



Cisco Unified Wireless IP Phone 792xG + Cisco Meraki Wireless LAN Deployment Guide



The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are adaptable for all mobile professionals, from users on the move within an office environment to nurses and doctors in a healthcare environment to associates working in the warehouse, on the sales floor, or in a call center. Staff, nurses, doctors, educators, and IT personnel can be easily reached when mobile utilizing a Bluetooth headset. The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are Bluetooth 2.0 + EDR (Enhanced Data Rate) compliant and supports both the headset and hands-free profiles. The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are MIL-STD-810F, Method 516.5, Procedure I compliant. The Cisco Unified Wireless IP Phone 7925G and 7926G is IP54 rated protecting it from dust, liquid splashes and moisture, where the Cisco Unified Wireless IP Phone 7925G-EX is IP64 rated for complete dust protection and also certified for use in explosive and hazardous environments.

The Cisco Meraki Wireless LAN solution provides powerful and intuitive centralized management via the cloud, while eliminating the traditional on-site wireless LAN controllers. The Cisco Meraki cloud seamlessly manages campus-wide Wi-Fi deployments and distributed multi-site networks with zero-touch access point provisioning, network-wide visibility and control, cloud-based RF optimization, seamless firmware updates and more. With an intuitive browser-based user interface, Cisco Meraki WLANs can be configured in minutes without prior training or dedicated staff.

This guide provides information and guidance to help the network administrator deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G successfully in a Cisco Meraki wireless LAN environment.

Revision History

Date	Comments
10/04/13	1.4(5) Release
07/16/14	1.4(5)SR1 Release
07/14/15	1.4(6) Release

Contents

Solution Overview	6
<i>Cisco Unified Wireless IP Phone 792xG Models</i>	<i>6</i>
World Mode (802.11d).....	9
Radio Characteristics	10
Bluetooth	11
Protocols.....	12
Language Support	12
Call Control Requirements.....	13
<i>Cisco Meraki Access Point Models</i>	<i>14</i>
Antennas.....	14
Site Survey.....	15
Security	16
<i>Protected Extensible Authentication Protocol (PEAP).....</i>	<i>17</i>
<i>Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)</i>	<i>17</i>
<i>Fast Secure Roaming (FSR).....</i>	<i>19</i>
<i>EAP and User Database Compatibility.....</i>	<i>19</i>
Power Management.....	19
<i>Protocols</i>	<i>20</i>
<i>Delivery Traffic Indicator Message (DTIM)</i>	<i>21</i>
<i>Scan Modes.....</i>	<i>21</i>
Quality of Service (QoS)	21
<i>Configuring QoS in Cisco Unified Communications Manager.....</i>	<i>22</i>
<i>Configuring QoS Policies for the Network.....</i>	<i>22</i>
Configuring Switch Ports.....	22
<i>Call Admission Control.....</i>	<i>23</i>
Roaming.....	23
<i>Interband Roaming.....</i>	<i>24</i>
Multicast.....	24
Designing the Wireless LAN.....	25
<i>Planning Channel Usage.....</i>	<i>25</i>
5 GHz (802.11a).....	25
2.4 GHz (802.11b/g)	26
Signal Strength and Coverage.....	26
<i>Configuring Data Rates.....</i>	<i>28</i>
<i>Call Capacity.....</i>	<i>28</i>
<i>Transmit Power</i>	<i>29</i>
<i>Rugged Environments.....</i>	<i>29</i>
Multipath	30
<i>Verification with Site Survey Tools</i>	<i>31</i>
Cisco 792xG Neighbor List	32

Cisco 792xG Site Survey	32
Configuring Cisco Unified Communications Manager.....	33
<i>Phone Button Templates</i>	33
<i>Sofikey Templates</i>	33
<i>Security Profiles</i>	34
<i>G.722 Advertisement</i>	35
<i>Common Settings</i>	35
<i>Audio Bit Rates</i>	35
<i>Product Specific Configuration Options</i>	36
Scanner Commands for Cisco 7926G	44
Configuring the Cisco Meraki WLAN	46
<i>Creating the Wireless Network</i>	46
<i>SSID Configuration</i>	48
<i>Radio Settings</i>	51
<i>Traffic Shaping</i>	52
<i>Monitoring Clients</i>	53
Configuring the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G	54
<i>Wireless LAN Settings</i>	55
<i>USB Settings</i>	59
<i>Installing Certificates</i>	60
<i>Using Templates to Configure Phones</i>	67
<i>Using the Bulk Deployment Utility</i>	68
Bulk Export	71
Default Export.....	72
Pushing Configuration Files to the Cisco 792xG.....	72
<i>Local Phone Book and Speed Dials</i>	72
<i>Bluetooth Settings</i>	74
<i>Increased Font</i>	75
<i>Using the Cisco Unified Wireless IP Phone 7925G Desktop Charger</i>	76
Bluetooth Pairing	77
Docking	77
<i>Using Phone Designer</i>	78
<i>Upgrading Firmware</i>	79
Hardware Compatibility	81
IP Phone Services	82
<i>Extensible Markup Language (XML)</i>	82
XSI Audio Path Control	83
<i>Java Mobile Information Device Profile (MIDP)</i>	84
Troubleshooting	85
<i>Device Homepage</i>	85
<i>Device Information</i>	85
Cisco Unified Wireless IP Phone 792xG + Cisco Meraki Wireless LAN Deployment Guide	4

<i>Wireless LAN Information</i>	86
<i>Network Information</i>	87
<i>Stream Statistics</i>	88
<i>Wireless LAN Statistics</i>	89
<i>Network Statistics</i>	90
<i>Cisco 7926G Barcode Status Messages</i>	92
<i>Phone Logs</i>	92
Trace Settings.....	92
Trace Modules	93
Trace Levels.....	94
Trace Logs.....	94
<i>Radio Status Indicator</i>	95
<i>Hardware Diagnostics</i>	96
<i>Firmware Recovery</i>	96
<i>Restoring Factory Defaults</i>	97
<i>Capturing a Screenshot of the Phone Display</i>	97
Healthcare Environments	98
Accessories	98
Additional Documentation	101

Solution Overview

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are IEEE 802.11a/b/g wireless IP phones that leverage the Cisco Meraki Wireless LAN to provide mobile voice communications within enterprises. Cisco's implementation permits time sensitive applications such as voice to operate efficiently across campus wide wireless LAN (WLAN) deployments.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are not medical devices and utilize an unlicensed RF spectrum that is susceptible to interference from other devices or equipment. 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in order to take advantage of the 802.11a data rates available. Despite the optimizations that Cisco have implemented in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is not intended as a medical device and should not be used to make clinical decisions.

Cisco Unified Wireless IP Phone 792xG Models

Cisco currently offers four Cisco Unified Wireless IP Phone 7925G models, one Cisco Unified Wireless IP Phone 7925G-EX model and one Cisco Unified Wireless IP Phone 7926G model.

The Cisco Unified Wireless IP Phone 7925G and 7926 models are grey in color, where the Cisco Unified Wireless IP Phone 7925G-EX is yellow in color.

All Cisco Unified Wireless IP Phone 7925G models support 802.11d therefore can adapt to local channels and transmit powers per region as necessary, where channels operating on frequencies 2.412 - 2.484 GHz and 5.180 GHz - 5.805 GHz can be utilized if available.

The Cisco Unified Wireless IP Phone 7925G-EX, and Cisco Unified Wireless IP Phone 7926G are configured like the Cisco Unified Wireless IP Phone 7925G -W model, which requires an 802.11d enabled access point.

The regulatory domain can be identified by navigating to **Settings > Model Information > WLAN Regulatory Domain** and then referencing the Regulatory Domain number in the table below.

7925G

Part Number	Regulatory Domain	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
CP-7925G-A-K9	1050 (Americas)	2.4 GHz = 2 dBi 5 GHz = 3 dBi	2.412 - 2.462 GHz	11	1-11
			5.180 - 5.240 GHz	4	36,40,44,48
			5.260 - 5.320 GHz	4	52,56,60,64
			5.500 - 5.700 GHz	8	100-140
			5.745 - 5.805 GHz	4	149,153,157,161
CP-7925G-E-K9	3051 (Europe)	2.4 GHz = 2 dBi 5 GHz = 3 dBi	2.412 - 2.472 GHz	13	1-13
			5.180 - 5.700 GHz	16	36-48,52-64,100-140
CP-7925G-P-K9	4157 (Japan)	2.4 GHz = 2 dBi 5 GHz = 3 dBi	2.412 - 2.472 GHz	13 (802.11g)	1-13
			2.412 - 2.484 GHz	14 (802.11b)	1-14

			5.180 - 5.700 GHz	16	36-48,52-64,100-140
CP-7925G-W-K9	5252 (Rest of World)	2.4 GHz = 2 dBi 5 GHz = 3 dBi	Uses 802.11d to identify available channels and transmit powers. Channels operating at 2.412 GHz - 2.484 GHz and 5.180 GHz - 5.805 GHz are supported.		

7925G-EX

Part Number	Regulatory Domain	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
CP-7925G-EX-K9	5252	2.4 GHz = 2 dBi 5 GHz = 3 dBi	2.412 - 2.484 GHz	14	1-14
			5.180 - 5.240 GHz	4	36,40,44,48
			5.260 - 5.320 GHz	4	52,56,60,64
			5.500 - 5.700 GHz	11	100-140
			5.745 - 5.805 GHz	4	149,153,157,161

7926G

Part Number	Regulatory Domain	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
CP-7926G -K9	5252	2.4 GHz = 2 dBi 5 GHz = 6 dBi	2.412 - 2.484 GHz	14	1-14
			5.180 - 5.240 GHz	4	36,40,44,48
			5.260 - 5.320 GHz	4	52,56,60,64
			5.500 - 5.700 GHz	11	100-140
			5.745 - 5.805 GHz	4	149,153,157,161

Note: The Cisco Unified Wireless IP Phone 7921G is not supported with the Cisco Meraki WLAN solution.

Cisco Meraki offers access points for the American and European countries only.

The US versions of Cisco Meraki access points do not offer UNII-2 and UNII-2 extended channel support.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G do not support channel 165.

7925G-EX Certifications

The Cisco Unified Wireless IP Phone 7925G-EX has both Atmospheres Explosibles (ATEX) Zone 2/Class 22 and Canadian Standards Association (CSA) Class1/Division II certifications in order to allow it to be used in hazardous and explosive environments.

Atmospheres Explosibles (ATEX) Zone 2/Class 22 Certification

Organizations in the European Union must follow the ATEX directives to protect employees from explosion risk in areas with an explosive atmosphere.

- **ATEX 95 equipment directive 94/9/EC**
Equipment and protective systems intended for use in potentially explosive atmospheres.
- **ATEX 137 workplace directive 99/92/EC**

Minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres.

Areas classified into zones (0, 1, 2 for gas-vapor-mist and 20, 21, 22 for dust) must be protected from effective sources of ignition. Equipment and protective systems intended to be used in zoned areas must meet the requirements of the directive. Zone 0 and 20 require Category 1 marked equipment, zone 1 and 21 required Category 2 marked equipment and zone 2 and 22 required Category 3 marked equipment. Zone 0 and 20 are the zones with the highest risk of an explosive atmosphere being present.

Certification ensures that the equipment is fit for its intended purpose and that adequate information is supplied with it to ensure that it can be used safely.

Canadian Standards Association (CSA) Class I/Division II Certification

Laws and regulations in most municipalities, states, and provinces in North America require certain products to be tested to a specific standard or group of standards when they are to be deemed intrinsically safe when used in an explosive environment.

In North America, hazardous locations have traditionally been defined by the following combination of Class and Division:

- **Class I** - A location where a quantity of flammable gas or vapor, sufficient to produce an explosive or ignitable mixture, may be present in the air.
 - **Class II** - A location made hazardous by the presence of combustible or electrically conductive dust, including Groups E (metal dust), F (coal dust) and G (grain dust).
 - **Class III** - A location made hazardous by the presence of easily ignitable fibers in the air, but not likely in sufficient quantities to produce ignitable mixtures.
-
- **Division 1** - A location where a classified hazard is likely to exist.
 - **Division 2** - A location where a classified hazard does not normally exist but is possible under abnormal conditions.

Internationally (and more recently in North America, for Class I hazardous locations), areas where explosive gas atmospheres are likely to be present are divided into three IEC-defined Zones:

- **Zone 0** - An area in which an explosive gas atmosphere is continuously present or present for long periods.
- **Zone 1** - An area in which an explosive gas atmosphere is likely to occur in normal operation.
- **Zone 2** - An area in which an explosive gas atmosphere does not normally exist.

7926G Barcode Scanner

The Cisco Unified Wireless IP Phone 7926G leverages the Cisco Unified Wireless IP Phone 7925G design, but with the addition of a 2D barcode scanner.

A Java MIDlet application is required to invoke the scanner.

Java MIDP support is included in the initial 1.4(1)SR1 release for the Cisco Unified Wireless IP Phone 7926G.

The Java MIDlet for the Cisco Unified Wireless IP Phone 7926G will be a custom built application for a customer, where lookups can be queried against their own databases.

The Cisco Unified Wireless IP Phone 7926G supports both the Basic and Extended barcode symbology groups.

- **Basic** - Code 39, Code 128, DataMatrix, EAN-13, UCC/EAN128, UPC, PDF 417
- **Extended** - Code 39, Code 128, DataMatrix, EAN-13, UCC/EAN128, UPC, PDF 417, Aztec, Codabar, Code 11, Code 93/93i, EAN Add-On 2, GS1 Databar, Interleave 2 of 5, Matrix 2 of 5, Maxicode, Micro PDF 417, Plessey, QRCode, Standard 2 of 5, Telepen

See the [Product Specific Configuration Options](#) section for information on how to configure barcode options.

For more info on creating Java MIDlet applications for the Cisco Unified Wireless IP Phone 7926G, refer to the following URL.

<https://developer.cisco.com/web/jmapi/home>



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.

If using the Cisco Unified Wireless IP Phone 7925G World (-W) model, the Cisco Unified Wireless IP Phone 7925G-EX or Cisco Unified Wireless IP Phone 7926G model, then it is required to enable 802.11d.

All Cisco Unified Wireless IP Phone 7925G models give precedence to 802.11d to determine the channels and transmit powers to use and inherits its client configuration from the associated access point.

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will passively scan DFS channels first before engaging in active scans of those channels.

If 802.11d information is not available from the access point, then the Cisco Unified Wireless IP Phone 7925G (-A, -E, -P) model uses the locally configured regulatory domain. If the Cisco Unified Wireless IP Phone 7925G -A, -E or -P model is taken to another country, where the access point uses a different regulatory domain, then 802.11d will be required for the Cisco Unified Wireless IP Phone 7925G to operate successfully.

If using 2.4 GHz (802.11b/g) and 802.11d is not enabled, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can attempt to use channels 1-11 and reduced transmit power.

Note: World Mode must be enabled manually for Cisco Meraki access points by selecting the necessary country code from drop-down menu in the **Power and Country Settings** menu located under **Configure > Radio Settings**.

Power and country settings

Country ⓘ

United States

Regulatory domain: FCC

Supported Countries

Below are the countries and their 802.11d codes that are supported by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Argentina (AR)

Australia (AU)

Austria (AT)

Belgium (BE)

Brazil (BR)

Bulgaria (BG)

India (IN)

Indonesia (ID)

Ireland (IE)

Israel (IL)

Italy (IT)

Japan (JP)

Poland (PL)

Portugal (PT)

Puerto Rico (PR)

Romania (RO)

Russian Federation (RU)

Saudi Arabia (SA)

<u>Canada (CA)</u>	<u>Korea (KR)</u>	<u>Singapore (SG)</u>
<u>Chile (CL)</u>	<u>Latvia (LV)</u>	<u>Slovakia (SK)</u>
<u>Colombia (CO)</u>	<u>Liechtenstein (LI)</u>	<u>Slovenia (SI)</u>
<u>Costa Rica (CR)</u>	<u>Lithuania (LT)</u>	<u>South Africa (ZA)</u>
<u>Cyprus (CY)</u>	<u>Luxembourg (LU)</u>	<u>Spain (ES)</u>
<u>Czech Republic (CZ)</u>	<u>Malaysia (MY)</u>	<u>Sweden (SE)</u>
<u>Denmark (DK)</u>	<u>Malta (MT)</u>	<u>Switzerland (CH)</u>
<u>Estonia (EE)</u>	<u>Mexico (MX)</u>	<u>Taiwan (TW)</u>
<u>Finland (FI)</u>	<u>Monaco (MC)</u>	<u>Thailand (TH)</u>
<u>France (FR)</u>	<u>Netherlands (NL)</u>	<u>Turkey (TR)</u>
<u>Germany (DE)</u>	<u>New Zealand (NZ)</u>	<u>Ukraine (UA)</u>
<u>Gibraltar (GI)</u>	<u>Norway (NO)</u>	<u>United Arab Emirates (AE)</u>
<u>Greece (GR)</u>	<u>Oman (OM)</u>	<u>United Kingdom (GB)</u>
<u>Hong Kong (HK)</u>	<u>Panama (PA)</u>	<u>United States (US)</u>
<u>Hungary (HU)</u>	<u>Peru (PE)</u>	<u>Venezuela (VE)</u>
<u>Iceland (IS)</u>	<u>Philippines (PH)</u>	<u>Vietnam (VN)</u>

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, ranges, and receiver sensitivity info for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

5 GHz - 802.11a	Data Rate	Modulation	Range	Receiver Sensitivity
Max Tx Power = 16 dBm	6 Mbps	OFDM - BPSK	604 ft (184 m)	-91 dBm
	9 Mbps	OFDM - BPSK	604 ft (184 m)	-90 dBm
	12 Mbps	OFDM - QPSK	551 ft (168 m)	-88 dBm
	18 Mbps	OFDM - QPSK	545 ft (166 m)	-86 dBm
	24 Mbps	OFDM - 16 QAM	512 ft (156 m)	-82 dBm
	36 Mbps	OFDM - 16 QAM	420 ft (128 m)	-80 dBm
	48 Mbps	OFDM - 64 QAM	322 ft (98 m)	-77 dBm
	54 Mbps	OFDM - 64 QAM	289 ft (88 m)	-75 dBm
2.4 GHz - 802.11g	Data Rate	Modulation	Range	Receiver Sensitivity
Max Tx Power = 16 dBm	6 Mbps	OFDM - BPSK	709 ft (216 m)	-91 dBm
	9 Mbps	OFDM - BPSK	650 ft (198 m)	-90 dBm
	12 Mbps	OFDM - QPSK	623 ft (190 m)	-87 dBm
	18 Mbps	OFDM - QPSK	623 ft (190 m)	-86 dBm
	24 Mbps	OFDM - 16 QAM	623 ft (190 m)	-82 dBm
	36 Mbps	OFDM - 16 QAM	495 ft (151 m)	-80 dBm
	48 Mbps	OFDM - 64 QAM	413 ft (126 m)	-77 dBm
	54 Mbps	OFDM - 64 QAM	394 ft (120 m)	-76 dBm

2.4 GHz - 802.11b	Data Rate	Modulation	Range	Receiver Sensitivity
Max Tx Power = 17 dBm	1 Mbps	DSSS - BPSK	1,010 ft (308 m)	-96 dBm
	2 Mbps	DSSS - QPSK	951 ft (290 m)	-85 dBm
	5.5 Mbps	DSSS - CCK	919 ft (280 m)	-90 dBm
	11 Mbps	DSSS - CCK	902 ft (275 m)	-87 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.

See the [Designing the Wireless LAN for Voice](#) section for more information on signal requirements.

Bluetooth

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support Bluetooth 2.0 + EDR 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Up to ten headsets can be paired, where the previously connected headset is given priority.

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

Bluetooth utilizes the 2.4 GHz frequency just like 802.11b/g 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support the Bluetooth Headset and Hands-Free Profiles.

Headset Profile (HP)

With Bluetooth Headset Profile (HSP) support, the following features can be available if supported by the Bluetooth headset.

- Ring
- Answer a call
- End a call
- Volume Control

Hands-Free Profile (HFP)

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

- Last Number Redial
- Call Waiting
- Divert / Reject
- 3 way calling (Hold & Accept and Release & Accept)
- Speed Dialing

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

Coexistence (802.11b/g + Bluetooth)

If using Coexistence where 802.11b/g 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 + Bluetooth), call capacity is reduced due to the utilization of CTS to protect the 802.11g 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 if using Bluetooth due to 802.11b/g and Bluetooth both utilizing 2.4 GHz, but also due to the above limitations.

Protocols

Supported voice and wireless LAN protocols include the following:

- CCX v4
- Wi-Fi MultiMedia (WMM)
- Unscheduled Auto Power Save Delivery (U-APSD)
- Traffic Specification (TSPEC)
- Traffic Classification (TCLAS)
- Skinny Call Control Protocol (SCCP)
- Real Time Protocol (RTP)
- G.711, G.722, G.729, iLBC
- Real Time Control Protocol (RTCP)
- Cisco Discovery Protocol (CDP)
- Syslog

Language Support

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support the following languages.

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

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

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

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

Call Control Requirements

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G utilize Skinny Client Control Protocol (SCCP) for call control with the following communications platforms.

7925G and 7925G-EX

- Cisco Unified Communications Manager (CUCM)
Minimum = 4.3
Recommended = 8.6 and later
- Cisco Unified Communications Manager Express (CUCME)
Minimum = 4.3
Recommended = 8.6 and later
- Cisco Unified Survivable Remote Site Telephony (SRST)
Minimum = 4.3
Recommended = 8.6 and later

7926G

- Cisco Unified Communications Manager (CUCM)
Minimum = 7.1(5)
Recommended = 8.6 and later
- Cisco Unified Communications Manager Express (CUCME)
Minimum = 8.6
Recommended = 8.6 and later
- Cisco Unified Survivable Remote Site Telephony (SRST)
Minimum = 8.6
Recommended = 8.6 and later

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 Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G device support.

Device packages for Cisco Unified Communications Manager are available at the following location.

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

Cisco Meraki Access Point Models

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are currently supported on the Cisco Meraki MR18, MR24, MR26, MR32, and MR34 access point platforms only.



<https://meraki.cisco.com/products/wireless#models>

Note: The Cisco Meraki MR12, MR16, and Z1 access point platforms are not certified for use with Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G deployments.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can take advantage of Cisco Client Extensions (CCX) enabled access points, however Cisco Meraki access points do not support CCX currently.

See the following link for more info on CCX.

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

Antennas

All indoor Cisco Meraki access points have internal antennas and all outdoor Cisco Meraki access points require external antennas.

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.

Site Survey

Before deploying the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G into a production environment, a site survey must be completed by a Cisco certified partner with the advanced wireless LAN specialization. During the site survey the RF spectrum can be analyzed to determine which channels are usable in the desired frequency 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 frequency band for operation and even more highly recommended when the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G 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.

The wireless LAN must be validated to ensure it meets the requirements to deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can hold a signal for at least 5 seconds.

Channel Utilization

Channel Utilization levels should be kept under 50%.

If using the 7925G, 7925G-EX, and 7926G phone, this is provided via the QoS Basic Service Set (QBSS), which equates to around 105.

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can meet 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 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

Security

When deploying a wireless LAN, security is essential.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support the following wireless security features.

WLAN Authentication

- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2)
- Open

WLAN Encryption

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G also support 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
- Settings Access (can limit user access to configuration menus)
- Locked network profiles
- Administrator password

Note: Cisco Meraki access points do not support EAP-FAST, LEAP, Shared Key, or WEP.

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 is the current supported inner authentication protocol (PEAP-GTC is not supported).

The screenshot shows a configuration panel for PEAP. At the top, there is a dropdown menu with a checkmark and the text 'Allow PEAP'. Below this, under the heading 'PEAP Inner Methods', there are several options: 'Allow EAP-TLS' (unchecked), 'Allow EAP-MS-CHAPv2' (checked), 'Allow Password Change' (checked) with a 'Retries' field set to '1', and 'Allow EAP-GTC' (checked) with another 'Allow Password Change' (checked) and 'Retries' field set to '1'.

PEAP-MSCHAPv2 requires that a user account be created on the authentication server.

The authentication server can be validated via importing a certificate into the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

See the [Installing Certificates](#) section for more information.

Note: If using a 3rd party RADIUS server, ensure that PEAP v0 (MSCHAPv2) is enabled. PEAP v1 (GTC) is not supported.

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.

Either the internal Manufacturing Installed Certificate (MIC) or a User Installed certificate can be used for authentication.

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

▼ ☒ Allow EAP-TLS

☒ Enable Stateless Session resume

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

Session ticket time to live

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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:

Description:

Authentication Method List

☒ Certificate Based Certificate Authentication Profile

☐ Password Based

Additional Attribute Retrieval Search List

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

Available		Selected	
Internal Hosts	> <	AD1	⬆ ⬆ ⬇ ⬇
Internal Users			
NAC Profiler			
>> <<			

▶ Advanced Options

⚙ = Required fields

General

⚙ Name:

Description:

Certificate Definition

Principal Username X509 Attribute:

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

Name:

⚙ = Required fields

See the [Installing Certificates](#) section for more information.

For 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)

Cisco Meraki access points support Sticky Key Caching (SKC) that enables PMKID caching for fast roaming.

SKC can also be referred to as **WPA2 Sticky** or **Sticky PMKID Caching**.

When the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is utilizing SKC, the first roam to a new access point will not be a fast roam, however subsequent roams to that access point would be.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G maintain a list of cached PMKIDs.

Note: Cisco Meraki access points do not support Cisco Centralized Key Management (CCKM).

EAP and User Database Compatibility

The following chart displays the EAP and database configurations supported by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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

Power Management

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have an option for a standard or extended battery.

When connected to a Cisco Meraki access point, the standard battery (1100 mAh) can provide up to 90 hours of standby time or

up to 9.5 hours of talk time.

When connected to a Cisco Meraki access point, the extended battery (1400-1450 mAh) can provide up to 120 hours of standby time or up to 13 hours of talk time.

Since proxy ARP is not supported, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G must wake up at each Delivery Traffic Indicator Message (DTIM) period to check for incoming frames.

To optimize battery life, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize either U-APSD power save methods depending on the access point's capabilities and whether Wi-Fi MultiMedia (WMM) is enabled in the access point configuration or not.

When on call U-APSD or active mode will be utilized depending on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G call power save mode configuration.

When in idle (no active call), the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize U-APSD.

Battery life can be reduced when on call and using Coexistence (802.11b/g + Bluetooth).

The current battery technology allows for around 300-500 full charging cycles (charging from empty to full) before it will lose around 20-30% of its capacity, therefore the battery should be replaced every 2-3 years.

The table below lists the maximum on call and idle times for each 802.11 mode and battery type.

802.11 Mode	Call State	Standard Battery	Extended Battery
2.4 GHz	On Call	9.5	13
	Idle	90	120
5 GHz	On Call	9	11
	Idle	90	120

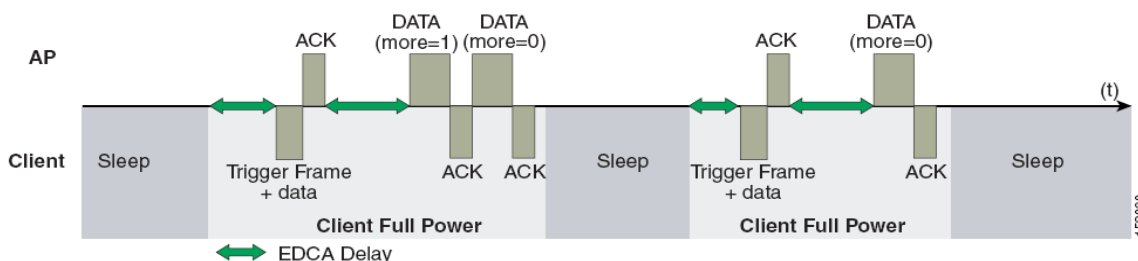
Protocols

Unscheduled Auto Power Save Delivery (U-APSD)

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize U-APSD (Unscheduled Auto Power Save Delivery) for power management as long as Wi-Fi MultiMedia (WMM) is enabled in the access point configuration and the call power save mode on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is set to U-APSD/PS-POLL.

U-APSD helps optimize battery life and reduces management overhead.

Below is a sample packet sequence when using U-APSD.



Active Mode

If the **Call Power Save Mode** is set to **None**, then the phone will use active mode and no power save will be used, which will reduce the battery life.

Delivery Traffic Indicator Message (DTIM)

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G uses the DTIM period to schedule wakeup periods to check for broadcast and multicast packets as well as any unicast packets.

Since proxy ARP is not supported by Cisco Meraki access points, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G must wake up at DTIM.

Cisco Meraki access points currently utilizes a DTIM period of **1** with a beacon period of **100 ms**; which is non-configurable.

The DTIM period is a tradeoff between battery life and multicast performance.

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.

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

Scan Modes

There are three different scan modes (**Auto**, **Continuous**, **Single AP**), which can be configured for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in the Cisco Unified Communications Manager.

When using multiple access points where seamless roaming is required, **Auto** (default) or **Continuous** scan mode should be enabled (**Single AP** scan mode should not be used if multiple access points exist).

Auto scan mode is the default scan mode, which will optimize idle battery life as well as offer seamless roaming.

When on an active call with **Auto** scan mode enabled, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will continuously be scanning. If in idle (not on an active call) and **Auto** scan mode is enabled, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will only start to scan once the scan threshold is met for the currently connected access point.

Continuous scan mode is recommended for environments where frequent roams occur or where smaller cells (pico cells) exist.

Continuous scan mode can also help with location tracking.

With **Continuous** scan mode, scans occur regardless of the current call state (idle or on call) or current access point signal level (RSSI). There will be a slight decrease in idle battery life when using **Continuous** scan mode in comparison to using **Auto** scan mode.

If using only one access point, select **Single AP** mode on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to reduce scanning and optimize battery life.

Quality of Service (QoS)

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

Below is the QoS and port information for voice and call control traffic used by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384 - 32767
Call Control	CS3 (24)	3	4	TCP 2000

Note: Cisco Meraki access points without any traffic shaping policy enabled, currently marks downstream voice frames as WMM UP 5 and call control frames as WMM UP 3.

Enable Differentiated Services Code Point (DSCP) trust on the switch.

For more information about TCP and UDP ports used by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 SCCP 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 SCCP packets as shown in the Enterprise Parameters Configuration page.

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 Switch Ports

Configure Cisco Meraki access point switch ports as well as any uplink switch ports for trust DSCP.

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

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

If utilizing Cisco IOS Switches, use the following switch port configuration for ports that have Cisco Meraki access points connected to enable DSCP trust.

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

Call Admission Control

Cisco Meraki access points does not support Call Admission Control / Traffic Specification (TSPEC).

Since TSPEC is not supported, TCLAS is also not supported.

Roaming

802.1x + Sticky Key Caching (SKC) is the recommended deployment model for all environment types where frequent roaming occurs.

WPA2 (AES) is recommended and required in order to utilize SKC.

802.1x without SKC can introduce delay during roaming due to its requirement for full re-authentication.

When SKC 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 first roam to a new access point will not be a fast roam, but subsequent roams will be.

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G manage 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
- Call Admission Control (not supported on Cisco Meraki access points)

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

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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.

Interband Roaming

Some deployments may use one frequency band for indoor (e.g. 5 GHz) and the other for outdoor coverage (e.g. 2.4 GHz). In this case, set the phone to either Auto-a or Auto-b/g mode, depending on the preferred frequency band.

For Auto-a and Auto-b/g modes, this is giving preference to one frequency band over another. At power on, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will scan all 2.4 GHz and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred frequency band if available. If the preferred frequency band is not available, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will try to use the less preferred frequency band if available. If the phone roams out of coverage of the preferred frequency band, where less preferred frequency band signal is available, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will attempt to associate to that less preferred frequency band.

Seamless interband roaming between 5 GHz and 2.4 GHz bands is supported as both frequency bands are now scanned simultaneously when on call or in idle if **Continuous** scan mode is enabled.

In order for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to roam from the preferred frequency band to the less preferred frequency band (e.g. roam to 2.4 GHz when configured for Auto-a mode), all access points in the preferred frequency band must have a signal lower than the preferred frequency band signal threshold as well as one access point in the less preferred frequency band meeting the RSSI differential threshold for roaming must be met. In order to roam back to the preferred frequency band, there must be at least one access point with adequate signal matching the preferred frequency band signal threshold.

It is recommended to perform a spectrum analysis to ensure that the desired frequency ranges can be enabled in order to perform seamless interband roaming.

Multicast

When enabling multicast in the wireless LAN, impacts on battery life, performance, and capacity must be considered.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G use the DTIM period to receive the queued broadcast and multicast packets.

If there are many packets queued up, then they client may have to stay awake longer thus potentially reducing battery life.

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

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure IGMP snooping is enabled as it will reduce unnecessary multicast traffic; enabled by default on Cisco Meraki MS Switches and Cisco IOS Switches.

Note: If using Coexistence where 802.11b/g 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Planning Channel Usage

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

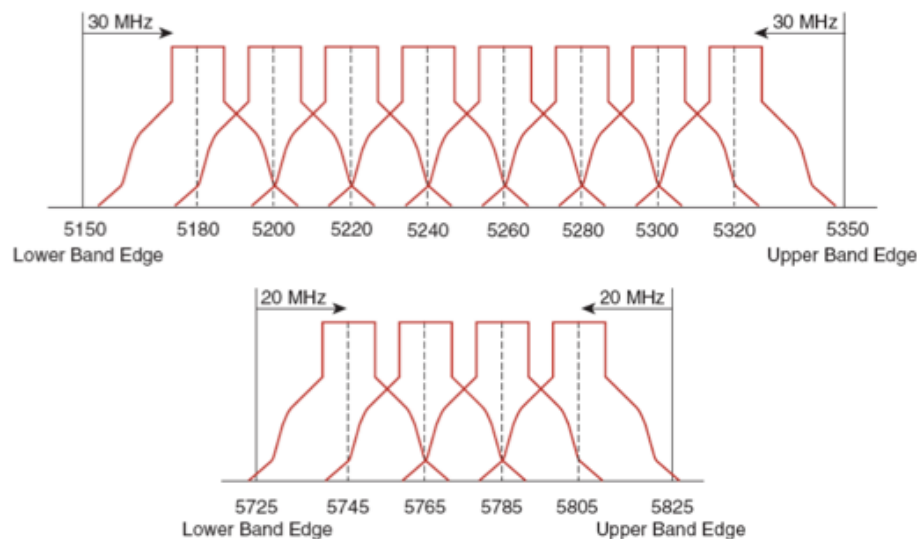
5 GHz (802.11a)

5 GHz is the recommended frequency band to utilize for operation of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support 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 (15 of the 23 possible channels).

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in the 802.11a 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 -67 dBm or better, while the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G also meet 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																UNII-3		

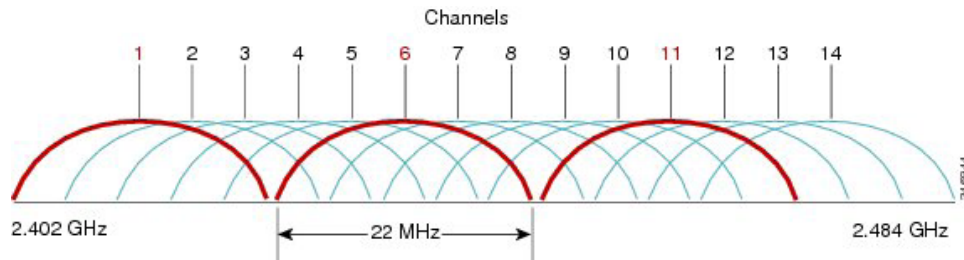
For 5 GHz, Cisco Meraki access points support 8 channels for the Americas and 16 channels for Europe.

Having many 5 GHz channels enabled in the wireless LAN can delay discovery of new access points.

2.4 GHz (802.11b/g)

In the 2.4 GHz (802.11b/g) 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in the 802.11b/g environment, which allows for seamless roaming.

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

Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G should always have a signal of -67 dBm or higher when using 5 GHz or 2.4 GHz, while the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G also meet 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%.

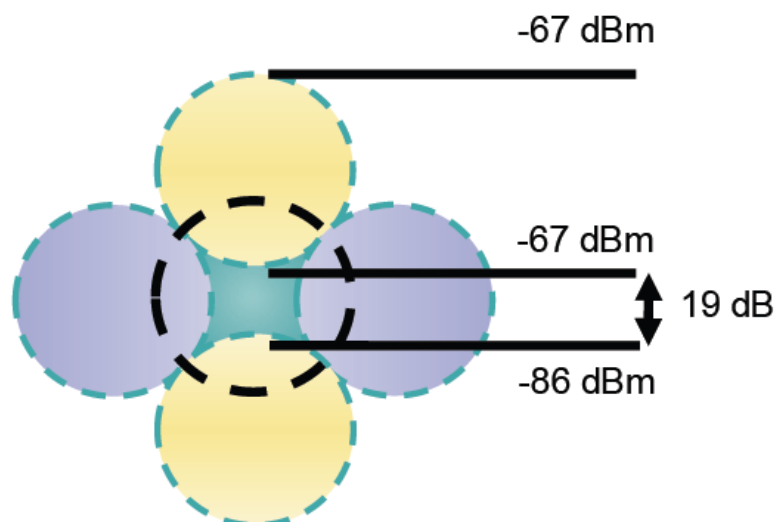
A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal should be maintained.

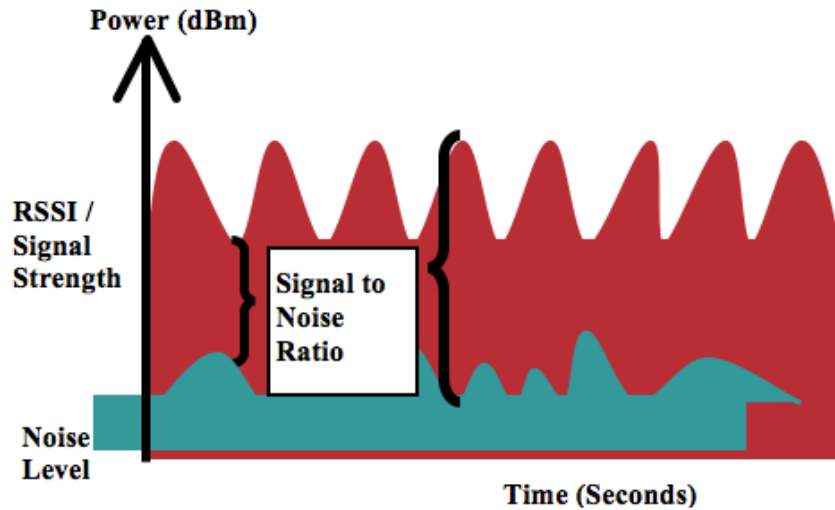
It is recommended to have at least two access points on non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.

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).

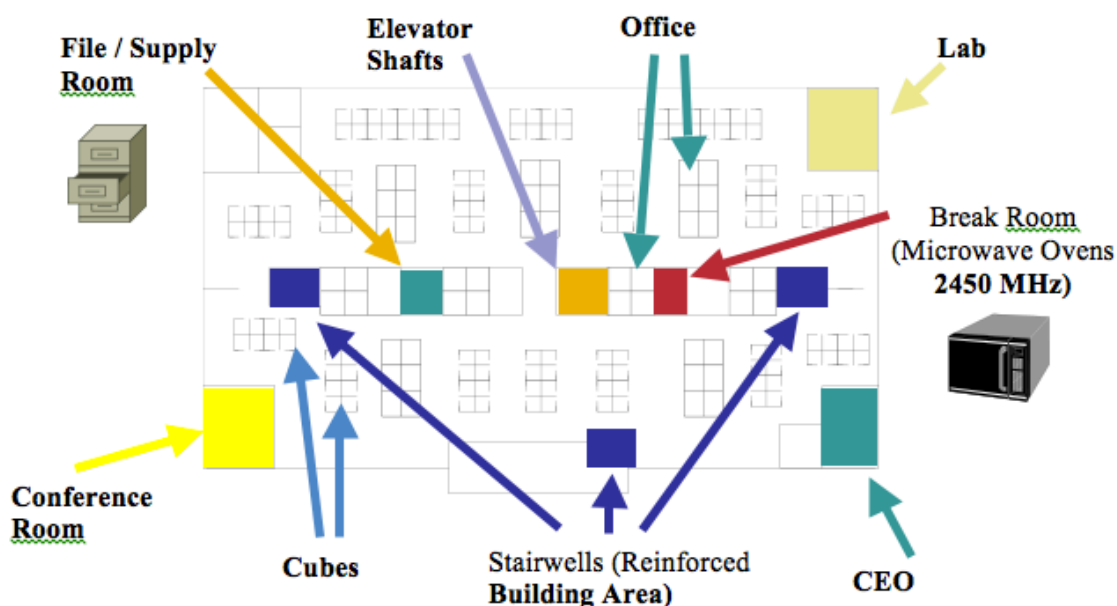
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

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. 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 technology provides more non-overlapping channels and typically lower initial RF utilization. For voice deployments, it is suggested to use 802.11a for voice and use 802.11b/g 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).



Configuring Data Rates

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

The recommended data rate configurations are the following:

802.11 Mode	Mandatory (Basic) Data Rates	Supported (Optional) Data Rates	Disabled Data Rates
802.11a	12 Mbps	18-24, <36-54> Mbps	6, 9, <36-54> Mbps
802.11b	11 Mbps	None	1, 2, 5.5 Mbps
802.11b/g	11 Mbps	12-24, <36-54> Mbps	1, 2, 5.5, 6, 9, <36-54> Mbps
802.11g	12 Mbps	18-24, <36-54> Mbps	1, 2, 5.5, 6, 9, 11, <36-54> Mbps

For a voice only application, data rates higher than 24 Mbps (36, 48 and 54 Mbps) provide no advantage from a capacity or throughput perspective and having these rates enabled 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.

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.

Capacity and throughput are reduced when lower rates are enabled.

Cisco Meraki access points do not have the capability to disable data rates below 11 Mbps.

Call Capacity

Design the network to accommodate the desired call capacity.

Can get up to 27 bi-directional voice streams for both 802.11a and 802.11g at a data rate of 24 Mbps or higher. To achieve this capacity, there must be minimal wireless LAN background traffic and radio frequency (RF) utilization.

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

Max # of Streams	802.11 Mode	Data Rate
13	802.11a or 802.11g + Bluetooth Disabled	6 Mbps
20	802.11a or 802.11g + Bluetooth Disabled	12 Mbps
27	802.11a or 802.11g + Bluetooth Disabled	24-54 Mbps

When using Coexistence (802.11b/g + Bluetooth), call capacity is reduced to the following:

Max # of Streams	802.11 Mode	Data Rate
4	802.11b/g + Bluetooth Enabled	11, <12-54> Mbps

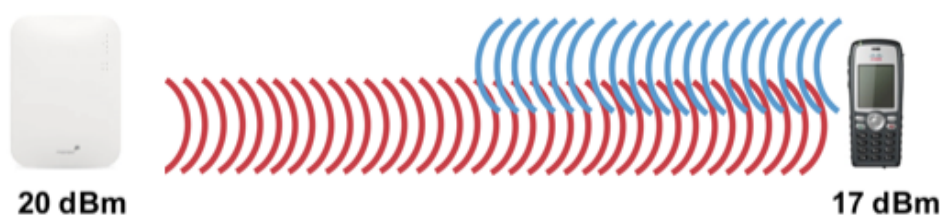
7	802.11g + Bluetooth Enabled	12, <18-54> Mbps
---	-----------------------------	------------------

Note: It is highly recommended to use 802.11a if using Bluetooth.

Transmit Power

To ensure packets are exchanged successfully between the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G and the access point, the transmit power should not exceed 17 dBm for 2.4 GHz and not exceed 16 dBm for 5 GHz.

Since Cisco Meraki access points do not support Cisco Client Extensions (CCX), Dynamic Transmit Power Control (DTPC) is also not supported, therefore the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize the maximum transmit power supported for the current channel and data rate.



Rugged Environments

When deploying the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G 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 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 and 3602i 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.

If 2.4 GHz must be used in some areas, either due to decreased 5 GHz coverage in some areas or due to range requirements, then it is recommended to set the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to Auto-a mode, which 5 GHz will be the preferred band, but can roam to 2.4 GHz as necessary.

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 of 12-54 Mbps 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 5 GHz is used for VoWLAN only, then it is also recommended to disable data rates above 24 Mbps (i.e. 36, 48, 54 Mbps) to increase first transmission success (e.g. 6 as mandatory, 12 and 24 as supported). If 5 GHz is also used for data, video or other applications, then is suggested to keep the higher data rates enabled (e.g. 6 as mandatory, 9, 12-54 as supported).

Transmit Power

Due to the potential of elevated multipath in rugged environments, the transmit power of the access point and Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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

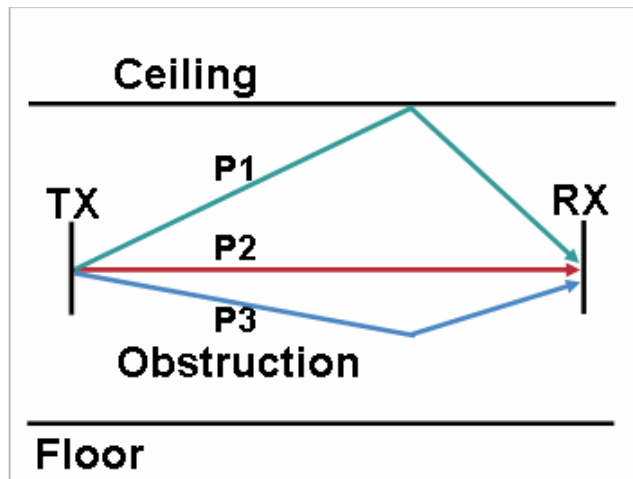
Occurs when the reflected waves arrive exactly out of phase with the main signal and cancel the main signal completely.

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 and 802.11g, 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 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
- Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G
http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-wireless-ip-phone-7925g/data_sheet_c78-504890.html
http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-wireless-ip-phone-7925g-ex/data_sheet_c78-565676.html
http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-wireless-ip-phone-7926g/data_sheet_c78-649589.html

Cisco 792xG Neighbor List

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can be utilized to verify coverage by using the Neighbor List menu.

To access the neighbor list menu on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, select **Settings > Status > Neighbor List**.

The connected access point will be highlighted in red.

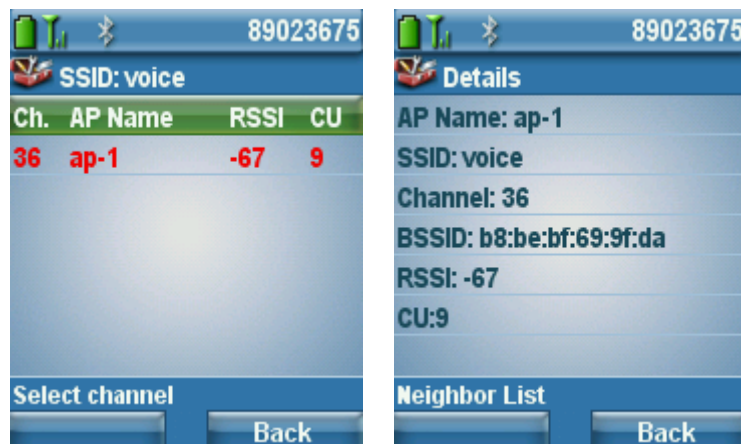
By default with the **Auto** scan mode enabled, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in idle (not on call) only scans when the current signal lowers to the scan threshold, so only a single access point may be visible in the list.

To see all access points in the neighbor list menu with **Auto** scan mode, place a call from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, where scanning occurs constantly while the phone call is active in **Auto** scan mode.

With **Continuous** scan mode, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will always be scanning regardless of call state (idle or on call) or current access point signal level (RSSI).

Neighbors will be listed in order from the strongest signal to the weakest signal when using Auto-RSSI, 802.11a or 802.11b/g mode. If using a Auto-a or Auto-b/g mode, then the neighbors will be displayed in the following order.

- Preferred Band Neighbors with ≥ -67 dBm RSSI
- Less Preferred Band Neighbors with ≥ -67 dBm RSSI
- Preferred Band Neighbors with < -67 dBm RSSI
- Less Preferred Band Neighbors with < -67 dBm RSSI



Cisco 792xG Site Survey

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G has a Site Survey application, which is an offline mode that gathers information about the access points for the configured network profile and generates an HTML report after exiting the application.

To access the Site Survey application, navigate to **Settings > Status > Site Survey**.

To view the HTML report, select **System > Site Survey** from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G webpage.

This information can be utilized to confirm access point configuration as well as coverage.

The neighbor table shows access points (along the column) that are neighbors of the access points with the strongest signal listed in the row. The percentage of time that the access point had the highest RSSI is displayed as well as the RSSI range for that access point when it was observed. The access point name is hyperlinked to the access point detail listed below.

Configuring Cisco Unified Communications Manager

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

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support 6 lines. The default phone button template includes support for 2 lines and 4 speed dials.

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 7925G

Button Information

Button	Feature
1	Line **
2	Line
3	Speed Dial
4	Privacy
5	Service URL
6	Speed Dial BLF
	Call Park BLF
	Intercom
	Mobility
	Do Not Disturb
	None


Softkey Templates

Custom softkey templates can be created with the option of giving additional feature access or limiting feature access.

Softkeys are assigned based on the state of the phone (on hook, connected, on hold, ring in, off hook, connected transfer, digits after first, connected conference, ring out, off hook with feature, remote in use, connected no feature).

The order of the softkeys can also be arranged when creating a custom softkey template.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have 2 softkeys available. The feature listed first in the softkey template will be displayed on the left softkey if on a call, where the other features will be listed under the options menu on the right softkey.

Status
 Status: Ready

Softkey Layout Configuration
 Softkey Template: Custom
 Select a call state to configure: On Hook

Unselected Softkeys
 Call Back (CallBack)
 Conference List (ConfList)
 Direct Transfer (DirTrfr)
 Group Pick Up (GPickUp)
 HLog (HLog)
 Immediate Divert (iDivert)
 Join (Join)
 Meet Me (MeetMe)
 Mobility (Mobility)
 Other Pickup (oPickup)
 Pick Up (PickUp)
 Quality Report Tool (QRT)
 Remove Last Conference Party (RmLstC)
 Select (Select)
 Toggle Do Not Disturb (DND)
 Undefined (Undefined)

On Hook
 Connected
 On Hold
 Ring In
 Off Hook
 Connected Transfer
 Digits After First
 Connected Conference
 Ring Out
 Off Hook With Feature
 Remote In Use
 Connected No Feature

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have a Manufacturing Installed Certificate (MIC), which can be utilized with a security profile as well.

Protocol Specific Information
 Packet Capture Mode* None
 Packet Capture Duration 0
 Presence Group* Standard Presence group
Device Security Profile* Cisco 7925 - Secure TFTP Encrypted
 SUBSCRIBE Calling Search Space SJC DN Unlimited
☐ Unattended Port

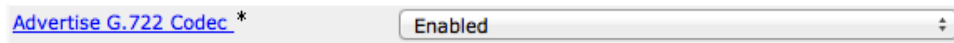
Certification Authority Proxy Function (CAPF) Information
 Certificate Operation* No Pending Operation
 Authentication Mode* By Existing Certificate (precedence to MIC)
 Authentication String

 Key Size (Bits)* 1024
 Operation Completes By 2008 10 5 12 (YYYY:MM:DD:HH)
 Certificate Operation Status: None
 Note: Security Profile Contains Addition CAPF Settings.

G.722 Advertisement

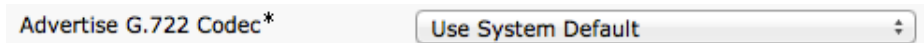
Cisco Unified Communications Manager versions 5.0 and later support the ability to configure whether G.722 is to be a supported codec system wide or not.

If using a recent version of Cisco Unified Communication Manager, G.722 can be disabled globally within **Enterprise Parameters** of Cisco Unified Communications Manager.



Earlier versions of Cisco Unified Communications Manager do not have this capability, where a Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will attempt to use G.722 assuming the other endpoint also advertises G.722 capabilities.

If using a version of Cisco Unified Communications Manager prior to 5.0 and want to disable G.722 capabilities, then the latest device package will need to be applied to the Cisco Unified Communications Manager to enable this product specific configuration option where **Advertise G.722 Codec** can be disabled for each Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G as necessary.



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>

Note: The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G do not support the iSAC codec.

Common Settings

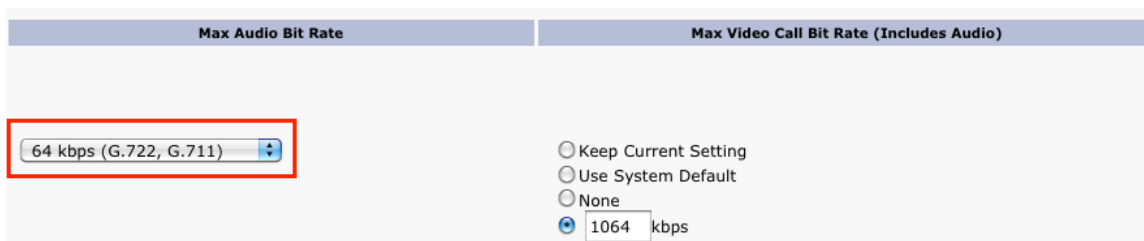
Some settings can be configured on an enterprise phone, common phone profile or individual phone level.

Override common settings can be enabled at either configuration level.

Audio Bit Rates

The audio 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.



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

Audio Codec	Audio Bit Rate
G.722 / G.711	64 Kbps
iLBC	16 Kbps
G.729	8 Kbps

Product Specific Configuration Options

In Cisco Unified Communications Manager Administration, the following Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G configuration options are available.

For a description of these options, click the ? on the configuration page.


Product specific configuration options can be configured in bulk via the Bulk Admin Tool if using Cisco Unified Communications Manager 5.0 and later. If using a prior version, then must be configured separately.

Multiple Level Vendor Configuration is allowed for a few options to override common settings.

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

Common Configuration Options

Product Specific Configuration Layout

 **Param** **Override Common Settings**

☐ Disable Speakerphone

Gratuitous ARP*

Settings Access* ☐

Web Access*

Profile 1*

Profile 2*

Profile 3*

Profile 4*

Load Server ☐

Admin Password

Special Numbers

Application URL

"Send" Key Action*

Phone Book Web Access*

Unlock-Settings Sequence (**#)*

Application Button Activation Timer*

Application Button Priority*

Out-of-Range Alert*

Scan Mode*

Restrict Data Rates*

Power Off When Charging*

Cisco Discovery Protocol (CDP)*

Advertise G.722 Codec*

Home Screen*

FIPS Mode*

Auto Line Select*

Bluetooth* ☐

File System Verification*

Minimum Ring Volume*

Java*

Field Name	Description
Disable Speakerphone	Speakerphone capabilities can optionally be disabled.
Gratuitous ARP	Determines whether the phone will learn MAC addresses from Gratuitous ARP responses or not.
Settings Access	Settings Access can be used to limit user access to certain menus (e.g. Network Profiles).

Web Access	This parameter indicates whether the phone will accept connections from a web browser or another HTTP client. Web Access can be set to Full, where configuration changes can be made remotely or Read Only to provide information but not allowing changes to be made.
Locked Profiles	Individual profiles can also be locked, which does not allow the user to modify those settings.
Load Server	A load server can be specified in IP format (x.x.x.x) if wanting to use an alternate TFTP server for phone firmware downloads.
Admin Password	The admin password is used for web access. With Cisco Unified Communications Manager 5.0 or later the admin password must be managed in Communications Manager Administrator page, where previous versions allow local management.
Special Numbers	Special numbers can be programmed to dial out regardless of keypad lock state (e.g. 911).
Application URL	<p>The application URL can be configured, which will convert the application button to a service URL button or as a speed dial.</p> <p>The application URL can be configured to link to a Push To Talk server for quick access.</p> <p>(e.g. PTT server = http://x.x.x.x:8085/PushToTalk/displayPhoneGroupsMenu.do?sep=#DEVICENAME#)</p> <p>To configure the application button as a speed dial, enter in the format as Dial:X (e.g. Dial:23675).</p>
“Send” Key Action	“Send” key action determines whether the green dial button is to use onhook dialing and serve as last number redial, where a list of previously dialed numbers will be listed, or to use offhook dialing, which will play dial tone.
Phone Book Web Access	Phone book web access must be set to Allow Admin in order to access the phone book via the web page.
Unlock-Settings Sequence	By default, *** must be entered to unlock a menu that contains configurable items, which can optionally be disabled.
Application Button Activation Timer	The activation timer and priority of the application button can also be specified. This determines how long the button must be pressed and held to activate.
Application Button Priority	If the priority is low, then will only function when the keypad is unlocked and on the home screen. Medium priority will allow the application button to function when in any menu or XML screen and high priority will allow the application button to function when in any state including keypad lock.
Out of Range Alert	An out of range alert can be configured to beep once or periodically to audibly notify the user that they have traveled out of the coverage area.
Scan Mode	Scan mode allows for Auto, Continuous, and Single AP options, where auto primarily scans only when on call and single AP only at power on.
Restrict Data Rates	This parameter enables or disables the restriction of the upstream and downstream PHY rates according to CCX V4 Traffic Stream Rate Set IE (S54.2.6).

Power Off When Charging	Power off when charging feature will power off the phone when placed on AC power.
Cisco Discover Protocol (CDP)	Enables or disables CDP.
Advertise G.722 Codec	G.722 capabilities can be configured on a phone by phone basis and optionally override the system default.
Home Screen	By default the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will show the traditional screen with the four icons for directory, services, settings and line access.
FIPS Mode	The Federal Information Process Standards (FIPS) mode can optionally be enabled.
Auto Line Select	When enabled, indicates that the phone will shift the call focus to incoming calls on all lines. When disabled, the phone will only shift the focus to incoming calls on the currently used line.
Bluetooth	Indicates whether the Bluetooth device on the phone is enabled or disabled.
File System Verification	This parameter indicates whether the phone will perform a file system integrity check as part of the firmware upgrade process. Enable this option to troubleshoot file system issues. This feature may impact phone performance if it is enabled.
Minimum Ring Volume	This parameter controls the minimum ring volume on the phone. This value is set by the administrator, and can not be changed by an end user. The end user can increase the ring volume, but may not decrease the ring volume below the level defined. The minimum ring volume range is from 0 to 7, with 0 (silent) being the default value.
Java	Indicates whether the Java on the phone is enabled or disabled.

7926G Specific Configuration Options

Bar Code Symbology Group*	Basic
Scanner Commands	

<u>Field Name</u>	<u>Description</u>
Bar Code Symbology Group	This parameter specifies the symbology the scanner will use to scan bar codes. Select Basic or Extended symbology.
Scanner Commands	Use this field to customize the scanner features. Use comma to separate multiple commands. Please refer to the Midlet Developer Guide for additional information.

Below shows the available menus when **Settings Access** is configured for either Enabled, Restricted, or Disabled.

Settings Access = Enabled



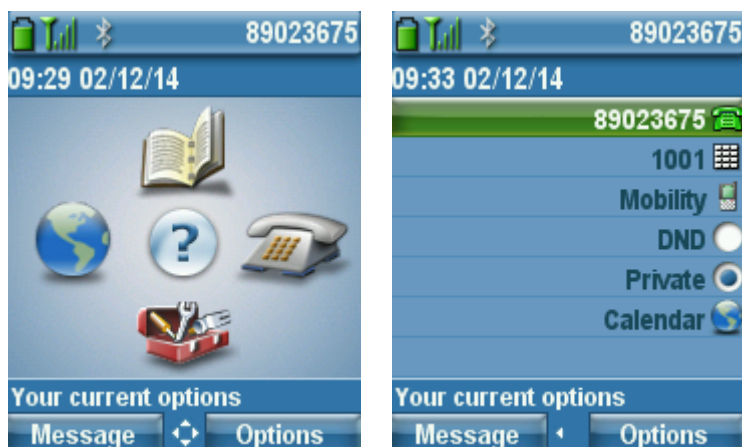
Settings Access = Restricted



Settings Access = Disabled



Below shows the main phone screen (left) and line view (right) display options for the home screen.



Note: If configuring the **Admin Password** in Cisco Unified Communications Manager versions 5.1 or later and web access is set to **Full**, then it is recommended to enable TFTP encryption via the device security profile.

As of the 1.4(6) release, Java can be disabled.

To configure product specific configuration options for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G with Cisco Unified Communications Manager Express, create an ephone template with the necessary options.

service phone <module> <value>

<u>Field Name</u>	<u>Module</u>	<u>Value</u>
Disable Speakerphone	disableSpeaker	false = Enabled true = Disabled
Gratuitous ARP	garp	0 = Enabled 1 = Disabled
Settings Access	settingsAccess	0 = Disabled 1 = Enabled 2 = Restricted
Web Access	webAccess	0 = Full 1 = Disabled 2 = ReadOnly
Locked Profiles	WlanProfile<1-4>	0 = Unlocked 1 = Locked 2 = Restricted
Load Server	loadServer	x.x.x.x
Admin Password	adminPassword	(e.g. Cisco)
Special Numbers	specialNumbers	(e.g. 411,911)
Application URL	PushToTalkURL	http://x.x.x.x

“Send” Key Action	sendKeyAction	0 = Onhook Dialing 1 = Offhook Dialing
Phone Book Web Access	phoneBookWebAccess	0 = Deny All 1 = Allow Admin
Unlock-Settings Sequence	unlockSettingsSequence	0 = Disabled 1 = Enabled
Application Button Activation Timer	appButtonTimer	0 = Disabled 1 = 1 second 2 = 2 second 3 = 3 second 4 = 4 second 5 = 5 seconds
Application Button Priority	appButtonPriority	0 = Low 1 = Medium 2 = High
Out of Range Alert	outOfRangeAlert	0 = Disabled 1 = Beep Once 2 = Beep every 10 seconds 3 = Beep every 30 seconds 4 = Beep every 60 seconds
Scan Mode	scanningMode	0 = Auto 1 = Single AP 2 = Continuous
Restrict Data Rates	restrictDataRates	0 = Disabled 1 = Enabled
Power Off When Charging	powerOffWhenCharging	0 = Disabled 1 = Enabled
Cisco Discover Protocol (CDP)	cdpEnable	0 = Disabled 1 = Enabled
Advertise G.722 Codec	g722CodecSupport	0 = Use System Default 1 = Disabled 2 = Enabled
Home Screen	homeScreen	0 = Main Phone Screen 1 = Line View
FIPS Mode	fipsMode	0 = Disabled 1 = Enabled

Auto Line Select	autoSelectLineEnable	0 = Disabled 1 = Enabled
Bluetooth	bluetooth	0 = Disabled 1 = Enabled
File System Verification	fileSystemVerificationEnable	0 = Disabled 1 = Enabled
Minimum Ring Volume	minimumRingVolume	0 = Silent 1 = Volume Level 1 2 = Volume Level 2 3 = Volume Level 3 4 = Volume Level 4 5 = Volume Level 5 6 = Volume Level 6 7 = Volume Level 7
Java	java	0 = Disabled 1 = Enabled
Bar Code Symbology Group	barCodeSymbologyGroup	0 = Basic 1 = Extended
Scanner Commands	scannerCommands	(e.g. 414b5a01) 414b5a01 enables UPC>EAN13 conversion 4170800005 will turn off the scanner after 5 seconds if no barcode is scanned
Application Button	thumbButton1	PTTH<1-6>

With Cisco Unified Communications Manager Express, the **thumbButton1** command can tie the application button to a specific line.

For example, if line 2 is an intercom line tied to a multicast paging group, then this can be configured to achieve Push To Talk.

Enable individual phone configuration files with the following commands.

```
telephony-service
cnf-file perphone
create cnf-files
```

For more information on these features, see the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide or the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Release Notes.

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-maintenance-guides-list.html>

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-release-notes-list.html>

Scanner Commands for Cisco 7926G

If wanting to use a barcode symbology type that is not included in either the Basic or Extended symbology groups, then a custom scanner command must be configured for the Cisco Unified Wireless IP Phone 7926G within the product specific configuration of Cisco Unified Communications Manager.

Below is a table listing which barcode symbology types are included in the Basic and Extended symbology groups as well as the GID/FID values to be used with a scanner command.

Use the following command syntax to configure a scanner command.

Enable: 41<GID/FID>01

Disable: 41<GID/FID>00

Mixed: 41<GID1/FID1>01<GID2/FID2>00...

<u>Barcode Symbology</u>	<u>Basic</u>	<u>Extended</u>	<u>ISCP GID/FID</u>
UPC-A	Y	Y	4B40
UPC-E	Y	Y	4B41
UPC-E1			4B4C
EAN-8			4B42
EAN-13	Y	Y	4B43
UPC/EAN Add-On 2		Y	4B45
UPC/EAN Add-On 5			4B46
GS1 Databar Omni-Directional		Y	4F40
GS1 Databar Limited		Y	4F41
GS1 Databar Expanded		Y	4F42
GS1 Composite CC-A/CC-B			5640
GS1 Composite CC-C			5641
Code 93/93i		Y	4140
Code 39	Y	Y	4240
Code 128	Y	Y	4340
ISBT-128			4341
UCC/EAN-128	Y	Y	4342
Interleaved 2 of 5		Y	4440
Matrix 2 of 5		Y	4540

Standard 2 of 5		Y	4840
Codabar		Y	4040
Codablock A			4D40
Codablock F			4D41
Code 11		Y	4A40
Plessey		Y	4740
MSI			4640
Telepen		Y	4940
Postnet			3040
Planet			3140
BPO			3240
Canada Post			3340
Australia Post			3440
Japan Post			3540
Dutch Post			3640
Sweden Post			3740
Infomail			3940
Intelligent Mail			3A40
PDF 417	Y	Y	4C40
Micro PDF 417		Y	4C42
TLC 39			4E40
Maxicode		Y	5240
Aztec		Y	5340
DataMatrix	Y	Y	5440
QRCode		Y	5540

Examples:

Enable GS1 Composite CC-A/CC-B: **41564001**

Disable GS1 Composite CC-A/CC-B: **41564000**

Enable GS1 Composite CC-C: **41564101**

Disable GS1 Composite CC-C: **41564100**

Enable GS1 Composite CC-A/CC-B and Disable GS1 Composite CC-C: **41564001564100**

Configuring the Cisco Meraki WLAN

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

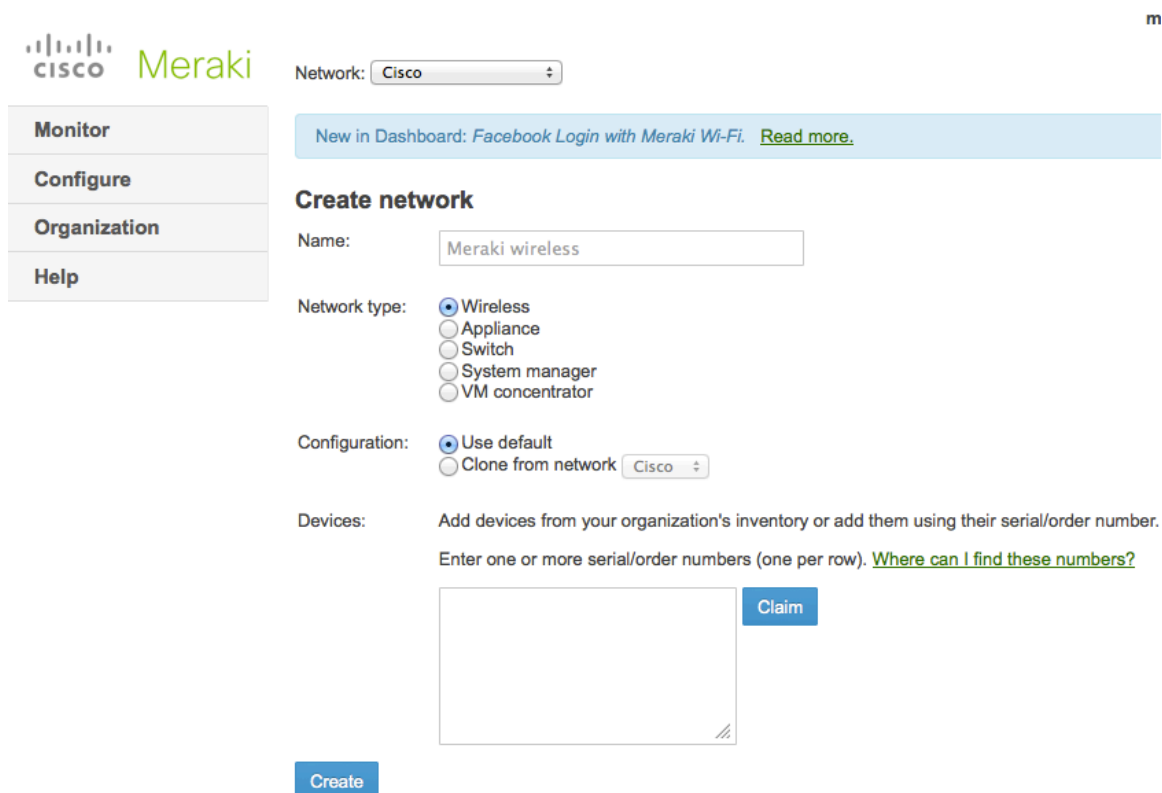
- Enable **Bridge Mode**
- Configure the **Frequency Band** for 5 GHz
- **Enable** VLAN Tagging
- Ensure WPA2-Enterprise is **Enabled** in order to utilize **Sticky Key Caching (SKC)**
- Configure the **Data Rates** as necessary
- Configure **Quality of Service (QoS)**
- Ensure Splash Page is **Disabled**

Creating the Wireless Network

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

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

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



The screenshot shows the Cisco Meraki dashboard interface. On the left is a navigation menu with 'Monitor', 'Configure', 'Organization', and 'Help'. The main content area is titled 'Create network' and includes a 'Network:' dropdown set to 'Cisco'. Below this is a blue banner for 'New in Dashboard: Facebook Login with Meraki Wi-Fi'. The 'Create network' section has a 'Name:' field with 'Meraki wireless'. The 'Network type:' section has radio buttons for 'Wireless' (selected), 'Appliance', 'Switch', 'System manager', and 'VM concentrator'. The 'Configuration:' section has radio buttons for 'Use default' (selected) and 'Clone from network' (with a 'Cisco' dropdown). The 'Devices:' section has a text prompt to add devices from inventory or by serial/order number, with a link 'Where can I find these numbers?'. Below this is a large text input area and a 'Claim' button. At the bottom left is a 'Create' button.

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

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

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

Claim by serial and/or order number



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

Close

Claim

Cisco Meraki access points can be added to the desired wireless network once they have been claimed.

Cisco Meraki access points can be added either via the **Organization > Inventory** or **Configure > Add access points** pages.

Monitor

Configure

Organization

Overview

Presence analytics

Change log

Settings

Configuration sync

License info

Inventory

Help

Network: Cisco

New in Dashboard: Facebook Login with Meraki Wi-Fi and 3 other features. [Read more.](#)

Inventory

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

Add to ...

Unclaim

Unused

Used

Both

Search inventory

Existing network

Cisco

New network

Add to existing

	Serial number
<input type="checkbox"/>	00:18:0a:21:45:93
<input checked="" type="checkbox"/>	00:18:0a:27:09:2a
<input checked="" type="checkbox"/>	00:18:0a:27:09:6c
<input type="checkbox"/>	00:18:0a:27:0d:82
<input type="checkbox"/>	00:18:0a:27:13:32
<input type="checkbox"/>	00:18:0a:34:7e:00
<input type="checkbox"/>	00:18:0a:34:7e:b8
<input type="checkbox"/>	00:18:0a:34:85:a6
<input type="checkbox"/>	00:18:0a:34:86:38
	Q2HN-CFGV-9JCW
	Q2HN-7KK2-ZJUN
	Q2CD-UGG9-DH4G
	Q2CD-7QJY-ELJB
	Q2ED-JZH9-R2MY
	Q2ED-K2RM-DBF3
	Q2ED-KQXJ-AUKN
	Q2ED-LP2H-FEQZ
	Q2DD-254E-CYJ9
	Q2DD-282D-U6HB
	Q2DD-326W-FEBZ
	Q2DD-34E7-KDXD

Cisco Unified Wireless IP Phone 792xG + Cisco Meraki Wireless LAN Deployment Guide

47

SSID Configuration

To create SSIDs, select the desired network from the drop-down menu then select **Configure > SSIDs**.

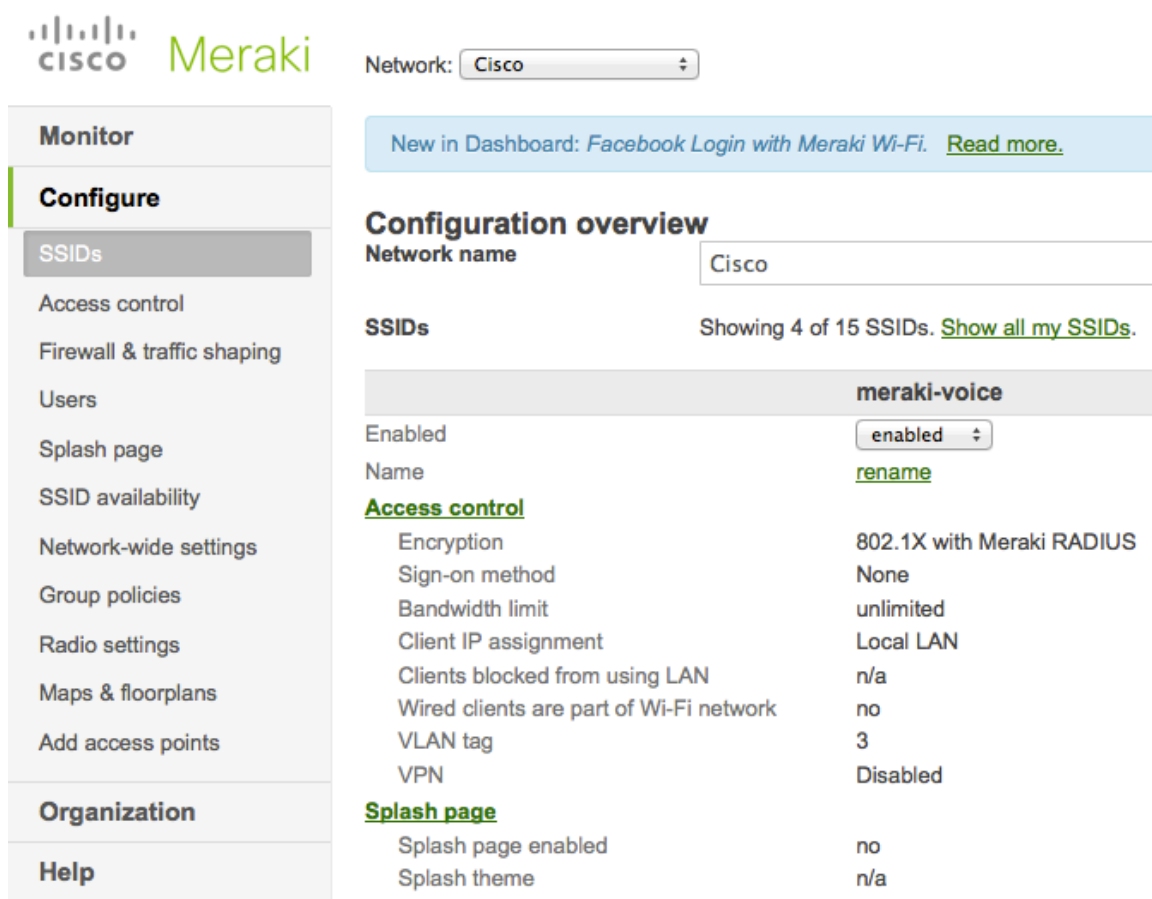
It is recommended to have a separate SSID for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G; data clients and other type of clients should utilize a different SSID and VLAN.

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

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

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

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



The screenshot displays the Cisco Meraki configuration interface. On the left is a navigation sidebar with sections: Monitor, Configure (selected), Organization, and Help. Under the Configure section, the following options are listed: SSIDs (selected), Access control, Firewall & traffic shaping, Users, Splash page, SSID availability, Network-wide settings, Group policies, Radio settings, Maps & floorplans, and Add access points. The main content area shows the 'Configuration overview' for the 'Cisco' network. A blue banner at the top reads 'New in Dashboard: Facebook Login with Meraki Wi-Fi. [Read more.](#)'. Below this, the 'Configuration overview' section shows the 'Network name' as 'Cisco'. The 'SSIDs' section indicates 'Showing 4 of 15 SSIDs' with a link to 'Show all my SSIDs.'. A table lists the configuration for the 'meraki-voice' SSID:

meraki-voice	
Enabled	enabled
Name	rename
Access control	
Encryption	802.1X with Meraki RADIUS
Sign-on method	None
Bandwidth limit	unlimited
Client IP assignment	Local LAN
Clients blocked from using LAN	n/a
Wired clients are part of Wi-Fi network	no
VLAN tag	3
VPN	Disabled
Splash page	
Splash page enabled	no
Splash theme	n/a

On the **Configure > Access control** page, select WPA2-Enterprise to enable 802.1x authentication. WPA2 is required in order to utilize SKC for fast roaming.

The Cisco Meraki authentication server or an external RADIUS server can be utilized when selecting WPA2-Enterprise.

The Cisco Meraki authentication server supports PEAP-MSCHAPv2 authentication and requires a valid email address. Ensure that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 792G are running firmware 1.4.4.3 or later if planning to utilize the Cisco Meraki authentication server.

Other authentication types (e.g. Pre-Shared Key) are available as well.

Ensure Splash page is set to **None** to enable direct access.

Monitor

Configure

SSIDs

Access control

Firewall & traffic shaping

Users

Splash page

SSID availability

Network-wide settings

Group policies

Radio settings

Maps & floorplans

Add access points

Network: Cisco

New in Dashboard: [Facebook Login with Meraki Wi-Fi](#). [Read more.](#)

Access control

SSID: meraki-voice

Network access

Association requirements

Open (no encryption)

Any user can associate

Pre-shared key with WPA2

Users must enter a passphrase to associate

MAC-based access control (no encryption)

RADIUS server is queried at association time

WPA2-Enterprise with Meraki authentication

User credentials are validated with 802.1X at association time

Splash page

None (direct access)

Users can access the network as soon as they associate

If WPA2-Enterprise is enabled where the Cisco Meraki authentication server will be utilized as the RADIUS server, then a user account must be created on the **Configure > Users** page, which the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will be configured to use for 802.1x authentication.

Monitor

Configure

SSIDs

Access control

Firewall & traffic shaping

Users

Splash page

Network: Cisco

New in Dashboard: [Facebook Login with Meraki Wi-Fi](#). [Read more.](#)

User management portal: Cisco

SSID: meraki-voice

Search...

Name	Email	Authorized for SSID ▲
Michael Gillespie	migilles@cisco.com	Yes

On the **Configure > Access control** page, Bridge Mode must be enabled, where the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will obtain DHCP from the local LAN instead of the Cisco Meraki network.

Once Bridge Mode is enabled, the VLAN tagging option will be available.

It is recommended to enable VLAN tagging for the SSID, which will require the access point to be connected to a switch port in trunking mode in which that VLAN is allowed.

If VLAN tagging is utilized, ensure that the Cisco Meraki access point is connected to a switch port configured for trunk mode allowing that VLAN.

Addressing and traffic

Client IP assignment

☐ NAT mode: Use Meraki DHCP
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.

☒ Bridge mode: Make clients part of the LAN
Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.

☐ VPN: tunnel data to a concentrator
Meraki devices send traffic over a secure tunnel to an MX or VM concentrator.

☐ Layer 3 roaming beta
Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.
Note: VPN and Layer 3 roaming require an MX or VM concentrator. To use them, [add an MX](#), or [create a concentrator](#).

VLAN tagging ⓘ
Bridge mode only

Use VLAN tagging ▾

VLAN ID ⓘ

AP tags	VLAN ID	Actions
All other APs	3	

[Add VLAN](#)

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

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

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

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

On the **Configure > Access control** page, the frequency band for the SSID to be used by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can be configured to only apply to a certain 802.11 radio type.

It is recommended to select **5 GHz band only** to have the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G operate on the 5 GHz band due to have many channels available and not as many interferers as the 2.4 GHz band has.

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

All data rates for 5 GHz and 2.4 GHz are enabled by default and only 1 Mbps, 2 Mbps, and 5.5 Mbps for 802.11b (2.4 GHz) can optionally be disabled.

If going to use 2.4 GHz, then it is recommended to disable the legacy data rates (1, 2, and 5.5 Mbps).

Wireless options

Band selection

☐ Dual band operation (2.4 GHz and 5 GHz)

☒ 5 GHz band only
5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.

☐ Dual band operation with Band Steering
Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.

Legacy 11b operation ⓘ

Disable legacy 11b bitrates (1, 2, & 5.5 Mbps) ▾

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

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

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

The screenshot shows the Cisco Meraki dashboard interface. On the left is a navigation menu with 'Monitor' and 'Configure' sections. Under 'Configure', 'SSID availability' is selected. The main content area shows the 'SSID availability' configuration for the 'meraki-voice' SSID. The 'Network' is set to 'Cisco'. A blue banner at the top says 'New in Dashboard: Facebook Login with Meraki Wi-Fi. Read more.' The settings are: 'SSID: meraki-voice', 'Visibility: Advertise this SSID publicly', 'Per-AP availability: This SSID is enabled on all APs', and 'Scheduled availability: disabled'.

Radio Settings

On the **Configure > Radio settings** page, configure the country in which the wireless LAN is deployed and what radio transmit power settings to use.

For the radio power setting, it is recommended to select **Enable power reduction on nearby APs** as co-channel interference can be potentially reduced.

If wanting to always use maximum radio power, then select **Always use 100% power**.

The screenshot shows the Cisco Meraki dashboard interface for 'Channel planning'. The left navigation menu has 'Configure' selected, with 'Channel planning' being the active sub-section. The main content area is titled 'Channel planning' and 'Power and country settings'. The 'Network' is 'Cisco'. A blue banner says 'New in Dashboard: Facebook Login with Meraki Wi-Fi and 4 other features. Read more.' The settings are: 'Country: United States' (with a dropdown arrow) and 'Regulatory domain: FCC'. The 'Radio power' setting is 'Enable power reduction on nearby APs'.

When using Cisco Meraki access points it is recommended to select **Auto** for the channel and transmit power.

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

The channel width for 5 GHz channels is set to 40 MHz by default, but can optionally be configured to use 20 MHz channels.

If wanting to utilize 40 MHz channels on 5 GHz to accommodate 802.11n clients, ensure that **5 GHz channel bonding** is **Enabled**. To utilize 20 MHz, ensure that **5 GHz channel bonding** is **Disabled**.

If the channel has a + or - beside it, then channel bonding is enabled.

2.4 GHz radios utilize 20 MHz channel width and can not be configured for 40 MHz channels.

When **Auto** is selected for 2.4 GHz channels, only channels 1, 6, and 11 will be utilized.

Individual access points can be configured with static channel and transmit power for either 5 or 2.4 GHz radios, which may be necessary if there is an intermittent interferer present in an area.

Other access points enabled can be enabled for **Auto** and work around the access points that are statically configured.

Channel settings

2.4 GHz 5 GHz Both

Access point	Radio #	Model	Band	Channel	Transmit power	5Ghz channel bonding	# Neighbors seen
MR24-27:09:2a	2	MR24	5 GHz	Auto (44)	Auto	Enabled	0
MR24-27:09:8C	2	MR24	5 GHz	Auto (44)	Auto	Enabled	0

Save Changes or cancel.

(Please allow 1-2 minutes for changes to take effect.)

Traffic Shaping

On the **Configure > Firewall & traffic shaping** page, traffic shaping rules can be defined.

To allow traffic shaping rules to be defined select **Shape traffic on this SSID** in the drop-down menu for **Shape traffic**.

CISCO Meraki Network: Cisco

New in Dashboard: Facebook Login with Meraki Wi-Fi and 4 other features. [Read more.](#)

Firewall & traffic shaping

SSID: meraki-voice

Firewall

Layer 3 firewall rules

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

[Add a layer 3 firewall rule](#)

Layer 7 firewall rules

There are no rules defined for this SSID.

[Add a layer 7 firewall rule](#)

Traffic shaping rules

Per-client bandwidth limit unlimited [details](#) ☐ Enable SpeedBurst

Per-SSID bandwidth limit unlimited [details](#)

Shape traffic

Don't shape traffic on this SSID

Shape traffic on this SSID

Don't shape traffic on this SSID



Once **Shape traffic on this SSID** has been applied, then select **Create a new rule** to define **Traffic shaping rules**.

By default, Cisco Meraki access points currently tag voice frames marked with DSCP EF (46) as WMM UP 5 instead of WMM UP 6 and call control frames marked with DSCP CS3 (24) as WMM UP 3 instead of WMM UP 4.



To tag voice frames as WMM UP 6, create a traffic shaping matching UDP ports 16384-32767 and select **6 (WMM Voice)**.


However when this is done, downstream RTP frames will then be marked as DSCP 54.



Since voice and video RTP streams utilize the same UDP port range, it is recommended to use a different SSID for any video capable devices or do not apply the policy specified below.

Rule #1  



Definition
This rule will be enforced on traffic matching *any* of these expressions.

port 16384-32767  



Per-device bandwidth limit
Choose a limit... 
5 Mbps [details](#)


PCP / DSCP tagging
Do not set PCP tag  / 6 (WMM Voice) 



To tag call control (SCCP) frames as WMM UP 4, create a traffic shaping matching TCP port 2000 and select **4 (WMM Video)**. If secure SCCP is utilized, then match on TCP port 2443.

Rule #2  

Definition
This rule will be enforced on traffic matching *any* of these expressions.

port 2000  

Per-device bandwidth limit
Choose a limit... 
5 Mbps [details](#)

PCP / DSCP tagging
Do not set PCP tag  / 4 (WMM Video) 

Monitoring Clients

On the **Monitor > Clients** page, client information and statistics can be displayed.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can be identified by inspecting the **Operating System** field, where **Cisco wireless phone** will be displayed.

Monitor

Overview

Map

Access points

Clients

Traffic analytics

Packet capture

Event log

Air Marshal

RF spectrum

Presence heatmap

Summary report

PCI report

Configure

Organization

Help

New in Dashboard: [Geofencing and 12 other features.](#) [Read more.](#)

[Clients](#) > **00:22:90:ea:9e:64**

Details | [Edit details](#)

MAC address: 00:22:90:ea:9e:64

IP: 10.116.167.206

Hostname: SEP002290EA9E64 (DHCP)

Network access: normal

Connection: wireless

Capabilities: 802.11a, 2.4 and 5 GHz

Manufacturer: Cisco Systems

Operating system: Cisco wireless phone

History: [Event log](#)

: [Run packet capture on this client](#)

Systems mgmt: Not installed ([install](#))

Status: Currently connected

Signal strength 47 dB

Duration: 20 minutes

Access point: [MR24-27:09:2a](#)

User: migilles

SSID: meraki-voice

Splash Authorization: None

Channel: 44 - 5.22 GHz (11a, 20MHz channel)

Packets: 12415 sent, 9721 received

Data: 3.8 MB sent, 1.8 MB received

Configuring the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

There are various methods for configuring network settings on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Configuring Phones with the Keypad

The network profiles can be configured by navigating to **Settings > Network Profiles**.

It may be required to unlock the screen by pressing ****#**.

For more information, refer to the **Configuring Settings on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G** in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide at this URL:

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-maintenance-guides-list.html>

Configuring Phones with the Web Interface

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have an HTTPS enabled web interface that can be accessed via the 802.11a/b/g radio or USB.

A PC running Microsoft Windows 7® 64 bit, Windows 7® 32 bit, Windows XP 32® bit or Windows 2000® 32 bit is required to utilize the USB interface on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

If using USB, then set a static IP on the PC's USB network interface (e.g. 192.168.1.X /24).

In order to make configuration changes via the web interface, then web access must be set to **Full**, which will also enable a few additional menus.

Log into the administration web pages by using these defaults:

username = **admin** / password = **Cisco**

The USB driver installation packages for Microsoft Windows 7 64 bit, Windows 7 32 bit, Windows XP 32 bit, and Windows 2000 32 bit are available for download at the following URL.

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

Note: It is not recommended to use the 192.168.1.0 /24 network for the wireless LAN interface as that network is used by the USB interface by default. If wanting to use the 192.168.1.0 /24 network for the wireless LAN, then either change the USB IP address on the phone or do not charge the phone via USB.

Configuring Phones with the Bulk Deployment Utility

The Bulk Deployment Utility (BDU) for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is intended to help quicken the provisioning and deployment process of many phones when unique 802.1x accounts are used with PEAP-MSCHAPv2 or if a common set of credentials are used by all phones (e.g. WPA2-PSK or a common 802.1x account).

For more information, refer to the Cisco Unified Wireless IP Phone 7925G Administration Guide at this URL:

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-maintenance-guides-list.html>

Wireless LAN Settings

Use the following guidelines to configure network profiles.

- The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support multiple network profiles that allow one SSID per network profile. 0 length SSIDs are not allowed.
- 5 different 802.11 modes are available.
 - Auto-RSSI
 - 802.11a
 - 802.11b/g
 - Auto-A
 - Auto-b/g

Auto-a is the default 802.11 mode, so it will scan both channels and attempt to on the 5 GHz band if the configured network is available.

In previous releases, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G would default to Auto-RSSI mode, which would attempt to associate to the access point with the strongest signal.

802.11a mode will only scan 5 GHz channels and 802.11b/g mode will only scan 2.4 GHz channels, where it will then attempt to associate to an access point if the configured network is available.

For Auto-a and Auto-b/g modes, this is giving preference to one frequency band over another. At power on, will scan all 2.4 GHz and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred frequency band if available. If the preferred frequency band is not available, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will try to use the less preferred frequency band if available. If the phone roams out of coverage of the preferred frequency band, where the less preferred frequency band signal is available, then the phone will attempt to associate to that less preferred frequency band.

It is highly recommended to set the frequency band on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to **802.11a** when wanting to utilize the 5 GHz frequency band only, which prevents scanning and potentially roaming to the 2.4 GHz frequency band.

- To optimize battery life, ensure the call power save mode is configured for U-APSD/PS-POLL mode to utilize power save mode during active calls.
- Active mode (**Call Power Save Mode** set to **None**) may need to be used instead of U-APSD/PS-POLL if the access point does not support power save enabled clients.
- The Prompt Mode feature can be optionally enabled. When enabled, the password will not be stored in flash, but only in memory after entering manually after each power on sequence for seamless roaming. However, the username can be stored after entering at the prompt, but can be overridden at the next login. If the prompt is dismissed, then there is a **Login** softkey presented in order to invoke the login process. The Prompt Mode feature is only supported with Network Profile 1. If multiple network profiles are enabled and Prompt Mode is enabled, then the user would have to dismiss the login in order to switch to other enabled network profiles.
- Below are the available security modes supported and the key management and encryption types can be used for each mode.

Security Mode	Key Management	Encryption
Open	N/A	N/A
EAP-TLS	WPA2, WPA	AES, TKIP
PEAP	WPA2, WPA	AES, TKIP
AKM	WP2-PSK, WPA-PSK	AES, TKIP

- The AKM security mode is an auto authentication mode that is to be used for WPA Pre-Shared Key.
- If using 802.11i (Pre-Shared key), enter the ASCII or hexadecimal formatted key.
Pre-Shared Key requires that a passphrase be entered in ASCII or hexadecimal format.

Key Style	Characters
ASCII	8-63
HEX	64 (0-9,A-F)


- AKM mode requires a key management type to be enabled on the Access Point.
For 802.1x authentication methods, WPA or WPA2 is required.
For non-802.1x authentication, WPA-PSK or WPA2-PSK is required.

Note: SKC will be negotiated if enabled on the access point when using WPA2 with EAP-TLS or PEAP modes.

If using 802.1x authentication via PEAP authentication mode, then a username and password must be configured.

Cisco Meraki access points do not support Open+WEP, Shared+WEP, LEAP, or EAP-FAST security types or WEP encryption.

- Select whether to use Dynamic Host Configuration Protocol (DHCP) or configure static IP information.
- If option 150 or 66 is not configured to provide the TFTP server IP address via the network's DHCP scope, then enter the TFTP server IP address info.
- To enable PEAP with server validation, select **Validate Server Certificate** after importing the authentication server certificate.
- When using EAP-TLS, select either **Manufacturing Issued** or **User Installed** for the **Client EAP-TLS Certificate** option after selecting EAP-TLS.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

HOME

SETUP

NETWORK PROFILES

Profile 1

Profile 2

Profile 3

Profile 4

USB SETTINGS

TRACE SETTINGS

WAVELINK SETTINGS

CERTIFICATES

CONFIGURATIONS

PHONE BOOK +

INFORMATION

NETWORK

WIRELESS LAN

DEVICE

STATISTICS

WIRELESS LAN

NETWORK

STREAM STATISTICS

STREAM 1

STREAM 2

SYSTEM

TRACE LOGS

BACKUP SETTINGS

PHONE UPGRADE

CHANGE PASSWORD

SITE SURVEY

DATE & TIME

PHONE RESTART

Phone DN 89023675

Network Profile 1 Settings [Advanced Profile 1](#)

Wireless

Profile Name

SSID

Call Power Save Mode

802.11 Mode

Scan Mode **Continuous**

Restricted Data Rates **False**

WLAN Security

Security Mode

Export Security Credentials ☐ True ☒ False

Wireless Security Credentials

Username

Password

Prompt Mode ☐ True ☒ False

WPA Pre-shared Key Credentials

Pre-shared Key Type ☐ ASCII ☐ Hex

Pre-shared Key

Wireless Encryption

Key Type ☒ Hex ☐ ASCII

	Transmit Key	Encryption Key	Key Size
Encryption Key 1	<input checked="" type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128
Encryption Key 2	<input type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128
Encryption Key 3	<input type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128
Encryption Key 4	<input type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128

Certificate Options

Client EAP-TLS Certificate

Manufacturing Issued

Validate Server Certificate

☐ True
☒ False

IP Network Configuration

☒ Obtain IP address and DNS servers automatically
☐ Use the following IP address and DNS servers

IP Address

Subnet Mask

Default Router

Primary DNS Server

Secondary DNS Server

Domain Name

TFTP

☒ Obtain TFTP servers automatically
☐ Use the following TFTP servers

TFTP Server 1

TFTP Server 2

Reset

Save

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Note: If the TFTP IP is changed which is not included in the current Certificate Trust List (CTL) file, then TFTP will fail and may prevent the phone from registering successfully to the Cisco Unified Communications Manager. The CTL file will need to be erased manually in the Security Configuration menu from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Configuring Advanced Network Profile Settings

The channels enabled for scanning can also be managed in the Advanced Network Profile settings.

By limiting number of channels to be scanned, this can potentially reduce the time for access point discovery.

If planning to manage the enabled channels, then only disable those channels that are not used in the wireless LAN then restart the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G via the Phone Restart option on the webpage. If a channel is disabled that is currently used by an access point, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G might not be able to associate to the wireless LAN successfully.

If all channels that are used in the wireless LAN are disabled on the phone, then use one of these methods to browse to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G webpage and re-enable the necessary channels:

- USB cable connected to the PC where full web access was previously enabled
- Re-enable all channels by using the factory default



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

HOME
SETUP
NETWORK PROFILES
Profile 1
Profile 2
Profile 3
Profile 4
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Phone DN 89023675

Network Profile 1 Advanced Settings

[Basic Profile 1](#)

TSPEC Settings

Minimum PHY Rate

Surplus Bandwidth

802.11 G Power Settings

Channel	Enabled	Max Tx Power	Channel	Enabled	Max Tx Power
1	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	2	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	4	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
5	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	6	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
7	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	8	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
9	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	10	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
11	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	12	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
13	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	14	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>

802.11 A Power Settings

Channel	Enabled	Max Tx Power	Channel	Enabled	Max Tx Power
36	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	40	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
44	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	48	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
52	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	56	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
60	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	64	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
100	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	104	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
108	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	112	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
116	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	120	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
124	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	128	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
132	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	136	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
140	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	149	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
153	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>	157	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>
161	<input checked="" type="checkbox"/>	<input type="text" value="17 dBm"/>			

Copyright (c) 2006-2009 by Cisco Systems, Inc.

USB Settings

By default, the USB interface USB of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is statically set to 192.168.1.100 /24, but can be changed as necessary.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

HOME	Phone DN 89023675
SETUP	
NETWORK PROFILES +	
USB SETTINGS	USB Settings
TRACE SETTINGS	<input type="radio"/> Obtain IP address automatically
WAVELINK SETTINGS	<input checked="" type="radio"/> Use the following IP address
CERTIFICATES	IP Address <input type="text" value="192.168.1.100"/>
CONFIGURATIONS	Subnet Mask <input type="text" value="255.255.255.0"/>
PHONE BOOK +	
INFORMATION	
NETWORK	
WIRELESS LAN	
DEVICE	
STATISTICS	
WIRELESS LAN	
NETWORK	
STREAM STATISTICS	
STREAM 1	
STREAM 2	
SYSTEM	
TRACE LOGS	
BACKUP SETTINGS	
PHONE UPGRADE	
CHANGE PASSWORD	
SITE SURVEY	
DATE & TIME	
PHONE RESTART	

Save

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Installing Certificates

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support DER encoded binary X.509 certificates, which can be utilized with EAP-TLS or for authentication server validation when using PEAP-MSCHAPv2.

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 Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G.

Can utilize either the internal Manufacturing Installed Certificate (MIC) or install a User Installed certificate to be used for authentication.

To use the Manufacturing Installed Certificate in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, the Manufacturing Root and Manufacturing CA certificates must be exported and installed onto the RADIUS server.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Certificates				
Type	Common Name	Issuer Name	Valid From	Valid To
User Installed	<not installed>	<not installed>		<input type="button" value="Install"/>
Manufacturing Issued	/O=Cisco Systems Inc./OU=EVVBU/CN=CP-7925G-SEP002290EA9E64	/O=Cisco Systems/CN=Cisco Manufacturing CA	11/03/2008 20:06:43	11/03/2018 21:16:43
Manufacturing Root CA	/O=Cisco Systems/CN=Cisco Root CA 2048	/O=Cisco Systems/CN=Cisco Root CA 2048	05/14/2004 16:17:12	05/14/2029 16:25:42 <input type="button" value="Export"/>
Manufacturing CA	/O=Cisco Systems/CN=Cisco Manufacturing CA	/O=Cisco Systems/CN=Cisco Root CA 2048	06/10/2005 18:16:01	05/14/2029 16:25:42 <input type="button" value="Export"/>
Authentication Server CA	/O=Digital Signature Trust Co./CN=DST Root CA X3	/O=Digital Signature Trust Co./CN=DST Root CA X3	09/30/2000 17:12:19	09/30/2021 10:01:15 <input type="button" value="Delete"/>
Authentication Server CA	<not installed>	<not installed>		<input type="button" value="Install"/>

Copyright (c) 2006-2009 by Cisco Systems, Inc.

After selecting **Export**, import the certificates into the RADIUS server and enable them in the Certificate Trust List (CTL).

For the User Installed certificate method, select **Install** on the main certificates page, which will launch the installation wizard.

To generate the certificate signing request, enter the certificate information and import the certificate from the Certificate Authority (CA) server that is signing the certificate. The signing CA root certificate is used for validation purposes to ensure that the user certificate was indeed signed by the correct CA.

The Common Name defaults to a string including the MAC address of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX or 7926G (CP-7925G-SEP<MAC_Address>), however the Common Name can be customized to a string with up to 32 characters.

Some special characters (e.g. ! @ # \$ % ^ & * _ [] { } \ | ; " < > ` ~) are not supported for the Common Name.

Organization, Organization Unit, City, and State fields can support up to 64 characters.

Browse to the Certificate Authority certificate that will be signing the user certificate then select **Submit**.

If using a CA configuration where one or more intermediate servers exist, ensure you upload the correct CA server certificate as this certificate will be used to validate whether the user certificate was signed by the intended CA or not.

Ensure that the signing CA server certificate uploaded is with DER encoding.

User Installed Certificates with a key size of 1024 or 2048 only are supported.

Server Certificates can have a key size of 1024, 2048, or 4096.

Ensure the CA server certificate is signed using the SHA-1 algorithm as the SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) and SHA-3 signature algorithms are not supported.

Certificates dated January 1 2038 and later are not supported.

Additional extensions in the CA server certificate such as information for certificate renewal and Certificate Revocation List (CRL) are not supported and can lead to certificate installation failures.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

User Certificate Installation

Step 1 of 4: Enter Identification Information

Common Name	<input type="text" value="CP-7925G-SEP002290EA9E64"/>
Organization	<input type="text" value="Cisco"/>
Organization Unit	<input type="text" value="TIPBU"/>
City	<input type="text" value="Raleigh"/>
State	<input type="text" value="NC"/>
Country	<input type="text" value="US"/>
Key Size	<input type="text" value="2048"/>

Step 2 of 4: Import Certificate Authority File

Certificate Authority File	<input type="button" value="Browse..."/> <input type="text" value="Signing_CA.cer"/>
----------------------------	--

Click the "Submit" button to submit all the above information and start generating a Certificate Signing Request data. This process may take a while to complete.

Copyright (c) 2006-2009 by Cisco Systems, Inc.

After **Submit** is selected, the user certificate will then be generated.

The user certificate will then be displayed and is now ready to be signed.

Select all of the user certificate data in order to copy it to the Certificate Authority server to be signed.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

User Certificate Installation

Step 3 of 4: Signing the Certificate

Please copy the generated Certificate Signing Request below and submit it to your Certificate Authority Server.

Please create the Signed Certificate in DER encoded format for this phone.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDNjCCA4CAQAwb2ELMAkGA1UEBhMCVVMxZzA1BgNVBAGTAk5DMRAwDgYDVQQH
EwdSYWxlaWdoM4wDAYDVQQKEwVDAhXNjZzEOMAwGA1UECzMFVE1Q1UxITAFBgNV
BAMTGENQLTc5MjVHbVNFUDAwMjI5MEVBOU2NDCCASiWdQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBANoySVLVBpwoKbthfyaQAt1vlnDiAKv8G9Ay+m6mkV62Fzk0
l4FLmqP1D81ZurWMOquTY+ZBQIQo751TwVE2/OHriMHESdOVMJ61Pfufwm7y9PKo8
Oh7whFFMwNbr/Ek8tINEuvSSloqRYzm30zG77wwkVJ6qojlkfpIpcYON157X9Imb
us8GQV6yEmFB+ZEKPOLN6qfyvUIC/5z7kbaQdkUV1gHN7LqM7cMz7GA2pgbjZbO
26gbZtWcnLVou+0/606KV0Wg40RBqBHxc71mzpSBwDm++2axmDk3z/c1CggDtOk
ywuP3Mk9/kMeBhXh86EiTCJ5+yErZEgndN28nKMCawEAAaCBgTB/BgkqhkiG9w0B
CQ4xcjBwMAwGA1UdEwEB/wQCAAAwJAYDVR0RBBOwG4YZQ1AtNzkyNUctU0VQMDAy
MjkwRUE5RTY0ADA0BgNVHQ8BAf8EBAMCA/gwKgYDVRO1AQH/BCAwHgYIKwYBBQUH
AwEGCCsGAQUFBwMCGgrBgEFBQcDBTANBgkqhkiG9w0BAQUFAAOCAQEAHuEndnaG
Be/Hmcy9z0GyNA4spBcqOFgCEtgUDqD1fB4S+sR1WEtKXgu8+g2HCVVM7yG6T7ri
JHhXtDAi+oPOJQmuxMPnQTzCX9f1NibTM4bqUF8C/XQUvXX4OJ8aM+7nJzSRLJsp
rYx87s6y/+FyCRXFcr7ybHMQXFJ4xn7+tLHM7SpI4sIheah/meOEpkup8Bh+iD7W
```

* If you need more time to complete the above step of creating Signed Certificate, you may select the "Postpone" button and attempt the Import step at later time. [Note: Select the "Install" option again in the main Certificates page to resume the installation step after you had postponed it.]

* If you ready have the Signed Certificate for this phone, you may select the "Import Step" button to continue with the installation steps.

Postpone Import Step

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Select the method to submit a certificate request by using a Base-64 (PEM) encoded PKCS file.

Paste the certificate data from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to the Certificate Authority signing server and submit for signing.

Microsoft Certificate Services -- peap-tls

Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

[Browse for a file to insert.](#)

Additional Attributes:

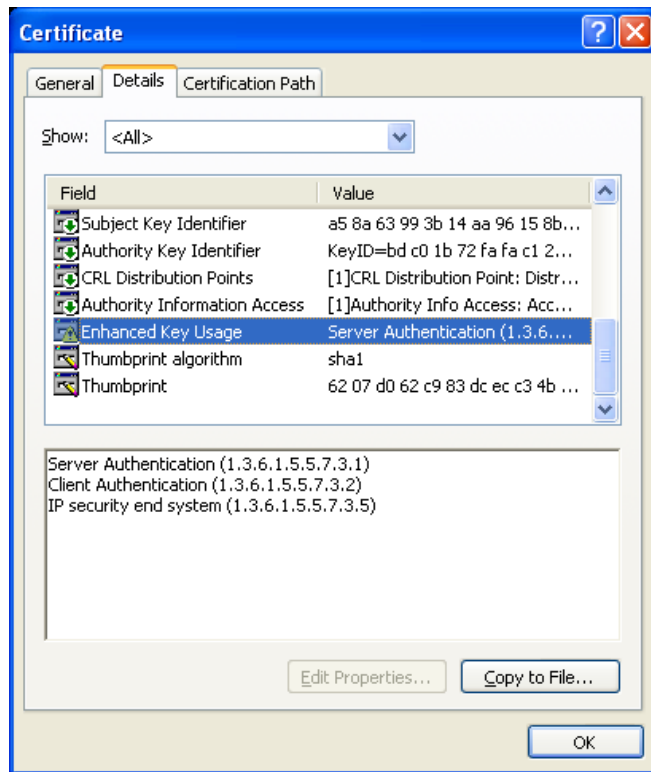
Attributes:

Submit >

When the user certificate has been signed, download the CA certificate in DER encoded format (Base-64 / PEM encoded certificates are not supported).

Ensure the user certificate is signed using the SHA-1 algorithm as the SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) and SHA-3 signature algorithms are not supported.

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



After selecting **Import Step**, browse to the signed user certificate then select **Import** to complete the process.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

User Certificate Installation

Final Step: Import Signed Phone Certificate (DER encoded format)

Certificate File To Install SEP002290EA9E64.cer

Please click the "Import" button below to install the Signed Certificate into the phone.

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Once the certificate is installed successfully, a confirmation page will be displayed.

The CA chain should already be enabled in the authentication server's certificate trust list.

The authentication server certificate must also be imported into the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G for both the Manufacturing Installed and User Installed methods. If the authentication server certificate was signed by a Certificate Authority (CA) server, then that DER encoded root certificate will need to be imported into the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

If the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G has not registered to a Cisco Unified Communications Manager yet, then the date and time must be configured manually for the first time.

Timezone support has been added, which can allow newly issued certificates to be immediately used.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

Date & Time Settings

Current Phone Date & Time

November 07, 2013 10:49:55

Note: Phone Date & Time may change when phone registered with Cisco Unified Communications Manager

Local Date & Time

Set Phone to Local Date & Time

Specify Date & Time

Date November 07 2013
Time 10 hours(24 hrs) 49 minutes 55 seconds

Set Phone to Specific Date & Time

NOTE: After changing the Date & Time, you must execute ["SYSTEM / PHONE RESTART"](#) before the new time can be used to validate Certificates.

Copyright (c) 2006-2009 by Cisco Systems, Inc.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G must be restarted after installing the certificate. Click on the hyperlink to navigate to the **Phone Restart** page. Click the **Restart** button to power cycle the phone.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Phone Restart

Please select the "Restart" button to reboot the phone.

NOTE: Phone will CLOSE this web connection before restarting!

Restart

Cancel

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Using Templates to Configure Phones

Phone configuration templates can be exported and imported to other phones for quick configuration. The phone configuration template will be encrypted using the specified encryption key (8-20 characters).

In order to access the Backup Settings menu, the web access must be set to **Full**.

For security reasons, the Wireless LAN security information (Username/Password, WPA Pre-shared key information) is not exported by default. In order to export this Wireless LAN security information, the network profile must be configured to allow this capability. For each network profile where the Wireless LAN security information is to be exported, configure the **Export Security Credentials** option to **True**. After selecting **True**, the Wireless LAN security information will need to be re-entered. This will then allow that information to be exported and then imported to other Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G phones.

Any installed certificates are not included in the exported template.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Phone DN 89023675

Backup Settings

Import Configuration

Encryption Key	<input type="text"/>
Import File	<input type="button" value="Browse..."/> No file selected.
<input type="button" value="Import"/>	

Export Configuration

Encryption Key	<input type="text"/>
<input type="button" value="Export"/>	

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Using the Bulk Deployment Utility

The Bulk Deployment Utility (BDU) for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G enables the creation of configuration files, which can be exported then enabled for TFTP download by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

A personal computer running Microsoft Windows® is required.

The Bulk Deployment Utility requires firmware 1.3(4) or later on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

This utility does not support certificate provisioning, which would be required in order to support server validation for PEAP or EAP-TLS.

The utility does allow PEAP to be configured, but without the server validation option.

The Bulk Deployment Utility supports up to **1000** entries per CSV for export. If more than 1000 phones are being deployed, then multiple CSV files will need to be created and imported.

If doing a bulk export, the username and password is applied to network profile 1 only.

Before exporting the TFTP downloadable configuration files, a template must be created containing the Network Profile, USB, Trace, and Wavelink settings.

Configure the Profile Name as necessary.

Configure the network profile WLAN settings (SSID, 802.11 mode, Security Mode, WLAN credentials) to match the WLAN that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize.

If planning to use unique 802.1x accounts with the Bulk Export method, the username and password do not need to be configured, as that will be specified in the CSV file.

The screenshot shows the Cisco7921PhoneConfig application window. The left sidebar displays a tree view with the following structure:

- Cisco7921PhoneConfig
 - ProfileSettings
 - Profile1
 - WLANSettings** (selected)
 - AdvancedWLANSettings
 - Profile2
 - Profile3
 - Profile4
 - USBSettings
 - TraceSettings
 - WavelinkSettings

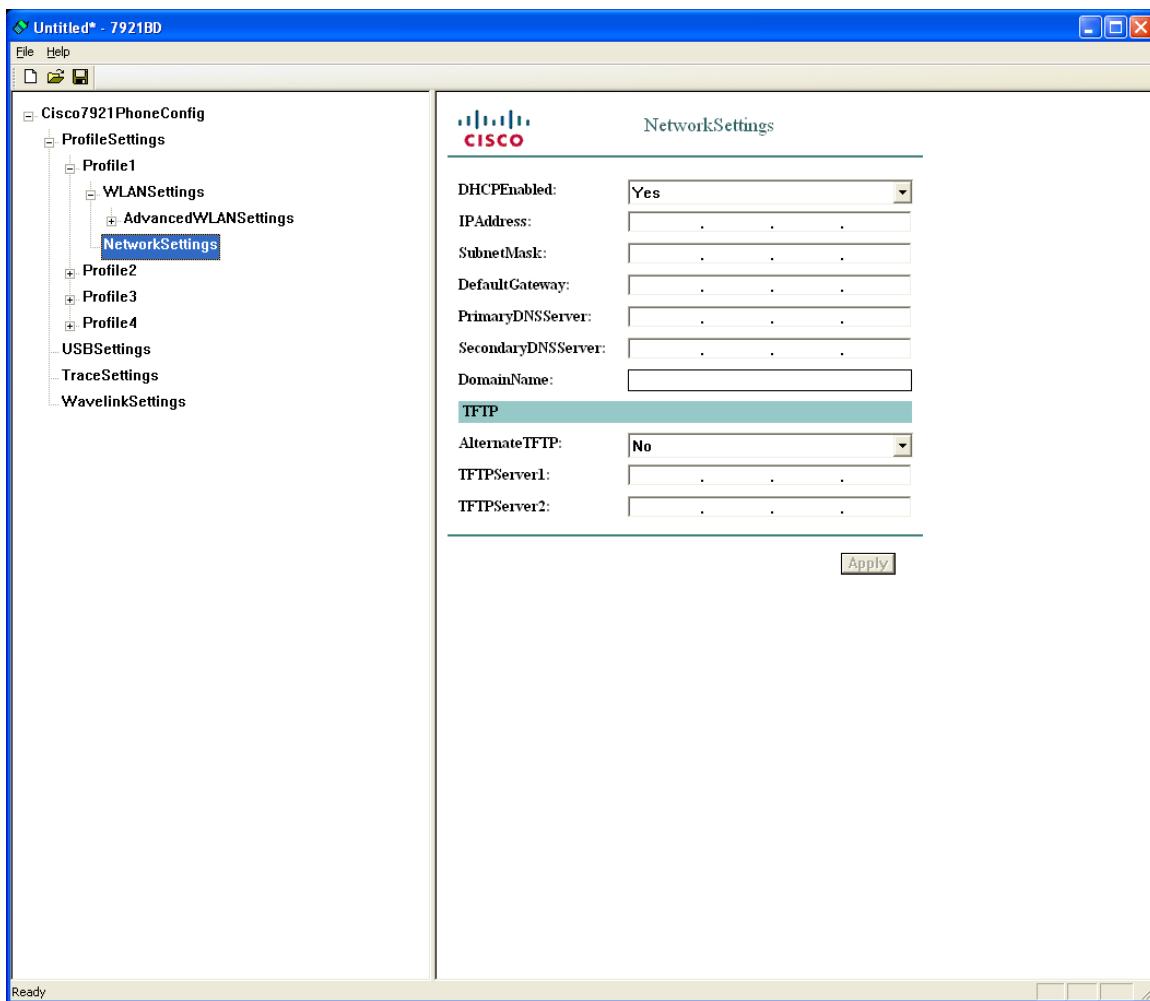
The main pane displays the 'WLANSettings' configuration page with the following fields:

- SSID:
- WLANMode:
- CallPowerSaveMode:
- AuthenticationMode:
- Wireless Security Credentials**
 - Username:
 - Password:
 - PromptMode:
- WPA Pre-shared Key Credentials**
 - PreSharedKeyType:
 - PreSharedKeyValue:
- Wireless Encryption**
 - WepKeyType:
 - WepKeysTxKey:
 - WepKey1Length:
 - WepKey1Value:
 - WepKey2Length:
 - WepKey2Value:
 - WepKey3Length:
 - WepKey3Value:
 - WepKey4Length:
 - WepKey4Value:

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

By default, DHCP is enabled and is the recommended method, otherwise would need a template per phone if planning to use static IP addressing.

An alternate TFTP server can be set if the Cisco Unified Communications Manager's TFTP server IP is not set in option 150 for the DHCP scope.



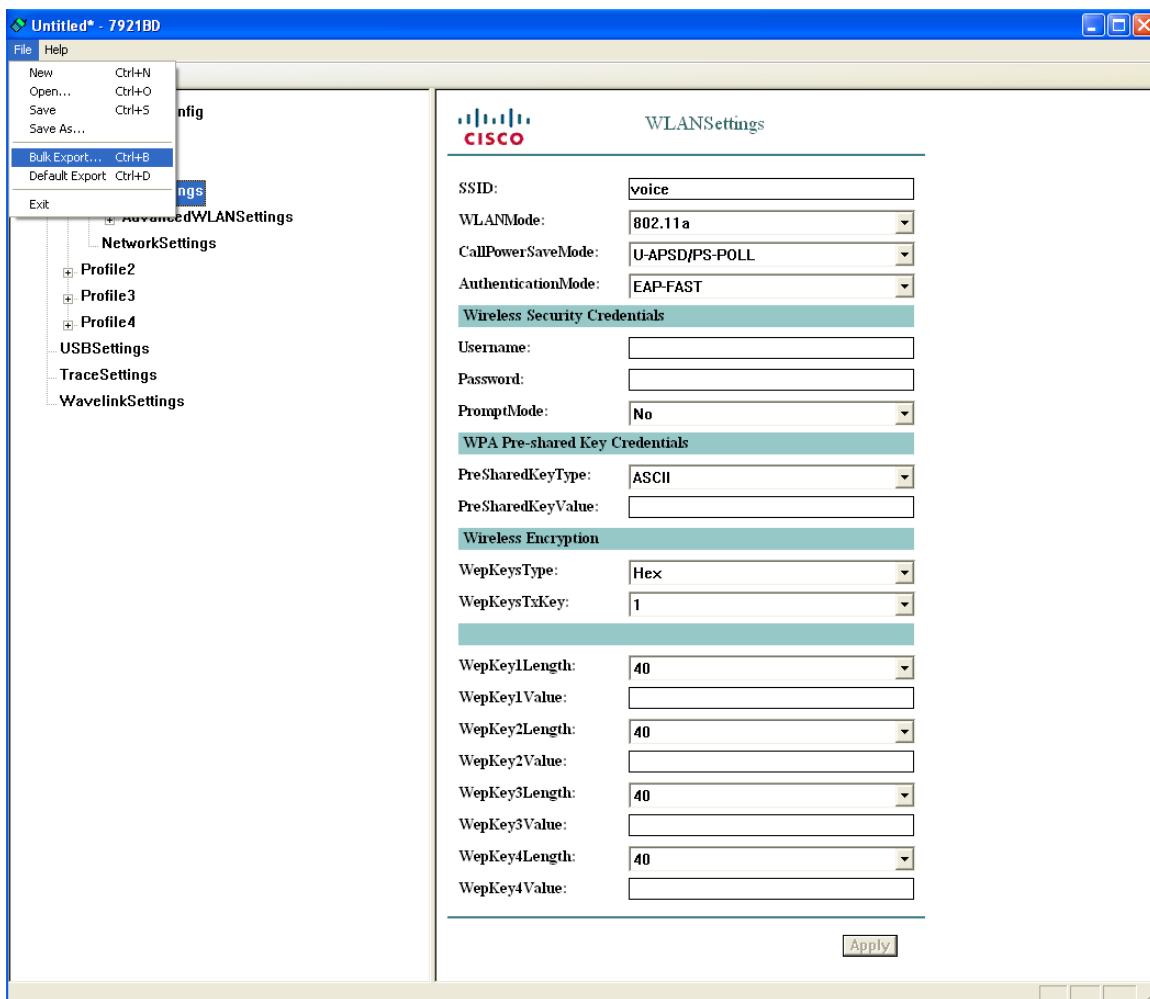
Templates can be created for later use, by selecting **File > Save As**.

Do not overwrite the **7921Cfg.xml** file, as that is the default template used when the utility opens.

Phone configuration files can be exported by either the **Default Export** method or the **Bulk Export** method.

If a common set of credentials is to be used by all phones (e.g. WPA2-PSK or a common 802.1x account), then use the Default Export method.

If unique 802.1x accounts are to be deployed, then use the Bulk Export method.



Bulk Export

If needing to deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G with unique 802.1x accounts utilizing PEAP, then select the **Bulk Export** method.

The common data entered plus a CSV containing the phone MAC address, username and password will be used to create the template.

After selecting **Bulk Export**, a prompt to display the CSV file will be presented.

Up to **1000** entries are supported per CSV file.

The **userinfo.csv** file in the install path can be used as a template.

MAC,Username,Password

001e7abb19c8,admin,Cisco

Once the CSV file is imported, the utility will create TFTP downloadable configuration files for each phone, which are exported to the application install path (C:\Program Files\Cisco Systems\7921BD).

A confirmation window will be displayed when the TFTP downloadable configuration files have been exported successfully.

The files will be in the format of **WLAN<MAC_Address>.xml**, which the phone does a TFTP get for when it powers on or re-provisions.

Default Export

If needing to deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G with identical WLAN settings, then select the **Default Export** method.

After selecting **Default Export** the utility will create a TFTP downloadable configuration file based on the common data entered, which is exported to the application install path (C:\Program Files\Cisco Systems\7921BD).

A confirmation window will be displayed when the default TFTP downloadable configuration file has been exported successfully.

The default file will be in the format of **WLANDefault.xml**, which the phone does a TFTP get for when it powers on or during re-provisioning.

Pushing Configuration Files to the Cisco 792xG

The Bulk Deployment Utility can be utilized for initial deployment or after the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G has been deployed.

Install the Bulk Deployment Utility on a computer running Microsoft Windows.

The Bulk Deployment Utility does not have TFTP server capabilities, so an external TFTP server will be required, where the phone configuration files will need to be copied to and enabled for TFTP download.

For initial deployment, the recommendation is to set up a staging environment where the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can connect to a wireless LAN using the default phone credentials, obtain an IP address via DHCP and TFTP download the phone configuration file. This setup will enable the phone to auto-download the configuration files by simply powering the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G on. The staging environment setup needs to consist of an access point with the SSID **cisco** configured and DHCP enabled either on the access point itself or another device in the local network, where DHCP option 150 is configured to point to the TFTP server's IP address that is hosting the phone configuration files.

For post-deployment where Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are already being utilized on the production wireless LAN, copy the phone configuration files to the TFTP server that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are pointed to, then reset the phones to reconnect to the production wireless LAN and TFTP download the phone configuration file. The TFTP service may need to be restarted prior to resetting the phones depending on which type of TFTP server is utilized.

After the phone received the configuration file, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G will then re-provision with the new settings and attempt to join the intended wireless LAN.

For additional security, the recommendation is to remove any phone configuration files from the TFTP server when not needed.

The Bulk Deployment Utility is available for download at the following URL.

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

Local Phone Book and Speed Dials


The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G contain local phone book and speed dials support.

As of the 1.4(1) release up to 200 contacts (100 contacts in previous releases).

99 speed dials referenced from the local phone book can be added for quick dial access. Speed dial #1 is reserved for voicemail.

The left softkey on the home screen can be programmed for **Message** to access voice mail or to **PhBook** to access the local phone book.

The local phone book and speed dials can be configured via the local keypad or via the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G web interface. Since the user does not manage the web password, the web interface is primarily intended for use by the system administrator, where they can upload information into the phone book for the user. This requires that the **Phone Book Web Access** product specific configuration item be set to **Allow Admin** as well as web access set to **Full**.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME

SETUP

NETWORK PROFILES +

USB SETTINGS

TRACE SETTINGS

WAVELINK SETTINGS

CERTIFICATES

CONFIGURATIONS

PHONE BOOK

Import/Export

INFORMATION

NETWORK

WIRELESS LAN

DEVICE

STATISTICS

WIRELESS LAN

NETWORK

STREAM STATISTICS

STREAM 1

STREAM 2

SYSTEM

TRACE LOGS

BACKUP SETTINGS

PHONE UPGRADE

CHANGE PASSWORD

SITE SURVEY

DATE & TIME

PHONE RESTART

Phone Book (New Contact)

Name Information

First Name

Last Name

Nickname

Company Name

Phone Information

Primary#

Speed Dial#

Work Number

Home Number

Mobile Number

Other Number

Contact Information

Email Address

IM Address

Mailing Address

Street Number

City

State/Province

ZIP/Postal Code

Country

Reset

Save

Cancel

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Exported phone book data can be imported onto other phones.

XML and CSV formats are supported as well as the CSV format used by the Cisco Unified Wireless IP Phone 7920.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK
Import/Export
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Phone Book (Import & Export)

Import Contact Info to Phone

Import from File: No file selected.

- ☐ DELETE ALL current Contacts before Importing
- ☐ DELETE ONLY the current Contact if matched
- ☒ MERGE current Contact info with Importing data

Matching Contacts:

- ☒ Using Unique Identifier (UID) value
- ☐ Using Name fields

To import using CSV format, please specify a filename with 32 characters or less, and with the file-extension of ".csv".

Export Contact Info to File

Create File of Type:

- ☒ XML Phone Book format
- ☐ Comma Separated Values (CSV) format

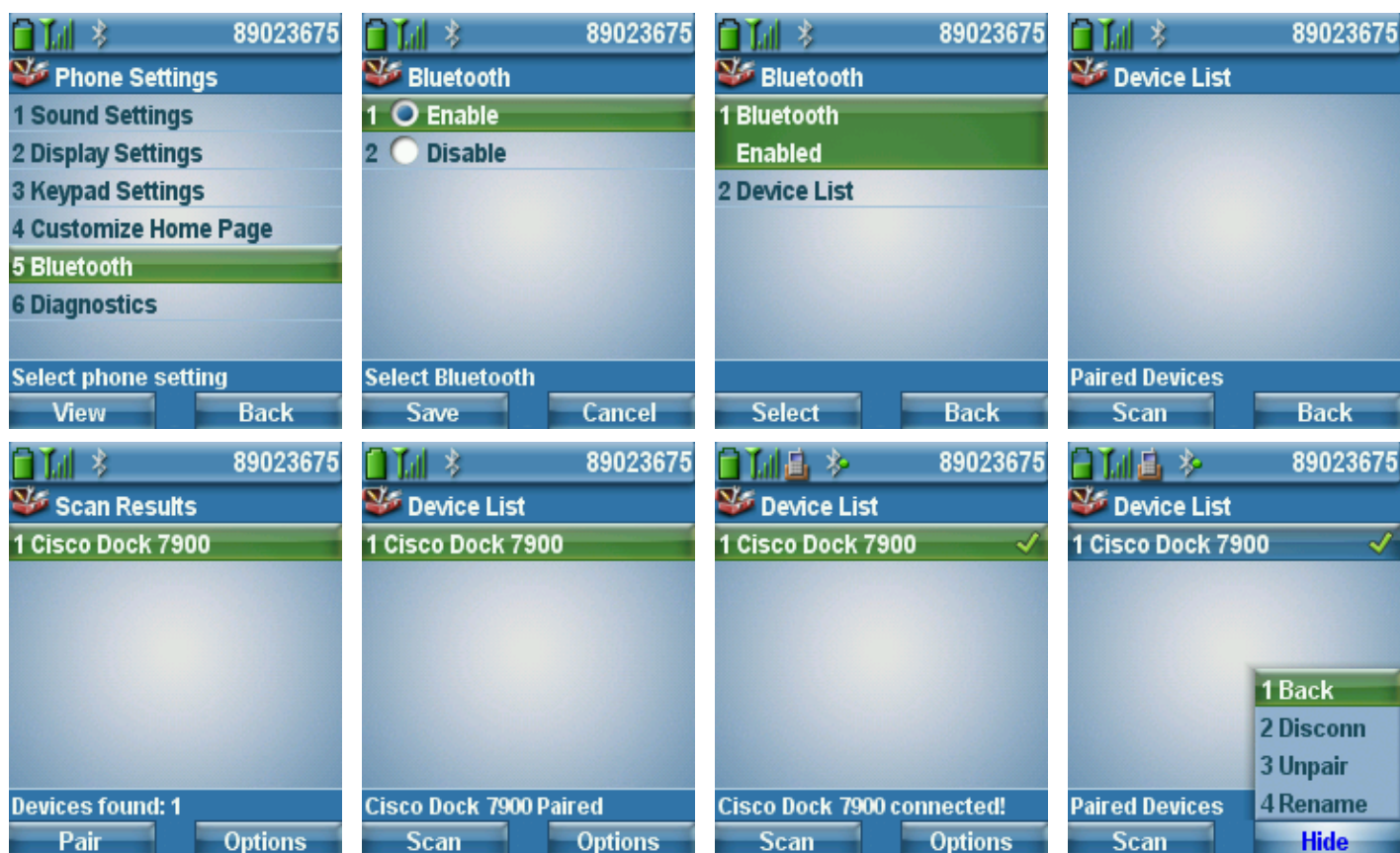
Copyright (c) 2006-2009 by Cisco Systems, Inc.

Bluetooth Settings

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have Bluetooth 2.0 + EDR support, which enables hands-free communications.

To pair the Cisco Unified Wireless IP Phone 7925G Desktop Charger or a Bluetooth headset to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, follow the instructions below.

1. Choose **Settings > Phone Settings > Bluetooth**.
2. Select **Enable** then select the left softkey **Save**.
3. Select **Device List**.
4. Select **Scan** (ensure the Bluetooth device is in pairing mode).
5. Select **Pair** after the Bluetooth headset is discovered.
6. If prompted, enter the Bluetooth passkey (will attempt to use 0000).
7. If the Bluetooth device is not connected automatically after paired successfully, select **Connect**.



Increased Font

As of the 1.4(1) release, there are options for **Default** (original) font or **Increased** font.

The font size can optionally be configured locally on the phone.

Settings > Phone Settings > Display Settings > Font Size



Default Font



Increased Font



Using the Cisco Unified Wireless IP Phone 7925G Desktop Charger

The Cisco Unified Wireless IP Phone 7925G Desktop Charger is a single phone charger including a Bluetooth speakerphone and supports the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G running firmware version 1.4(1) or later.

When the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is paired to the Cisco Unified Wireless IP Phone 7925G Desktop Charger, the audio path will automatically switch to the Bluetooth speakerphone once the phone is docked. And when removed from the desktop charger, the audio path will return to the previously used audio path (e.g. handset or speakerphone mode).

The audio volume is controlled from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G by pressing the volume up or volume down button located on the left side of the phone. Mute can also be initiated by pressing the Mute button on the left side of the phone.

The audio path is controlled from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G by pressing and holding the button located on the right side of the phone.

There is a battery slot in the rear of the Cisco Unified Wireless IP Phone 7925G Desktop Charger, which can be utilized for charging a spare battery or even powering the desktop charger.

Bluetooth Pairing

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can be paired to the Cisco Unified Wireless IP Phone 7925G Desktop Charger by performing the following steps.

1. Connect the power supply to the Cisco Unified Wireless IP Phone 7925G Desktop Charger.
2. Insert the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G into the desktop charger.
3. Power on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G.
4. Press and hold the **Control** button on the right side of the desktop charger for 5 seconds.
The Power/Bluetooth status LED begins to flash, which indicates that the desktop charger is now in pairing mode.
5. From the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, choose **Settings > Phone Settings > Bluetooth**.
6. If Bluetooth is **Disabled**, press **Select**, select **Enable**, and then press **Save**.
7. Select **Device List**, then press **Scan**, which will then list the available devices. To rescan, press **Rescan**.
8. Select **Cisco Dock 7900** and press **Pair**.
9. If prompted, enter **0000** for the passkey and press **Select** or choose **Options > OK**, and the pairing will be completed.
10. Press the **End** button on the phone to return to the main screen.

If paired successfully, then the Power/Bluetooth status LED will turn to solid blue.



Docking

After inserting the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G into the Cisco Unified Wireless IP Phone 7925G Desktop Charger, the Power/Bluetooth status LED will begin to flash blue to indicate a Bluetooth connection attempt is being made.

After the Bluetooth connection is established, the Power/Bluetooth status LED will turn to solid blue.

If currently on a call when the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is docked, there will be a small delay to switch the audio path to the desktop charger's Bluetooth speakerphone while the Bluetooth connection completes. The call will continue using the Cisco Unified Wireless IP Phone 7925G Desktop Charger's Bluetooth speakerphone after the Bluetooth connection is made.

When the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is undocked, the Bluetooth connection will be disconnected and the phone will return to the previously used audio path (e.g. handset or speakerphone mode).

See the following links for more information on the Cisco Unified Wireless IP Phone 7925G Desktop Charger.

Cisco Unified Wireless IP Phone 792xG + Cisco Meraki Wireless LAN Deployment Guide

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0_1/english/user_guide/P256_BK_EBE22FA_00_wireless-ip-phones-user-guide/P256_BK_EBE22FA_00_wireless-ip-phones-user-guide_chapter_01001.html
http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0/english/quick_start/7925Ch_qs.pdf

Using Phone Designer

The Phone Designer application allows the ability to have a customer wallpaper and ringtone for each phone.

The Cisco Unified Wireless IP Phone 7925G and 7925G-EX is supported in Phone Designer version 7.1(3) and later.

Personalization must also be enabled in the Cisco Unified Communications Manager either in Enterprise Parameters, Common Phone Profile or on a per phone level.

After installing the phone designer, a username and password as well as the IP address of the Cisco Unified Communications Manager must be configured.

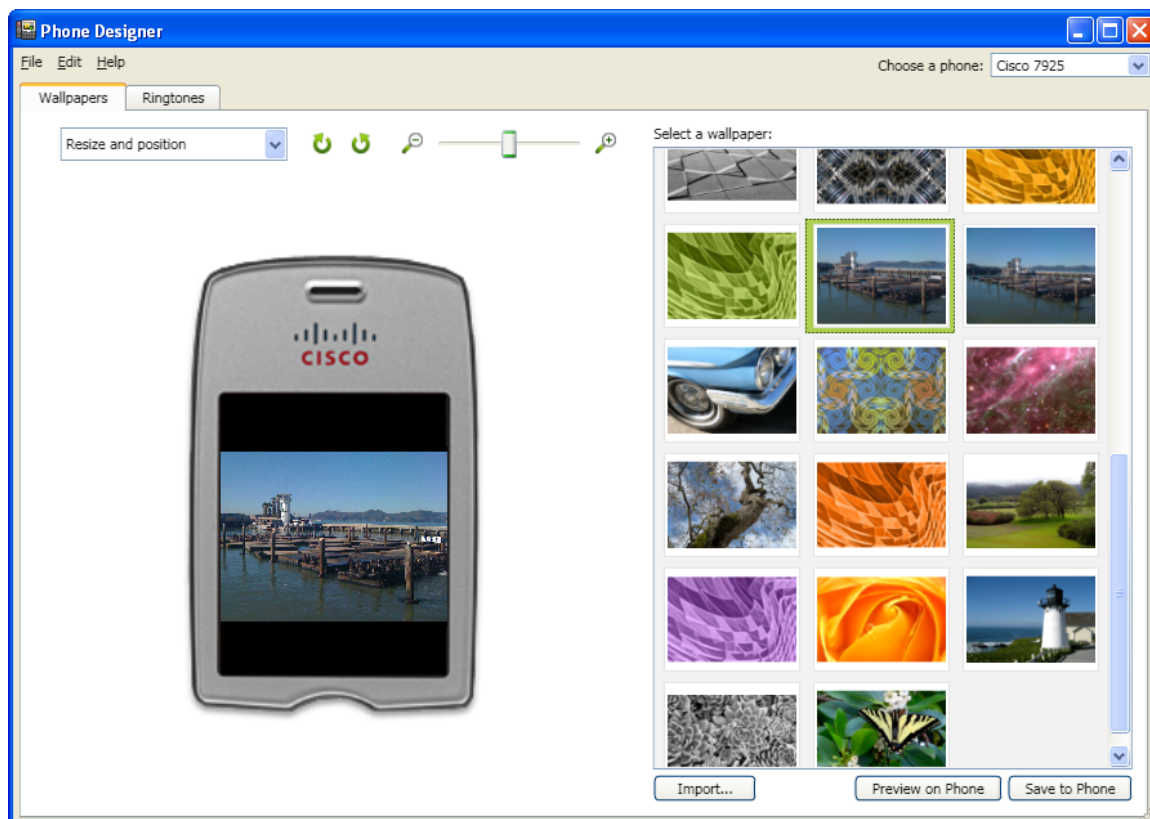
The user account must be created in the Cisco Unified Communications Manager and associated to the corresponding phone.

In order to configure the wallpaper, either select a pre-defined wallpaper or import a wallpaper from the local computer by selecting **Import**.

To display the wallpaper on the phone, select **Preview on Phone**.

To activate and save the wallpaper to the phone flash, select **Save to Phone**.

The default background image can be restored by navigating to **Settings > Phone Settings > Customize Home Page > Background Image**.

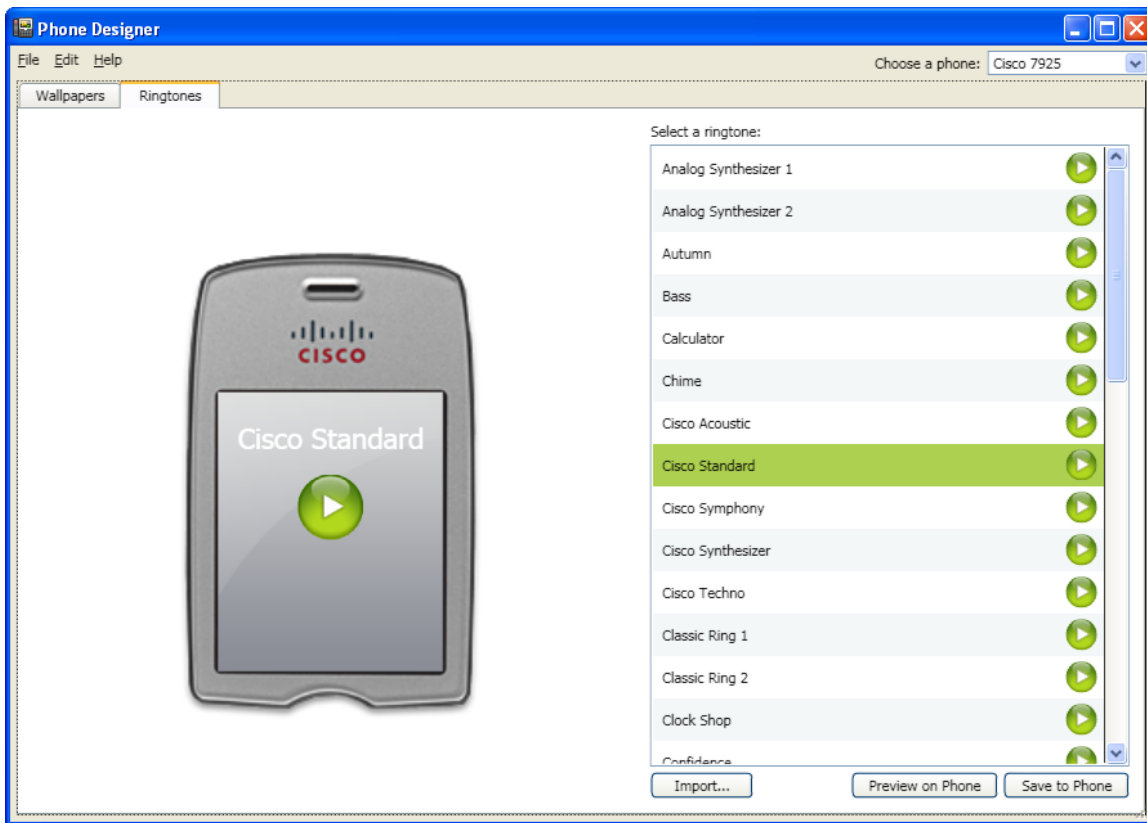


In order to configure the ringtone, either select a pre-defined ringtone or import a ringtone from the local computer by selecting **Import**.

To hear the ringtone on the phone, select **Preview on Phone**.

To activate and save the ringtone to the phone flash, select **Save to Phone**.

A pre-defined ringtone can be enabled by navigating to **Settings > Phone Settings > Sound Settings > Ring Tone**.



The Phone Designer application can be downloaded from the following location.

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

Upgrading Firmware

There are two methods for upgrading the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G firmware, which is either via wireless TFTP or the phone web interface.

Wireless TFTP

To upgrade the phone firmware, run the executable for Cisco Unified Communications Manager version 4.3 or install the COP file for versions 5.1, 6.0, 6.1, 7.0, 7.1, 8.0, 8.5, 8.6, and later.

For information on how to install the COP file on CM versions 5.1 and later, 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 phone configuration file is parsed and the device load is identified. The phone 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 in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G product specific configuration in Cisco Unified Communications Manager Administration.

To install the firmware on Cisco Unified Communications Manager Express, extract the contents of the TAR file and upload into the router's flash. Each file will need to be enabled for TFTP download. Configure the phone load and reset the phones to upgrade the firmware.

7925G Example:

```
tftp-server flash: CP7925G-1.4.6.3.LOADS
tftp-server flash:APPSH-1.4.6.3.SBN
tftp-server flash:GUIH-1.4.6.3.SBN
tftp-server flash:JSYSH-1.4.6.3.SBN
tftp-server flash:JUIH-1.4.6.3.SBN
tftp-server flash:SYSH-1.4.6.3.SBN
tftp-server flash:TNUXH-1.4.6.3.SBN
tftp-server flash:TNUXRH-1.4.6.3.SBN
tftp-server flash:WLANH-1.4.6.3.SBN
!
telephony-service
load 7925 CP7925G-1.4.6.3.LOADS
```

7926G Example:

```
tftp-server flash: CP7926G-1.4.6.3.LOADS
tftp-server flash:APPSS-1.4.6.3.SBN
tftp-server flash:GUIS-1.4.6.3.SBN
tftp-server flash:JSYSS-1.4.6.3.SBN
tftp-server flash:JUIS-1.4.6.3.SBN
tftp-server flash:SYSS-1.4.6.3.SBN
tftp-server flash:TNUXS-1.4.6.3.SBN
tftp-server flash:TNUXRS-1.4.6.3.SBN
tftp-server flash:WLANS-1.4.6.3.SBN
tftp-server flash: EA15FW-BF3-220.SBN
!
telephony-service
load 7925 CP7926G-1.4.6.3.LOADS
```


Web Interface

The phone firmware can be upgraded via the web interface by navigating to Phone Upgrade and browsing to the firmware TAR file.

In order to access the Phone Upgrade menu, the web access must be set to **Full**.

The screenshot displays the web interface for a Cisco Unified Wireless IP Phone 7925G. The interface has a dark blue header with the Cisco logo and the phone model name. Below the header, the phone's unique ID (SEP002290EA9E64) and its Phone DN (89023675) are shown. A left-hand navigation menu lists various settings categories, with 'PHONE UPGRADE' highlighted in yellow. The main content area is titled 'Phone Upgrade' and contains a section for 'Upgrade Phone Software'. This section includes a label 'Phone Software TAR File', a 'Browse...' button, and the text 'No file selected.'. At the bottom right of the interface is an 'Upload' button. The footer contains a copyright notice for Cisco Systems, Inc. from 2006 to 2009.

Cisco Unified Wireless IP Phone 7925G	
SEP002290EA9E64	
Phone DN 89023675	
<ul style="list-style-type: none">HOMESETUPNETWORK PROFILES +USB SETTINGSTRACE SETTINGSWAVELINK SETTINGSCERTIFICATESCONFIGURATIONSPHONE BOOK +INFORMATIONNETWORKWIRELESS LANDEVICESTATISTICSWIRELESS LANNETWORKSTREAM STATISTICSSTREAM 1STREAM 2SYSTEMTRACE LOGSBACKUP SETTINGSPHONE UPGRADECHANGE PASSWORDSITE SURVEYDATE & TIMEPHONE RESTART	Phone Upgrade
	Upgrade Phone Software
	Phone Software TAR File
	<input type="button" value="Browse..."/> No file selected.
	<input type="button" value="Upload"/>

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Note: If the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G registers to Cisco Unified Communications Manager, web access to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G gets set to read-only mode by default. In this mode, firmware upgrades via the web interface are not allowed. Full web access must be enabled in Cisco Unified Communications Manager in order to make changes.

Ultimately the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will use what is set as the phone load in the Cisco Unified Communications Manager.

Hardware Compatibility

The following hardware and software compatibility matrix displays the minimum firmware version for each hardware revision of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

To view the hardware revision information, select **Information > Device** from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G webpage.

Model Type	Hardware Revision	Minimum Firmware Version
7925G & 7925G-EX	1.0	1.3(1)
	1.1	1.3(2)
	2.0, 2.1	1.3(3)
	3.x	1.4(3)SR1
	4.x	1.4(5)SR1
7926G	3.1	1.4(1)SR1
	4.x	1.4(3)SR1
	5.x	1.4(5)SR1

IP Phone Services

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are capable of supporting Extensible Markup Language (XML) applications as well as Java Mobile Information Device Profile (MIDP) applications.

Java MIDP support is included in the 1.4(1) release for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

For information on IP phone services configuration, refer to the following URL.

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_6_1/ccmcfg/bccm-861-cm/b06phsrv.html

Extensible Markup Language (XML)

The following document provides the information needed for eXtensible Markup Language (XML) and X/Open System Interface (XSI) programmers and system administrators to develop and deploy IP phone services.

<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html>

Below are features that are unique to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Vibrate URI

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/all_models/xsi/9-1-1/CUIP_BK_P82B3B16_00_phones-services-application-development-notes/CUIP_BK_P82B3B16_00_phones-services-application-development-notes_chapter_0101.html#CUIP_RF_V4DA08A0_00

Device URI

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/all_models/xsi/9-1-1/CUIP_BK_P82B3B16_00_phones-services-application-development-notes/CUIP_BK_P82B3B16_00_phones-services-application-development-notes_chapter_0101.html#CUIP_RF_DADA79D4_00

As of the 1.4(3) release, if a tone is pushed to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G via XSI while on call, an alternate tone to the standard call waiting tone will be played so the user can distinguish the event type audibly.

Also in the 1.4(3) release, pressing the red button can silence a tone pushed via XSI.

XSI Audio Path Control

With the 1.4(4) release, the RTP URI has been extended to give an admin the option to specify whether audio received via XSI is played via the speakerphone or the handset speaker of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G.

In releases prior to 1.4(4), the audio path is always set to speakerphone mode when an XSI “call” is received unless a headset is connected. The audio path could then be changed to the handset as necessary by the user.

The current RTP URI format is RTPRx:i:p:v or RTPMRx:i:p:v, where **i** equals IP address (x.x.x.x), **p** equals UDP port (20480-32768), and **v** equals volume (0-100). The volume value is a percentage of the maximum volume supported by the endpoint.

With the 1.4(4) release, there will be an additional parameter (speakerphone) supported (e.g. RTPRx:i:p:v:s or RTPMRx:i:p:v:s). The **s** parameter is to specify which audio path the Cisco Unified Wireless Phone 7925G, 7925G-EX, and 7926G should utilize.

If **s** is set to 0 then the speakerphone will be utilized; unless a headset is connected, where the audio will then be played to the headset.

If **s** is set to 1, then the handset or headset speaker will be utilized depending on whether a headset is currently connected or not.

If **s** is set to 2, then the current local mode will be utilized depending on whether speakerphone is enabled or not. If a headset is connected, audio will always be played to the headset.

If the **s** parameter is not specified, then the Cisco Unified Wireless Phone 7925G, 7925G-EX, and 7926G will set the audio path to speakerphone mode; unless a headset is connected, where the audio will then be played to the headset.

If currently on call and an XSI “call” comes in, then the current audio path will be used regardless of the **s** parameter value.

The audio path can be switched to the speakerphone or handset after a XSI “call” is received.

If wanting to utilize the **s** parameter for XSI “calls”, the port and volume parameters are optional, but if not specified the colon must still be specified for that parameter (e.g. RTPRx:10.0.0.10:20500::1, RTPRx:10.0.0.10:::1, RTPMRx:10.0.0.10:20500::1, RTPMRx:10.0.0.10:::1).

If the port parameter is not specified, then the endpoint will select a UDP port and respond to the XSI push with that info.

If the volume parameter is not specified, then the endpoint will utilize its current volume setting.

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/all_models/xsi/9-1-1/CUIP_BK_P82B3B16_00_phones-services-application-development-notes/CUIP_BK_P82B3B16_00_phones-services-application-development-notes_chapter_0101.html#CUIP_RF_X9E58C52_00

The chart below provides a few examples of the supported XSI audio path configurations per stream type.

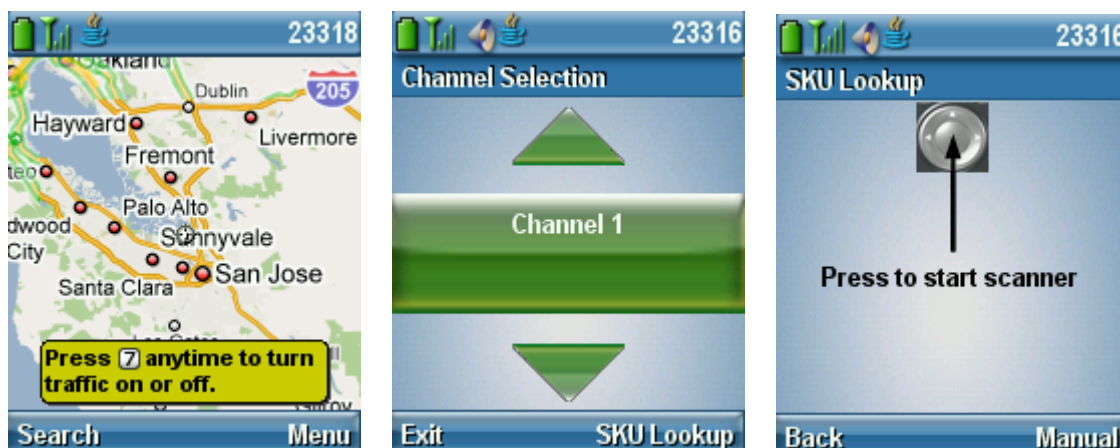
XSI Audio Path	Stream Type	RTP URI Example
Speakerphone	Unicast	RTPRx:10.0.0.10:20500 RTPRx:10.0.0.10:20500::0 RTPRx:10.0.0.10:20500:100:0
Handset / Headset	Unicast	RTPRx:10.0.0.10:20500::1 RTPRx:10.0.0.10:20500:100:1

Speakerphone	Multicast	RTPMRx:10.0.0.10:20500 RTPMRx:10.0.0.10:20500::0 RTPMRx:10.0.0.10:20500:100:0
Handset / Headset	Multicast	RTPMRx:10.0.0.10:20500::1 RTPMRx:10.0.0.10:20500:100:1

Java Mobile Information Device Profile (MIDP)

The following document provides the information needed for Java Mobile Information Device Profile (MIDP) programmers and system administrators to develop and deploy IP phone services.

<https://developer.cisco.com/web/jmapi/home>



As of the 1.4(4) release, timezone support has been added; therefore the Java Timezone API is now supported.

As of the 1.4(5) release, a Java MIDlet can now be automatically launched then minimized to the background after the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is powered on by utilizing the Idle URL feature.

Prior to the 1.4(5) release, a Java MIDlet had to be manually launched.

To have a Java MIDlet auto-launch, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G must be subscribed to the Java MIDlet application that is to be specified in the Idle URL configuration. If the Java MIDlet is not subscribed to, then the auto-launch will fail.

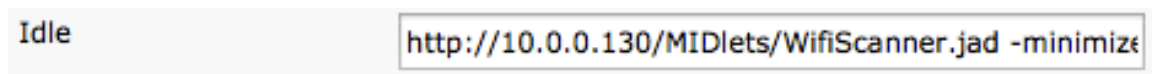
Once the Java MIDlet is subscribed to, configure the Idle URL to point to the Java MIDlet application then add **-minimize** to the end of the URL (e.g. <http://10.0.0.130/MIDlets/WifiScanner.jad> -minimize)

The Java MIDlet will then automatically launch then minimize to the background once the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G registers to CUCM after being powered on.

If the Java MIDlet is closed manually after the Java MIDlet is automatically launched then minimized, then the Java MIDlet must be manually re-launched or the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G must be power cycled.

The Idle URL Timer parameter is not utilized for this feature as the Java MIDlet is only auto-launched immediately once the CUCM registration event occurs after powering the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G on.

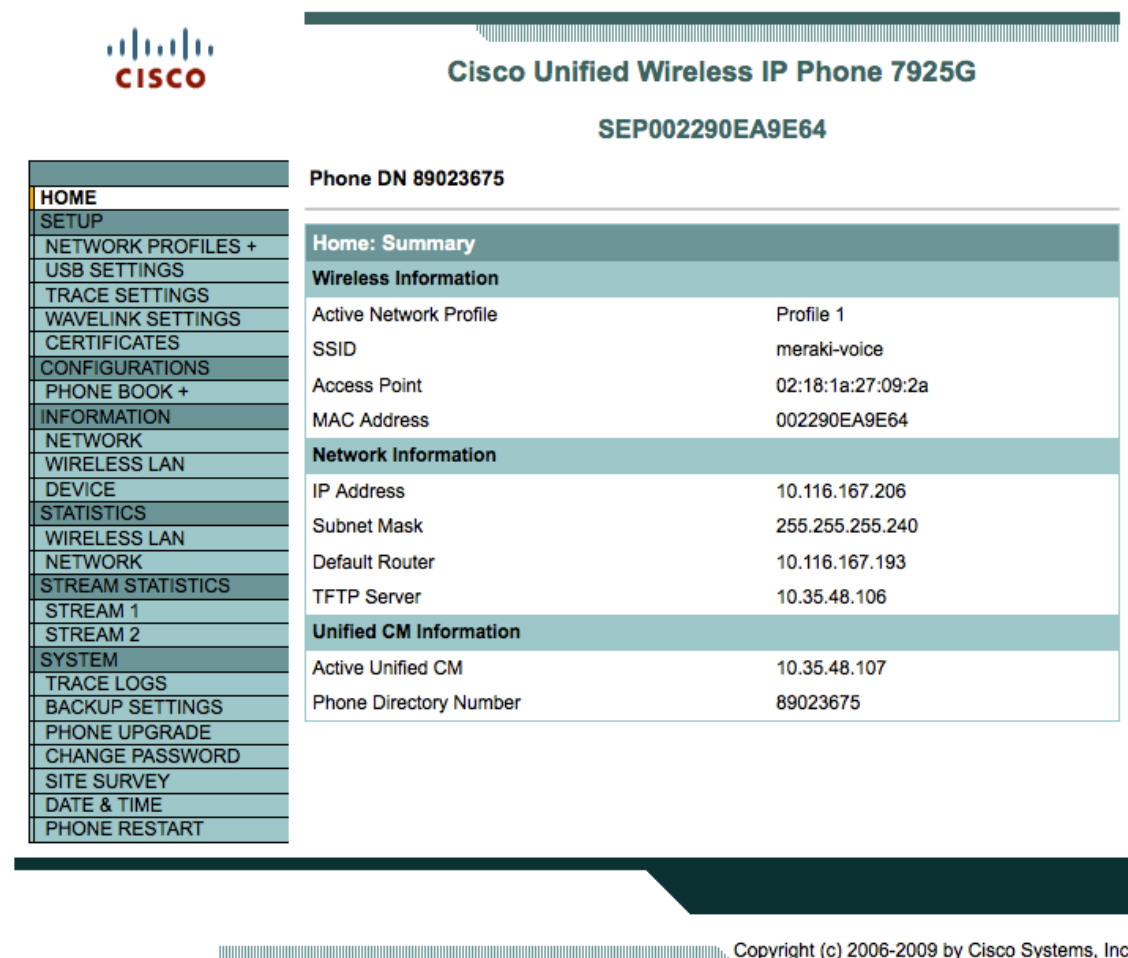
Note: There is a space between the end of the URL and **-minimize**, but there is not a space between **-** and **minimize**.



Troubleshooting

Device Homepage

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G webpage provides wireless, network, and Unified CM information.



Cisco Unified Wireless IP Phone 7925G
SEP002290EA9E64

Phone DN 89023675

Home: Summary

Wireless Information	
Active Network Profile	Profile 1
SSID	meraki-voice
Access Point	02:18:1a:27:09:2a
MAC Address	002290EA9E64

Network Information	
IP Address	10.116.167.206
Subnet Mask	255.255.255.240
Default Router	10.116.167.193
TFTP Server	10.35.48.106

Unified CM Information	
Active Unified CM	10.35.48.107
Phone Directory Number	89023675

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Device Information

MAC address, hostname, directory number, and hardware and software version information is displayed in the Device Information section of the phone webpage.

Browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Device** under the Information menu to view this information.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Device Information

MAC Address	002290EA9E64
Host Name	SEP002290EA9E64
Directory Number	89023675
System Load ID	CP7925G-1.4.5.3.LOADS
Version	V01
Serial Number	IAC1244A0R3
Model Number	CP-7925G
Message Waiting	False
UDI	Phone
	Cisco Unified Wireless IP Phone 7925G
	CP-7925G
	V01
	IAC1244A0R3
Time	05.09PM
TimeZone	UTC
Date	11/07/13
Hardware Revision	1.0
WLAN Regulatory Domain	0x1050
USB Vendor/Product ID	0x05A6 / 0x000A
USB RNDIS Device Address	002333309E5C
USB RNDIS Host Address	002333309E5D
MIDlet Memory Usage	1650 kB

Copyright (c) 2006-2009 by Cisco Systems, Inc.

This information is also available locally on the phone under **Settings > Model Information**.

Wireless LAN Information

Detailed WLAN information is displayed in the Wireless LAN Information section of the phone webpage.

Browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Wireless LAN** under the Information menu to view this information.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

WLAN Information

Active Network Profile	Profile 1
MAC Address	002290EA9E64
SSID	meraki-voice
802.11 Mode	802.11a
Scan Mode	Continuous
Restricted Data Rates	False
Call Power Save Mode	U-APSD/PS-POLL
BSSID	02181a27092a
Access Point	02:18:1a:27:09:2a
Tx Power	15 dBm
Channel	44
RSSI	-46
Channel Utilization	0
DTIM period (ms)	1
Security Mode	PEAP
Encryption	AES
Key Management	WPA2

Copyright (c) 2006-2009 by Cisco Systems, Inc.

This information is also available locally on the phone under **Settings > Device Information > WLAN**.

Network Information

IP, Unified CM, SRST, MLPP, QoS, security, URL, and locale information is displayed in the Network Information section of the phone webpage.

Browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Network** under the Information menu to view this information.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Network Information

IP Information

DHCP Server	10.116.167.193
BOOTP Server	No
MAC Address	002290EA9E64
Host Name	SEP002290EA9E64
Domain Name	cisco.com
CDP	Enabled
IP Address	10.116.167.206
Subnet Mask	255.255.255.240
Default Router1	10.116.167.193
DNS Server1	64.102.6.247
DNS Server2	161.44.124.122
TFTP Server1	10.35.48.106
Alternate TFTP enabled	Yes
TFTP Server2	

Unified CM Information

Unified CM 1	gigantic-7 : Active
Unified CM 2	ccm-sjctg-013 : Standby
Unified CM 3	
Unified CM 4	
Unified CM 5	

This information is also available locally on the phone under **Settings > Device Information**.

Stream Statistics

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G provide call statistic information, where MOS, jitter and packet counters are displayed.

DSCP for transmit and receive paths are also displayed, which can help to ensure that packets are being placed into the correct queues upstream and downstream.

The MOS value should be greater than or equal to 4.0 when using G.722 or G.711.

A MOS value of 3.8 is the highest possible value when using G.729.

Browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Stream Statistics**.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Stream Statistics

RTP Statistics

Domain Name	snmpUDPDomain	Remote Address	10.81.12.51
Remote Port	26862	Local Address	10.81.12.32
Local Port	22032	Sender Joins	4
Receiver Joins	4	Byes	3
Start Time	10:59:56	Row Status	Active
Host Name	SEP002290EA9E64	Sender DSCP	EF
Sender Packets	605	Sender Octets	104060
Sender Tool	G.722	Sender Reports	1
Sender Report Time	11:00:02	Sender Start Time	10:59:56
Receiver DSCP (Previous, Current)	EF, EF	Receiver Packets	594
Receiver Octets	95040	Receiver Tool	G.722
Receiver Lost Packets	0	Receiver Jitter	18
Receiver Reports	2	Receiver Start Time	10:59:56

Voice Quality Metrics

MOS LQK	4.5000	Avg MOS LQK	4.4580
Min MOS LQK	4.3828	Max MOS LQK	4.5000
MOS LQK Version	0.95	Cumulative Conceal Ratio	0.0017
Interval Conceal Ratio	0.0000	Max Conceal Ratio	0.0079
Conceal Seconds	1	Severely Conceal Seconds	0

Refresh Stop

Copyright (c) 2006-2009 by Cisco Systems, Inc.

This information is also available locally on the phone under **Settings > Status > Call Statistics** or if on a phone call press the center button twice.


For more information, see the **Troubleshooting the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G** chapter in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide at this URL:

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-maintenance-guides-list.html>

Wireless LAN Statistics

Wireless LAN transmit and receive statistic information is displayed in the Wireless LAN Statistics section of the phone webpage.

Browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Wireless LAN** under the Statistics menu to view this information.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME	Stream Statistics			
SETUP	RTP Statistics			
NETWORK PROFILES +	Domain Name	snmpUDPDomain	Remote Address	10.81.12.51
USB SETTINGS	Remote Port	32386	Local Address	10.116.167.206
TRACE SETTINGS	Local Port	29680	Sender Joins	2
WAVELINK SETTINGS	Receiver Joins	2	Byes	1
CERTIFICATES	Start Time	17:17:10	Row Status	Active
CONFIGURATIONS	Host Name	SEP002290EA9E64	Sender DSCP	EF
PHONE BOOK +	Sender Packets	1084	Sender Octets	186448
INFORMATION	Sender Tool	G.722	Sender Reports	4
NETWORK	Sender Report Time	17:17:30	Sender Start Time	17:17:10
WIRELESS LAN	Receiver DSCP (Previous, Current)	EF, EF	Receiver Packets	1072
DEVICE	Receiver Octets	171520	Receiver Tool	G.722
STATISTICS	Receiver Lost Packets	2	Receiver Jitter	12
WIRELESS LAN	Receiver Reports	3	Receiver Start Time	17:17:11
NETWORK	Voice Quality Metrics			
STREAM STATISTICS	MOS LQK	4.5000	Avg MOS LQK	4.3718
STREAM 1	Min MOS LQK	4.2915	Max MOS LQK	4.5000
STREAM 2	MOS LQK Version	0.95	Cumulative Conceal Ratio	0.0019
SYSTEM	Interval Conceal Ratio	0.0000	Max Conceal Ratio	0.0066
TRACE LOGS	Conceal Seconds	2	Severely Conceal Seconds	0
BACKUP SETTINGS				
PHONE UPGRADE				
CHANGE PASSWORD				
SITE SURVEY				
DATE & TIME				
PHONE RESTART				

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Network Statistics

IP, TCP, and UDP statistic information is displayed in the Network Statistics section of the phone webpage.

Browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Network** under the Statistics menu to view this information.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Network Statistics

IP Statistics

IpInReceives	33963	IpInHdrErrors	0
IpInAddrErrors	0	IpForwDatagrams	0
IpInUnknownProtos	0	IpInDiscards	0
IpInDelivers	26902	IpOutRequests	35451
IpOutDiscards	0	IpOutNoRoutes	0
IpReasmTimeout	0	IpReasmReqds	0
IpReasmOKs	0	IpReasmFails	0
IpFragOKs	0	IpFragFails	0
IpFragCreates	0		

TCP Statistics

TcpRtoAlgorithm	0	TcpRtoMin	0
TcpRtoMax	0	TcpMaxConn	0
TcpActiveOpens	281	TcpPassiveOpens	66
TcpAttemptFails	0	TcpEstabResets	0
TcpCurrEstab	8	TcpInSegs	15016
TcpOutSegs	23516	TcpRetransSegs	996
TcpInErrs	0	TcpOutRsts	119

UDP Statistics

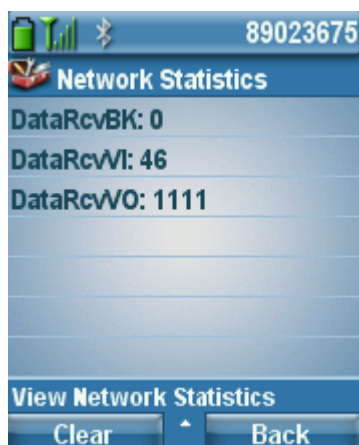
UdpInDatagrams	11158	UdpNoPorts	728
UdpInErrors	0	UdpOutDatagrams	11205

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Queue statistics can also be displayed by navigating to **Settings > Status > Network Statistics**.

If on a phone call, should see the **DataRcvVO** counter increasing assuming QoS has been deployed correctly.

This reflects that voice packets are being properly marked as UP6 (VO) downstream to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

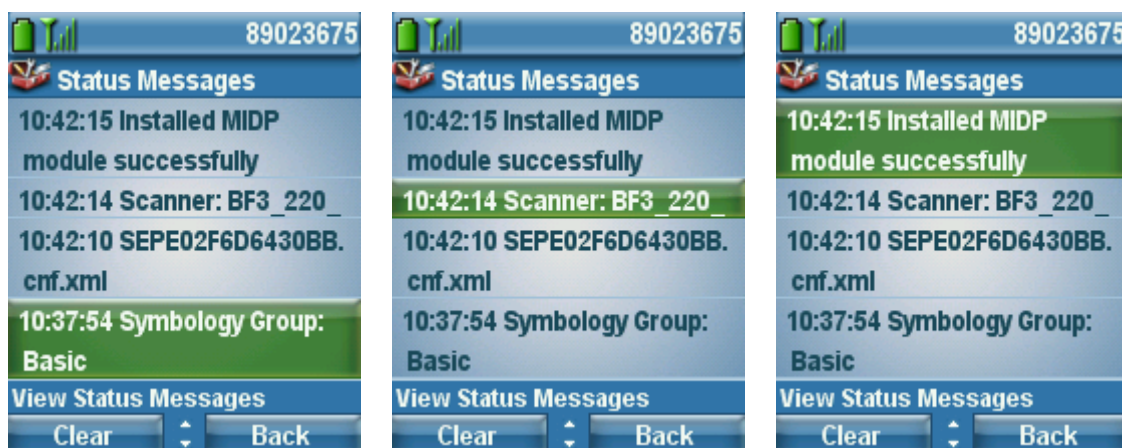


Cisco 7926G Barcode Status Messages

Status messages on the Cisco Unified Wireless IP Phone 7926G provide information in regards to barcode scanner firmware installation, Java MIDP Add On Module (AOM) installation, and barcode scanner symbology group configuration events for the Cisco Unified Wireless Phone 7926G.

To view the status messages navigate to **Settings > Status > Status Messages**.

The barcode scanner firmware for the Cisco Unified Wireless IP Phone 7926G is included in the signed COP and ZIP files (scanner firmware is not included in the TAR file).



Phone Logs


Phone logs for troubleshooting purposes can be obtained from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G web interface.

Trace Settings

Browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Trace Settings** to enable debugging.

The phone logs are stored in memory only by default, but can optionally enable **Preserve Logs** where the logs will be stored in flash.

Syslog can also be enabled to capture logging real-time via the wireless LAN or USB interface.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

- HOME
- SETUP
- NETWORK PROFILES +
- USB SETTINGS
- TRACE SETTINGS**
- WAVELINK SETTINGS
- CERTIFICATES
- CONFIGURATIONS
- PHONE BOOK +
- INFORMATION
- NETWORK
- WIRELESS LAN
- DEVICE
- STATISTICS
- WIRELESS LAN
- NETWORK
- STREAM STATISTICS
- STREAM 1
- STREAM 2
- SYSTEM
- TRACE LOGS
- BACKUP SETTINGS
- PHONE UPGRADE
- CHANGE PASSWORD
- SITE SURVEY
- DATE & TIME
- PHONE RESTART

Phone DN 89023675

Trace Settings

General

Number of Files

2

File Size

50

Kilo Bytes

Remote Syslog Server

☐ Enable Remote Syslog

IP Address

0.0.0.0

Port (Valid range is 514, 1024-65535)

514

Module Trace Level

Kernel

Error

Wireless LAN Driver

Error

Wireless LAN Manager

Error

Configuration

Error

Call Control

Error

Network Services

Error

Security Subsystem

Error

User Interface

Error

Audio System

Error

System

Error

Java

Error

Bluetooth

Error

Advanced Trace Settings

Preserve Logs

☐ True
 ☒ False

Reset Trace Settings upon Reboot

☒ Yes
 ☐ No

Save

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Trace Modules

Kernel	Operating System
Wireless LAN Driver	Channel scanning, roaming, authentication
Wireless LAN Manager	WLAN Management, QoS
Configuration	Phone configuration, firmware upgrade
Call Control	Cisco Unified Communications Manager messaging (SCCP)
Network Services	DHCP, TFTP, CDP, WWW, Syslog

Security Subsystem	Application level security
User Interface	Keypad, softkeys, MMI
Audio System	RTP, SRTP, RTCP, DSP
System	Event Manager
Java	Java MIDP
Bluetooth	Bluetooth

Trace Levels

Various levels of tracing are available, that can provide different levels of messaging.

Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug

Note: All trace modules are set to Error level by default.

Voice quality can potentially be impacted if higher trace levels are configured or if **Preserve Logs** is enabled, which will write the logs to flash memory.

The trace level will reset to **Error** level by default unless configured to preserve the trace levels where **Reset Trace Settings upon Reboot** is set to **No**.

Trace Logs

To download the phone logs, browse to the web interface (<https://x.x.x.x>) of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G then select **Trace Logs**.



Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

HOME

SETUP

NETWORK PROFILES +

USB SETTINGS

TRACE SETTINGS

WAVELINK SETTINGS

CERTIFICATES

CONFIGURATIONS

PHONE BOOK +

INFORMATION

NETWORK

WIRELESS LAN

DEVICE

STATISTICS

WIRELESS LAN

NETWORK

STREAM STATISTICS

STREAM 1

STREAM 2

SYSTEM

TRACE LOGS

BACKUP SETTINGS

PHONE UPGRADE

CHANGE PASSWORD

SITE SURVEY

DATE & TIME

PHONE RESTART

Phone DN 89023675

System Trace Logs

messages.0

messages

Download Logs

Copyright (c) 2006-2009 by Cisco Systems, Inc.

Radio Status Indicator

The Cisco Unified Wireless IP Phone 7925 can help determine whether the radios is functional or not by displaying a number of bars for the signal indicator.

The number of bars equates to the signal received by the access point and will display those bars in either grey, yellow or green depending on the current status.

Below the correlation between the color and status are defined.

Grey - The phone is in range of some network, but it may not be in range of the configured network.

This could also be due to a SSID configuration issue.

Yellow - The phone has detected it is in range of the configured network and 802.11 band and is attempting to authenticate to the access point. If the indicator does not move to the green status, then there could be an issue with the authentication configuration.

Green - The phone is currently authenticated to the access point.



Hardware Diagnostics

A self-diagnostics tool is available that can help with hardware analysis.

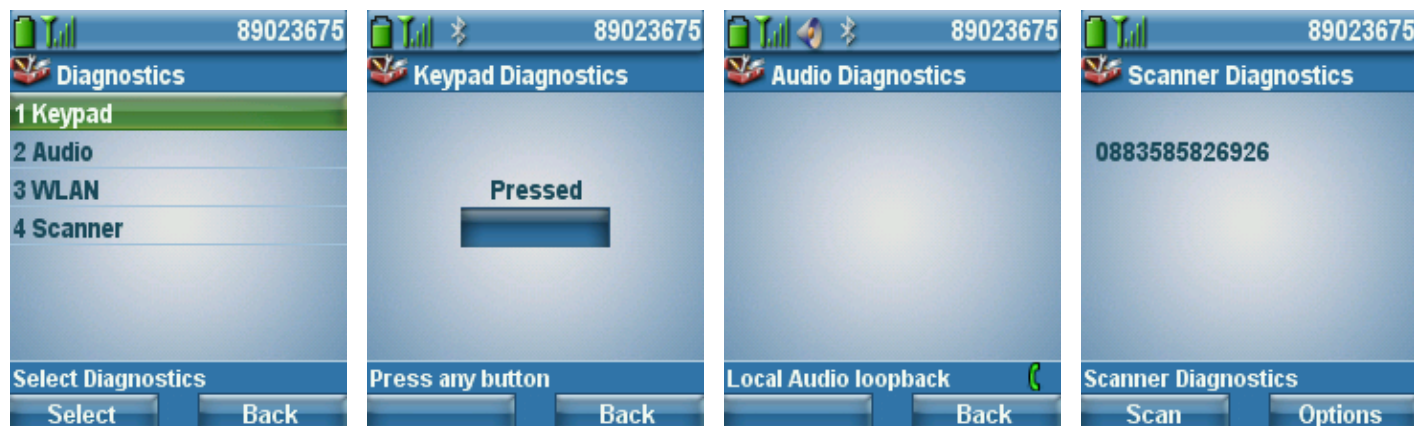
The Diagnostics menu is located under Phone Settings menu, where the Keypad, Speaker and Microphone, Barcode Scanner, and Wireless LAN Radio and Antenna can be validated.

The keypad diagnostics allows for a button to be pressed and released to ensure they are functional.

The audio diagnostics performs an audio loopback, so the speaker and microphone can be validated.

The WLAN diagnostics menu is the standard Site Survey utility, which will use the current network profile information to perform passive and active scans for the configured SSID and 802.11 mode.

The scanner diagnostics will allow to scan a 2D barcode to ensure the scan engine is functional. A **Reset** option is available to reinitialize the barcode scanner.



Firmware Recovery

If the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G does not boot properly, then the firmware can be recovered via the USB connection.

Be aware that the current settings will be reset to factory defaults when performing the firmware recovery process.

Use the following steps to perform a firmware recovery.

1. Power on the phone while holding down the application button and the speakerphone button simultaneously and keep it held until **Starting Recovery Mode** is displayed.
2. A firmware check will then be performed.
3. Insert the USB cable into the phone after USB initialization is complete.
(Ensure that the USB driver has been installed prior and that an IP in the 192.168.1.0 /24 network has been configured for that network connection)
4. When **Web Access Available...** is displayed, then navigate to <http://192.168.1.100>.
5. Browse to the TAR file and then click **Upload**.



Cisco Unified Wireless IP Phone 7925G

Phone Recovery	
Update Phone Software	
Phone Software TAR File	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upload"/>	
Device Information	
System Load ID	CP7925G-1.3.3.LOADS *** Integrity Check Success ***
Version	V01
Serial Number	IAC1245A013
Model Number	CP-7925G
Hardware Revision	1.0
WLAN Regulatory Domain	0x1050
USB Vendor/Product ID	0x05A6 / 0x000A
USB RNDIS Device Address	002333309AF8
USB RNDIS Host Address	002333309AF9

Restoring Factory Defaults

The configuration can be cleared by using the factory default menu option on the phone.

The factory default option erases all user-defined entries in Network Profiles, Phone Settings, and Call History.

To erase the local configuration, follow these steps:

1. Choose **Settings > Phone Settings**.
2. Press ****2** on the keypad.
The phone briefly displays **Restore to Default?**
3. Press the **Yes** softkey to confirm or **No** to cancel.
The phone resets after selecting **Yes**.

Capturing a Screenshot of the Phone 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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G. At the prompt enter the username and password for the account for which the phone is associated to.

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 Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

For more information, refer to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Accessories Guide at this URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0_1/english/accessory_guide/P256_BK_W4FDAA91_00_wireless-ip-phone-accessories-guide.html

- Cisco Unified Wireless IP Phone 7925G Desktop Charger
- Multi-Charger
- Batteries (Standard and Extended)
- Carry Cases (Holster and Leather)
- Ruggedized Case (for 7925G and 7925G-EX only)
- Lock Set
- USB Cable

For more information on the Cisco Unified Wireless IP Phone 7925G Desktop Charger, refer to the following URL:

http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0/english/quick_start/7925Ch_qs.pdf

For more information on Jawbone ICON for Cisco Bluetooth Headset, refer to the following URL:

http://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/jawbone-icon-bluetooth-headset/C78-615196-00_Jawbone_ICON_Cisco_Bluetooth_Headset_DS.pdf



3rd Party Accessories

- Headsets www.plantronics.com (Quick Disconnect 2.5 mm Adapter - part # 65287-01)
www.jabra.com
www.jawbone.com
www.vxicorp.com
www.motorola.com





Note: The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are unable to utilize accessories from the Cisco Unified Wireless IP Phone 7921G, as they are not compatible.

The Cisco Unified Wireless IP Phone 7925G and 7925G-EX utilize the same accessories.

The batteries and chargers are the same for the 7925G, 7925G-EX, and 7926G, but have different cases.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G has a 2.5 mm, 3 band / 4 conductor wired headset jack (Nokia compatible).

Additional Documentation

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Data Sheets

http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-wireless-ip-phone-7925g/data_sheet_c78-504890.html

http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-wireless-ip-phone-7925g-ex/data_sheet_c78-565676.html

http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-wireless-ip-phone-7926g/data_sheet_c78-649589.html

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-maintenance-guides-list.html>

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-user-guide-list.html>

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Accessory Guide

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0_1/english/accessory_guide/P256_BK_W4FDA91_00_wireless-ip-phone-accessories-guide.html

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Release Notes

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-release-notes-list.html>

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Software

<http://software.cisco.com/download/type.html?mdfid=282359287>

<http://software.cisco.com/download/type.html?mdfid=283471435>

Open Source License Notices for the Cisco Unified IP Phones 7900 Series

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-licensing-information-listing.html>

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>

Cisco Unified Wireless IP Phone 792xG + Cisco Meraki Wireless LAN Deployment Guide

Cisco Unified IP Phone Services Application Development Notes

<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html>

Cisco Meraki Wireless LAN Documentation

<https://meraki.cisco.com/products/wireless>

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>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

 The Bluetooth word mark and logo are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Cisco Systems, Inc., is under license.

© 2015 Cisco Systems, All rights reserved.