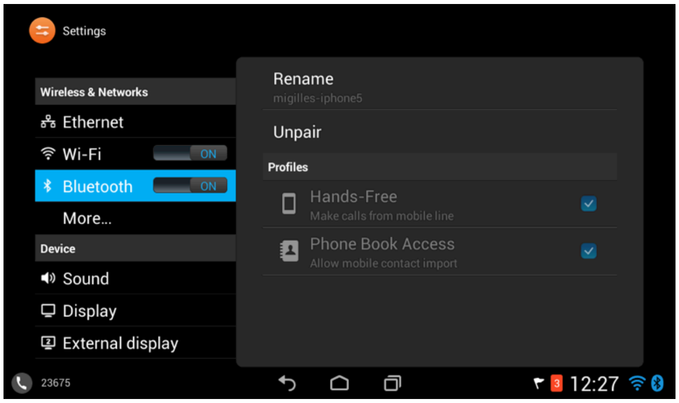


migilles-iphone5
Bluetooth

Contacts ☑
Syncing now...

Save ☑
Contacts are available when mobile phone is out of range

- Additional Bluetooth device options can be configured in the Bluetooth device settings.



Rename
migilles-iphone5

Unpair

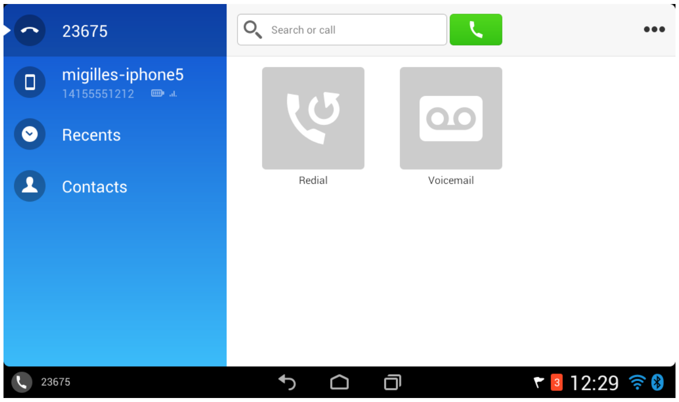
Profiles

Hands-Free ☑
Make calls from mobile line

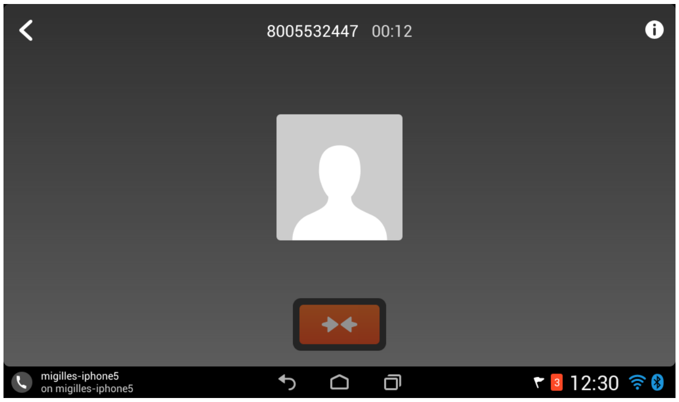
Phone Book Access ☑
Allow mobile contact import

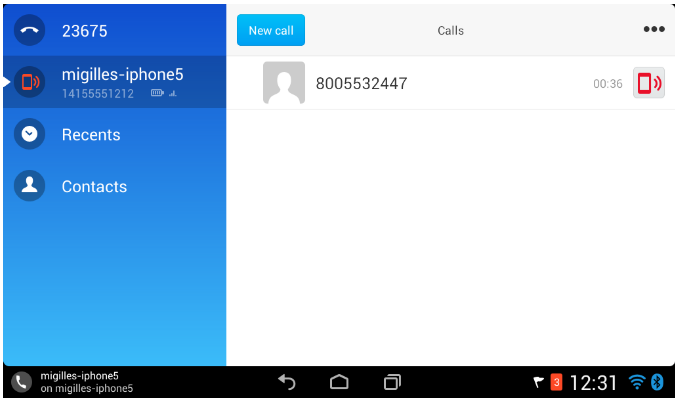
- The Cisco DX Series can answer calls bound for the Bluetooth enabled mobile phone and make outbound calls utilizing the mobile phone’s line.

  Need to ensure that **Allow Bluetooth Mobile Handsfree Mode** is enabled in the Cisco Unified Communications Manager.

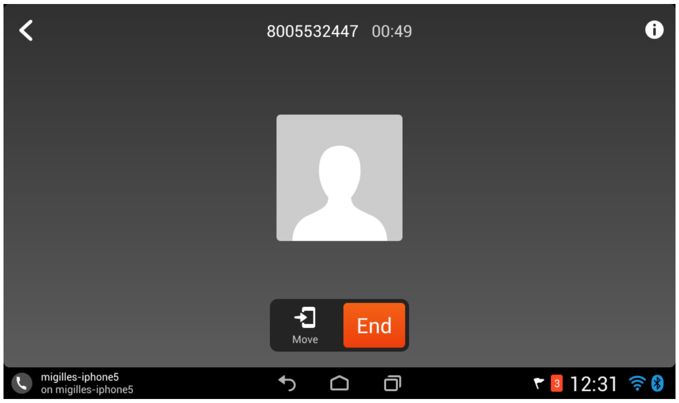


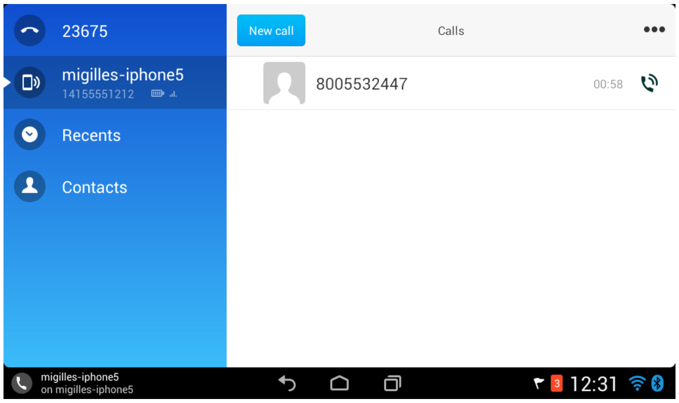
- Calls can easily be moved between the Cisco DX Series and the Bluetooth enabled mobile phone.
- To move a call from the Bluetooth enabled mobile phone to the Cisco DX Series, simply press the orange button or the red mobile phone icon on the main phone screen.





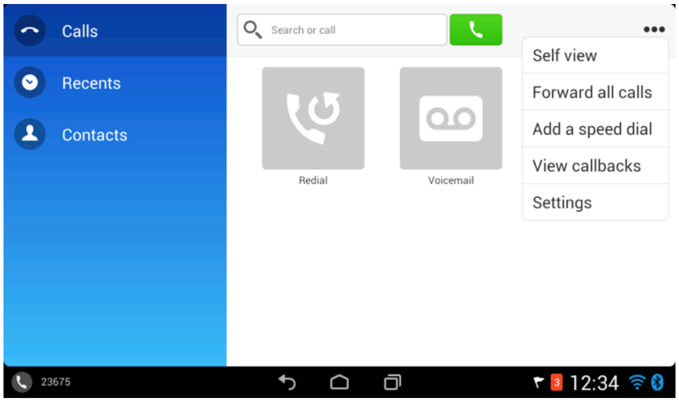
- The call will then be directed to the Cisco DX Series via the Bluetooth enabled mobile phone.
- Select **Move** to switch the call back to the Bluetooth enabled mobile phone.





Video Call Settings

Video call settings can be configured by selecting **…** in the upper right corner of the phone application, then selecting **Settings**.



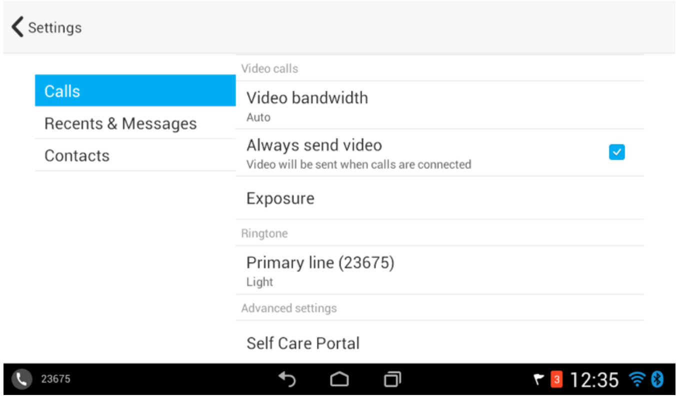
Pressing the audio mute softkey will stop the transmitted audio.

Pressing the video mute softkey will stop the transmitted video.

When on a video call, the local video can be displayed along with the video of the remote endpoint.

Always send video determines if the Cisco DX Series is to start streaming video immediately at the beginning of the call or not assuming the far end device has video capabilities. If disabled, the video can be unmuted at any time to start streaming video. This is enabled by default.

Brightness can be configured to accommodate for the current working environment by selecting **Exposure** within the phone settings.



Video calls

Video bandwidth
Auto

Always send video ☑
Video will be sent when calls are connected

Exposure

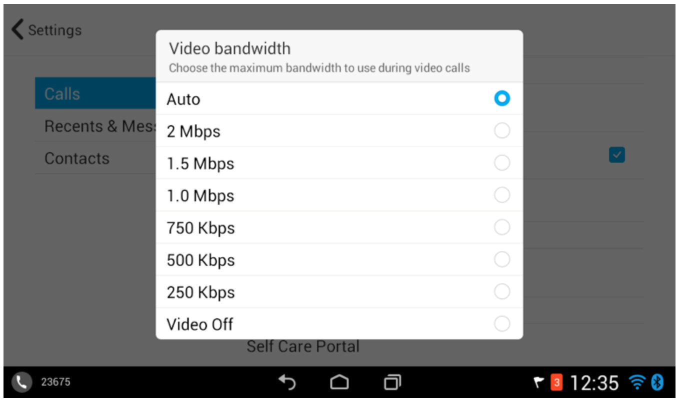
Ringtone

Primary line (23675)
Light

Advanced settings

Self Care Portal

The video bandwidth can be configured as necessary depending on the current working environment. This is set to **Auto** by default, which enables video bandwidth adaptation.



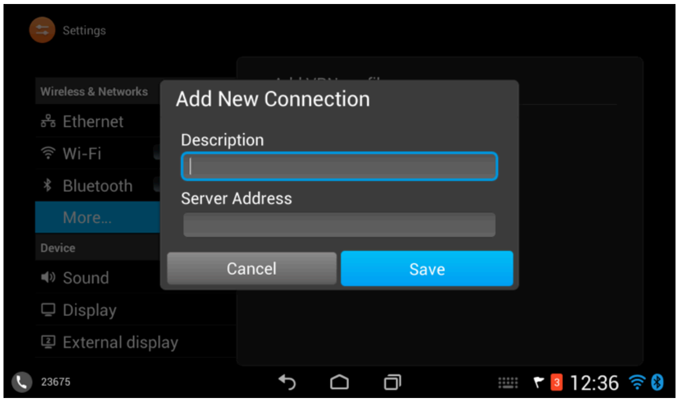
Video bandwidth
Choose the maximum bandwidth to use during video calls

- Auto ●
- 2 Mbps ○
- 1.5 Mbps ○
- 1.0 Mbps ○
- 750 Kbps ○
- 500 Kbps ○
- 250 Kbps ○
- Video Off ○

VPN Settings

VPN connections can be configured if allowed by the administrator.

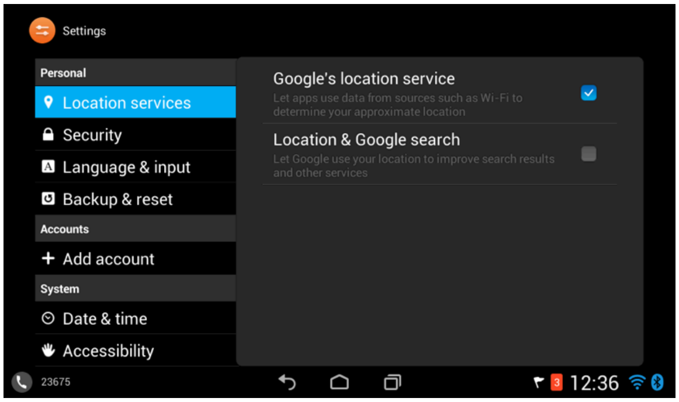
Enter the connection description and server address.



Location Settings

Location can be better determined via a current Wi-Fi connection, where that info can then be shared with applications.

Select **Google's location service**, in Location services.



Google's location service ☑
Let apps use data from sources such as Wi-Fi to determine your approximate location

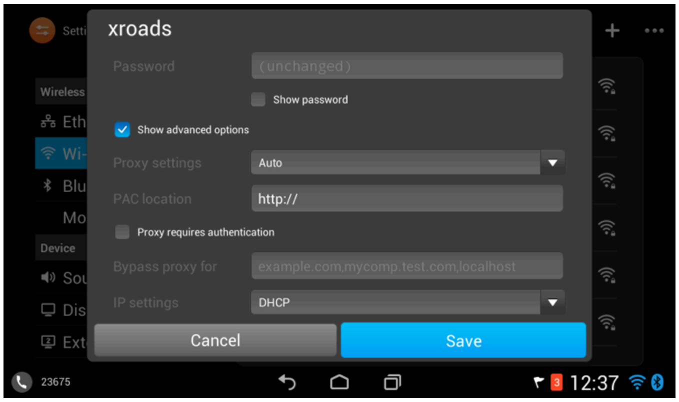
Location & Google search □
Let Google use your location to improve search results and other services

Proxy Settings

Proxy settings can be configured via the **Proxy settings** option in the wireless LAN profile configuration after checking **Show advanced options**.

No proxy is configured by default.

Auto or Manual proxy mode can be optionally be enabled and configured.



xroads

Password (unchanged)

□ Show password

☑ Show advanced options

Proxy settings: Auto

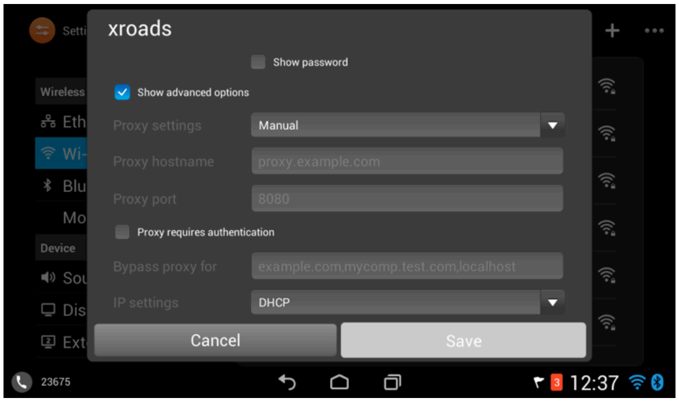
PAC location: http://

□ Proxy requires authentication

Bypass proxy for: example.com,mycomp.test.com,localhost

IP settings: DHCP

Cancel | Save



xroads

□ Show password

☑ Show advanced options

Proxy settings: Manual

Proxy hostname: proxy.example.com

Proxy port: 8080

□ Proxy requires authentication

Bypass proxy for: example.com,mycomp.test.com,localhost

IP settings: DHCP

Cancel | Save

Device UI Profiles

The Cisco DX Series can be configured for **Simple** mode (Phone Only), **Enhanced** or **Public** mode.

Simple mode offers basic video calling capabilities, but prevents access to collaboration applications such as Email, Calendar, Webex, Jabber IM, Google Play, etc.

To enable Simple mode, set the **Device UI Profile** in Cisco Unified Communications Manager to **Simple**.

The following features are some features still available when in **Simple** mode.

- Visual Voicemail
- Dual Independent Display
- Registration over VPN
- Mobile Phone Sharing
- Problem Report Tool

Enhanced mode enables all collaboration capabilities.

Public mode is to be used for phones that are for community purposes.

Upgrading Firmware

To upgrade the firmware, install the signed COP file for Cisco Unified Communications Manager.

For information on how to install the COP file, refer to the Cisco Unified Communications Manager Operating System Administrator Guide at this URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

During TFTP server download, the configuration file is parsed and the device load is identified. The Cisco DX Series then downloads the firmware files to flash if it is not running the specified image already.

The Load Server can be specified as an alternate TFTP server to retrieve firmware files, which is located in the product specific configuration section of the Cisco DX Series within Cisco Unified Communications Manager Administration.

Using the Cisco DX Series

Application Market

Various types of applications are available for download from Google Play.

Google Play is an application market developed by Google™ for Android OS. The **Play Store** application allows users to browse and download applications published by third-party developers.

Google Play offers applications such as Books & Reference, Business, Comics, Communication, Education, Entertainment, Finance, Games, Health & Fitness, Libraries & Demo, Lifestyle, Live Wallpaper, Media & Video, Medical, Music & Audio, News & Magazines, Personalization, Photography, Productivity, Shopping, Social, Sports, Tools, Transportation, Travel & Local, Weather, and Widgets.

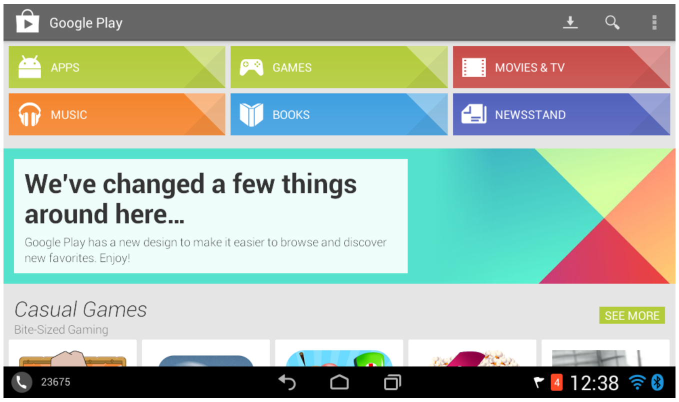
The **Play Store** application will be visible only if **Allow Applications from Google Play** is enabled by the systems administrator in the Cisco Unified Communications Manager.

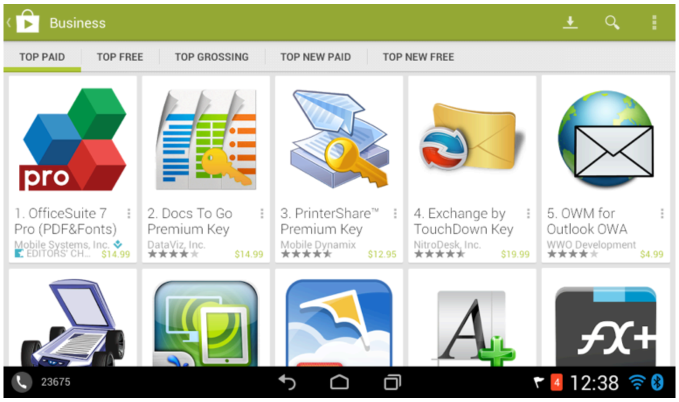
A Google account is necessary to download applications.

When first launching Google Play, you will be prompted to sign in with your credentials or register if you do not have an account already.

Google Play can also be accessed at this URL.

https://play.google.com/store


Google Play
APPS
GAMES
MOVIES & TV
MUSIC
BOOKS
NEWSSTAND
We've changed a few things around here...
Google Play has a new design to make it easier to browse and discover new favorites. Enjoy!
Casual Games
Bite-Sized Gaming
SEE MORE
23675
12:38

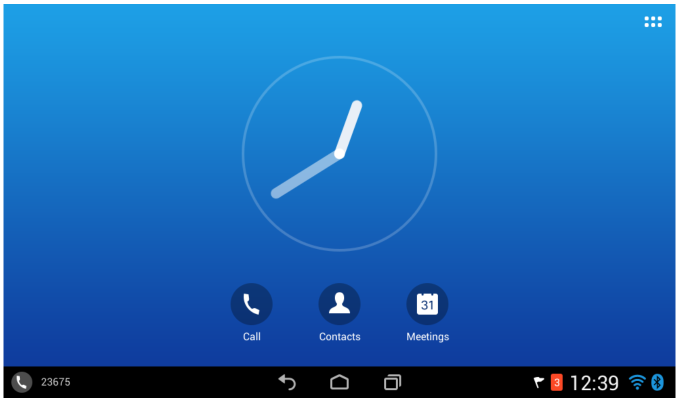


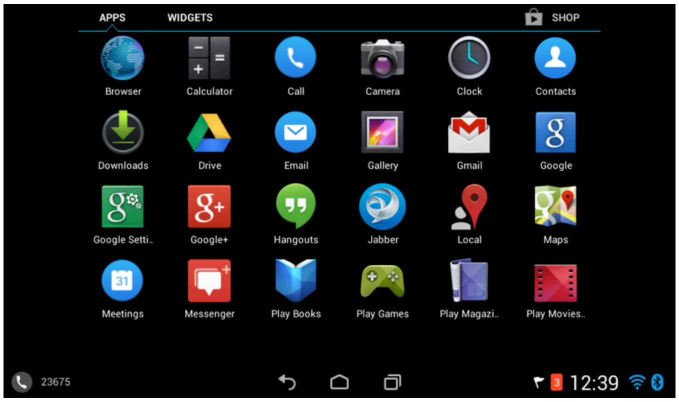
Applications

Aside of applications offered by Google Play, there are pre-installed applications such as Cisco Unified Communications Manager Phone Client for voice and video calling, Cisco Jabber IM, Cisco Unified Presence, Cisco WebEx, Email, Calendar and Contacts.

Phone Application

To launch the phone application, select the phone icon on the taskbar, from the applications menu or from a shortcut created on the main page.





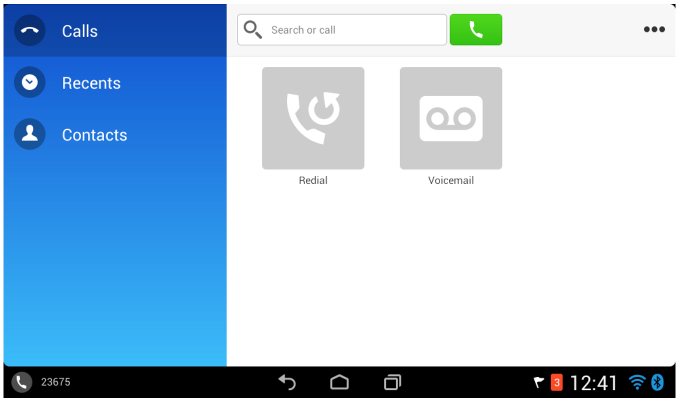
After the phone application is launched, the lines, speed dials and other options configured in the phone button template will be displayed in the **Calls** menu.

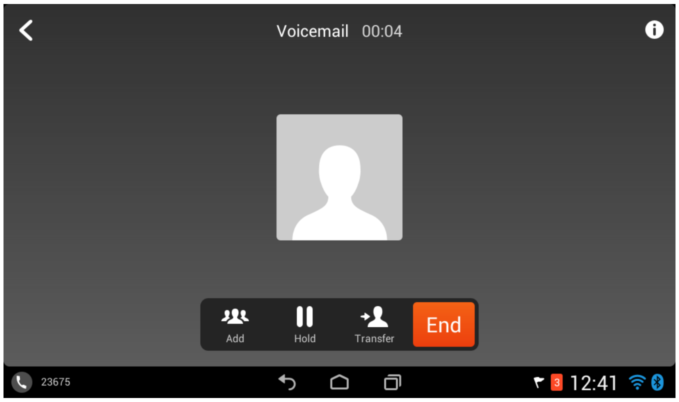
Call history and messages are located in the **Recents** menu.

Contacts and favorites are accessible via the contact icon in the upper right corner.

The Cisco DX Series will attempt to register to Cisco Unified Communications Manager after power on, so the application does not have to be launched manually.

The Cisco DX Series is registered to Cisco Unified Communications Manager when the phone icon with name and/or extension are displayed.

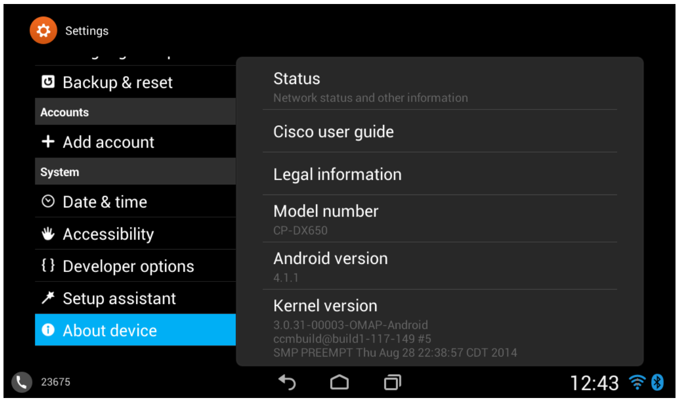




Troubleshooting

About Device

Status and version information is displayed in **About Device** in the Settings menu.



Status
Network status and other information

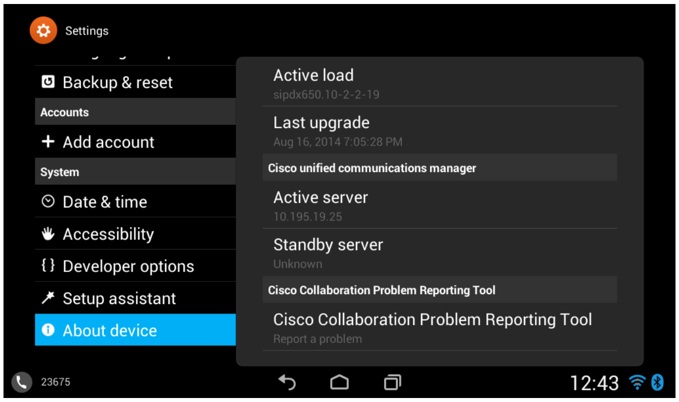
Cisco user guide

Legal information

Model number
CP-DX650

Android version
4.1.1

Kernel version
3.0.31-00003-OMAP-Android
ccmbuild@build1-117-149 #5
SMP PREEMPT Thu Aug 28 22:38:57 CDT 2014



Active load
sipdx650.10-2-2-19

Last upgrade
Aug 16, 2014 7:05:28 PM

Cisco unified communications manager

Active server
10.195.19.25

Standby server
Unknown

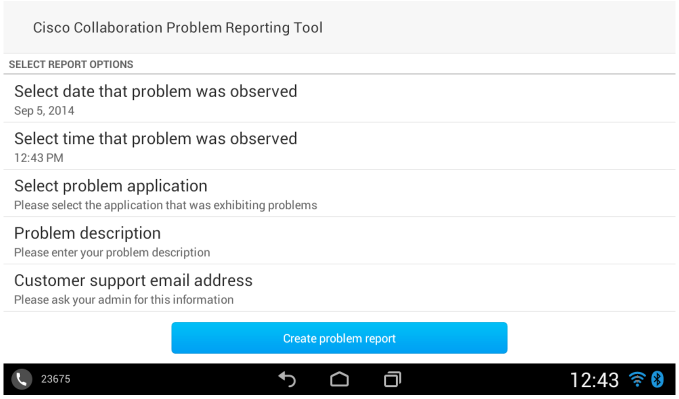
Cisco Collaboration Problem Reporting Tool

Cisco Collaboration Problem Reporting Tool
Report a problem

Cisco Collaboration Problem Reporting Tool

A problem report can be created via the Cisco Collaboration Problem Reporting Tool, which is located in the **About Device** menu.

The date and time, problem application, problem description and customer support email address can be defined.



Cisco Collaboration Problem Reporting Tool

SELECT REPORT OPTIONS

Select date that problem was observed
Sep 5, 2014

Select time that problem was observed
12:43 PM

Select problem application
Please select the application that was exhibiting problems

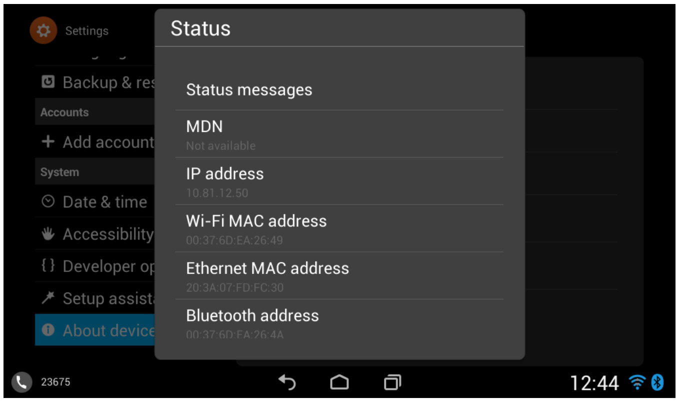
Problem description
Please enter your problem description

Customer support email address
Please ask your admin for this information

Create problem report

Status

Status messages, IP Address, MAC address, DHCP information, up time, current access point and statistical information can be displayed by selecting **About Device > Status**.



Status

Status messages

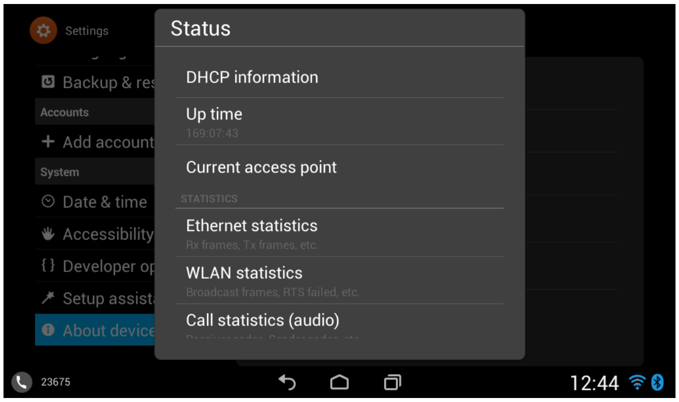
MDN
Not available

IP address
10.81.12.50

Wi-Fi MAC address
00:37:6D:EA:26:49

Ethernet MAC address
20:3A:07:FD:FC:30

Bluetooth address
00:37:6D:EA:26:4A



Status

DHCP information

Up time
169:07:43

Current access point

STATISTICS

Ethernet statistics
Rx frames, Tx frames, etc.

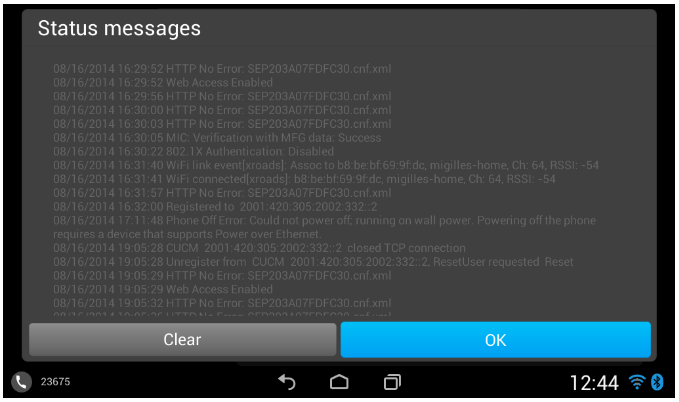
WLAN statistics
Broadcast frames, RTS failed, etc.

Call statistics (audio)

Status Messages

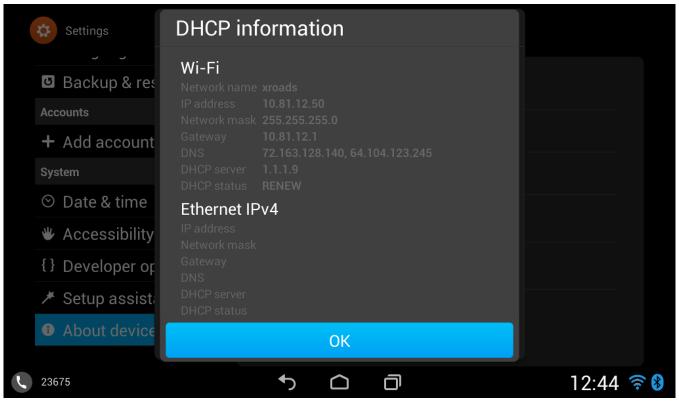
Select **Status messages** to display the message log.

Select **Clear** to reset the message log.



```
08/16/2014 16:29:52 HTTP No Error: SEP203A07FDFC30.cnf.xml
08/16/2014 16:29:52 Web Access Enabled
08/16/2014 16:29:56 HTTP No Error: SEP203A07FDFC30.cnf.xml
08/16/2014 16:30:00 HTTP No Error: SEP203A07FDFC30.cnf.xml
08/16/2014 16:30:03 HTTP No Error: SEP203A07FDFC30.cnf.xml
08/16/2014 16:30:05 MIC: Verification with MFG data: Success
08/16/2014 16:30:22 802.1X Authentication: Disabled
08/16/2014 16:31:40 WiFi link event[xroads]: Assoc to b8:be:bf:69:9f:dc, migilles-home, Ch: 64, RSSI: -54
08/16/2014 16:31:41 WiFi connected[xroads]: b8:be:bf:69:9f:dc, migilles-home, Ch: 64, RSSI: -54
08/16/2014 16:31:57 HTTP No Error: SEP203A07FDFC30.cnf.xml
08/16/2014 16:32:00 Registered to  2001:420:305:2002:332::2
08/16/2014 17:11:48 Phone Off Error: Could not power off; running on wall power. Powering off the phone
requires a device that supports Power over Ethernet.
08/16/2014 19:05:28 CUCM  2001:420:305:2002:332::2  closed TCP connection
08/16/2014 19:05:28 Unregister from  CUCM  2001:420:305:2002:332::2, ResetUser requested  Reset
08/16/2014 19:05:29 HTTP No Error: SEP203A07FDFC30.cnf.xml
08/16/2014 19:05:29 Web Access Enabled
08/16/2014 19:05:32 HTTP No Error: SEP203A07FDFC30.cnf.xml
```

Select **DHCP information** to display the DHCP information for Wi-Fi and Ethernet interfaces.



DHCP information

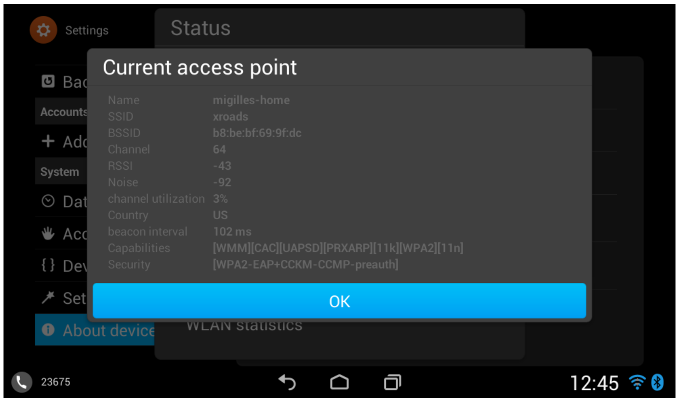
Wi-Fi

Network name	xroads
IP address	10.81.12.50
Network mask	255.255.255.0
Gateway	10.81.12.1
DNS	72.163.128.140, 64.104.123.245
DHCP server	1.1.1.9
DHCP status	RENEW

Ethernet IPv4

IP address	
Network mask	
Gateway	
DNS	
DHCP server	
DHCP status	

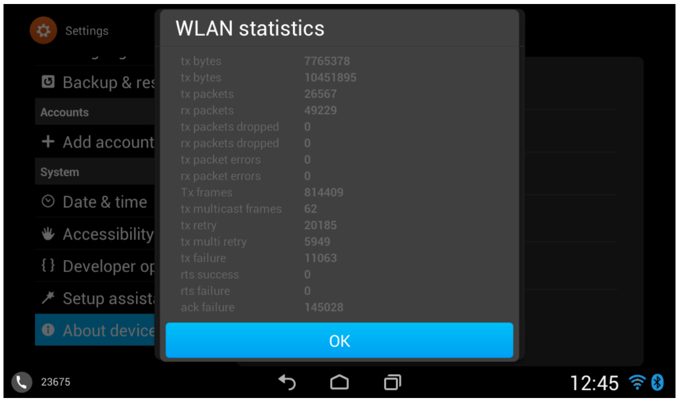
Select **Current access point** to display the details about the current access point connection.



Current access point

Name	migilles-home
SSID	xroads
BSSID	b8:be:bf:69:9f:dc
Channel	64
RSSI	-43
Noise	-92
channel utilization	3%
Country	US
beacon interval	102 ms
Capabilities	[WMM][CAC][UAPSD][PRXARP][11k][WPA2][11n]
Security	[WPA2-EAP+CCKM-CCMP-preauth]

Select **WLAN statistics** to display transmitted and received byte, packet, packets dropped, packet error, retry counter, and ACK failure information.

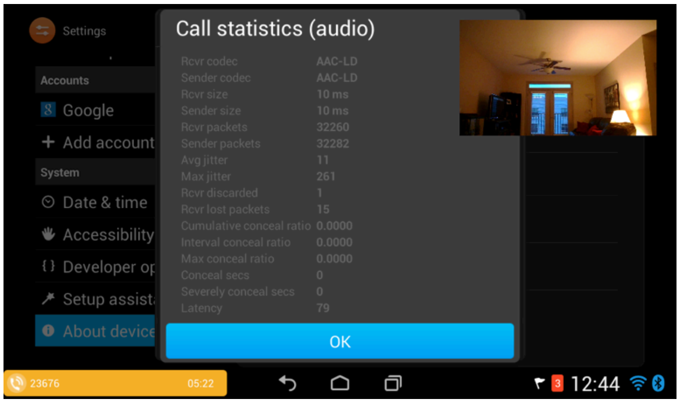


WLAN statistics

tx bytes	7765378
tx bytes	10451895
tx packets	26567
rx packets	49229
tx packets dropped	0
rx packets dropped	0
tx packet errors	0
rx packet errors	0
Tx frames	814409
tx multicast frames	62
tx retry	20185
tx multi retry	5949
tx failure	11063
rts success	0
rts failure	0
ack failure	145028

OK

Select **Call statistics (audio)** to display the information about the current or last voice stream.

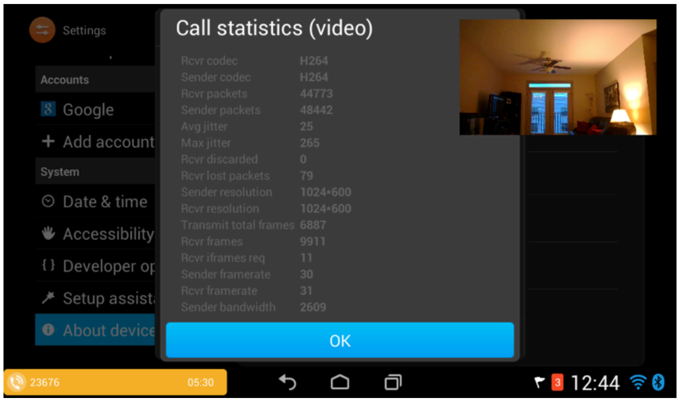


Call statistics (audio)

Rcvr codec	AAC-LD
Sender codec	AAC-LD
Rcvr size	10 ms
Sender size	10 ms
Rcvr packets	32260
Sender packets	32282
Avg jitter	11
Max jitter	261
Rcvr discarded	1
Rcvr lost packets	15
Cumulative conceal ratio	0.0000
Interval conceal ratio	0.0000
Max conceal ratio	0.0000
Conceal secs	0
Severely conceal secs	0
Latency	79

OK

Select **Call statistics (video)** to display the information about the current or last video stream.



Call statistics (video)

Rcvr codec	H264
Sender codec	H264
Rcvr packets	44773
Sender packets	48442
Avg jitter	25
Max jitter	265
Rcvr discarded	0
Rcvr lost packets	79
Sender resolution	1024*600
Rcvr resolution	1024*600
Transmit total frames	6887
Rcvr frames	9911
Rcvr iframes req	11
Sender framerate	30
Rcvr framerate	31
Sender bandwidth	2609

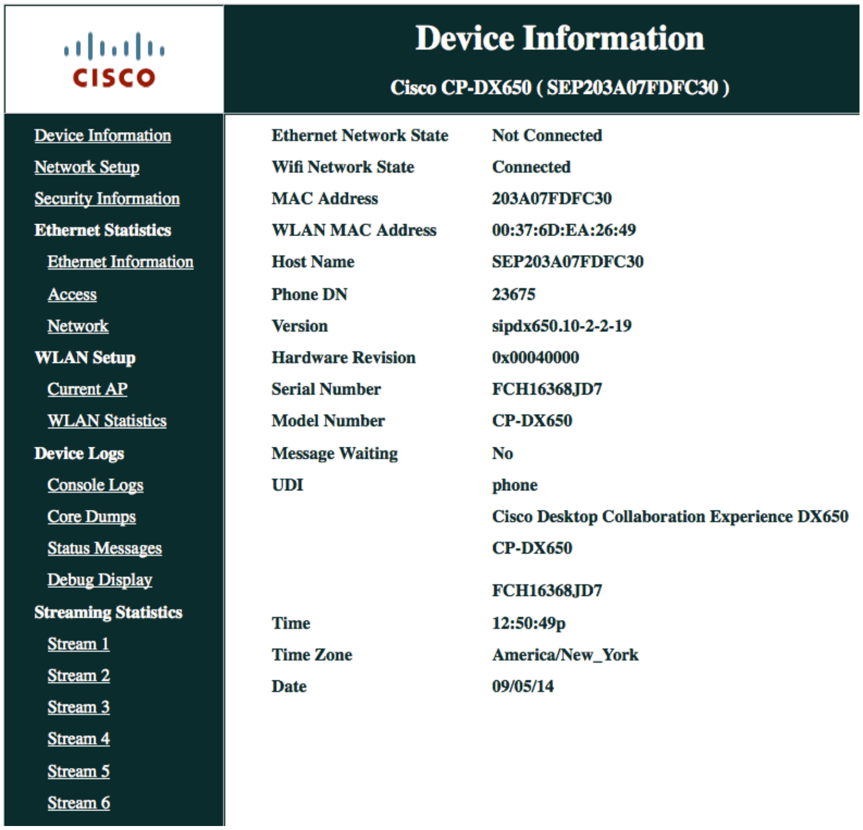
OK

Device Webpage

The Cisco DX Series webpage provides device information, network setup, WLAN setup, streaming and other statistical information as well as access to device logs.

Device Information

The Cisco DX Series provides device information, where network status, MAC address and version information is displayed. Browse to the web interface (https://x.x.x.x) of the Cisco DX Series then select **Device Information** to view this information.



Device Information

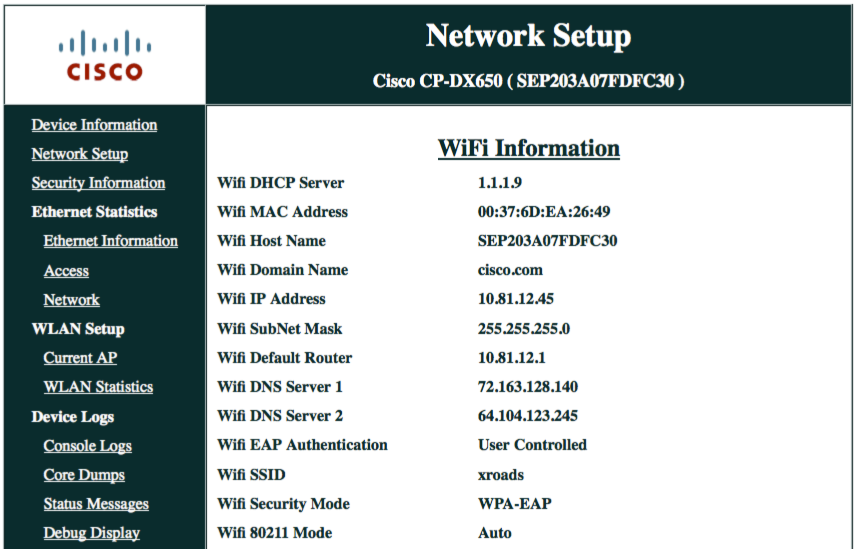
Cisco CP-DX650 (SEP203A07FDFC30)

Ethernet Network State	Not Connected
Wifi Network State	Connected
MAC Address	203A07FDFC30
WLAN MAC Address	00:37:6D:EA:26:49
Host Name	SEP203A07FDFC30
Phone DN	23675
Version	sipdx650.10-2-2-19
Hardware Revision	0x00040000
Serial Number	FCH16368JD7
Model Number	CP-DX650
Message Waiting	No
UDI	phone Cisco Desktop Collaboration Experience DX650 CP-DX650 FCH16368JD7
Time	12:50:49p
Time Zone	America/New_York
Date	09/05/14

Network Setup

The Cisco DX Series provides network setup information, where Wi-Fi, Ethernet and Cisco Unified Communications Manager information is displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco DX Series then select **Network Setup** to view this information.



Network Setup

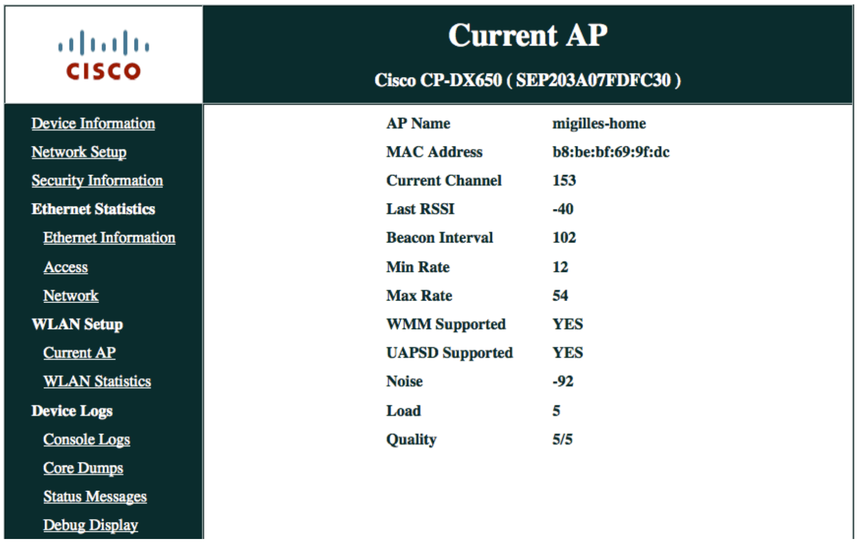
Cisco CP-DX650 (SEP203A07FDFC30)

WiFi Information

Wifi DHCP Server	1.1.1.9
Wifi MAC Address	00:37:6D:EA:26:49
Wifi Host Name	SEP203A07FDFC30
Wifi Domain Name	cisco.com
Wifi IP Address	10.81.12.45
Wifi SubNet Mask	255.255.255.0
Wifi Default Router	10.81.12.1
Wifi DNS Server 1	72.163.128.140
Wifi DNS Server 2	64.104.123.245
Wifi EAP Authentication	User Controlled
Wifi SSID	xroads
Wifi Security Mode	WPA-EAP
Wifi 80211 Mode	Auto

Current Access Point

Detailed information in regards to the current access point can also be seen in the Cisco DX Series' web interface.
Browse to the web interface (https://x.x.x.x) of the Cisco DX Series then select **Current AP** to view this information.



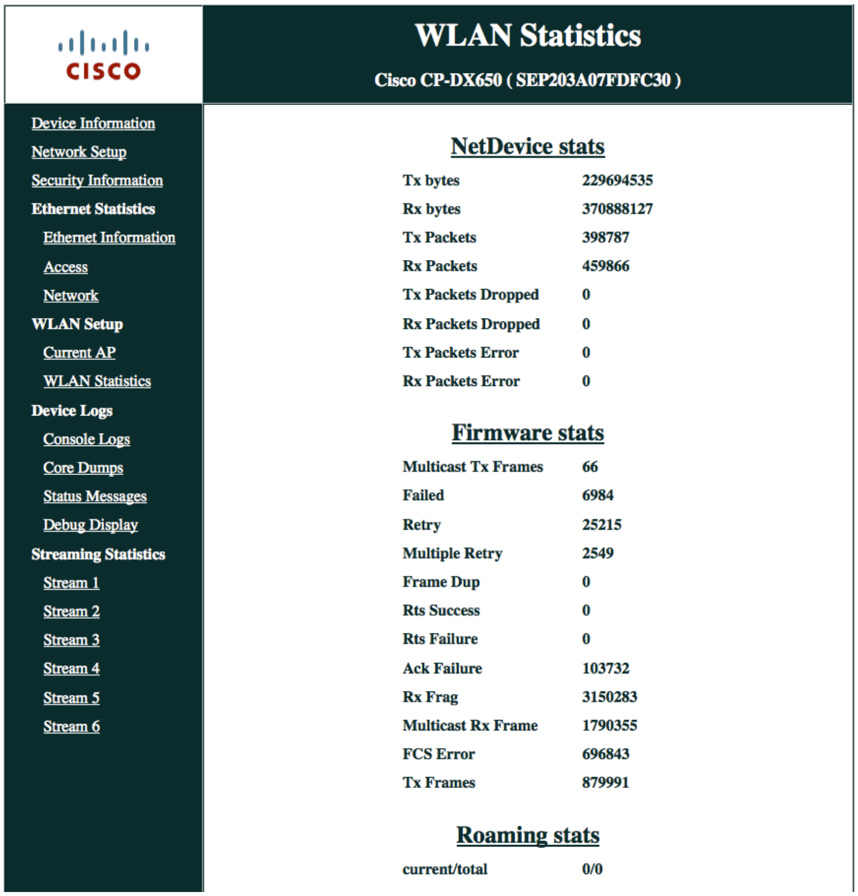
Current AP

Cisco CP-DX650 (SEP203A07FDFC30)

AP Name	migilles-home
MAC Address	b8:be:bf:69:9f:dc
Current Channel	153
Last RSSI	-40
Beacon Interval	102
Min Rate	12
Max Rate	54
WMM Supported	YES
UAPSD Supported	YES
Noise	-92
Load	5
Quality	5/5

WLAN Statistics

The Cisco DX Series provides WLAN statistic information, where packet and counters are displayed.
Browse to the web interface (https://x.x.x.x) of the Cisco DX Series then select **WLAN Statistics** to view this information.



WLAN Statistics

Cisco CP-DX650 (SEP203A07FDFC30)

NetDevice stats

Tx bytes	229694535
Rx bytes	370888127
Tx Packets	398787
Rx Packets	459866
Tx Packets Dropped	0
Rx Packets Dropped	0
Tx Packets Error	0
Rx Packets Error	0

Firmware stats

Multicast Tx Frames	66
Failed	6984
Retry	25215
Multiple Retry	2549
Frame Dup	0
Rts Success	0
Rts Failure	0
Ack Failure	103732
Rx Frag	3150283
Multicast Rx Frame	1790355
FCS Error	696843
Tx Frames	879991

Roaming stats

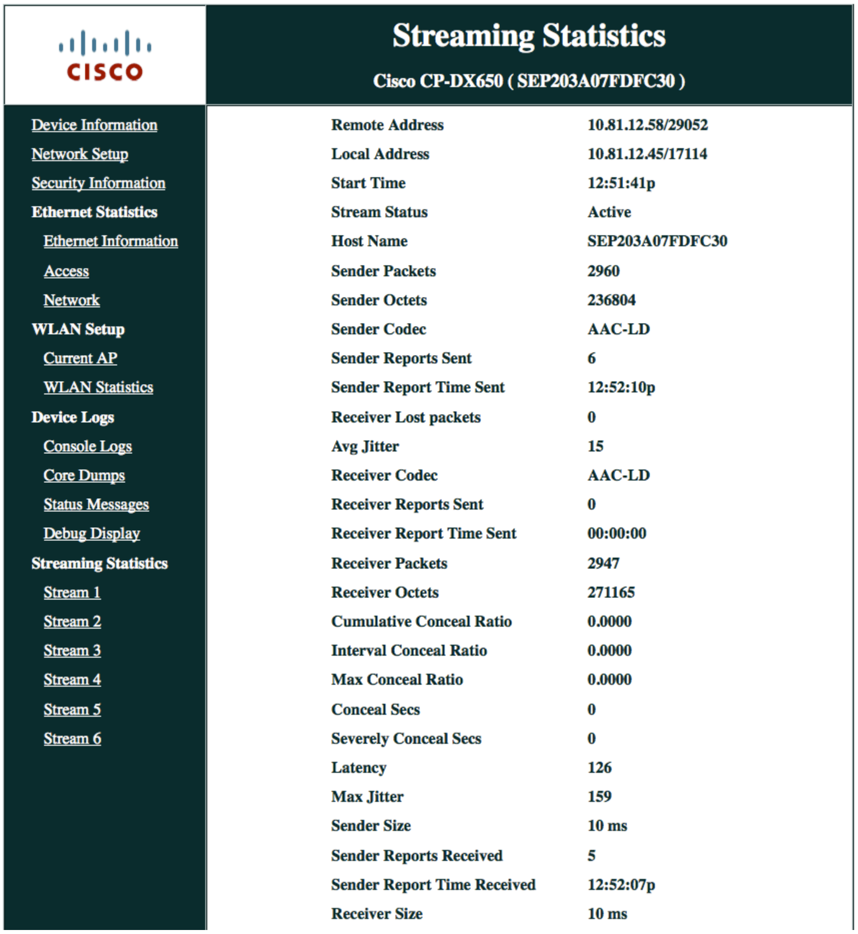
current/total	0/0

Streaming Statistics

The Cisco DX Series provides call statistic information, where jitter and packet counters are displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco DX Series then select **Streaming Statistics** to view this information.

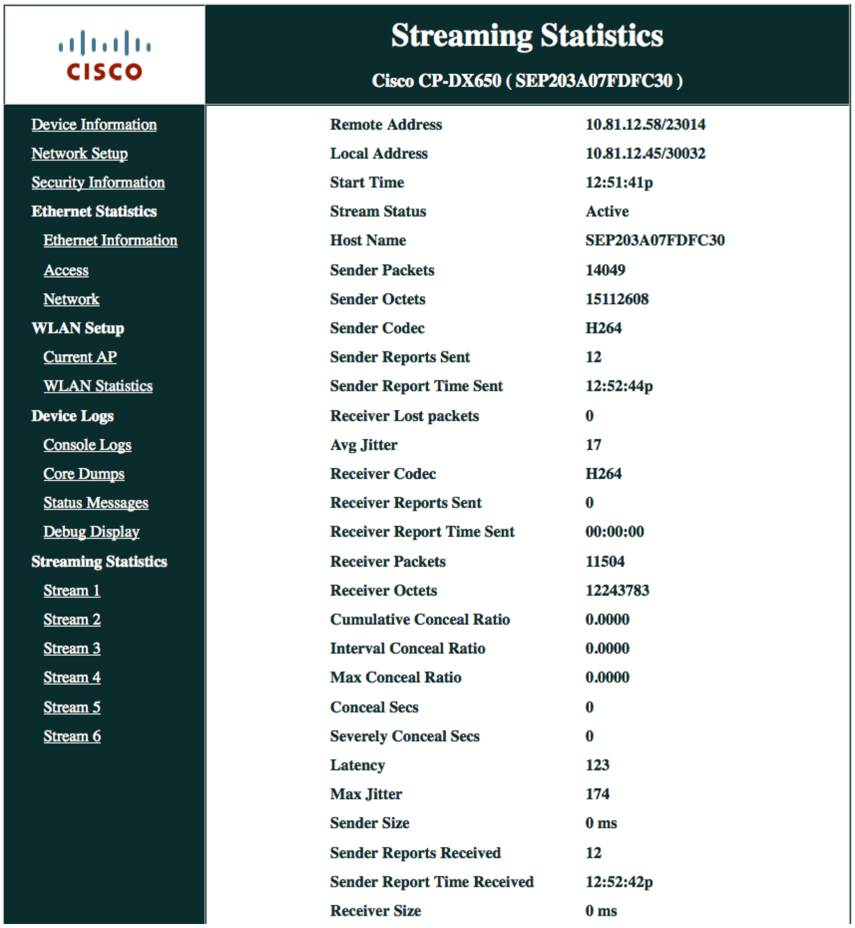
The Cisco DX Series does not display MOS (call quality) statistics for audio or video.



Streaming Statistics

Cisco CP-DX650 (SEP203A07FDFC30)

Remote Address	10.81.12.58/29052
Local Address	10.81.12.45/17114
Start Time	12:51:41p
Stream Status	Active
Host Name	SEP203A07FDFC30
Sender Packets	2960
Sender Octets	236804
Sender Codec	AAC-LD
Sender Reports Sent	6
Sender Report Time Sent	12:52:10p
Receiver Lost packets	0
Avg Jitter	15
Receiver Codec	AAC-LD
Receiver Reports Sent	0
Receiver Report Time Sent	00:00:00
Receiver Packets	2947
Receiver Octets	271165
Cumulative Conceal Ratio	0.0000
Interval Conceal Ratio	0.0000
Max Conceal Ratio	0.0000
Conceal Secs	0
Severely Conceal Secs	0
Latency	126
Max Jitter	159
Sender Size	10 ms
Sender Reports Received	5
Sender Report Time Received	12:52:07p
Receiver Size	10 ms



Streaming Statistics

Cisco CP-DX650 (SEP203A07FDFC30)

Remote Address	10.81.12.58/23014
Local Address	10.81.12.45/30032
Start Time	12:51:41p
Stream Status	Active
Host Name	SEP203A07FDFC30
Sender Packets	14049
Sender Octets	15112608
Sender Codec	H264
Sender Reports Sent	12
Sender Report Time Sent	12:52:44p
Receiver Lost packets	0
Avg Jitter	17
Receiver Codec	H264
Receiver Reports Sent	0
Receiver Report Time Sent	00:00:00
Receiver Packets	11504
Receiver Octets	12243783
Cumulative Conceal Ratio	0.0000
Interval Conceal Ratio	0.0000
Max Conceal Ratio	0.0000
Conceal Secs	0
Severely Conceal Secs	0
Latency	123
Max Jitter	174
Sender Size	0 ms
Sender Reports Received	12
Sender Report Time Received	12:52:42p
Receiver Size	0 ms

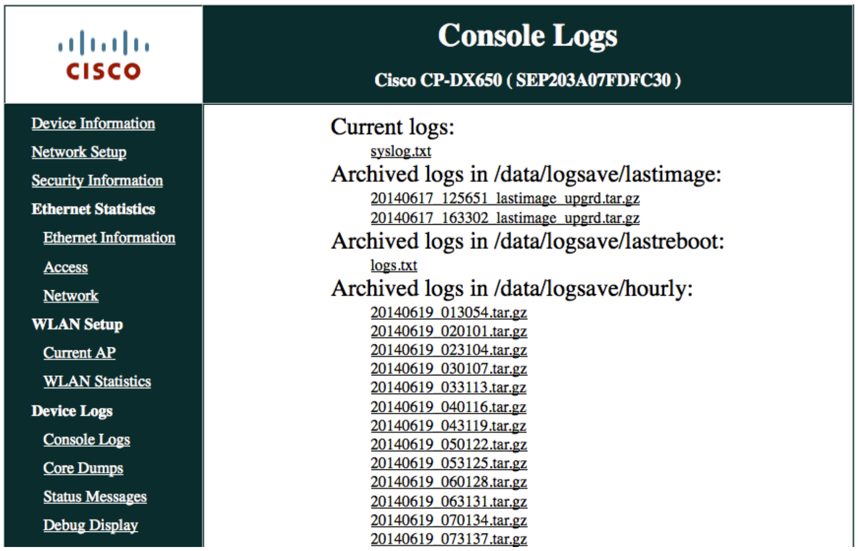
For more information, see the Cisco DX Series Administration Guide at this URL:

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

Device Logs

Console logs, core dumps, status messages for troubleshooting purposes can be obtained from the web interface of the Cisco DX Series.

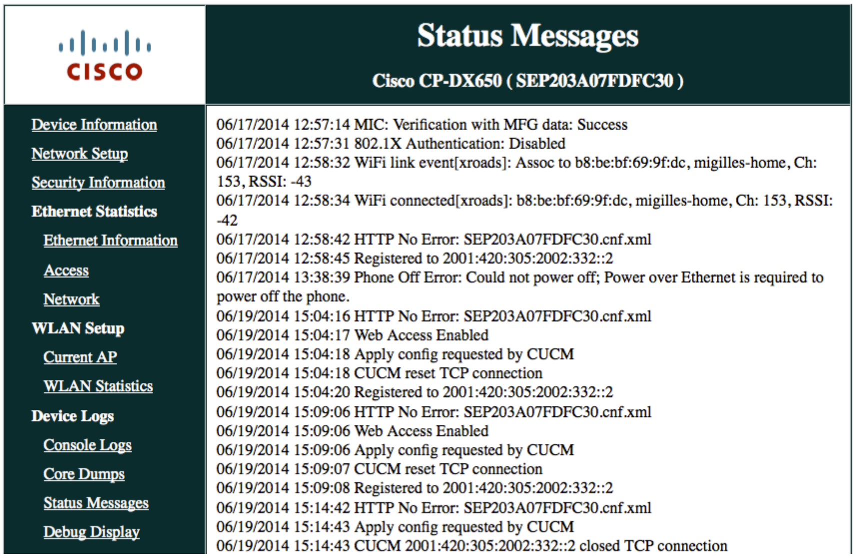
Browse to the web interface (https://x.x.x.x) of the Cisco DX Series then select the necessary menu item under **Device Logs** to view this information.



Console Logs

Cisco CP-DX650 (SEP203A07FDFC30)

```
Current logs:
    syslog.txt
Archived logs in /data/logsave/lastimage:
    20140617_125651_lastimage_upgrd.tar.gz
    20140617_163302_lastimage_upgrd.tar.gz
Archived logs in /data/logsave/lastreboot:
    logs.txt
Archived logs in /data/logsave/hourly:
    20140619_013054.tar.gz
    20140619_020101.tar.gz
    20140619_023104.tar.gz
    20140619_030107.tar.gz
    20140619_033113.tar.gz
    20140619_040116.tar.gz
    20140619_043119.tar.gz
    20140619_050122.tar.gz
    20140619_053125.tar.gz
    20140619_060128.tar.gz
    20140619_063131.tar.gz
    20140619_070134.tar.gz
    20140619_073137.tar.gz
```



Status Messages

Cisco CP-DX650 (SEP203A07FDFC30)

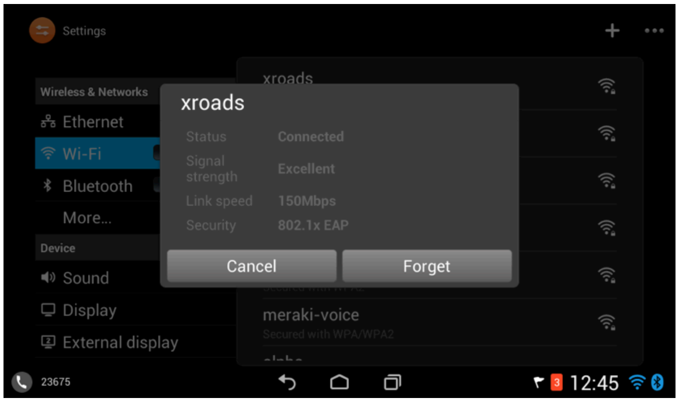
```
06/17/2014 12:57:14 MIC: Verification with MFG data: Success
06/17/2014 12:57:31 802.1X Authentication: Disabled
06/17/2014 12:58:32 WiFi link event[xroads]: Assoc to b8:be:bf:69:9f:dc, migilles-home, Ch:
153, RSSI: -43
06/17/2014 12:58:34 WiFi connected[xroads]: b8:be:bf:69:9f:dc, migilles-home, Ch: 153, RSSI:
-42
06/17/2014 12:58:42 HTTP No Error: SEP203A07FDFC30.cnf.xml
06/17/2014 12:58:45 Registered to 2001:420:305:2002:332::2
06/17/2014 13:38:39 Phone Off Error: Could not power off; Power over Ethernet is required to
power off the phone.
06/19/2014 15:04:16 HTTP No Error: SEP203A07FDFC30.cnf.xml
06/19/2014 15:04:17 Web Access Enabled
06/19/2014 15:04:18 Apply config requested by CUCM
06/19/2014 15:04:18 CUCM reset TCP connection
06/19/2014 15:04:20 Registered to 2001:420:305:2002:332::2
06/19/2014 15:09:06 HTTP No Error: SEP203A07FDFC30.cnf.xml
06/19/2014 15:09:06 Web Access Enabled
06/19/2014 15:09:06 Apply config requested by CUCM
06/19/2014 15:09:07 CUCM reset TCP connection
06/19/2014 15:09:08 Registered to 2001:420:305:2002:332::2
06/19/2014 15:14:42 HTTP No Error: SEP203A07FDFC30.cnf.xml
06/19/2014 15:14:43 Apply config requested by CUCM
06/19/2014 15:14:43 CUCM 2001:420:305:2002:332::2 closed TCP connection
```

WLAN Information

Connection status, WLAN signal indicator, and neighbor list information can be displayed locally on the Cisco DX Series.

Connection Status

The current connection information including status, security type, signal strength, link speed, and IP address can be displayed if the currently connected network is tapped.



xroads

Status Connected

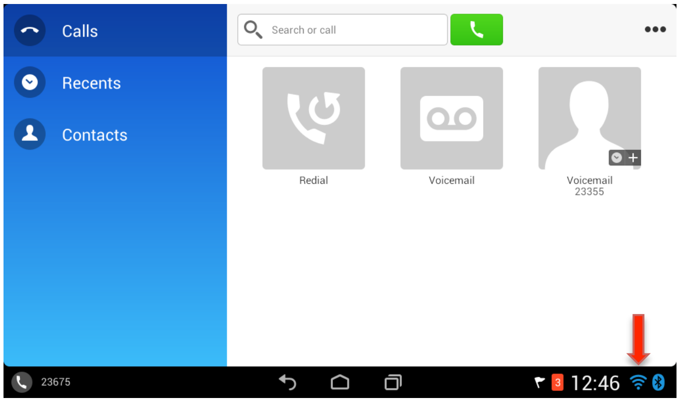
Signal strength Excellent

Link speed 150Mbps

Security 802.1x EAP

WLAN Signal Indicator

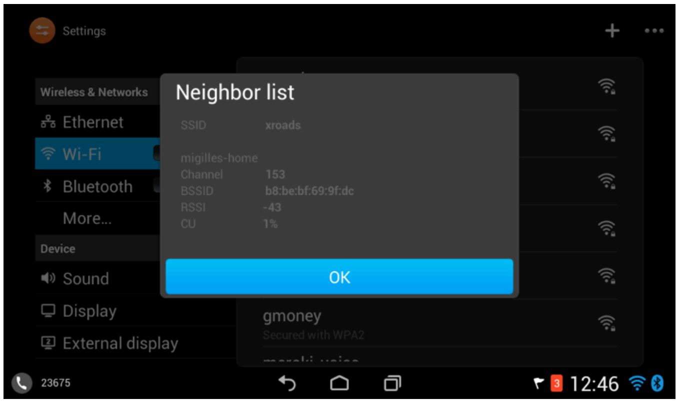
The WLAN signal indicator will always be visible in the lower right corner.



Neighbor List

The Cisco DX Series will display the current neighbors in the neighbor list menu.

To view the neighbor list, select **…** in the upper right corner from **Settings > Wireless & Networks > Wi-Fi**, then select **Neighbor list**.



Neighbor list

SSID xroads

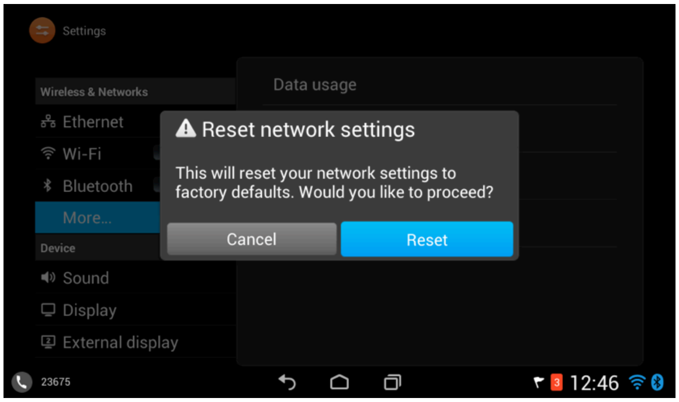
migilles-home
Channel 153
BSSID b8:be:bf:69:9f:dc
RSSI -43
CU 1%

For more information, refer to the Cisco DX Series Administration Guide at this URL:

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

Reset Network Settings

Network settings can be reset by selecting **Reset network settings** from **Settings > Wireless & Networks > More…**.

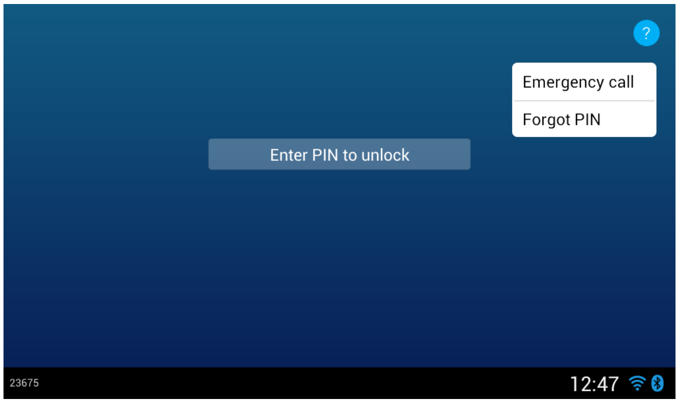


Reset network settings

This will reset your network settings to factory defaults. Would you like to proceed?

Reset a Forgotten Pin

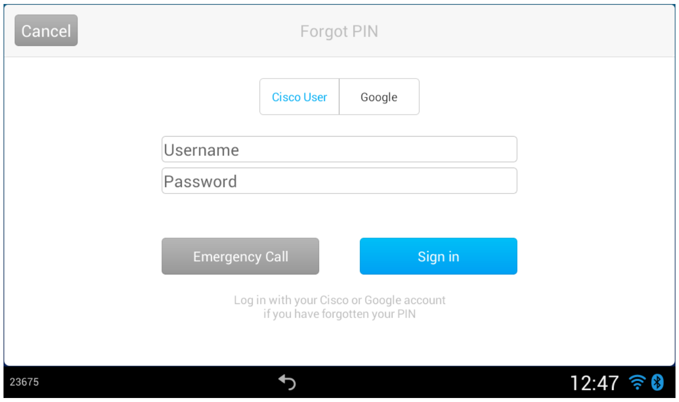
If the pin is forgotten, it can be reset by selecting **?** then **Forgot PIN** at the unlock screen.



After **Forgot PIN** is selected, a screen to authenticate via one of the following accounts will be displayed.

- Cisco User
- Google

When the authentication is successful, the pin can then be reset.



Log in with your Cisco or Google account
if you have forgotten your PIN

Remote Lock and Wipe

An administrator of the Cisco Unified Communications Manager has the capability to lock or wipe any Cisco DX Series remotely.

Select the **Lock** option on the phone configuration page if wanting to remotely lock the Cisco DX Series, which will force the user to enter their pin to gain access to the Cisco DX Series.

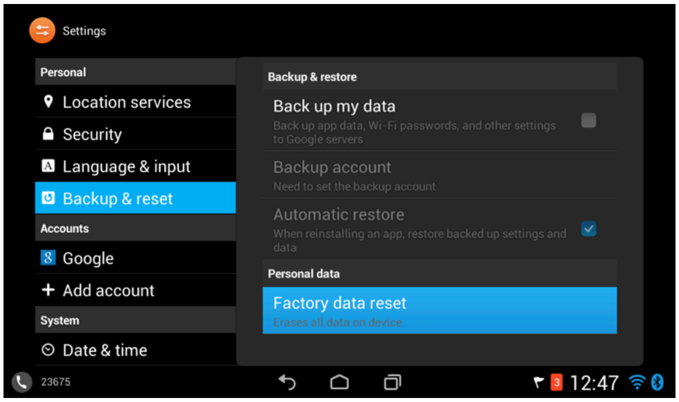
Select the **Wipe** option on the phone configuration page if wanting to remotely erase all the data on the Cisco DX Series.

Enabling **Always on VPN** can help to ensure that the Cisco DX Series is always online in order to lock or wipe the device.

Restoring Factory Defaults

All data can be erased from the Cisco DX Series, by selecting **Factory data reset** in **Settings > Backup & reset**.

A confirmation screen will appear where **Reset device** must be selected to proceed with the factory data reset.

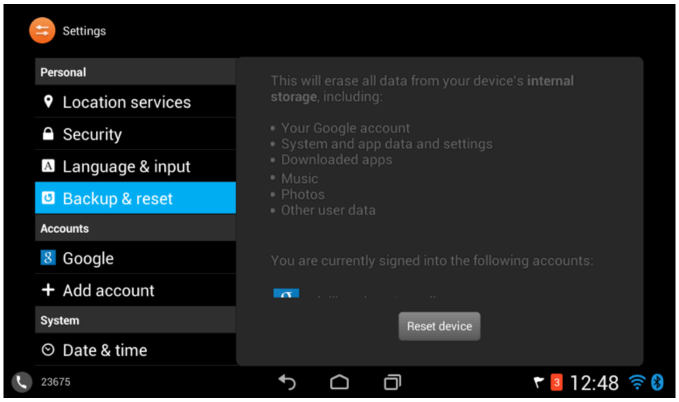


Back up my data
Back up app data, Wi-Fi passwords, and other settings to Google servers

Backup account
Need to set the backup account

Automatic restore ☑
When reinstalling an app, restore backed up settings and data

Factory data reset
Erases all data on device



This will erase all data from your device's **internal storage**, including:

- Your Google account
- System and app data and settings
- Downloaded apps
- Music
- Photos
- Other user data

You are currently signed into the following accounts:

If the Cisco DX Series is not able to boot properly, a factory reset can also be initiated via the following procedure:

- Turn the device off by disconnecting the power.
- Press and hold the # key, then connect the power supply.
- Keep the # key held until the message LED becomes solid.
- When the message LED becomes solid, release the # key.
- Press 1 2 3 4 5 6 7 8 9 * 0 #.
- The message LED will then flash 3 times to indicate the factory reset sequence has been accepted.
- The Cisco DX Series will then continue the normal boot process and have the factory settings restored.

To boot the alternate image, perform the following procedure.

- Turn the device off by disconnecting the power.
- Press and hold the * key, then connect the power supply.
- Keep the * key held until the message LED becomes solid.
- When the message LED flashes 3 times, release the * key.
- The Cisco DX Series will then boot using the alternate image.

Device Debugging

Device debugging can optionally be enabled by accessing the Cisco DX Series via SSH or Android Debug Bridge (ADB) shell.

If wanting to use ADB, ensure it is enabled in the Cisco DX Series configuration within Cisco Unified Communications Manager.
Download the Android SDK, which contains ADB from the following location.

http://developer.android.com/sdk

If wanting to use SSH, ensure a username and password are configured in the SSH section of the Cisco DX Series configuration within Cisco Unified Communications Manager.
The local login = cisco and the password = default.

Capturing a Screenshot of the Device Display

The current display can be captured by browsing to http://x.x.x.x/CGI/Screenshot, where **x.x.x.x** is the IP address of the Cisco DX Series. At the prompt enter the username and password for the account that the Cisco DX Series is associated to in Cisco Unified Communications Manager.

Healthcare Environments

This product is not a medical device and uses an unlicensed frequency band that is susceptible to interference from other devices or equipment.

Accessories

The following accessories are available for the Cisco DX Series.

3rd Party Accessories

- Bluetooth Headsets	www.plantronics.com
	www.jabra.com
	www.jawbone.com
	www.vxicorp.com
	www.motorola.com

Additional Documentation

Cisco DX Series Data Sheets

http://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/datasheet-listing.html

Cisco DX Series Administration Guides

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

Cisco DX Series User Guides

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

Cisco DX Series Release Notes

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html

Cisco DX Series Software

http://software.cisco.com/download/navigator.html?mdfid=284711383

Cisco Unified Communications Manager

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Unified Communications Manager Express

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

Cisco Voice Software

http://software.cisco.com/download/navigator.html?mdfid=278875240

Real-Time Traffic over Wireless LAN SRND

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

Cisco Unified Communications SRND

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html

Cisco Unified Wireless LAN Controller Documentation

http://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html

Cisco DX Series Wireless LAN Deployment Guide

Cisco Autonomous Access Point Documentation

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4-25d-JA/Configuration/guide/cg_12_4_25d_JA.html