Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide

First Published: 2017-11-22

Last Modified: 2019-08-05

CONTENTS

New and Changed Information

New and Changed for Firmware Release 11.2(4)

Revision	New and Changed Sections
Updated the hardware-related topics with Cisco IP Phone 6861 Multiplatform Phones	Physical and Operating Environment Specifications, on page 11
	Network and Computer Port Pinouts, on page 13
	Phone Power Requirements, on page 14
	Power Negotiation Over LLDP, on page 16
	Overview of the Cisco IP Phone 6800 Series Multiplatform Phones, on page 23
	Cisco IP Phone 6841, 6851, and 6861 Multiplatform Phones Buttons and Hardware, on page 29
	Install the Cisco IP Phone, on page 36
Uppdated the supported accessories for Cisco IP Phone 6861 Multiplatform Phones	Supported Accessories, on page 99
	Headsets, on page 107
	Install a Cisco IP Phone 6841, 6851, or 6861 with the Wall Mount Kit, on page 114
	Enable Electronic Hookswitch, on page 180
Added a topic about how to connect Cisco IP Phone 6861 Multiplatform Phones	Cisco IP Phone 6861 Multiplatform Phones Connections, on page 26

Revision	New and Changed Sections
Added topics about Wi-Fi settings on Cisco IP Phone 6861 Multiplatform Phones	Wi-Fi Settings, on page 45
	Turn the Wi-Fi On or Off from Your phone, on page 45
	Turn the Wi-Fi On or Off from the Phone Web Page, on page 45
	Connect the Phone to a Wi-Fi Manually, on page 46
	Connect Your Phone to a Wireless Network with WPS, on page 47
	Set Up a Wi-Fi Profile from the Phone, on page 48
	Set Up a Wi-Fi Profile from the Phone Web Page and the XML Provisioning Server, on page 50
	Delete a Wi-Fi Profile, on page 52
	Change the Order of a Wi-Fi Profile , on page 53
	Scan and Save a Wi-Fi Network, on page 53
	View the Wi-Fi Status, on page 55
	View Wi-Fi Status Messages on the Phone, on page 56
	Wi-Fi Settings, on page 229
	Wi-Fi Profile (n) , on page 229

New and Changed for Firmware Release 11.2(3)SR1

Revision	New and Changed Sections
Added a new task to support Activation Code Onboarding	Activation Code Onboarding, on page 37

New and Changed for Firmware Release 11.2(3)

Revisions	New and Changed Sections
Added Catalan to the supported language list	Supported Languages for the Phone Display, on page 85
Updated the `--key` keyword details and added a note about RFC 8188-based encryption.	Report Current Phone Configuration to the Provisioning Server, on page 90
Added a new task and a new field to support audio compliance standards: ETSI and TIA	Specify Audio Compliance Standard, on page 138
	Audio Compliance, on page 295

Revisions	New and Changed Sections
Added a new task on how to phone users to configure speed dial and monitor a coworker's line.	Enable Users to Configure Features on Line Keys, on page 157
Added a new topic replacing the existing *Busy Lamp Field Configuration on a Monitoring Phone* topic.	Phone Configuration for Monitoring Other Phones, on page 162
Added a new topic replacing the existing *Configure the Phone to Monitor Multiple Users' Lines* topic.	Configure the Phone to Monitor Multiple Users' Lines, on page 162
Added a new task on how to enable early media support	Enable P-Early-Media Support, on page 188
Added topics replacing the "Set up Profile Account" topic to support the enhancements in profile authentication	Profile Authentication, on page 189 Specify the Profile Authentication Type, on page 190
Added new fields and topics to support the feature of DND and call forwarding status sync	DND and Call Forwarding Status Sync, on page 192 Enable Feature Key Sync, on page 193 Enable Call Forwarding Status Sync via XSI Service, on page 194 Enable DND Status Sync via XSI Service, on page 194 XSI Line Service, on page 287
Added a new topic about including a device identifier in uploaded syslog messages.	Include a Device Identifier in Uploaded Syslog Messages, on page 203
Added new fields and a new task on how to remotely report phone problems.	Report a Phone Problem Remotely, on page 316 PRT Status, on page 215
Added the *Syslog Identifier* field.	Optional Network Configuration, on page 225
Replaced the *Profile Account Enable* parameter with the *Profile Authentication Type* field Updated the description of the *Profile Rule* parameter.	Configuration Profile, on page 241
Updated *Report Rule* and added new parameters: *Report to Server*, *periodic Upload to Server*, and *Upload Delay on Local Change*.	Upload Configuration Options, on page 247
Updated the *Wideband Handset Support* parameter to support the wideband handset enhancement.	**Voice** > **Phone** > General, on page 264
Updated the description for the *Extension* field.	Line Key, on page 264
Updated the description of the *First Name Filter* and *Last Name Filter* fields.	LDAP, on page 271

Revisions	New and Changed Sections
Example XML parameter configuration is added for the *Line Enable* parameter.	**Voice** > **Ext (n)** > General, on page 276
The new fields *Customizable PLK Options* and *BLF List*, and their descriptions are added to the table. The description for the *BLF List URI* and *Use Line Keys For BLF List* fields are updated.	**Voice** > **Att Console** > General, on page 297

New and Changed for Firmware Release 11.2(2)

Revisions	New and Changed Sections
Added a new topic to introduce the phone buttons and hardware of Cisco IP Phone 6821 Multiplatform Phones	Cisco IP Phone 6821 Multiplatform Phones Buttons and Hardware, on page 27
Added a new topic to explain how to connect your of Cisco IP Phone 6821 Multiplatform Phones	Cisco IP Phone 6821 Multiplatform Phones Connections, on page 24
Added a new topic to show how to install your Cisco IP Phone 6821 Multiplatform Phones on a wall	Install the Cisco IP Phone 6821 Multiplatform Phones on a Wall, on page 110
Updated the topic to include the information about the new phone model of 6821	Overview of the Cisco IP Phone 6800 Series Multiplatform Phones, on page 23
Updated the topic with the information of 6821 softkeys, line, and feature buttons	Softkey, Line, and Feature Buttons, on page 30
Updated the topic with 6821 specifications	Physical and Operating Environment Specifications, on page 11
Updated the topic with power requirements for Cisico IP Phone 6821 Multiplatform Phones	Phone Power Requirements, on page 14
Updated the supported accessories for Cisico IP Phone 6821 Multiplatform Phones	Supported Accessories, on page 99
Updated the topic with 6821 wall mount kit information	Wall Mount Kit Components, on page 109
Updated the topic with the information of 6821 display screen size	Add a Logo as the Boot Display, on page 128
Updated the topic to indicate that only 6851 support the EHS feature	Enable Electronic Hookswitch, on page 180

Along with the above changes, some existing sections have been retitled to include Cisco IP Phone 6841 and 6851 Multiplatform Phones.

New and Changed for Firmware Release 11.2(1)

Revisions	New or Changed Sections
Updated the topics to support LCD screen does not honor "ro" and "na" attribute	Enable User Access to the Phone Interface Menus, on page 94 System Configuration, on page 222
Added a new topic to support NAPTR	Configure the SIP Transport, on page 186
Updated the topics to support NAPTR	Telephony Features for Cisco IP Phone, on page 148 SIP Settings, on page 277
Added a new topic to support SIP privacy header	Configure a Privacy Header, on page 187.
Updated the topic to support SIP privacy header	SIP Settings, on page 277
Added a new topic to support blocking of SIP message from a non-proxy device	Block Non-Proxy SIP Messages to a Phone, on page 186
Updated the topic to support blocking of SIP message from a non-proxy device	System Configuration, on page 222
Added a new topic to support Peer Firmware Sharing	Peer Firmware Sharing, on page 188 Enable Peer Firmware Sharing, on page 189
Updated the topic to support Peer Firmware Sharing	Telephony Features for Cisco IP Phone, on page 148 Firmware Upgrade, on page 249
Updated the topic to support profile account	Configuration Profile, on page 241
Added new topic to support call silence	Add Ignore Programmable Soft Key to Silence an Incoming Call, on page 190
Updated the topics to support call silence	Programmable Softkeys, on page 171 Telephony Features for Cisco IP Phone, on page 148
Added new topics to support XSI BroadWorks Anywhere	Enable BroadWorks Anywhere, on page 191 XSI Line Service, on page 287
Added new topics to support XSI caller ID blocking	Sync the Block Caller ID Feature with the Phone and the BroadWords XSI Server, on page 191 XSI Line Service, on page 287
Added new topics to support XSI call logs	Enable Viewing BroadWorks XSI Call Logs on a Line , on page 192
Updated the topics to support XSI call logs	XSI Phone Service, on page 268 Telephony Features for Cisco IP Phone, on page 148

Revisions	New or Changed Sections
Updated the topic to support screen saver type "lock" removal	Configure the Screen Saver with the Phone Web Page, on page 160

New and Changed for Firmware Release 11.1(2)

Feature	New or Changed Sections
Add support for LDAP over TLS(LDAPS). Updated administration information with a new task to configure LDAP over TLS	Configure LDAP over TLS, on page 124
Add support for DHCP VLAN options. Updated administration information with new tasks to set up DHCP VLAN options	Set Up DHCP VLAN Option from Phone Web Page, on page 65
Update field description with a new field **DHCP VLAN Option**.	VLAN Settings, on page 227
Update Ethernet configuration menu on the phone with a new field **DHCP VLAN Option**.	Network Configuration Fields, on page 39
Add XSI over HTTPS support. Updated **XSI Host Server** parameter in the **XSI Service** section.	XSI Phone Service, on page 268
Add a troubleshooting scenario when phone cannot access BroadSoft directory for XSI	Phone Cannot Access BroadSoft Directory for XSI, on page 312
Add Cisco IP Phone 6800 Key Expansion Module support	Cisco 6800 Series Key Expansion Module Setup Overview, on page 100
Add controlling reverse name lookup for incoming and outgoing calls	Reverse Name Lookup for Incoming and Outgoing Calls, on page 129
Emergency Call Support	Emergency Call Support Background, on page 184 Emergency Call Support Terminology, on page 185 Configure a Phone to Make Emergency Calls, on page 185 E911 Geolocation Configuration, on page 292 An Emergency Call Doesn't Connect to Emergency Services, on page 311

New and Changed for Firmware Release 11.1(1)

Feature	New or Changed Sections
Asian Language Support	Phone Display Language, on page 84
	Phone Display Problems, on page 313
	The Font is Too Small or Has Unusual Characters, on page 313
	Phone Screen Displays Boxes Instead of Asian Characters, on page 314
	Phone Locale is Not Displayed, on page 315
	Softkey Labels are Truncated, on page 314
Call Center Support	Set Up a Call Center Agent Phone, on page 183
	ACD Call Information Missing, on page 310
	ACD Settings, on page 282
	Phone Doesn't Show ACD Softkeys, on page 310
Call Recording	Enable Remote Call Recording with SIP REC, on page 180
	Enable Remote Call Recording with SIP INFO, on page 182
	Call Doesn't Record, on page 311
Factory Reset Button in the Phone Web Page	Factory Reset the Phone with the Web UI Button, on page 196
	Factory Reset, on page 216
Gigabit Support	Network Configuration Fields, on page 39
IPv6 Support	Network Configuration Fields, on page 39
	IPv6 Information, on page 210
	Network Settings, on page 223
	IPv6 Settings, on page 224
Presence	Set Up a Phone for Presence, on page 183
	Presence Status Doesn't Work, on page 312
	Phone Presence Message: Disconnected from Server, on page 312
	Broadsoft XMPP, on page 269
Wideband Handset Support	General, on page 264

PART I

About the Cisco IP Phone

CHAPTER 2

Technical Details

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco IP Phone 6800 Series Multiplatform Phones.

Table 1: Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Storage relative hunidity	10% to 95% (noncondensing)
Height	8.14 in. (207 mm), excluding the footstand
Width	6821: 6.73 in. (171 mm) 6841, 6851, and 6861: 8.11 in. (206 mm)
Depth	6821: 1.48 in. (37.5 mm), excluding the footstand 6841, 6851, and 6861: 1.30 in. (33 mm), excluding the footstand

Specification	Value or Range
Weight	6821: 1.005 lb. (456 g), excluding footstand and handset
	6841 and 6851: 1.356 lb. (615 g), excluding footstand and handset
	6861: 1.329 lb. (602.8 g), excluding footstand and handset
Power	• 100-240 VAC, 50-60 Hz, 0.5 A—When using the AC adapter
	• 6841 and 6861: 5 VDC, 2 A—When using the in-line power over the network cable
	• 6821 and 6851: 48 VDC, 0.2 A—When using the in-line power over the network cable
Cables	• Category 3/5/5e/6 for 10-Mbps cables with 4 pairs
	• Category 5/5e/6 for 100-Mbps cables with 4 pairs
	• Category 5/5e/6 for 1000-Mbps cables with 4 pairs
	Note The Cisco IP Phone 6821 and 6861 Multiplatform Phones do not support 1000-Mbps.
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each Cisco IP Phone and the switch is 100 meters (330 feet).

For detailed technical information about the phone, see the datasheet at:

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/datasheet-listing.html

Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.

- RJ-45 jack for the LAN 10/100/1000BaseT connection.

- RJ-45 jack for a second 10/100/1000BaseT connection.

- 5-volt power connector.

Network and Computer Port Pinouts

Although both the network and computer (access) ports are used for network connectivity, they serve different purposes and have different port pinouts:

- The network port is the 10/100/1000 SW port.

Note The Cisco IP Phone 6821 Multiplatform Phones and Cisco IP Phone 6861 Multiplatform Phones have a 10/100 SW port.

- The computer (access) port is the 10/100/1000 PC port.

Note Cisco IP Phone 6861 Multiplatform Phones doesn't have a PC port.

Network Port Connector

The following table describes the network port connector pinouts.

Table 2: Network Port Connector Pinouts

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Note BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.	

Computer Port Connector

The following table describes the computer port connector pinouts.

Table 3: Computer (Access) Port Connector Pinouts

Pin Number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
Note	BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.

Phone Power Requirements

The following table describes the ways to provide power to the phones.

Phone	PoE Through Ethernet	Separate External Power
Cisco IP Phone 6821 Multiplatform Phones	Supported	Supported
Cisco IP Phone 6841 Multiplatform Phones	Not supported	Supported
Cisco IP Phone 6851 Multiplatform Phones	Supported	Supported
Cisco IP Phone 6861 Multiplatform Phones	Not supported	Supported

Note When you install a phone that is powered with external power, connect the power supply to the phone and to a power outlet before you connect the Ethernet cable to the phone. When you remove a phone that is powered with external power, disconnect the Ethernet cable from the phone before you disconnect the power supply.

Table 4: Guidelines for Cisco IP Phone Power

Power Type	Guidelines
External power: Provided through the external power supply	The phones use a custom power supply.
External power—Provided through the Cisco IP Phone Power Injector connected to the Cisco IP Phone 6841 Multiplatform Phones and Cisco IP Phone 6861 Multiplatform Phones.	The Cisco IP Phone Power Injector may be used with the phones. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco IP Phone Power Injector connects between a switch port and the IP Phone, and supports a maximum cable length of 100 m between the unpowered switch and the IP phone.
PoE power—Provided by a switch through the Ethernet cable attached to the Cisco IP Phone 6821 Multiplatform Phones and Cisco IP Phone 6851 Multiplatform Phones.	To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. Make sure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information.

The documents in the following table provide more information on the following topics:

- Cisco switches that work with Cisco IP Phones

- Cisco IOS releases that support bidirectional power negotiation

- Other requirements and restrictions about power

Document topics	URL
PoE Solutions	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
Cisco Catalyst Switches	http://www.cisco.com/c/en/us/products/switches/index.html
Integrated Service Routers	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS Software	http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html

Power Outage

Your access to emergency service through the phone requires that the phone receive power. If a power interruption occurs, service or emergency calling service dialing does not function until power is restored. If a power failure or disruption occurs, you may need to reset or reconfigure the equipment before you can use service or emergency calling service dialing.

Power Reduction

You can reduce the amount of energy that the Cisco IP Phone consumes by using Power Save mode.

Power Save

In Power Save mode, the backlight on the screen is not lit when the phone is not in use. The phone remains in Power Save mode until the user lifts the handset or presses any button. Set up each phone to enable or disable Power Save settings.

Note   The Cisco IP Phone 6821 Multiplatform Phones do not support the Power Save feature.

Power Negotiation Over LLDP

The phone and the switch negotiate the power that the phone consumes. Cisco IP Phone operates at multiple power settings, which lowers power consumption when less power is available.

After a phone reboots, the switch locks to one protocol (CDP or LLDP) for power negotiation. The switch locks to the first protocol (containing a power Threshold Limit Value [TLV]) that the phone transmits. If the system administrator disables that protocol on the phone, the phone cannot power up any accessories because the switch does not respond to power requests in the other protocol.

Cisco recommends that Power Negotiation always be enabled (default) when connecting to a switch that supports power negotiation.

If Power Negotiation is disabled, the switch may disconnect power to the phone. If the switch does not support power negotiation, disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the phone can power the accessories up to the maximum that the IEEE 802.3af-2003 standard allows.

Note
- When CDP and Power Negotiation are disabled, the phone can power the accessories up to 15.4W.

- The Cisco IP Phone 6841 Multiplatform Phones and Cisco IP Phone 6861 Multiplatform Phones do not support the Power Negotiation over LLDP feature.

Network Protocols

Cisco IP Phones support several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the phones support.

Table 5: Supported Network Protocols on the Cisco IP Phone

Network Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device, such as the Cisco IP Phone, to discover certain startup information, such as its IP address.	—
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. A device can use CDP to advertise its existence to other devices and receive information about other devices in the network.	The Cisco IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Domain Name Server (DNS)	DNS translates domain names to IP addresses.	Cisco IP Phones have a DNS client to translate domain names into IP addresses.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, and gateway on each phone locally. We recommend that you use the DHCP custom option 160, 159.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard protocol for transfer of information and movement of documents across the Internet and the web.	Cisco IP Phones use HTTP for XML services, provisioning, upgrade and for troubleshooting purposes.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Cisco IP Phones that support HTTPS choose the HTTPS URL. A lock icon is displayed to the user if the connection to the service is via HTTPS.

Network Protocol	Purpose	Usage Notes
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate with IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco IP Phone supports LLDP on the PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	The Cisco IP Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper at this URL: [www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.html](#)
Network Transport Protocol (NTP)	NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.	Cisco IP Phones have an NTP client integrated into the software.
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default.

Network Protocol	Purpose	Usage Notes
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by a Third-Party Call Control System or a Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Secure Real-Time Transfer protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints.	Cisco IP Phones use SRTP for media encryption.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	—
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco IP Phones use the TLS protocol when securely registering with the third-party call control system.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP uses UDP, TCP, and TLS.

Related Topics

VLAN Interaction

The Cisco IP Phone contains an internal Ethernet switch, enabling forwarding of packets to the phone, and to the computer (access) port and the network port on the back of the phone.

If a computer is connected to the computer (access) port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices that connect to the same port.

- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.

- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port to which the phone connects would be configured for separate VLANs for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN on the Cisco Catalyst 6000 series, for example)

- Data traffic to and from the PC that connects to the switch through the computer (access) port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network that does not have enough IP addresses for each phone.

For more information, see the documentation that is included with a Cisco switch. You can also access switch information at this URL:

http://cisco.com/en/US/products/hw/switches/index.html

External Devices

We recommend that you use good-quality external devices that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals. External devices include headsets, cables, and connectors.

Depending on the quality of these devices and their proximity to other devices, such as mobile phones or two-way radios, some audio noise may still occur. In these cases, we recommend that you take one or more of these actions:

- Move the external device away from the source of the RF or AF signals.

- Route the external device cables away from the source of the RF or AF signals.

- Use shielded cables for the external device, or use cables with a better shield and connector.

- Shorten the length of the external device cable.

- Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of external devices, cables, and connectors.

⚠

Caution   In European Union countries, use only external speakers, microphones, and headsets that are fully compliant with the EMC Directive [89/336/EC].

CHAPTER **3**

Cisco IP Phone Hardware

- Overview of the Cisco IP Phone 6800 Series Multiplatform Phones, on page 23
- Cisco IP Phone 6821 Multiplatform Phones Connections, on page 24
- Cisco IP Phone 6841 Multiplatform Phones Connections, on page 25
- Cisco IP Phone 6851 Multiplatform Phones Connections, on page 25
- Cisco IP Phone 6861 Multiplatform Phones Connections, on page 26
- Cisco IP Phone 6821 Multiplatform Phones Buttons and Hardware, on page 27
- Cisco IP Phone 6841, 6851, and 6861 Multiplatform Phones Buttons and Hardware, on page 29
- Softkey, Line, and Feature Buttons, on page 30
- Terminology Differences, on page 31

Overview of the Cisco IP Phone 6800 Series Multiplatform Phones

The Cisco IP Phone 6800 Series Multiplatform Phones comprises a set of full-featured VoIP (Voice-over-Internet Protocol) phones that provide voice communication over an IP network. The phones provide all the features of traditional business phones, such as call forwarding, redialing, speed dialing, transferring calls, and conference calling. The Cisco IP Phone 6800 Series Multiplatform Phones is targeted for solutions that are centered on third-party SIP-based IP PBX.

In the following figure, the Cisco IP Phone 6821 Multiplatform Phones is on the left. The Cisco IP Phone 6841 and 6851 Multiplatform Phones look the same, and are in the middle. The Cisco IP Phone 6851 Multiplatform Phones support Key Expansion Module(KEM). The Cisco IP Phone 6861 Multiplatform Phones is on the right.

Figure 1: Cisco IP Phone 6800 Series Multiplatform Phones

Note   In this document, the terms *Cisco IP Phone*, *phone*, or *device* mean Cisco IP Phone 6800 Series Multiplatform Phones.

Cisco IP Phone 6821 Multiplatform Phones Connections

Connect your phone to your LAN with an Ethernet cable to enable full functionality of your phone. If your Ethernet port is equipped with Power over Ethernet (PoE), you can power the phone through the LAN port. If you don't have PoE available, then you need to use a power adapter to power the phone. Do not extend the Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.

Figure 2: Cisco IP Phone 6821 Multiplatform Phones Connections
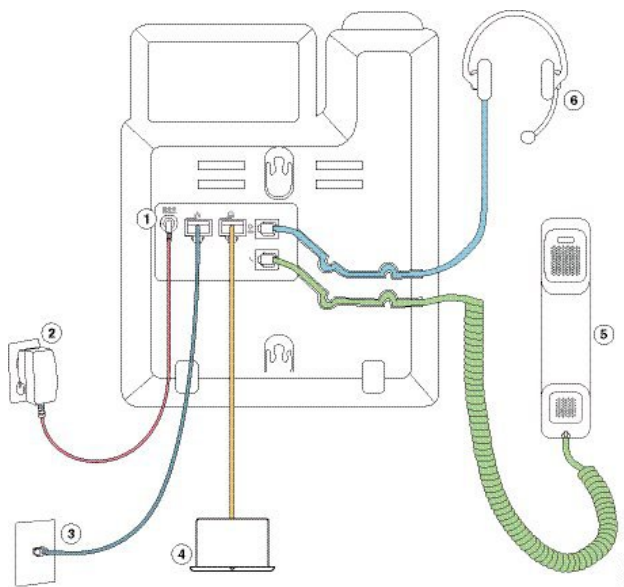
1	DC adapter port (optional)	4	Access port (10/100 PC) connection (optional)
2	Power adapter (optional)	5	Handset connection
3	Network port (10/100 SW) connection; IEEE 802.3af power enabled	6	Analog headset connection (optional)

Cisco IP Phone 6841 Multiplatform Phones Connections

Connect your phone to your LAN with an Ethernet cable to enable full functionality of your phone. You need to use a power adapter to power the phone. Do not extend the LAN Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.
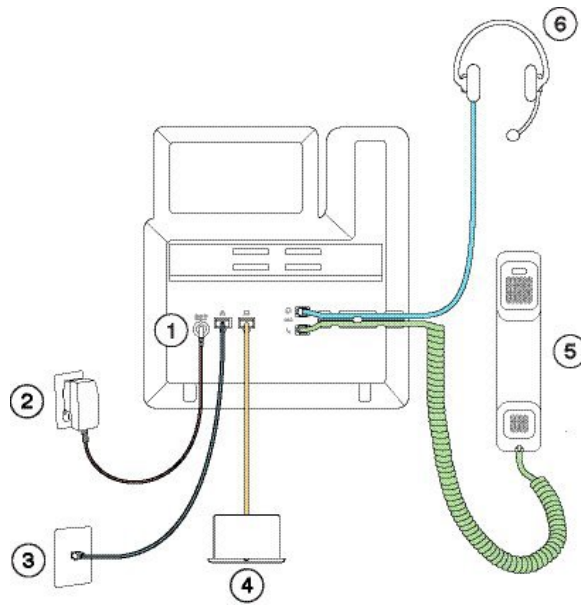
1	DC adapter port	4	Access port (10/100/1000 PC) connection (optional)
2	Power adapter	5	Handset connection
3	Network port (10/100/1000 SW) connection	6	Analog headset connection (optional)

Cisco IP Phone 6851 Multiplatform Phones Connections

Connect your phone to your LAN with an Ethernet cable to enable full functionality of your phone. If your Ethernet port is equipped with Power over Ethernet (PoE), you can power the phone through the LAN port. If you don't have PoE available, then you need to use a power adapter to power the phone. Do not extend the

LAN Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.

1	Key Expansion Module port	5	Access port (10/100/1000 PC) connection (optional)
2	DC adapter port (optional)	6	Auxiliary port (optional)
3	Power adapter (optional)	7	Handset connection
4	Network port (10/100/1000 SW) connection; IEEE 802.3af power enabled	8	Analog headset connection (optional)

Cisco IP Phone 6861 Multiplatform Phones Connections

Connect your phone to your LAN with an Ethernet cable or with Wi-Fi to enable full functionality of your phone. You need to use a power adapter to power the phone. If you connect your phone to a wired network, do not extend the LAN Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.
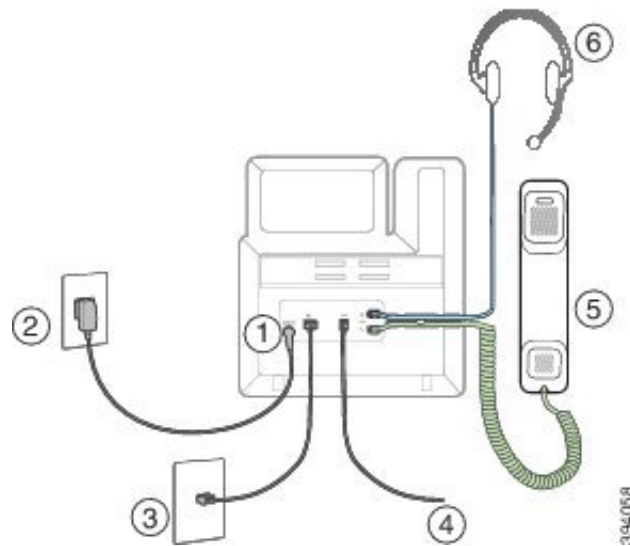
1	DC adapter port	4	Auxiliary port (optional)
2	Power adapter	5	Handset connection
3	Network port (10/100 SW) connection	6	Analog headset connection (optional)

Cisco IP Phone 6821 Multiplatform Phones Buttons and Hardware

The following figure shows the Cisco IP Phone 6821 Multiplatform Phones.

Figure 3: Cisco IP Phone 6821 Multiplatform Phones

1	Light strip	Indicates whether you have an incoming call (flashing red) or a new voice message (steady red).
2	Programmable feature buttons and line buttons	▭ Access your phone lines, features, and call sessions. For more information, see Softkey, Line, and Feature Buttons, on page 30.
3	Softkey buttons	▭ Access functions and services such as Conference and Transfer. For more information, see Softkey, Line, and Feature Buttons, on page 30.
4	Navigation cluster	Navigation ring and **Select** ● button. Scroll through menus, highlight items, and select the highlighted item.
5	**Applications** and **Headset**	**Applications** ⚙ Access call history, user preferences, phone settings, and phone model information. **Headset** ☊ Toggle the headset on or off. When a headset is active, a headset icon is displayed in the header.
6	**Mute** and **Speakerphone**	**Mute** 🎤 Toggle the microphone on or off. When the microphone is muted, a mute icon flashes on the screen. **Speakerphone** 🔊 Toggle the speakerphone on or off.

7	**Volume** button	− +
		Adjust the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).

Cisco IP Phone 6841, 6851, and 6861 Multiplatform Phones Buttons and Hardware

The following figure shows the Cisco IP Phone 6841.

Figure 4: Cisco IP Phone 6841, 6851, and 6861 Multiplatform Phones Buttons and Features

1	Handset and Handset light strip	Indicates whether you have an incoming call (flashing red) or a new voice message (steady red).
2	Programmable feature buttons and line buttons	Access your phone lines, features, and call sessions. For more information, see Softkey, Line, and Feature Buttons, on page 30.
3	Softkey buttons	Access functions and services. For more information, see Softkey, Line, and Feature Buttons, on page 30.
4	Navigation cluster	Navigation ring and **Select** button. Scroll through menus, highlight items, and select the highlighted item.

5	**Hold/Resume**, **Conference**, and **Transfer**	**Hold/Resume** ⏸ Place an active call on hold and resume the held call. **Conference** ☷ Create a conference call. **Transfer** ↱ Transfer a call.
6	**Speakerphone**, **Mute**, and **Headset**	**Speakerphone** ◀ Toggle the speakerphone on or off. When the speakerphone is on, the button is lit. **Mute** 🔇 Toggle the microphone on or off. When the microphone is muted, the button is lit. **Headset** ⌖ Toggle the headset on or off. When the headset is on, the button is lit.
7	**Contacts**, **Applications**, and **Messages**	**Contacts** 📖 Access personal and corporate directories. **Applications** ⚙ Access call history, user preferences, phone settings, and phone model information. **Messages** ▭ Autodial your voice messaging system.
8	**Volume** button	▮ + − Adjust the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).

Softkey, Line, and Feature Buttons

You can interact with the features on your phone in several ways:

- Softkeys, located below the screen, give you access to the function displayed on the screen above the softkey. The softkeys change depending on what you are doing at the time. The **More ...** softkey shows you that more functions are available.

- Feature and line buttons give you access to phone features and phone lines. On the Cisco IP Phone 6821, these are the buttons on the left side of the screen. On the Cisco IP Phone 6841, 6851 and 6861, these are the buttons on either side of the screen.

  - Feature buttons—Used for features such as **Speed dial** or **Call pickup**, and to view your status on another line.

  - Line buttons—Used to initiate or answer a call or resume a held call. You can also use a line key to open and close the call session window, and to navigate through the call session window. Open the call session window to see the calls on the line.

Feature and line buttons illuminate to indicate status:

- or Green—Line is idle.

- or Red, steady—Line is active or in use.

- or Red, flashing—Line is on hold or there is an inbound call.

- or Amber, steady—Line is unregistered (cannot be used).

Some functions can be set up as softkeys or as feature buttons. You can also access some functions with softkeys or the associated hard button.

The Cisco IP Phone 6821 has a limited number of hard buttons. You use the softkeys to access most call features.

Terminology Differences

The following table highlights some of the terminology differences in the *Cisco IP Phone 6800 Series Multiplatform Phones User Guide* and the *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*

Table 6: Terminology Differences

User Guide	Administration Guide
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Voicemail System	Voice Messaging System
Phone Web Page	Configuration Utility

PART II

Phone Installation

Cisco IP Phone Installation

Verify the Network Setup

Upon deployment of a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service.

For the phone to operate successfully as an endpoint in your network, your network must meet specific requirements.

Note The phone displays the date and time from Third-Party Call Control. The time displayed on the phone can differ from the Third-Party Call Control time by up to 10 seconds.

Procedure

Step 1 Configure a VoIP Network to meet the following requirements:

- VoIP is configured on your Cisco routers and gateways.

- Third-Party Call Control is installed in your network and is configured to handle call processing.

Step 2 Set up the network to support one of the following:

- DHCP support

- Manual assignment of IP address, gateway, and subnet mask

Install the Cisco IP Phone

After the phone connects to the network, the phone startup process begins, and the phone registers with the Third-Party Call Control System. To finish phone installation, you need to configure the network settings on the phone either manually or with DHCP.

Note Before using external devices, read External Devices, on page 20.

If you only have one LAN cable at your desk, you can plug your phone into the LAN with the SW port and then connect your computer into the PC port.

You can also daisy chain two phones together. Connect the PC port of the first phone to the SW port of the second phone.

Note Cisco IP Phone 6861 Multiplatform Phones doesn't have a PC port. You can connect Cisco IP Phone 6861 to a wireless network through Wi-Fi.

Caution Do not connect the SW and PC ports into the LAN.

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE)—Cisco IP Phone 6821 and 6851 Multiplatform Phones

- External power supply

For more information, see Phone Power Requirements, on page 14.

Step 2 Connect the handset to the handset port.

The Cisco IP Phone 6861 Multiplatform Phones ship with a wideband handset. The Cisco IP Phone 6821, 6841, and 6851 Multiplatform Phones ship with a narrowband handset. You can buy a wideband-capable handset that is designd especially for use with the phone.

The handset includes a light strip that indicates incoming calls and waiting voice messages.

Step 3 Connect a headset to the headset port. You can add a headset later if you do not connect one now.

Step 4   Connect your phone to a network. Do one of the following actions:

- Connect a straight-through Ethernet cable from the switch to the network port on the phone. Each phone ships with one Ethernet cable in the box.

  Use Category 3, 5, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100 Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts, on page 13.

- Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the computer port on the phone. You can connect another network device later if you do not connect one now.

  Use Category 3, 5, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100 Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts, on page 13 for guidelines.

- For Cisco IP Phone 6861 Multiplatform Phones, you can connect the phone to a wireless network through Wi-Fi. For more information, see Wi-Fi Settings, on page 45.

Step 5   If the phone is wall-mounted, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle. For more information, see Adjust the Handset Rest, on page 117.

Step 6   Monitor the phone startup process. This step verifies that the phone is configured properly.

Step 7   Use DHCP or manually enter an IP address for the phone.

See Configure the Network from the Phone, on page 38.

Step 8   Upgrade the phone to the current firmware image.

Firmware upgrades over the WLAN interface may take longer than upgrading over the wired interface, depending on the quality and bandwidth of the wireless connection. Some upgrades may take more than one hour.

Step 9   Make calls with the phone to verify that the phone and features work correctly.

See the *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*.

Step 10   Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their phones.

Activation Code Onboarding

If your network is configured for Activation Code Onboarding, you can set up new phones to register automatically in a secure way. You generate and provide each user with a unique 16-digit activation code. The user enters the activation code, and the phone automatically registers.

Activation codes can be used only once, and have an expiry date. If a user enters an expired code, the phone displays `Invalid activation code` on the screen. If this happens, provide the user with a new code.

This feature is available in firmware release 11-2-3MSR1, BroadWorks Application Server Release 22.0 (patch AP.as.22.0.1123.ap368163 and its dependencies). However, you can change phones with older firmware to use this feature. To do this, use the following procedure.

Note   Cisco IP Phone 6861 Multiplatform Phones don't support the Activation Code Onboarding feature.

Before you begin

Ensure that you allow the activation.webex.com service through your firewall to support onboarding via activation code.

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Reset the phone to the factory settings.
Step 2	Select **Voice** > **Provisioning** > **Configuration Profile**.
Step 3	Enter the profile rule in the **Profile Rule** field in this format: `gds://`
Step 4	Select **Firmware Upgrade**.
Step 5	Enter the upgrade rule in the **Upgrade Rule** field in this format: `http://<server ip address>/sip88xx.11-2-3MSR1-1.loads/`
Step 6	Submit All Changes.

See below a sample cfg.xml file showing the profile rule, and upgrade rule.

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

Configure the Network from the Phone

The phone includes many configurable network settings that you may need to modify before it is functional for your users. You can access these setting through the phone menus.

The Network configuration menu provides you with options to view and configure a variety of network settings.

You can configure settings that are display-only on the phone in your Third-Party Call Control system.

Procedure

Step 1	Press **Applications** ⚙.
Step 2	Select **Network configuration**.
Step 3	Use the navigation arrows to select the desired menu and edit.
Step 4	To display a submenu, repeat step 3.
Step 5	To exit a menu, press **Back** .

Network Configuration Fields

Table 7: Network Configurations Menu Options

Field	Field Type or Choices	Default	Description
Ethernet configuration			See the following Ethernet configuration submenu table.
IP mode	Dual mode IPv4 only IPv6 only	Dual mode	Select the Internet Protocol mode for which the phone operates. In dual mode, the phone can have both IPv4 and IPv6 addresses.
Wi-Fi configuration			See Set Up a Wi-Fi Profile from the Phone, on page 48 For Cisco IP Phone 6861 Multiplatform Phones only.
IPv4 address settings	DHCP Static IP Release DHCP IP	DHCP	See the IPv4 address submenu table in the following tables.
IPv6 address settings	DHCP Static IP	DHCP	See the IPv6 address submenu table in the following tables.
DHCPv6 option to use		17, 160, 159	Indicates the order in which the phone uses the IPv6 addresses provided by DHCP server.
Web server	On Off	On	Indicates whether the phone has web server enabled or disabled.

Table 8: Ethernet Configuration Submenu

Field	Field Type or Choices	Default	Description
802.1x authentication	Device authentication	Off	Enables you to turn on or turn off the 802.1x authentication. Valid options are: • On • Off
	Transaction status	Disabled	• Transaction status—Indicates different authentication status when you turn on 802.1x in the **Device authentication** field. 　• Disabled—Default status. 　• Connecting—802.1x authentication started in the device. 　• Authenticated—802.1x authentication established in the device. • Protocol—Specifies the protocol of the server.
Switch port config	Auto 10MB half 10MB full 100MB half 100MB full 1000 full	Auto	Select speed and duplex of the network port. If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate. If you change the setting of this option, you must change the PC Port config option to the same setting.
PC port config	Auto 10MB half 10MB full 100 MB half 100MB full 100 half 1000 full	Auto	Select Speed and duplex of the Computer (access) port. If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate. If you change the setting of this option, you must change the Switch Port config option to the same setting.
CDP	On Off	On	Enable or disable Cisco Discovery Protocol (CDP). CDP is a device-discovery protocol that runs on all Cisco manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.

Field	Field Type or Choices	Default	Description
LLDP-MED	On Off	On	Enable or disable LLDP-MED. LLDP-MED enables the phone to advertise itself to devices that use the discovery protocol.
Startup delay		3 seconds	Set a value that causes a delay for the switch to get to the forwarding state before the phone sends out the first LLDP-MED packet. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use the Spanning Tree Protocol. Default delay is 3 seconds.
VLAN	On Off	Off	Enable or disable VLAN. Permits you to enter a VLAN ID when you use VLAN without CDP or LLDP. When you use a VLAN with CDP or LLDP, that associated VLAN takes precedent over the VLAN ID you manually entered.
VLAN ID		1	Enter a VLAN ID for the IP phone when you use a VLAN without CDP (VLAN enabled and CDP disabled). Note that only voice packets are tagged with the VLAN ID. Do not use the 1 value for the VLAN ID. If VLAN ID is 1, you cannot tag voice packets with the VLAN ID.
PC port VLAN ID		1	Enter a value of the VLAN ID that is used to tag communications from the PC port on the phone. The phone tags all the untagged frames coming from the PC (it does not tag any frames with an existing tag). Valid values: 0 through 4095 Default: 0
PC port mirror	On Off	Off	Adds the ability to port mirror on the PC port. When enabled, you can see the packets on the phone. Select **On** to enable PC port mirroring and select **Off** to disable it.

Field	Field Type or Choices	Default	Description
DHCP VLAN option			Enter a predefined DHCP VLAN option to learn the voice VLAN ID. When you use a VLAN ID with CDP, LLDP, or manually select a VLAN ID, that VLAN ID takes precedent over the selected DHCP VLAN option. Valid values are: • Null • 128 to 149 • 151 to 158 • 161 to 254 Default value is null. Cisco recommends that you use DHCP Option 132.

Table 9: IPv4 Address Settings Submenu

Field	Field Type or Choices	Default	Description
Connection type	DHCP		Indicates whether the phone has DHCP enabled. • DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses. • DNS2—Identifies the secondary Domain Name System (DNS) server that the phone uses. • DHCP address released—Releases the IP address that DHCP assigned. You can edit this field if DHCP is enabled. To remove the phone from the VLAN and release the IP address for reassignment, set this field to Yes and press **Set**.
	Static IP		When DHCP is disabled, you must set the Internet Protocol (IP) address of the phone. • Static IP address—Identifies the IP that you assign to the phone. The phone uses this IP address instead of acquiring an IP from the DHCP server on the network. • Subnet Mask—Identifies the subnet mask used by the phone. When DHCP is disabled, you must set the subnet mask. • Gateway address—Identifies the default router used by the phone. • DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually. • DNS2—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually. When you assign an IP address using this field, you must also assign a subnet mask and a gateway address. See the Subnet Mask and Default Router fields in this table.

Table 10: IPv6 Address Settings Submenu

Field	Field Type or Choices	Default	Description
Connection type	DHCP		Indicates whether the phone has Dynamic Host Configuration Protocol (DHCP) enabled. • DNS1—Identifies the primary DNS server that the phone uses. • DNS2—Identifies the secondary DNS server that the phone uses. • Broadcast Echo—Identifies if the phone responses to multicast ICMPv6 message with destination address of ff02::1. • Auto config— Identifies if the phone uses automatic configuration for the address.
	Static IP		When DHCP is disabled, you must set the Internet Protocol (IP) address of the phone and must set the values of the fields: • Static IP—Identifies the IP that you assign to the phone. The phone uses this IP address instead of acquiring an IP from the DHCP server on the network. • Prefix length—Identifies how many bits of a Global Unicast IPv6 Address are there in the network part. • Gateway—Identifies the default router used by the phone. • Primary DNS—Identifies the primary DNS server that the phone uses. When DHCP is disabled, you must set this field manually. • Secondary DNS—Identifies the primary DNS server that the phone uses. When DHCP is disabled, you must set this field manually. • Broadcast Echo—Identifies if the phone responses to multicast ICMPv6 message with destination address of ff02::1.

Text and Menu Entry From the Phone

When you edit the value of an option setting, follow these guidelines:

• Use the arrows on the navigation pad to highlight the field that you wish to edit. Press **Select** in the navigation pad to activate the field. After the field is activated, you can enter values.

• Use the keys on the keypad to enter numbers and letters.

- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.

- Press the softkey ⌫ if you make a mistake. This softkey deletes the character to the left of the cursor.

- Press **Back** before pressing **Set** to discard any changes that you made.

- To enter a period (for example, in an IP address), press ***** on the keypad.

Note   The Cisco IP Phone provides several methods to reset or restore option settings, if necessary.

Wi-Fi Settings

Wi-Fi settings are available only on Cisco IP phone 6861 Multiplatform Phones.

You can customize Wi-Fi settings for your phone from the **Wi-Fi configuration** menu under the **Network configuration** menu on the phone. Some of the Wi-Fi settings are also available on the phone web page.

Turn the Wi-Fi On or Off from Your phone

You can enable or disable the wireless LAN of your phone from the **Wi-Fi configuration** menu.

Procedure

Step 1   Press **Applications** ⚙.

Step 2   Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi** .

Step 3   Press the **Select** button, to turn the Wi-Fi on or off.

Step 4   Press **Set** to save the changes.

Turn the Wi-Fi On or Off from the Phone Web Page

You can enable or disable the wireless LAN of your phone from the phone web page. You turn on the Wi-Fi so that the phone connects to a wireless network automatically or manually.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **System**.

Step 2 Set the **Wi-Fi Settings** fields as described in the table.

Connect the Phone to a Wi-Fi Manually

When you set up a Wi-Fi profile, it provides you the options to connect the phone manually to a wireless network. You can establish the connection from the **Wi-Fi profile** screen or from the **Setup Wi-Fi** screen.

The top most Wi-Fi profile in the **Wi-Fi profile** screen gets connected automatically when the phone provisions.

Before you begin

- Turn on the Wi-Fi of your phone.

- Disconnect your phone with the wired network.

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi profile**.

Step 3 In the **Wi-Fi profile** screen, do any of the actions to connect to Wi-Fi.

- Select any of the configured Wi-Fi profile and click **Connect**.
- Press **Scan** and select one wireless in the **Connect to Wi-Fi** screen. In the **Setup Wi-Fi** screen, enter values in the fields and press **Connect**.

See the **Profile Parameter** table in the for the field values.

You can also configure the Wi-Fi settings using the configuration file.

```
<!--  Wi-Fi Settings  -->
<Phone-wifi-on ua="rw">Yes</Phone-wifi-on>
<Phone-wifi-type ua="na">WLAN</Phone-wifi-type>
<!--  available options: WLAN|WPS  -->
 <!--  Wi-Fi Profile 1  -->
<Network_Name_1_ ua="rw">AP_SSID</Network_Name_1_>
<Security_Mode_1_ ua="rw">Auto</Security_Mode_1_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_1_ ua="rw">User_ID</Wi-Fi_User_ID_1_>
 <!--
 <Wi-Fi_Password_1_ ua="rw">Password</Wi-Fi_Password_1_>
-->
 <!--  <WEP_Key_1_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_1_ ua="rw"/>  -->
<Frequency_Band_1_ ua="rw">Auto</Frequency_Band_1_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_1_ ua="rw">1</Wi-Fi_Profile_Order_1_>
<!--  available options: 1|2|3|4  --><!--  Wi-Fi Profile 2  -->
```

```
<Network_Name_2_ ua="rw">AP_SSID</Network_Name_2_>
<Security_Mode_2_ ua="rw">PSK</Security_Mode_2_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_2_ ua="rw"/>
 <!--  <Wi-Fi_Password_2_ ua="rw"/>  -->
 <!--  <WEP_Key_2_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_2_ ua="rw"/>  -->
<Frequency_Band_2_ ua="rw">Auto</Frequency_Band_2_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_2_ ua="rw">2</Wi-Fi_Profile_Order_2_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 3  -->
<Network_Name_3_ ua="rw"/>
<Security_Mode_3_ ua="rw">None</Security_Mode_3_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_3_ ua="rw"/>
 <!--  <Wi-Fi_Password_3_ ua="rw"/>  -->
 <!--  <WEP_Key_3_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_3_ ua="rw"/>  -->
<Frequency_Band_3_ ua="rw">Auto</Frequency_Band_3_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_3_ ua="rw">3</Wi-Fi_Profile_Order_3_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 4  -->
<Network_Name_4_ ua="rw"/>
<Security_Mode_4_ ua="rw">PSK</Security_Mode_4_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_4_ ua="rw"/>
 <!--  <Wi-Fi_Password_4_ ua="rw"/>  -->
 <!--  <WEP_Key_4_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_4_ ua="rw"/>  -->
<Frequency_Band_4_ ua="rw">Auto</Frequency_Band_4_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_4_ ua="rw">4</Wi-Fi_Profile_Order_4_>
<!--  available options: 1|2|3|4  -->
```

Connect Your Phone to a Wireless Network with WPS

Wi-Fi Protected Setup (WPS) provides an easier way to connect your phone to a wireless network. With WPS, you don't need to enter detailed settings for the access point to connect as you do with the connection through Wi-Fi profile. You can either use the WPS button on your access point or the PIN code to connect to the network through WPS.

The WPS option is available only in the menu on the phone screen. On the phone web page, you can only configure your phone to connect to a wireless network using Wi-Fi profile.

Before you begin

Enable WPS on your access point.

Procedure

Step 1   Press **Applications** ⚙.

Step 2   Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi type**.

Step 3   Press the navigation key to switch the Wi-Fi type to **WPS**.

Step 4   Press **Set**.
            Push-button configuration and **PIN configuration** display under **Wi-Fi type**. Follow either one of the
            following steps to connect to the network.

Step 5   Connect to the network using the WPS button on your access point.

   a) Select **Push-button configuration**.

   b) Press the WPS button on your access point.

       The button name may vary on your access point.

   c) Press **Continue** on your phone.

Step 6   Connect to the network using a PIN code.

   a) Select **PIN configuration**.
       An 8-digit PIN code displays on your phone screen.

   b) Go to the web page of your access point and enter the PIN code.

       The procedure of entering PIN code may vary on your access points. See the respective user guide of your
       access point for more details.

Upon either a successful connection or a connection failure, the connection status displays on your phone
screen.

Set Up a Wi-Fi Profile from the Phone

You can add maximum of four Wi-Fi profiles. You can use this profile to connect your phone to a Wi-Fi
network.

Procedure

Step 1   Press **Applications** ⚙.

Step 2   Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi profile**.

Step 3   In the **Wi-Fi profile** screen, move to a row in the list on which you want to set up the profile.

Step 4   Press the **Select** button.

            You can also press **Options** and then select **Edit**.

Step 5   In the **Edit profile** screen, set the parameters as mentioned in the **Profile Parameters** table.

Table 11: Profile Parameters

Parameter	Description
Security mode	Allows you to select the authentication method that is used to secure access to the Wi-Fi network. Depending on the method you choose, a password, passphrase, or key field appears so that you can provide the credentials that are required to join this Wi-Fi network. Options are: • Auto • EAP-FAST • PEAP-GTC • PEAP-MSCHAPV2 • PSK • WEP • None Default: None
Network name	Allows you to enter a name for the SSIDs. This name displays on the phone. Multiple profiles can have the same network name with different security mode.This name displays on the phone.
User ID	Allows you to enter a user ID for the network profile. This field is available when you set the security mode to Auto, EAP-FAST, PEAP-GTC, PEAP-MSCHAPV2. This is a mandatory field and it allows maximum length of 32 alphanumeric characters.
Password	Allows you to enter password for the network profile that you create. This field is available when you set the security mode to Auto, EAP-FAST, PEAP-GTC, PEAP-MSCHAPV2. This is a mandatory field and it allows maximum length of 64 alphanumeric characters.
WEP key	Allows you to enter password for the network profile that you create. This field is available when you set the security mode to WEP. This is a mandatory field and it allows maximum length of 32 alphanumeric characters.

Parameter	Description
Passphrase	Allows you to enter password for the network profile that you create. You need to enter this value when the security mode is PSK.
Frequency band	Allows you to select the wireless signal frequency band that is used in the WLAN. Options are: • Auto • 2.4 GHz • 5 GHz Default: Auto

Step 6   Press **Save**.

Set Up a Wi-Fi Profile from the Phone Web Page and the XML Provisioning Server

You can configure a Wi-Fi profile from the phone web page or from remote device profile resync and then associate the profile to the available Wi-Fi networks. You can use this Wi-Fi profile to connect to a Wi-Fi. You can configure maximum of four profiles.

The profile contains the parameters required for phones to connect to the phone server with Wi-Fi. When you create and use a Wi-Fi profile, you or your users do not need to configure the wireless network for individual phones.

A Wi-Fi profile enables you to prevent or limit changes to the Wi-Fi configuration on the phone by the user.

We recommend that you use a secure profile with TFTP encryption enabled to protect keys and passwords when you use a Wi-Fi profile.

When you set up the phones to use EAP-FAST, PEAP-MSCHAPV, or PEAP-GTC authentication or security mode, your users need individual credentials to connect to an access point.

Before you begin

• Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **System**.

Step 2   Set the **Wi-Fi Profile** fields as described in the following table.

Field	Field Type or Choices	Default	Description
Security mode	Auto EAP-FAST PEP-GCT PEAP-MSCHAPV2 PSK WEP None	None	Allows you to select the type of authentication that the phone uses to access the WLAN. The security mode depends on the settings on your access point.
Network name			Allows you to enter a unique name for the Wi-Fi profile. This name displays on the phone.
User ID			Allows you to enter a user ID for the network profile.
Password WEP Key Passphrase			Allows you to enter password for the network profile that you create. The type of password depends on the security mode that you have selected. • Password: Security mode is Auto. • Passphrase: Security mode is PSK. • WEP Key: Security mode is WEP.
Frequency band	• Auto • 2.4 GHz • 5 GHz	Auto	Allows you to select the wireless signal standard that the WLAN uses.

You can also configure Wi-Fi profile in the XML Configuration file in the format:

```
<!--  Wi-Fi Settings  -->
<Phone-wifi-on ua="rw">Yes</Phone-wifi-on>
<Phone-wifi-type ua="na">WLAN</Phone-wifi-type>
<!--  available options: WLAN|WPS  -->
 <!--  Wi-Fi Profile 1  -->
<Network_Name_1_ ua="rw">wipp</Network_Name_1_>
<Security_Mode_1_ ua="rw">Auto</Security_Mode_1_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_1_ ua="rw"></Wi-Fi_User_ID_1_>
 <!--
 <Wi-Fi_Password_1_ ua="rw">*************</Wi-Fi_Password_1_>
-->
 <!--  <WEP_Key_1_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_1_ ua="rw"/>  -->
<Frequency_Band_1_ ua="rw">Auto</Frequency_Band_1_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
```

```
<Wi-Fi_Profile_Order_1_ ua="rw">1</Wi-Fi_Profile_Order_1_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 2  -->
<Network_Name_2_ ua="rw">internet</Network_Name_2_>
<Security_Mode_2_ ua="rw">None</Security_Mode_2_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_2_ ua="rw"/>
 <!--  <Wi-Fi_Password_2_ ua="rw"/>  -->
 <!--  <WEP_Key_2_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_2_ ua="rw"/>  -->
<Frequency_Band_2_ ua="rw">Auto</Frequency_Band_2_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_2_ ua="rw">2</Wi-Fi_Profile_Order_2_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 3  -->
<Network_Name_3_ ua="rw"/>
<Security_Mode_3_ ua="rw">None</Security_Mode_3_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_3_ ua="rw"/>
 <!--  <Wi-Fi_Password_3_ ua="rw"/>  -->
 <!--  <WEP_Key_3_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_3_ ua="rw"/>  -->
<Frequency_Band_3_ ua="rw">Auto</Frequency_Band_3_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_3_ ua="rw">3</Wi-Fi_Profile_Order_3_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 4  -->
<Network_Name_4_ ua="rw"/>
<Security_Mode_4_ ua="rw">None</Security_Mode_4_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_4_ ua="rw"/>
 <!--  <Wi-Fi_Password_4_ ua="rw"/>  -->
 <!--  <WEP_Key_4_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_4_ ua="rw"/>  -->
<Frequency_Band_4_ ua="rw">Auto</Frequency_Band_4_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_4_ ua="rw">4</Wi-Fi_Profile_Order_4_>
<!--  available options: 1|2|3|4  -->
```

Step 3   Click **Submit All Changes**.

If the phone has an active call, you can not save the changes.

Delete a Wi-Fi Profile

You can remove a Wi-Fi profile from the list when the profile is no more required.

Procedure

Step 1   Press **Applications** ⚙ .

Step 2	Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi profile**.
Step 3	In the **Wi-Fi profile** screen, select the Wi-Fi profile that you want to remove.
Step 4	Press **Options**.
Step 5	Select **Delete** and then confirm the deletion.

Change the Order of a Wi-Fi Profile

You can determine the position of a Wi-Fi profile in the list. The Wi-Fi profile at the top of the list has the highest priority. When the Wi-Fi is turned on, the phone uses the Wi-Fi profile on the top of the list to connect automatically to a wirless network while provisioning.

Procedure

Step 1	If you change the Wi-Fi profile order from the phone, follow these steps:
	a) Press **Applications** .
	b) Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi profile**.
	c) In the **Wi-Fi profile screen**, select a Wi-Fi of which you want to change the order.
	d) Press **Options**.
	e) Select **Move up** or **Move down** to move the Wi-Fi profile one level up or one level down respectively in the list.
Step 2	If you change the Wi-Fi profile order from the phone web page, follow these steps:
	a) Select **Voice** > **System**.
	b) In the **Wi-Fi Profile (n)** section, set the **Wi-Fi Profile Order** field to the desired order.
	c) Click **Submit All Changes**.

Scan and Save a Wi-Fi Network

You can scan a Wi-Fi profile to get the list of available wireless networks (SSID). The security mode and the network name have the same value of the scanned SSID. You can then edit the fields of any of the wireless networks. When you save the changes, it saves as a Wi-Fi profile in the phone Wi-Fi profile list. You can then use this new Wi-Fi profile to connect the phone to a wireless network.

Note

- When the security mode of a wireless network is None, PSK, and WEP, you can't modify the security mode. On the **Security mode** screen, you only see the security mode that is set for the network. For example, if the security mode of a network is PSK, you see only PSK in the **Security mode** screen.

- When you scan a wireless network (SSID) which is the current connected wireless, you can't edit the **Network name** of this SSID.

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi profile**.

Step 3 In the **Wi-Fi profile** screen, press **Scan** to get all available wireless networks.

Step 4 (Optional) In the **Connect to Wi-Fi** screen, press **Scan** again to rescan the list.

Step 5 Select a wireless and press **Select** or the **Select** button.

Step 6 In the **Setup Wi-Fi** screen, set the parameters as mentioned in the **Profile Parameters** table.

Table 12: Profile Parameters

Parameter	Description
Security mode	Allows you to select the authentication method that is used to secure access to the Wi-Fi network. Depending on the method you choose, a password, passphrase, or key field appears so that you can provide the credentials that are required to join this Wi-Fi network. Options are: • Auto • EAP-FAST • PEAP-GTC • PEAP-MSCHAPV2 • PSK • WEP • None Default: None
Network name	Allows you to enter a name for the SSIDs. This name displays on the phone. Multiple profiles can have the same network name with different security mode.This name displays on the phone.
User ID	Allows you to enter a user ID for the network profile. This field is available when you set the security mode to Auto, EAP-FAST, PEAP-GTC, PEAP-MSCHAPV2. This is a mandatory field and it allows maximum length of 32 alphanumeric characters.

Parameter	Description
Password	Allows you to enter password for the network profile that you create.
	This field is available when you set the security mode to Auto, EAP-FAST, PEAP-GTC, PEAP-MSCHAPV2. This is a mandatory field and it allows maximum length of 64 alphanumeric characters.
WEP key	Allows you to enter password for the network profile that you create.
	This field is available when you set the security mode to WEP. This is a mandatory field and it allows maximum length of 32 alphanumeric characters.
Passphrase	Allows you to enter password for the network profile that you create. You need to enter this value when the security mode is PSK.
Frequency band	Allows you to select the wireless signal frequency band that is used in the WLAN. Options are:
	• Auto
	• 2.4 GHz
	• 5 GHz
	Default: Auto

Step 7 Press **Save**.

View the Wi-Fi Status

You may experience issues related to Wi-Fi connection. You can gather information from the **Wi-Fi status** page to help you troubleshoot.

You can also view the status from the phone web page by selecting **User Login** > **Advanced** > **Info** > **Status** > **System Information**.

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Network configuration** > **Wi-Fi configuration** > **Wi-Fi status**.

You see the information:

• **Wi-Fi status**: Displays if the Wi-Fi is connected or disconnected.

• **Network name**: Indicates the name of the SSID.

• **Signal strength**: Indicates strength of the network signal.

• **MAC address**: Indicates MAC address of the phone.

• **AP MAC address**: Indicates MAC address of the access point (SSID).

• **Channel**: Indicated the channel on which the Wi-Fi network transmits and receives data.

• **Frequency**: Indicates the wireless signal frequency band that is used in the Wireless LAN.

• **Security mode**: Indicates the security mode that is set for the wireless LAN.

View Wi-Fi Status Messages on the Phone

You can view messages about the Wi-Fi connection status of your phone. The messages can help you diagnose Wi-Fi connection problems. The messages contain:

• connection time and MAC address of the access point

• disconnection time and diagnostic code from the access point

• connection failure time and reason code from the access point

• time that weak signal of the access point continues over 12 seconds

Procedure

Step 1   Press **Applications** ⚙.

Step 2   Select **Status** > **Wi-Fi messages**.

Step 3   Use the outer ring of the navigation cluster to scroll through the messages.

Step 4   Press **Details** to view more details of the selected message.

Step 5   (Optional) Press **Clear** to delete all the messages.

Verify Phone Startup

After the Cisco IP Phone has power connected to it, the phone automatically cycles through a startup diagnostic process.

Procedure

Step 1   If you are using Power over Ethernet, plug the LAN cable into the Network port.

Step 2   If you are using the power cube, connect the cube to the phone and plug the cube into an electrical outlet.

The buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.

If the phone completes these stages successfully, it has started up properly.

Configure the Voice Codecs

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. Negotiation of the optimal voice codec sometimes depends on the ability of the Cisco IP Phone to match a codec name with the far-end device or gateway codec name. The phone allows the network administrator to individually name the various codecs that are supported such that the correct codec successfully negotiates with the far-end equipment.

The Cisco IP Phone supports voice codec priority. You can select up to three preferred codecs. The administrator can select the low-bit-rate codec that is used for each line. G.711a and G.711u are always enabled.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **Audio Configuration** section, configure the parameters.

Step 3 Click **Submit All Changes**.

Set the Optional Network Servers

Optional network servers provide resources such as DNS lookup, network time, logging, and device discovery. It also enables you to add PC port mirroring on the user phone. Your user can also enable or disable this service from the phone.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **System**.

Step 2 In the **Optional Network Configuration** section, set up the fields as described in Optional Network Configuration, on page 225.

Step 3   Click **Submit All Changes**.

VLAN Settings

The software tags your phone voice packets with the VLAN ID when you use a virtual LAN (VLAN).

In the VLAN Settings section of the **Voice** > **System** window, you can configure the different settings:

- LLDP-MED
- Cisco Discovery Protocol (CDP)
- Network Startup Delay
- VLAN ID (manual)
- DHCP VLAN Option

The multiplatform phones support these four methods to obtain VLAN ID information. The phone attempts to obtain the VLAN ID information in this order:

1. LLDP-MED
2. Cisco Discovery Protocol (CDP)
3. VLAN ID (manual)
4. DHCP VLAN Option

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is negotiation-based and determines which virtual LAN (VLAN) the Cisco IP Phone resides in. If you are using a Cisco switch, Cisco Discovery Protocol (CDP) is available and is enabled by default. CDP has these attributes:

- Obtains the protocol addresses of neighboring devices and discovers the platform of those devices.
- Shows information about the interfaces your router uses.
- Is media and protocol-independent.

If you are using a VLAN without CDP, you must enter a VLAN ID for the Cisco IP Phone.

LLDP-MED

The Cisco IP Phone supports Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) for deployment with Cisco or other Third-Party network connectivity devices that use a Layer 2 auto discovery mechanism. Implementation of LLDP-MED is done in accordance with IEEE 802.1AB (LLDP) Specification of May 2005, and ANSI TIA-1057 of April 2006.

The Cisco IP Phone operates as a LLDP-MED Media End Point Class III device with direct LLDP-MED links to Network Connectivity Devices, according to the Media Endpoint Discovery Reference Model and Definition (ANSI TIA-1057 Section 6).

The Cisco IP Phone supports only the following limited set of Type-Length-Values (TLV) as an LLDP-MED Media Endpoint device class III:

- Chassis ID TLV

- Port ID TLV

- Time to live TLV

- Port Description TLV

- System Name TLV

- System Capabilities TLV

- IEEE 802.3 MAC/PHY Configuration/Status TLV (for wired network only)

- LLDP-MED Capabilities TLV

- LLDP-MED Network Policy TLV (for application type=Voice only)

- LLDP-MED Extended Power-Via-MDI TLV (for wired network only)

- LLDP-MED Firmware Revision TLV

- End of LLDPDU TLV

The outgoing LLDPDU contains all the preceding TLVs if applicable. For the incoming LLDPDU, the LLDPDU is discarded if any of the following TLVs are missing. All other TLVs are not validated and ignored.

- Chassis ID TLV

- Port ID TLV

- Time to live TLV

- LLDP-MED Capabilities TLV

- LLDP-MED Network Policy TLV (for application type=Voice only)

- End of LLDPDU TLV

The Cisco IP Phone sends out the shutdown LLDPDU if applicable. The LLDPDU frame contains the following TLVs:

- Chassis ID TLV

- Port ID TLV

- Time to live TLV

- End of LLDPDU TLV

There are some restrictions in the implementation of LLDP-MED on the Cisco IP Phones:

- Storage and retrieval of neighbor information are not supported.

• SNMP and corresponding MIBs are not supported.

• Recording and retrieval of statistical counters are not supported.

• Full validation of all TLVs does not take place; TLVs that do not apply to the phones are ignored.

• Protocol state machines as stated in the standards are used only for reference.

Chassis ID TLV

For the outgoing LLDPDU, the TLV supports subtype=5 (Network Address). When the IP address is known, the value of the Chassis ID is an octet of the INAN address family number followed by the octet string for the IPv4 address used for voice communication. If the IP address is unknown, the value for the Chassis ID is `0.0.0.0`. The only INAN address family supported is IPv4. Currently, the IPv6 address for the Chassis ID is not supported.

For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Chassis ID TLV is mandatory as the first TLV. Only one Chassis ID TLV is allowed for the outgoing and incoming LLDPDUs.

Port ID TLV

For the outgoing LLDPDU, the TLV supports subtype=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID.

For the incoming LLDPDU, the Port ID TLV is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Port ID TLV is mandatory as the second TLV. Only one Port ID TLV is allowed for the outgoing and incoming LLDPDUs.

Time to Live TLV

For the outgoing LLDPDU, the Time to Live TTL value is 180 seconds. This differs from the 120-second value that the standard recommends. For the shutdown LLDPDU, the TTL value is always 0.

The Time to Live TLV is mandatory as the third TLV. Only one Time to Live TLV is allowed for the outgoing and incoming LLDPDUs.

End of LLDPDU TLV

The value is 2-octet, all zero. This TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs.

Port Description TLV

For the outgoing LLDPDU, in the Port Description TLV, the value for the port description is the same as "Port ID TLV" for CDP. The incoming LLDPDU, the Port Description TLV, is ignored and not validated. Only one Port Description TLV is allowed for outgoing and incoming LLDPDUs.

System Name TLV

For the Cisco IP Phone, the value is SEP+MAC address.

Example: SEPAC44F211B1D0

The incoming LLDPDU, the System Name TLV, is ignored and not validated. Only one System Name TLV is allowed for the outgoing and incoming LLDPDUs.

System Capabilities TLV

For the outgoing LLDPDU, in the System Capabilities TLV, the bit values for the 2 octet system capabilities fields should be set for Bit 2 (Bridge) and Bit 5 (Phone) for a phone with a PC port. If the phone does not have a PC port, only Bit 5 should be set. The same system capability value should be set for the enabled capability field.

For the incoming LLDPDU, the System Capabilities TLV is ignored. The TLV is not validated semantically against the MED device type.

The System Capabilities TLV is mandatory for outgoing LLDPDUs. Only one System Capabilities TLV is allowed.

Management Address TLV

The TLV identifies an address associated with the local LLDP agent (that may be used to reach higher layer entities) to assist discovery by network management. The TLV allows the inclusion of both the system interface number and an object identifier (OID) that are associated with this management address, if either or both are known.

- TLV information string length—This field contains the length (in octets) of all the fields in the TLV information string.

- Management address string length—This field contains the length (in octets) of the management address subtype + management address fields.

System Description TLV

The TLV allows the network management to advertise the system description.

- TLV information string length—This field indicates the exact length (in octets) of the system description.

- System description—This field contains an alphanumeric string that is the textual description of the network entity. The system description includes the full name and version identification of the system hardware type, software operating system, and networking software. If implementations support IETF RFC 3418, the sysDescr object should be used for this field.

IEEE 802.3 MAC/PHY Configuration/Status TLV

The TLV is not for autonegotiation, but for troubleshooting purposes. For the incoming LLDPDU, the TLV is ignored and not validated. For the outgoing LLDPDU, for the TLV, the octet value autonegotiation support/status should be:

- Bit 0—Set to 1 to indicate that the autonegotiation support feature is supported.

- Bit 1—Set to 1 to indicate that autonegotiation status is enabled.

- Bit 2-7—Set to 0.

The bit values for the 2 octets PMD autonegotiation advertised capability field should be set to:

- Bit 13—10BASE-T half duplex mode

- Bit 14—10BASE-T full duplex mode

- Bit 11—100BASE-TX half duplex mode

- Bit 10—100BASE-TX full duplex mode

- Bit 15—Unknown

Bit 10, 11, 13 and 14 should be set.

The value for 2 octets operational MAU type should be set to reflect the real operational MAU type:

- 16—100BASE-TX full duplex

- 15—100BASE-TX half duplex

- 11—10BASE-T full duplex

- 10—10BASE-T half duplex

For example, usually, the phone is set to 100BASE-TX full duplex. The value 16 should then be set. The TLV is optional for a wired network and not applicable for a wireless network. The phone sends out this TLV only when in wired mode. When the phone is not set for autonegotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value autonegotiation support/status should be clear (0) to indicate that autonegotiation is disabled. The 2 octets PMD autonegotiation advertised capability field should be set to 0x8000 to indicate unknown.

LLDP-MED Capabilities TLV

For the outgoing LLDPDU, the TLV should have the device type 3 (End Point Class III) with the following bits set for 2-octet Capability field:

Bit Position	Capability
0	LLDP-MED Capabilities
1	Network Policy
4	Extended Power via MDI-PD
5	Inventory

For the incoming TLV, if the LLDP-MED TLV is not present, the LLDPDU is discarded. The LLDP-MED Capabilities TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs. Any other LLDP-MED TLVs will be ignored if they present before the LLDP-MED Capabilities TLV.

Network Policy TLV

In the TLV for the outgoing LLDPDU, before the VLAN or DSCP is determined, the Unknown Policy Flag (U) is set to 1. If the VLAN setting or DSCP is known, the value is set to 0. When the policy is unknown, all other values are set to 0. Before the VLAN is determined or used, the Tagged Flag (T) is set to 0. If the tagged VLAN (VLAN ID > 1) is used for the phone, the Tagged Flag (T) is set to 1. Reserved (X) is always set to 0. If the VLAN is used, the corresponding VLAN ID and L2 Priority will be set accordingly. VLAN ID valid

value is range from 1-4094. However, VLAN ID=1 will never be used (limitation). If DSCP is used, the value range from 0-63 is set accordingly.

In the TLV for the incoming LLDPDU, Multiple Network Policy TLVs for different application types are allowed.

LLDP-MED Extended Power-Via-MDI TLV

In the TLV for the outgoing LLDPDU, the binary value for Power Type is set to "0 1" to indicate the power type for phone is PD Device. The Power source for the phone is set to "PSE and local" with binary value "1 1". The Power Priority is set to binary "0 0 0 0" to indicate unknown priority while the Power Value is set to maximum power value. The Power Value for the Cisco IP Phone is 12900mW.

For the incoming LLDPDU, the TLV is ignored and not validated. Only one TLV is allowed in the outgoing and incoming LLDPDUs. The phone will send out the TLV for the wired network only.

The LLDP-MED standard was originally drafted in the context of Ethernet. Discussion is ongoing for LLDP-MED for Wireless Networks. Refer to ANSI-TIA 1057, Annex C, C.3 Applicable TLV for VoWLAN, table 24. It is recommended that the TLV is not applicable in the context of the wireless network. This TLV is targeted for use in the context of PoE and Ethernet. The TLV, if added, will not provide any value for network management or power policy adjustment at the switch.

LLDP-MED Inventory Management TLV

This TLV is optional for Device Class III. For the outgoing LLDPDU, we support only Firmware Revision TLV. The value for the Firmware Revision is the version of firmware on the phone. For the incoming LLDPDU, the TLVs are ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

Final Network Policy Resolution and QoS

Special VLANs

VLAN=0, VLAN=1, and VLAN=4095 are treated the same way as an untagged VLAN. Because the VLAN is untagged, Class of Service (CoS) is not applicable.

Default QoS for SIP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on configuration for the specific extension. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. Type of Service (ToS) is based on configuration for the specific extension.

Default QoS for SPCP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on a predefined value of 5. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. Type of Service (ToS) is based on configuration for the specific extension.

QoS Resolution for CDP

If there is a valid network policy from CDP:

- If the VLAN=0, 1, or 4095, the VLAN will not be set, or the VLAN is untagged. CoS is not applicable, but DSCP is applicable. ToS is based on the default as previously described.

- If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.

- The phone reboots and restarts the fast start sequence.

QoS Resolution for LLDP-MED

If CoS is applicable and if CoS = 0, the default is used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on the value used for extension 1. If CoS is applicable and if CoS != 0, CoS is used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP = 0, the default is used for the specific extension as previously described. But the value show on DSCP for TLV for outgoing LLDPDU is based on value used for the extension 1. If DSCP is applicable and if DSCP != 0, DSCP is used for all extensions.

If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is set, the VLAN, L2 Priority (CoS), and DSCP (mapped to ToS) are all applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is not set, only the DSCP (mapped to ToS) is applicable.

The Cisco IP Phone reboots and restarts the fast start sequence.

Coexistence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN determines the last policy set or changed with either one of the discovery modes. If both LLDP-MED and CDP are enabled, during startup the phone sends CDP and LLDP-MED PDUs.

Inconsistent configuration and behavior for network connectivity devices for CDP and LLDP-MED modes could result in an oscillating rebooting behavior for the phone due to switching to different VLANs.

If the VLAN is not set by CDP and LLDP-MED, the VLAN ID that is configured manually is used. If the VLAN ID is not configured manually, no VLAN is supported. DSCP is used and the network policy determines LLDP-MED if applicable.

LLDP-MED and Multiple Network Devices

If the same application type is used for the network policy but different Layer 2 or Layer 3 QoS Network policies are received by the phones from multiple network connectivity devices, the last valid network policy is honored. To ensure deterministic and consistent of Network Policy, multiple network connectivity devices should not send out conflicting network policies for the same application type.

Configure VLAN Settings

Before you begin

Access the phone administration web page. See .

Procedure

Step 1 Select **Voice** > **System**.

Step 2 In the **VLAN Settings** section, configure the fields.

Step 3 Click **Submit All Changes**.

Set Up DHCP VLAN Option from Phone Web Page

.

You can add a predefined DHCP option to configure the voice VLAN for your phone.

Before you begin

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

- Disable CDP/LLDP and manual VLAN.

Procedure

Step 1 Select **Voice** > **System**.

Step 2 In the **VLAN Settings** section, enter a value in the **DHCP VLAN Option** field.

The field is empty, by default.

Valid values are:

- Null

- 128 to 149

- 151 to 158

- 161 to 254

Set the **DHCP VLAN Option** value to **Null** to disable the voice VLAN configuration.

Cisco recommends that you use DHCP Option 132.

Step 3 Click **Submit All Changes**.

What to do next

In the **VLAN Settings** section of the **Voice** > **System** tab, you can configure these settings:

- Cisco Discovery Protocol (CDP)

- LLDP-MED

- Network Startup Delay

• VLAN ID

• DHCP VLAN Option

SIP and NAT Configuration

SIP and the Cisco IP Phone

The Cisco IP Phone uses Session Initiation Protocol (SIP), which allows interoperation with all IT service providers that support SIP. SIP is an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

In typical commercial IP telephony deployments, all calls go through a SIP Proxy Server. The receiving phone is called the SIP user agent server (UAS), while the requesting phone is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response routes back to the UAS, and the two UAs connect using a direct peer-to-peer session. Voice traffic transmits between UAs over dynamically assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; RTP does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP.

SIP Over TCP

To guarantee state-oriented communications, the Cisco IP Phone can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem of UDP port-blocking by corporate firewalls. With TCP, new ports do not need to be open or packets dropped, because TCP is already in use for basic activities, such as internet browsing or e-commerce.

SIP Proxy Redundancy

An average SIP Proxy Server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. Cisco phones support the use of backup SIP Proxy Servers to minimize or eliminate service disruption.

A static list of proxy servers is not always adequate. If your user agent serves different domains, for example, you do not want to configure a static list of proxy servers for each domain into every Cisco IP Phone.

A simple way to support proxy redundancy is to configure a SIP Proxy Server in the Cisco IP Phone configuration profile. The DNS SRV records instruct the phones to contact a SIP Proxy Server in a domain named in SIP messages. The phone consults the DNS server. If configured, the DNS server returns an SRV record that contains a list of SIP Proxy Servers for the domain, with their hostnames, priority, listening ports, and so forth. The Cisco IP Phone tries to contact the hosts in the order of their priority.

If the Cisco IP Phone currently uses a lower-priority proxy server, the phone periodically probes the higher-priority proxy and switches to the higher-priority proxy when available.

Dual Registration

The phone always registers to both primary (or primary outbound) and alternate (or alternate outbound) proxies. After registration, the phone sends out Invite and Non-Invite SIP messages through primary proxy first. If there is no response for the new INVITE from the primary proxy, after timeout, the phone attempts to connect with the alternate proxy. If the phone fails to register to the primary proxy, it sends an INVITE to the alternate proxy without trying the primary proxy.

Dual registration is supported on a per-line basis. Three added parameters can be configured through web user interface and remote provisioning:

- Alternate Proxy—Default is empty.

- Alternate Outbound Proxy—Default is empty.

- Dual Registration—Default is NO (turned off).

After you configure the parameters, reboot the phone for the feature to take effect.

Note Specify a value for primary proxy (or primary outbound proxy) and alternate proxy (or alternate outbound proxy) for the feature to function properly.

Dual Registration and DNS SRV Limitations

- When Dual Registration is enabled, DNS SRV Proxy Fallback or Recovery must be disabled.

- Do not use Dual Registration along with other Fallback or Recovery mechanisms. For example: Broadsoft mechanism.

- There is no recovery mechanism for feature request. However, the administrator can adjust the reregistration time for a prompt update of the registration state for primary and alternate proxy.

Dual Registration and Alternate Proxy

When the Dual Register parameter is set to **No**, Alternate Proxy is ignored.

Failover and Recovery Registration

- Failover—The phone performs a failover when transport timeout/failure or TCP connection failures; if Try Backup RSC and Retry Reg RSC values are datafilled.

- Recovery—The phone attempts to reregister with the primary proxy while registered or actively connected to the secondary proxy.

  Auto register when failover parameter controls the failover behavior when there is an error. When this parameter is set to yes, the phone re-registers upon failover or recovery.

Fallback Behavior

The fallback occurs when the current registration expires or Proxy Fallback Intvl fires.

If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to primary proxy.

For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback triggers 600 seconds later.

When the value for Register Expires is 800 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback triggers at 800 seconds.

After successful registration back to the primary server, all SIP messages go to the primary server.

RFC3311

The Cisco IP Phone supports RFC-3311, the SIP UPDATE Method.

SIP NOTIFY XML-Service

The Cisco IP Phone supports the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message can contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

SIP Configuration

SIP settings for the Cisco IP Phone are configured for the phone in general and for the extensions.

Configure the Basic SIP Parameters

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **SIP**.

Step 2   In the **SIP Parameters** section, set the SIP parameters as described in SIP Parameters, on page 231.

Step 3   Click **Submit All Changes**.

Configure the SIP Timer Values

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **SIP**.

Step 2   In the **SIP Timer Values** section, set the SIP timer values in seconds as described in SIP Timer Values (sec), on page 234.

Step 3   Click **Submit All Changes**.

Configure the Response Status Code Handling

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **SIP**.

Step 2   In the **Response Status Code Handling** section, set the values as specified:

- **Try Backup RSC**—SIP response code that retries a backup server for the current request. Defaults to blank. For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the latter, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??.

- **Retry Reg RSC**—SIP response code that the phone retries registration after failing during the last registration. Defaults to blank. For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the latter, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??.

Step 3   Click **Submit All Changes**.

Configure the RTP Parameters

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **SIP**.
Step 2	In the **RTP Parameters** section, set the Real-Time Transport Protocol (RTP) parameter values as described in RTP Parameters, on page 237.
Step 3	Click **Submit All Changes**.

Configure the SDP Payload Types

Configured dynamic payloads are used for outbound calls only when the Cisco IP Phone presents a Session Description Protocol (SDP) offer. For inbound calls with an SDP offer, the phone follows the caller's assigned dynamic payload type.

The Cisco IP Phone uses the configured codec names in outbound SDP. For incoming SDP with standard payload types of 0-95, the phone ignores the codec names. For dynamic payload types, the phone identifies the codec by the configured codec names (comparison is case-sensitive).

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **SIP**.
Step 2	In the **SDP Payload Types** section, set the value as specified in SDP Payload Types, on page 238.
	• **AVT Dynamic Payload**—Any nonstandard data. Both sender and receiver must agree on a number. Ranges from 96 to 127. Default: 101.
Step 3	Click **Submit All Changes**.

Configure the SIP Settings for Extensions

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Ext(n)**, where n is an extension number.
Step 2	In the **SIP Settings** section, set the parameter values as described in SIP Settings, on page 277.
Step 3	Click **Submit All Changes**.

Configure the SIP Proxy Server

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2   In the **Proxy and Registration** section, set the parameter values as described in Proxy and Registration, on page 283.

Step 3   Click **Submit All Changes**.

Configure the Subscriber Information Parameters

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2   In the **Subscriber Information** section, set the parameter values as described in Subscriber Information, on page 286.

Step 3   Click **Submit All Changes**.

Managing NAT Transversal with Phones

Network Address Translation (NAT) allows multiple devices to share a single, public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. For VoIP to coexist with NAT, NAT traversal is required.

Not all service providers provide NAT traversal. If your service provider does not provide NAT traversal, you have several options:

- NAT Mapping with Session Border Controller
- NAT Mapping with SIP-ALG Router
- NAT Mapping with a Static IP Address
- NAT Mapping with STUN

Enable NAT Mapping

You must enable NAT mapping to set NAT parameters.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Ext(n)**.
Step 2	Set up the fields as described in NAT Settings, on page 276.
Step 3	Click **Submit All Changes**.

NAT Mapping with Session Border Controller

We recommend that you choose an service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

NAT Mapping with SIP-ALG Router

NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.

NAT Mapping with the Static IP Address

You can configure NAT mapping on the phone to ensure interoperability with the service provider.

- You must have an external (public) IP address that is static.

- The NAT mechanism used in the router must be symmetric. For more information, see Determining Symmetric or Asymmetric NAT, on page 74 .

Use NAT mapping only if the service provider network does not provide a Session Border Controller functionality.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **SIP**.
Step 2	In the **NAT Support Parameters** section, set **Handle VIA received**, **Insert VIA received**, **Substitute VIA Addr**, **Handle VIA rport**, **Insert VIA rport**, and **Send Resp To Src Port** fields to **Yes**.
Step 3	In the **NAT Support Parameters** section, set a value for the **NAT Keep Alive Intvl** field.
Step 4	Enter the public IP address for your router in the **EXT IP** field.
Step 5	Click the **Ext(n)** tab.
Step 6	In the **NAT Settings** section, set **NAT Mapping Enable** to **Yes**.
Step 7	(Optional) Set **NAT Keep Alive Enable** to **Yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

Step 8   Click **Submit All Changes**.

What to do next

Configure the firewall settings on your router to allow SIP traffic.

Configure NAT mapping with STUN

If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. The STUN protocol allows applications operating behind a network address translator (NAT) to discover the presence of the network address translator and to obtain the mapped (public) IP address (NAT addresses) and the port number that the NAT has allocated for the User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a third-party network server (STUN server) located on the opposing (public) side of the NAT, usually the public Internet. This option is considered a last resort and should be used only if the other methods are not available. To use STUN:

- The router must use asymmetric NAT. See .

- A computer running STUN server software is available on the network. You can also use a public STUN server or set up your own STUN server.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **SIP**.

Step 2   In the **NAT Support Parameters** section, set **Handle VIA received**, **Insert VIA received**, **Substitute VIA Addr**, **Handle VIA rport**, **Insert VIA rport**, and **Send Resp To Src Port** fields to **Yes**.

Step 3   In the **NAT Support Parameters** section, set **STUN Enable** field to **Yes**.

Step 4   Enter the IP address for your STUN server in the **STUN Server** field.

Step 5   Click the **Ext(n)** tab.

Step 6   In the **NAT Settings** section, set **NAT Mapping Enable** to **Yes**.

Step 7   (Optional) Set **NAT Keep Alive Enable** to **Yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

Step 8   Click **Submit All Changes**.

What to do next

Configure the firewall settings on your router to allow SIP traffic.

Determining Symmetric or Asymmetric NAT

STUN does not work on routers with symmetric NAT. With symmetric NAT, IP addresses are mapped from one internal IP address and port to one external, routable destination IP address and port. If another packet is sent from the same source IP address and port to a different destination, a different IP address and port number combination is used. This method is restrictive because an external host can send a packet to a particular port on the internal host only if the internal host first sent a packet from that port to the external host.

This procedure assumes that a syslog server is configured and is ready to receive syslog messages.

To Determine Whether the Router Uses Symmetric or Asymmetric NAT:

Procedure

Step 1 Verify that the firewall is not running on your PC. (It can block the syslog port.) By default, the syslog port is 514.

Step 2 Click **Voice** > **System** and navigate to **Optional Network Configuration**.

Step 3 Enter the IP address for the **Syslog Server**, if the port number is anything other than the default, 514. It is not necessary to include the port number if it is the default.

The address and port number must be reachable from the Cisco IP phone. The port number appears on the output log file name. The default output file is `syslog.514.log` (if port number was not specified).

Step 4 Set the **Debug Level** to **Error**, **Notice**, or **Debug**.

Step 5 To capture SIP signaling messages, click the **Ext** tab and navigate to **SIP Settings**. Set the **SIP Debug Option** to **Full**.

Step 6 To collect information about what type of NAT your router uses click the **SIP** tab and navigate to **NAT Support Parameters**.

Step 7 Click **Voice** > **SIP** and navigate to **NAT Support Parameters**.

Step 8 Set **STUN Test Enable** to **Yes**.

Step 9 Determine the type of NAT by viewing the debug messages in the log file. If the messages indicate that the device is using symmetric NAT, you cannot use STUN.

Step 10 Click **Submit All Changes**.

Dial Plan

Related Topics

Dial Plan Overview

Dial plans determine how digits are interpreted and transmitted. They also determine whether the dialed number is accepted or rejected. You can use a dial plan to facilitate dialing or to block certain types of calls such as long distance or international.

Use the phone web user interface to configure dial plans on the IP phone.

This section includes information that you must understand about dial plans, and procedures to configure your own dial plans.

The Cisco IP Phone has various levels of dial plans and processes the digits sequence.

When a user presses the speaker button on the phone, the following sequence of events begins:

1. The phone begins to collect the dialed digits. The interdigit timer starts to track the time that elapses between digits.

2. If the interdigit timer value is reached, or if another terminating event occurs, the phone compares the dialed digits with the IP phone dial plan. This dial plan is configured in the phone web user interface in **Voice** > **Ext(n)** under the **Dial Plan** section.

Digit Sequences

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements that are individually matched to the keys that the user presses.

White space is ignored, but can be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 0 * #	Characters that represent a key that the user must press on the phone keypad.
x	Any character on the phone keypad.
[sequence]	Characters within square brackets create a list of accepted key presses. The user can press any one of the keys in the list. A numeric range, for example, [2-9] allows a user to press any one digit from 2 through 9. A numeric range can include other characters. For example, [35-8*] allows a user to press 3, 5, 6, 7, 8, or *.
. (period)	A period indicates element repetition. The dial plan accepts 0 or more entries of the digit. For example, 01. allows users to enter 0, 01, 011, 0111, and so forth.

Digit Sequence	Function

<dialed:substituted>	This format indicates that certain *dialed* digits are replaced by the *substituted* characters when the sequence is transmitted. The *dialed* digits can be zero to 9. For example:
	
	`<8:1650>xxxxxxx`
	
	When the user presses 8 followed by a seven-digit number, the system automatically replaces the dialed 8 with the sequence 1650. If the user dials **85550112**, the system transmits **16505550112**.
	
	If the *dialed* parameter is empty and there is a value in the *substituted* field, no digits are replaced and the *substituted* value is always prepended to the transmitted string. For example:
	
	`<:1>xxxxxxxxxx`
	
	When the user dials **9725550112**, the number 1 is added at the beginning of the sequence; the system transmits **19725550112**.

, (comma)	An intersequence tone played (and placed) between digits plays an outside line dial tone. For example: `9, 1xxxxxxxxxx` An outside line dial tone plays after the user presses 9. The tone continues until the user presses 1.
! (exclamation point)	Prohibits a dial sequence pattern. For example: `1900xxxxxxx!` Rejects any 11-digit sequence that begins with 1900.
*xx	Allows a user to enter a 2-digit star code.
S0 or L0	For Interdigit Timer Master Override, enter s0 to reduce the short interdigit timer to 0 seconds, or enter L0 to reduce the long interdigit timer to 0 seconds.
P	To pause, enter P, the number of seconds to pause, and a space. This feature is typically used for implementation of a hotline and warm line, with a 0 delay for the hot line, and a nonzero delay for a warm line. For example: `P5` A pause of 5 seconds is introduced.

Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

- Extensions on your system:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`[1-8]xx` Allows a user to dial any three-digit number that starts with the digits 1 to 8. If your system uses four-digit extensions, enter the following string: `[1-8]xxx`

- Local dialing with seven-digit number:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111)
```

`9, xxxxxxx` After a user presses 9, an external dial tone sounds. The user can enter any seven-digit number, as in a local call.

- Local dialing with 3-digit area code and a 7-digit local number:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`9, <:1>[2-9]xxxxxxxxx` This example is useful where a local area code is required. After a user presses 9, an external dial tone sounds. The user must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before it transmits the number to the carrier.

- Local dialing with an automatically inserted 3-digit area code:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`8, <:1212>xxxxxxx` This example is useful where a local area code is required by the carrier but most calls go to one area code. After the user presses 8, an external dial tone sounds. The user can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before it transmits the number to the carrier.

- U.S. long-distance dialing:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`9, 1 [2-9] xxxxxxxxx` After the user presses 9, an external dial tone sounds. The user can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

- Blocked number:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`9, 1 900 xxxxxxx !` This digit sequence is useful if you want to prevent users from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S. After the user presses 9, an external dial tone sounds. If the user enters an 11-digit number that starts with the digits 1900, the call is rejected.

- U.S. international dialing:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`9, 011xxxxxx` After the user presses 9, an external dial tone sounds. The user can enter any number that starts with 011, as in an international call from the U.S.

- Informational numbers:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`0 | [49]11` This example includes two-digit sequences, separated by the pipe character. The first sequence allows a user to dial 0 for an operator. The second sequence allows the user to enter 411 for local information or 911 for emergency services.

Acceptance and Transmission of the Dialed Digits

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As the user enters more digits, the set of candidates diminishes until only one or none is valid. When a terminating event occurs, the IP PBX either accepts the user-dialed sequence and initiates a call, or else rejects the sequence as invalid. The user hears the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
Dialed digits have not matched any sequence in the dial plan.	The number is rejected.
Dialed digits exactly match one sequence in the dial plan.	If the dial plan allows the sequence, the number is accepted and is transmitted according to the dial plan.
	If the dial plan blocks the sequence, the number is rejected.
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the time that the applicable interdigit timer specifies.
	The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan.
	Default: 10 seconds.
	The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. Default: 3 seconds.
A user presses the # key or the dial softkey on the IP phone screen.	If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan.
	If the sequence is incomplete or is blocked by the dial plan, the number is rejected.

Dial Plan Timer (Off-Hook Timer)

You can think of the Dial Plan Timer as the off-hook timer. This timer starts when the phone goes off hook. If no digits are dialed within the specified number of seconds, the timer expires and the null entry is evaluated. Unless you have a special dial plan string to allow a null entry, the call is rejected. The default length of the Dial Plan Timer is 5 seconds.

Syntax for the Dial Plan Timer

SYNTAX: (P*s*<:n> | dial plan)

- **s:** The number of seconds; if no number is entered after P, the default timer of 5 seconds applies. With the timer set to 0 seconds, the call transmits automatically to the specified extension when the phone goes off hook.

- **n:** (optional): The number to transmit automatically when the timer expires; you can enter an extension number or a DID number. No wildcard characters are allowed because the number is transmitted as shown. If you omit the number substitution, <:n>, the user hears a reorder (fast busy) tone after the specified number of seconds.

Examples for the Dial Plan Timer

Allow more time for users to start dialing after taking a phone off hook:

```
(P9 | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

P9 means that after taking a phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the user hears a reorder (fast busy) tone. By setting a longer timer, you allow more time for users to enter digits.

To create a hotline for all sequences on the System Dial Plan:

```
(P9<:23> | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

P9<:23> means that after taking the phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the call is transmitted automatically to extension 23.

To create a hotline on a line button for an extension:

```
(P0 <:1000>)
```

With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook. Enter this sequence in the Phone Dial Plan for Ext 2 or higher on a client phone.

Interdigit Long Timer (Incomplete Entry Timer)

You can think of this timer as the incomplete entry timer. This timer measures the interval between dialed digits. It applies as long as the dialed digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value is 10 seconds.

This section explains how to edit a timer as part of a dial plan. Alternatively, you can modify the Control Timer that controls the default interdigit timers for all calls.

Syntax for the Interdigit Long Timer

SYNTAX: L:s, (dial plan)

- **s:** The number of seconds; if no number is entered after L:, the default timer is 5 seconds. With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook.

- Note that the timer sequence appears to the left of the initial parenthesis for the dial plan.

Example for the Interdigit Long Timer

```
L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

L:15 means that this dial plan allows the user to pause for up to 15 seconds between digits before the Interdigit Long Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Interdigit Short Timer (Complete Entry Timer)

You can think of this timer as the complete entry timer. This timer measures the interval between dialed digits. The timer applies when the dialed digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If the entry is valid, the call proceeds. If the entry is invalid, the call is rejected.

Default: 3 seconds.

Syntax for the Interdigit Short Timer

SYNTAX 1: S:s, (dial plan)

Use this syntax to apply the new setting to the entire dial plan within the parentheses.

SYNTAX 2: *sequence* Ss

Use this syntax to apply the new setting to a particular dialing sequence.

s: The number of seconds; if no number is entered after S, the default timer of 5 seconds applies.

Examples for the Interdigit Short Timer

To set the timer for the entire dial plan:

```
S:6, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

S:6 means that while the user enters a number with the phone off hook, the user can pause for up to 15 seconds between digits before the Interdigit Short Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Set an instant timer for a particular sequence within the dial plan:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

9,8,1[2-9]xxxxxxxxxS0 means that with the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

Edit the Dial Plan on the IP Phone

Note You can edit the dial plan in the XML configuration file. Locate the `Dial_Plan_n_` parameter in the XML configuration file, where n denotes the extension number. Edit the value of this parameter. The value must be specified in the same format as in the **Dial Plan** field on the phone administration web page, described below.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2 Scroll to the **Dial Plan** section.

Step 3 Enter the digit sequences in the **Dial Plan** field.

The default (US-based) systemwide dial plan appears automatically in the field.

Step 4 You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan.

Separate each digit sequence with a pipe character, and enclose the entire set of digit sequences within parentheses. Example:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

Step 5 Click **Submit All Changes**.

The phone reboots.

Step 6 Verify that you can successfully complete a call with each digit sequence that you entered in the dial plan.

Note If you hear a reorder (fast busy) tone, review your entries and modify the dial plan appropriately.

Related Topics

Dial Plan, on page 74

Reset the Control Timers

If you need to edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Regional**.
Step 2	Scroll to the **Control Timer Values (sec)** section.
Step 3	Enter the desired values in the **Interdigit Long Timer** field and the **Interdigit Short Timer** field.
Step 4	Click **Submit All Changes**.

Regional Parameters and Supplementary Services

Regional Parameters

In the phone web user interface, use the **Regional** tab to configure regional and local settings, such as control timer values, dictionary server script, language selection, and locale to change localization. The Regional tab includes these sections:

- Call Progress Tones—Displays values of all ringtones.

- Distinctive Ring Patterns—Ring cadence defines the ringing pattern that announces a telephone call.

- Control Timer Values—Displays all values in seconds.

- Vertical Service Activation Codes—Includes Call Back Act Code and Call Back Deact Code.

- Outbound Call Codec Selection Codes—Defines the voice quality.

- Time—Includes local date, local time, time zone, and Daylight Saving Time.

- Language—Includes Dictionary Server Script, Language Selection, and Locale.

Set the Control Timer Values

Before you begin

Access the phone administration web page. See .

Procedure

Step 1	Select **Voice** > **Regional**.
Step 2	Configure the values in the fields in the **Control Timer Values (sec)** section.
Step 3	Click **Submit All Changes**.

Localize Your Cisco IP Phone

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Regional**.
Step 2	Configure the values in the fields in the **Time** and **Language** sections.
Step 3	Click **Submit All Changes**.

Time and Date Settings

The Cisco IP Phone obtains the time settings in one of three ways:

- NTP Server—When the phone boots up, it tries to contact the first Network Time Protocol (NTP) server to get the time. The phone periodically synchronizes its time with the NTP server. The synchronization period is fixed at 1 hour. Between updates, the phone tracks time with its internal clock.

  Note   NTP time takes priority over the time you set using the menu options on the phone screen. When you manually enter a time, this setting takes effect. On the next NTP synchronization, the time id is corrected so that the NTP time is displayed.

  When you manually enter the phone time, a pop-up is available that alerts you of this behavior.

- Manual Setup—You can use the phone web user interface to enter the time and date manually. However, the NTP time or SIP Message Date overwrites this value when either is available to the phone. Manual setup requires that you enter the time in 24-hour format only.

The time that the NTP Server and the SIP Date Header serve is expressed in GMT time. The local time is obtained by offsetting the GMT according to the time zone of the region.

You can configure the Time Zone parameter with the phone web user interface or through provisioning. This time can be further offset by the Time Offset (HH/mm) parameter. This parameter must be entered in 24-hour format and can also be configured from the IP phone screen.

The Time Zone and Time Offset (HH/mm) offset values are not applied to manual time and date setup

Note   The time of the log messages and status messages are in UTC time and are not affected by the time zone setting.

Configure Daylight Saving Time

The phone supports automatic adjustment for daylight saving time.

Note The time of the log messages and status messages are in UTC time. The time zone setting does not affect them.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1 Select **Voice** > **Regional**.

Step 2 Set the **Daylight Saving Time Enable** drop-down list box to **Yes**.

Step 3 In the **Daylight Saving Time Rule** field, enter the DST rule. This value affects the time stamp on the CallerID.

Step 4 Click **Submit All Changes**.

Daylight Saving Time Examples

The following example configures daylight saving time for the U.S, adding one hour starting at midnight on the first Sunday in April and ending at midnight on the last Sunday of October; add 1 hour (USA, North America):

```
start=4/1/7/0:0:0;end=10/31/7/0:0:0;save=1
start=4/1/7;end=10/-1/7;save=1
start=4/1/7/0;end=10/-1/7/0;save=1
```

The following example configures daylight saving time for Egypt, starting at midnight on the last Sunday in April and ending at midnight on the last Sunday of September:

```
start=4/-1/7;end=9/-1/7;save=1 (Egypt)
```

The following example configures daylight saving time for New Zealand (in version 7.5.1 and higher), starting at midnight on the first Sunday of October and ending at midnight on the third Sunday of March.

```
start=10/1/7;end=3/22/7;save=1 (New Zealand)
```

The following example reflects the new change starting in March. DST starts on the second Sunday in March and ends on the first Sunday in November:

```
start=3/8/7/02:0:0;end=11/1/7/02:0:0;save=1
```

The following example configures the daylight saving time starting on the last Monday (before April 8) and ending on the first Wednesday (after May 8.)

```
start=4/-8/1;end=5/8/3;save=1
```

Phone Display Language

The Cisco IP Phone supports multiple languages for the phone display.

By default, the phone is set up for English. To enable the use of another language, you must set up the dictionary for the language. For some languages, you must also set up the font for the language.

After the setup is complete, you or your users can specify the desired language for the phone display.

Supported Languages for the Phone Display

On the phone administration web page, go to **Admin Login** > **Advanced** > **Voice** > **Regional**. In the **Language** section, click the **Locale** drop-down list box to see the supported languages for the phone display.

- bg-BG (Bulgarian)
- ca-ES (Catalan)
- cs-CZ (Czech)
- da-DK (Danish)
- de-DE (German)
- en-AU (English-Australia)
- en-CA (English-Canada)
- en-GB (English-Great Britain)
- en-NZ (English-New Zealand)
- en-US (English-United States)
- es-ES (Spanish-Spain)
- es-MX (Spanish-Mexico)
- fi-FI (Finish)
- fr-CA (French-Canada)
- fr-FR (French-France)

- hr-HR (Hungarian)
- it-IT (Italian)
- ja-JP (Japanese)
- ko-KR (Korean)
- nl-NL (Dutch)
- nn-NO (Norwegian)
- pl-PL (Polish)
- pt-BZ (Portuguese-Brazil)
- pt-PT (Portuguese-Portugal)
- ru-RU (Russian)
- sk-SK (Slovak)
- sv-SE (Swedish)
- tr-TR (Turkish)
- zh-CN (Chinese-Simplified)
- zh-HK (Chinese-Hong Kong)

Set Up Dictionaries and Fonts

Languages other than English require dictionaries. Some languages also require a font.

Procedure

Step 1 Download the locale zip file for your firmware version, from cisco.com. Place the file on your server, and unzip the file.

Dictionaries and fonts for all the supported languages are included in the zip file. Dictionaries are XML scripts. Fonts are standard TTF files.

Step 2 On the phone administration web page, go to **Admin Login** > **Advanced** > **Voice** > **Regional**. In the **Language** section, specify the necessary parameters and values in the **Dictionary Server Script** field as described below. Use a semicolon (;) to separate multiple parameter and value pairs.

- Specify the location of the dictionary and font files with the `serv` parameter.

For example: `serv=http://10.74.128.101/Locales/`

Make sure to include the IP address of the server, the path, and folder name.

• For each language that you want to set up, specify a set of parameters as described below.

Note   In these parameter specifications, *n* denotes a serial number. This number determines the sequential order in which the language options are displayed in the **Settings** menu of the phone.

0 is reserved for US-English, which has a default dictionary. You can use it optionally, to specify your own dictionary.

Use numbers starting with 1 for other languages.

• Specify the language name with the `dn` parameter.

For example: `d1=Chinese-Simplified`

This name is displayed as a language option in the **Settings** menu of the phone.

• Specify the name of the dictionary file with the `xn` parameter.

For example: `x1=zh-CN_78xx_68xx-11.2.1.1004.xml`

Make sure to specify the correct file for the language and phone model that you use.

• If a font is required for the language, specify the name of the font file with the `fn` parameter.

For example: `f1=zh-CN_78xx_68xx-11.2.1.1004.ttf`

Make sure to specify the correct file for the language and phone model that you use.

See Setup for Latin Languages, on page 86 for specific details on setting up Latin languages.

See Setup for an Asian Language, on page 86 for specific details on setting up an Asian language.

Step 3   Click **Submit All Changes**.

Setup for Latin Languages

If you use Latin languages such as French or German, you can configure up to 9 language options for the phone. The options are displayed in the **Settings** menu of the phone. To enable the options, set up a dictionary for each language that you want to include. To do this, specify a pair of the `dn` and `xn` parameters and values in the **Dictionary Server Script** field, for each language that you want to include.

Example for including French and German:

```
serv=http://10.74.128.101/Locales/;d1=French;x1=fr-FR_78xx_68xx-11.2.1.1004.xml;
d2=German;x2=de-DE_78xx_68xx-11.2.1.1004.xml
```

Setup for an Asian Language

If you use an Asian language such as Chinese, Japanese, or Korean, you can only set up one language option for the phone.

You must set up the dictionary and the font for the language. To do this, specify the `d1`, `x1` and `f1` parameters and values in the **Dictionary Server Script** field.

Example for setting up Chinese-Simplified:

```
serv=http://10.74.128.101/Locales/;d1=Chinese-Simplified;
x1=zh-CN_78xx_68xx-11.2.1.1004.xml;f1=zh-CN_78xx_68xx-11.2.1.1004.ttf
```

Specify a Language for the Phone Display

Note	Your users can select the language on the phone, from **Settings** > **Device Administration** > **Language**.

Before you begin

The dictionaries and fonts required for the language are set up. See Set Up Dictionaries and Fonts, on page 85 for details.

Procedure

Step 1   On the phone administration web page, go to **Admin Login** > **Advanced** > **Voice** > **Regional**, **Language** section. In the **Language Selection** field, specify the value of the appropriate `dn` parameter value from the **Dictionary Server Script** field, for the language of your choice.

Step 2   Click **Submit All Changes**.

Cisco IP Phone 6800 Series Documentation

See the publications that are specific to your language, phone model, and multiplatform firmware release. Navigate from the following Uniform Resource Locator (URL):

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/tsd-products-support-series-home.html

Third Party Call Control Setup

Determine the Phone MAC Address

To add phones to the Third-Party Call Control system, determine the MAC address of a Cisco IP Phone.

Procedure

Perform one of the following actions:

- On the phone, press **Applications** > **Status** > **Product Information**, and look at the MAC address field.

- Look at the MAC label on the back of the phone.

- Display the web page for the phone and select **Info** > **Status** > **Product Information**.

Network Configuration

The Cisco IP Phone is used as a part of a SIP network, because the phone supports Session Initiation Protocol (SIP). The Cisco IP Phone is compatible with other SIP IP PBX call control systems, such as BroadSoft, MetaSwitch, and Asterisk.

Configuration of these systems is not described in this document. For more information, see the documentation for the SIP PBX system to which you are connecting the Cisco IP Phone.

This document describes some common network configurations; however, your configuration can vary, depending on the type of equipment that your service provider uses.

Provisioning

Phones can be provisioned to download configuration profiles or updated firmware from a remote server when they are connected to a network, when they are powered up, and at set intervals. Provisioning is typically part of high-volume, Voice-over-IP (VoIP) deployments and is limited to service providers. Configuration profiles or updated firmware are transferred to the device through use of TFTP, HTTP, or HTTPS.

The *Cisco IP Phone 6800 Series Multiplatform Phone Provisioning Guide* describes provisioning in detail.

Report Current Phone Configuration to the Provisioning Server

You can configure the phone to report its full configuration, delta changes in the configuration, or the status data to the server. You can add up to two URLs in the **Report Rule** field to specify the destination for the report, and include an optional encryption key.

When requesting delta configuration and status reports at once, separate report rules with a **space**. Include a destination upload-URL in each of the report rules. You can optionally precede the report rule by one or more content arguments that are enclosed in square brackets `[ ]`.

When a report upload is attempted, the *HTTP Report Method* field specifies whether the HTTP Request that the phone sends should be an *HTTP PUT* or an *HTTP POST*. Choose:

- **PUT Method**–To create a new report or overwrite an existing report at a known location on the server. For example, you may want to keep overwriting each report that you send and only store the most *current* configuration on the server.

- **POST Method**–To send the report data to the server for processing, such as, by a PHP script. This approach provides more flexibility for storing the configuration information. For example, you may want to send a series of phone status reports and store *all* the reports on the server.

Use the following content arguments in the **Report Rule** field to send specific configuration reports:

Content Argument	Report Content
Default: Blank	Full Configuration report
`[--delta]`	Configuration report containing *only* the latest changed fields For example, - Report 1 contains ABC changes. - Report 2 contains XYZ changes (*not* ABC and XYZ).
`[--status]`	Full Phone Status report

Note The preceding arguments can be combined with other arguments, such as, `--key`,`--uid`, and `--pwd`. These arguments control upload authentication and encryption, and are documented in the **Profile Rule** field.

• When you specify the **[--key <encryption key>]** argument in the **Report Rule**, the phone applies AES-256-CBC encryption to the file (configuration, status, or delta), with the specified encryption key.

Note | If you have provisioned the phone with Input Keying Material (IKM) and want the phone to apply RFC 8188-based encryption to the file, do not specify the **--key** argument.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Provisioning** > **Upload Configuration Options**.

Step 2   Set the parameter for each of the five fields as described in .

Step 3   Click **Submit All Changes**.

Example of user inputs and the resulting actions of the phone and provisioning server for the **Report Rule**:

• **HTTP PUT ALL configuration:**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

http://my_http_server/config-mpp.xml

Then the phone will report the configuration data to *http://my_http_server/config-mpp.xml*.

• **HTTP PUT Changed Configuration**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

[--delta]http://my_http_server/config-mpp-delta.xml;

Then the phone will report changed configuration to *http://my_http_server/config-mpp-delta.xml*.

• **HTTP PUT Encrypted Delta Configuration**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

[--delta --key test123]http://my_http_server/config-mpp-delta.enc.xml;

The phone will report status data to *http://my_http_server/config-mpp-delta.enc.xml*

On the report server side, the file can be decrypted like this: **# openssl enc -d -aes-256-cbc -k test123 -**in config-mpp-delta.enc-delta.enc -out cfg.xml

• **HTTP PUT Status Data**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

[--status]http://my_http_server/config-mpp-status.xml;

The phone will report status data to *http://my_http_server/config-mpp-status.xml*

• **HTTP PUT Changed Configuration and Status**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

```
[--status]http://my_http_server/config-mpp-status.xml
[--delta]http://my_http_server/config-mpp-delta.xml
```

The phone will report status data to *http://my_http_server/config-mpp-status.xml* and *http://my_http_server/config-mpp-delta.xml*

- **HTTP POST Changed Configuration**

  If the report method is POST, you enter the URL for the report rule in this format:

  ```
  [--delta]http://my_http_server/report_upload.php
  ```

  The report upload file format"

  ```
  // report_upload.php content
  <?php
  $filename = "report_cfg.xml";  // report file name
  // where to put the file
  $file = "/path/to/file".$filename;
  // get data from http post
  $report_data = file_get_contents('php://input');
  // save the post data to file
  $file_put_contents($file, $report_data);
  ?>
  ```

  The phone will upload changed data to *http://my_http_server/report_cfg.xml*

Web-Based Configuration Utility

Your phone system administrator can allow you to view the phone statistics and modify some or all the parameters. This section describes the features of the phone that you can modify with the phone web user interface.

Access the Phone Web Page

If your service provider has disabled access to the configuration utility, contact the service provider before proceeding.

Procedure

Step 1   Ensure that the computer can communicate with the phone. No VPN in use.

Step 2   Start a web browser.

Step 3   Enter the IP address of the phone in your web browser address bar.

- User Access: **http://<ip address>**
- Admin Access: **http://<ip address>/admin/advanced**
- Admin Access: **http://<ip address>**, click **Admin Login** and click **advanced**

For example, `http://10.64.84.147/admin`

Step 4 Enter the password when prompted.

Related Topics

Configure a Speed Dial with the Configuration Utility Page, on page 159

Determine the IP Address of the Phone

A DHCP server assigns the IP address, so the phone must be booted up and connected to the subnetwork.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Info** > **Status**.

Step 2 Scroll to **IPv4 Information**. Current IP displays the IP address.

Step 3 Scroll to **IPv6 Information**. Current IP displays the IP address.

Allow Web Access to the Cisco IP Phone

To view the phone parameters, enable the configuration profile. To make changes to any of the parameters, you must be able to change the configuration profile. Your system administrator might have disabled the phone option to make the phone web user interface viewable or writable.

For more information, see the *Cisco IP Phone 6800 Series Multiplatform Phones Provisioning Guide*.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Click **Voice** > **System**.

Step 2 In the **System Configuration** section, set **Enable Web Server** to **Yes**.

Step 3 To update the configuration profile, click **Submit All Changes** after you modify the fields in the phone web user interface.

The phone reboots and the changes are applied.

Step 4 To clear all changes that you made during the current session (or after you last clicked **Submit All Changes**), click **Undo All Changes**. Values return to their previous settings.

Web Administration Tabs

Each tab contains parameters that are related to a particular feature. Some tasks require that you set multiple parameters in different tabs.

Info, on page 209 briefly describes each parameter that is available on the phone web user interface.

Administrator and User Accounts

The Cisco IP Phone firmware provides specific administrator and user accounts. These accounts provide specific login privileges. The administrator account name is **admin**; the user account name is **user**. These account names cannot be changed.

The **admin** account gives the service provider or Value-added Reseller (VAR) configuration access to the Cisco IP phone. The **user** account gives limited and configurable control to the device end user.

The **user** and **admin** accounts can be password protected independently. If the service provider sets an administrator account password, you are prompted for it when you click **Admin Login**. If the password does not yet exist, the screen refreshes and displays the administration parameters. No default passwords are assigned to either the administrator or the user account. Only the administrator account can assign or change passwords.

The administrator account can view and modify all web profile parameters, including web parameters, that are available to the user login. The Cisco IP Phone system administrator can further restrict the parameters that a user account can view and modify through use of a provisioning profile.

Configuration parameters that are available to the user account are configurable on the Cisco IP Phone. User access to the phone web user interface can be disabled.

Enable User Access to the Phone Interface Menus

Use the **admin** account to enable or disable access to the phone web user interface by the **user** account. If the user account has access, users can set parameters through the phone web user interface.

Note

- Connection_Type ua="rw", you can read and change the information on the user phone web and phone screen.

- Connection_Type ua="ro", you can only read, not change, the information on the user phone web and phone screen.

- Connection_Type ua="na", you can not access the information on the user phone web or phone screen.

For more information on provisioning, see the *Cisco IP Phone 6800 Series Multiplatform Phones Provisioning Guide*.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **System**.
Step 2	Under **System Configuration** in the **Phone-UI-User-Mode** field, choose **Yes**.
Step 3	Click **Submit All Changes**.

Access Administrative Options by Login

Before you begin

Access the phone administration web page. See .

Procedure

If prompted, enter the **Admin Password**.

Access Administrative Options by IP Address

Procedure

Enter the IP address of the Cisco IP Phone in a web browser and include the **admin/** extension.

For example: `http://10.64.84.147/admin/`

PART III

Phone Accessories

Cisco IP Phone Accessories

Supported Accessories

The Cisco IP Phone 6800 Series Multiplatform Phones supports both Cisco and third-party accessories.

Table 13: Accessory Support for the Cisco IP Phone 6800 Series Multiplatform Phones

Accessory	Type	6821	6841	6851	6861
Cisco Accessories					
Cisco IP Phone 6800 Key Expansion Module	Add-on module	Not supported	Not supported	Supported Supports one key expansion module	Not supported
Cisco IP Phone 6800 Wall Mount Kit	Add-on module	Not supported	Supported	Supported	Supported
Third-Party Accessories					
Headsets	Analog	Supported	Supported	Supported	Supported
	Analog Wideband	Supported	Supported	Supported	Supported
Microphone	External	Not supported	Not supported	Not supported	Not supported
Speakers	External	Not supported	Not supported	Not supported	Not supported

Cisco 6800 Series Key Expansion Module Setup Overview

The Cisco IP Phone 6800 Key Expansion Module add extra programmable buttons to the phone. The programmable buttons can be set up as speed-dial buttons, or phone feature buttons.

The Cisco IP Phone 6851 Multiplatform Phone supports only one key expansion module. The key expansion module provides 14 lines or programmable buttons, and two pages. Each page contains 14 lines or buttons.

Key Expansion Module Buttons and Hardware
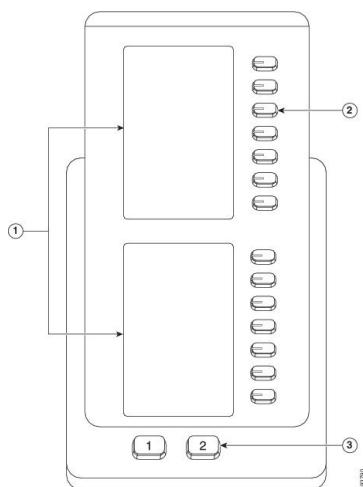
The following table describes the features of the key expansion module.

1	LCD screens—Displays the phone number, name, and icon. Icons indicate the line status and the phone service assigned on that line.
2	Lighted buttons—14 buttons. Each button corresponds to one line (same as on the phone). The lights beneath each button indicate the state of the corresponding line as follows: • light off—Button is not configured. • green steady—Line is configured correctly, registered successfully, and is in idle state. • red steady—Line is in use and has an active call on it or has one parked call. • amber steady/blinking—A configuration error occurred when this feature was being set up.

3	Page buttons—2 buttons. The button for page 1 is labeled as **1** and the button for page 2 is labeled as **2**. The lights in each button indicate the state of the page as follows:
	• green steady—Page is in view.
	• light off—Page is not in view.
	• amber steady—Page is not in view but has one or more alerting calls on the page.

Key Expansion Module Power Information

The phone uses an RJ9 jack to connect to the key expansion module. The key expansion module requires the phone to use either Power over Ethernet (PoE) or the Cisco IP Phone 6800 Power Adapter. The key expansion module draws 9V DC, 5W from the phone.

Table 14: Power-Supply Compatibility Table

Configuration	802.3af Power over Ethernet (PoE)	802.3at PoE	Cisco IP Phone 6800 Power Adapter
6851 with 1 expansion module	Yes	Yes	Yes

Install a Key Expansion Module

Your new key expansion module comes with a short cable and a new footstand to hold the phone and key expansion module together.

Procedure

Step 1 If the phone is powered on, unplug the LAN cable and power adapter (if used).

Step 2 Remove the footstand from the phone.

Step 3 Position the phone so that the front of the phone faces down.

Step 4 Place the key expansion module with the front facing down and to the left of the phone.

Step 5 Use the short cable to connect the RJ9 ports on the phone and key expansion module.
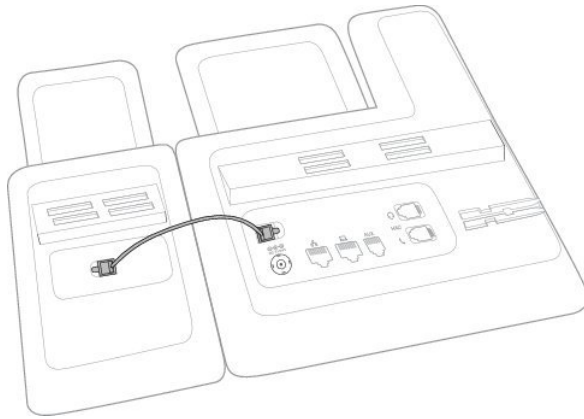
Step 6 Align the new footstand into the slots in the phone and into the slots in the key expansion module. Press the footstand firmly in place.

This step ensures that the phone and key expansion module remain connected at all times.
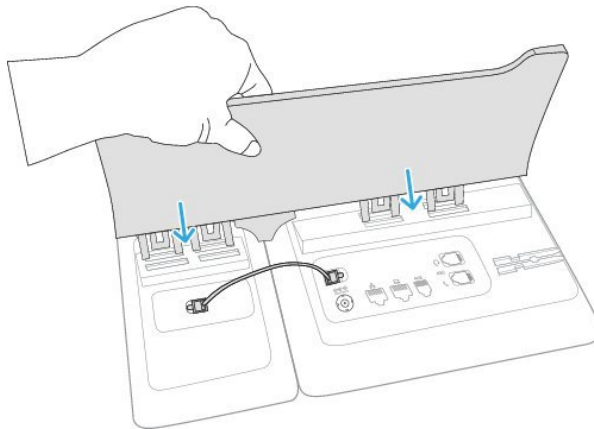
Step 7 Plug the LAN cable into the phone and into the LAN port.
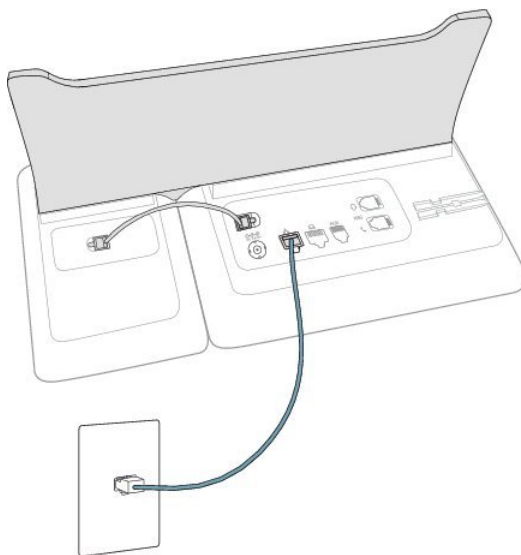
Step 8 If used, plug in the power adapter.
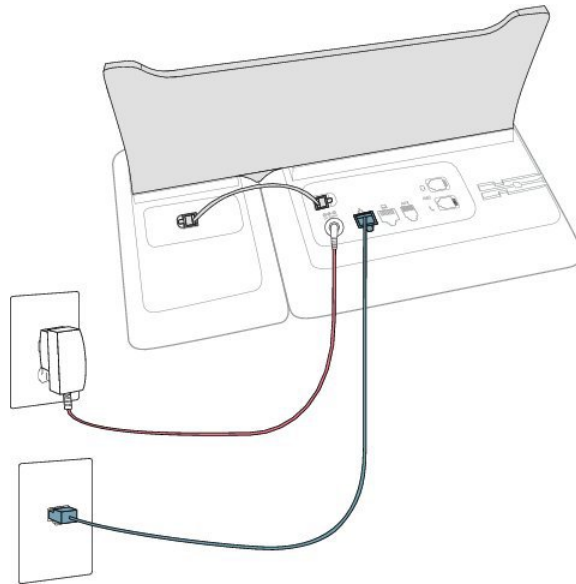
Step 9 Stand the phone upright and ensure that the stand is not on top of the phone cables.

Configure the Key Expansion Module from the Phone Web Page

You can set up your 6800 Key Expansion Module from the phone web page.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Att Console**.

Step 2 From the **Number of Units** list, select **1** as the number of supported key expansion modules.

Step 3 Click **Submit All Changes**.

Configure a Speed Dial on a Key Expansion Module

You can configure speed dial on a key expansion module line. The user can then press the line key to call a frequently dialed number.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Att Console**.
Step 2	Select a key expansion module line key on which to enable the speed dial.
Step 3	Enter a string in this format:

```
fnc=sd;ext=9999@$PROXY;vid=n;nme=xxxx
```

where:

- fnc= sd means function=speed dial

- ext= 9999 is the phone that the line key calls. Replace 9999 with numbers.

- vid=n is the line index of the phone.

- nme= XXXX is the name displayed on the phone for the speed-dial line key. Replace XXXX with a name.

You can also configure an XML service on key expansion module key. Enter the string in this format:

```
fnc=xml;url=http://xml.service.url;nme=name
```

Step 4	Click **Submit All Changes**.

Configure Call Park on a Key Expansion Module line

You can enable call park on a key expansion module line. The user can then use the line to park a call. and then retrieve the call either from own phone or another phone.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1	Select **Voice** > **Att Console**.
Step 2	Select a key expansion module line key on which to enable the call park.
Step 3	Enter a string in this format:

```
fnc=prk;ext=9999@$PROXY;vid=n;nme=xxxx
```

where:

- fnc= prk means function=call park
- ext= 9999 is the phone that the line key calls. Replace 9999 with numbers.
- vid=n is the line index of the phone.

- nme= XXXX is the name displayed on the phone for the call park line key. Replace XXXX with a name.

You can also configure an XML service on key expansion module key. Enter the string in this format:

```
fnc=xml;url=http://xml.service.url;nme=name
```

Configure the Busy Lamp Field on a Key Expansion Module

You can configure the busy lamp field on a key expansion module line so that the user can monitor a coworker's availability to receive a call.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Att Console**.

Step 2   Select a key expansion module line key.

Step 3   Enter a string in this format:

fnc=blf;sub=xxxx@$PROXY;usr=8888@$PROXY.

Where:

- fnc= blf means function=busy lamp field
- sub= the URI to which the SUBSCRIBE message is sent. This name must be identical to the name defined in the List URI: sip: parameter. xxxx is the name that is defined in List URI: sip: parameter. Replace xxxx with the exact defined name. $PROXY is the server. Replace $PROXY with the server address or name.
- usr= the BroadSoft user being monitored by BLF with 8888 as the phone being monitored. Replace 8888 with the exact number of the monitored phone. $PROXY is the server. Replace $PROXY with the server address or name.

Step 4   (Optional) To enable the busy lamp field to work with both speed dial and call pickup enter a string in the following format:

```
fnc=blf+sd+cp;sub=xxxx@$PROXY;usr=yyyy@$PROXY.
```

Where:

sd= speed dial

cp= call pickup

You can also enable busy lamp field only with call pickup or speed dial. Enter the string in the following format:

```
fnc=blf+cp;sub=xxxx@$PROXY;usr=yyyy@$PROXY
```

```
fnc=blf+sd;sub=xxxx@$PROXY;usr=yyyy@$PROXY
```

Step 5   Click **Submit All Changes**.

Access Key Expansion Module Setup

After you install a key expansion module on the phone and configure it on the phone web page, the phone automatically recognizes the key expansion module.

When the phone automatically recognizes the key expansion module, you can then choose the **Details** softkey for additional information about the selected key expansion module.

Procedure

Step 1 On the phone, press **Applications** ⚙.

Step 2 Press **Status** > **Accessories**.

Installed and configured key expansion module display in the list of accessories.

Adjust the Contrast of Key Expansion Module LCD from the Phone Web Page

You can adust the LCD contrast of the Key Expansion Module from the phone web page and the value gets updated on the phone. You can modify this value from the phone.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Att Console**.

Step 2 In the **General** section, enter a value in the **Attendant Console LCD Contrast** field.

Valid values: 4 to 12

Step 3 Click **Submit All Changes**.

Change the Display Mode of Key Expansion Module from the Phone Web Page

You can modify the busy lamp field (BLF) label of Key Expansion Module line. The labels can be displayed by name, extension, or both. The change updates the phone. You can also modify the display mode from the phone.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Att Console**.
Step 2	In the **General** section, select the type of display mode from the **BLF Label Display Mode** field.
Step 3	Click **Submit All Changes**.

Connect the Footstand

If your phone is placed on a table or desk, connect the footstand to the back of the phone. The footstand sets the phone at fixed angle and you cannot change the angle.

Procedure

Align the connectors with the slots and press firmly until the connectors snap into the slots.

Headsets

We perform internal testing of third-party headsets for use with Cisco IP Phones. But we do not certify or support products from headset or handset vendors.

Headsets connect to your phone using the headset port or the auxiliary (AUX) port. Only the Cisco IP Phone 6851 Multiplatform Phones and the Cisco IP Phone 6861 Multiplatform Phones have an AUX port. Depending upon your headset model, you have to adjust your phone's audio settings for the best audio experience, including the headset sidetone setting.

Headset sidetone is the feedback you hear through a headset when you speak.

After you apply a new sidetone setting, wait one minute and then reboot the phone for the setting to be stored in flash.

The phone reduces some background noise that a headset microphone detects. You can use a noise canceling headset to further reduce the background noise and improve the overall audio quality.

We recommend the use of good quality external devices; for example, headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of headsets and their proximity to other devices, such as mobile (cell) phones and two-way radios, some audio noise or echo may still occur. Either the remote party or both the remote party and the Cisco IP Phone user may hear an audible hum or buzz. A range of outside sources can cause humming or buzzing sounds; for example, electric lights, electric motors, or large PC monitors.

Note Sometimes, use of a local power cube or power injector may reduce or eliminate hum.

Environmental and hardware inconsistencies in the locations where Cisco IP Phones are deployed mean that no single headset solution is optimal for all environments.

We recommend that customers test headsets in the intended environment to determine performance before making a purchasing decision to deploy on a large scale.

You can use only one headset at a time. The most-recently connected headset is the active headset.

Audio Quality

Beyond physical, mechanical, and technical performance, the audio portion of a headset must sound good to the user and to the party on the far end. Sound quality is subjective, and we cannot guarantee the performance of any headsets. However, various headsets from leading headset manufacturers are reported to perform well with Cisco IP Phones.

For additional information, see https://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html

Analog Headsets

The phones support analog headsets that you plug into the headset port of the phone. The phone automatically detects the headset.

Wall Mount Kit

Wall Mount Kit Components

You can mount the phone to a wall.

- The Cisco IP Phone 6821 Multiplatform Phones use a commercially-available wall plate.

- The Cisco IP Phone 6841, 6851, and 6861 Multiplatform Phones use the Cisco IP Phone 6800 Series Multiplatform Phones Wall Mount Kit.

Figure 5: Cisco IP Phone 6800 Series Multiplatform Phones Wall Mount Kit
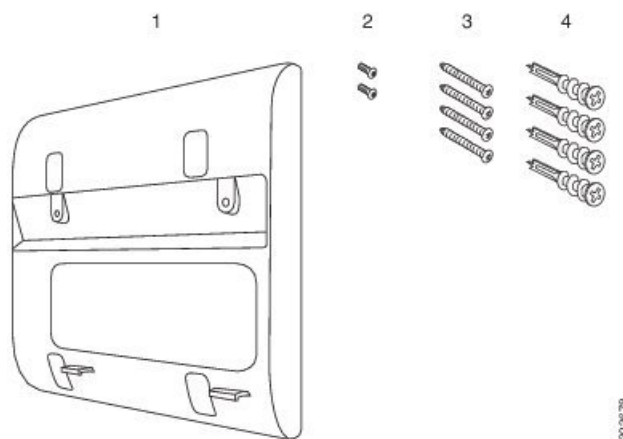
The kit is made up of these components:

- Wall bracket

- Two M3-7L screws

- Four M4-25L screws

• Four drywall anchors

Install the Cisco IP Phone 6821 Multiplatform Phones on a Wall

Before you begin

You can mount the Cisco IP Phone 6821 Multiplatform Phones on the wall with a standard telephone wall plate with an opening for an RJ-45 connector. Cisco recommends that you use Leviton Wall Mount plate (Leviton type number: 4108W-0SP) to wall mount the phone.

The following figure shows a list of items required to mount the phone.

Figure 6: Leviton Wall Mount Plate
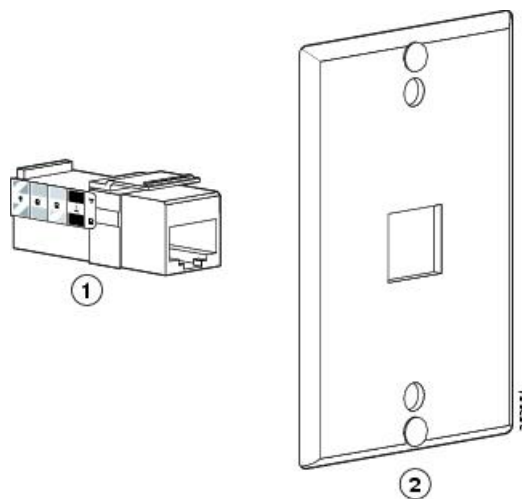
1	RJ45 Connector	2	Leviton Wall Mount Plate

Procedure

Step 1   If you need to use the power adapter, ensure that the adapter will reach from the phone to the electrical outlet.

Step 2   Use the manufacturer's instructions to install the wall mount plate and connect the wall mount plate RJ45 connector to the LAN.

Step 3   Plug the LAN cable (RJ45 connector) into the phone jack at the base of the phone as shown in the following figure.

Figure 7: RJ45 Connector in the Phone Jack
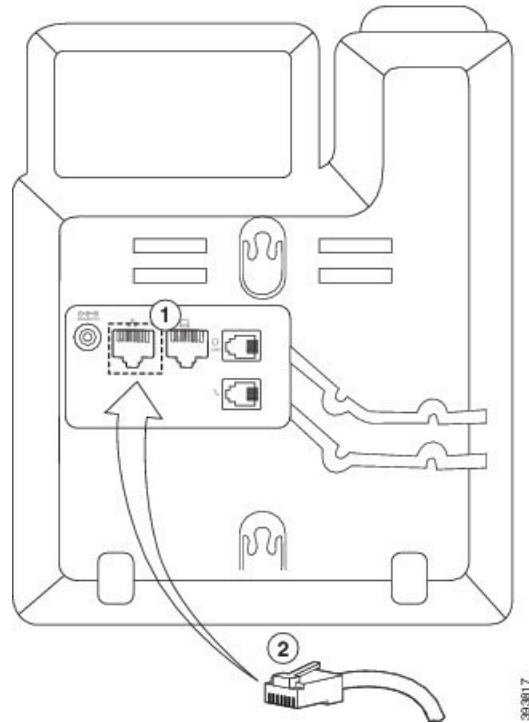
1	Network Port on the Phone
2	RJ45 Connector

Step 4 Plug the RJ45 connector into the wall mount phone jack as shown in the following figure.

Figure 8: RJ45 Connector in the Wall Mount Jack
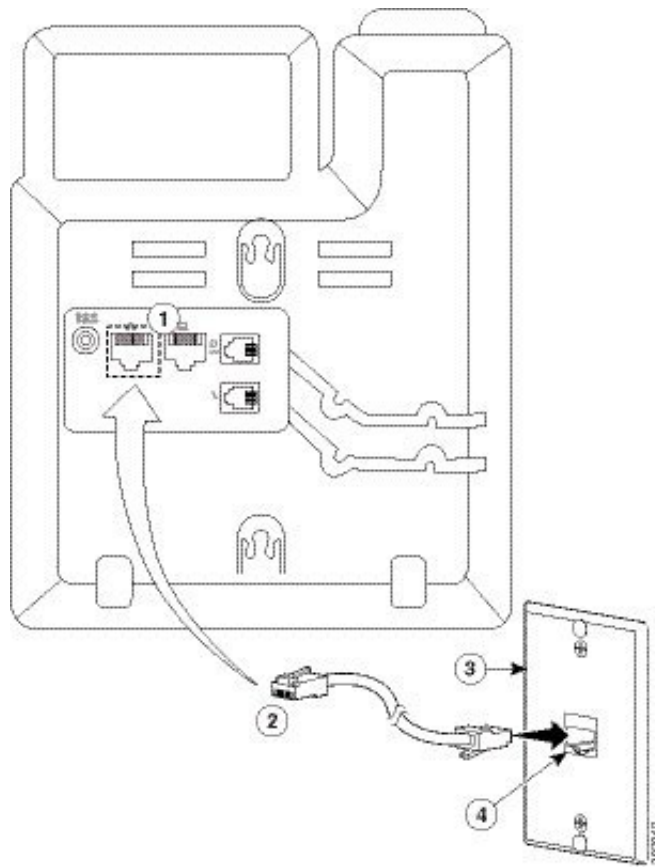
1	Network Port on the Phone	3	Wall Mount Plate
2	RJ45 Connector	4	Network Port on the Wall Mount Plate

Step 5   Press the LAN cable into one of the cable channels.

Step 6   (Optional) If you do not use PoE, plug the power adapter into the phone and the electrical outlet, and press the power cable into the other cable channel.

Step 7   Slip the mounting holes on the phone over the wall mount pins as shown in the following figure.

Figure 9: Mounting Holes
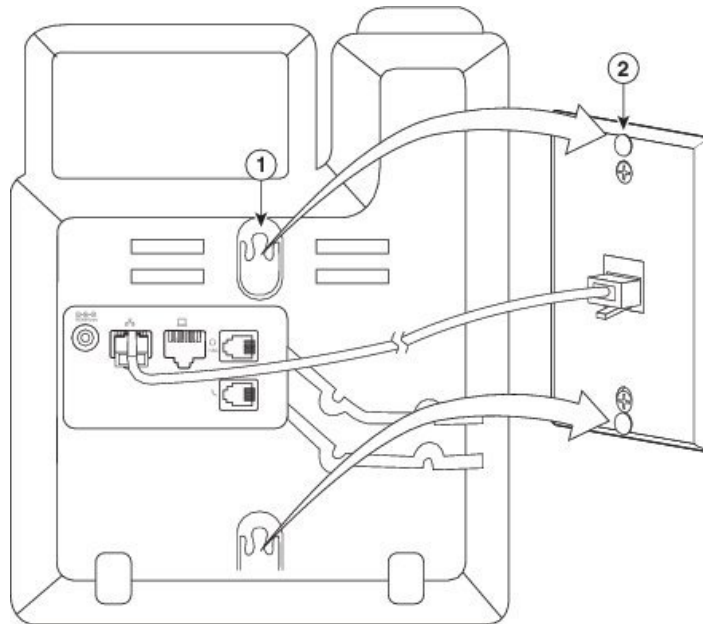
1	Mounting Hole on the Phone
2	Wall Mount Pin on the Wall Mount Plate

Step 8   Firmly slide the phone down into place as shown in the following image:

Figure 10: Sliding the IP Phone
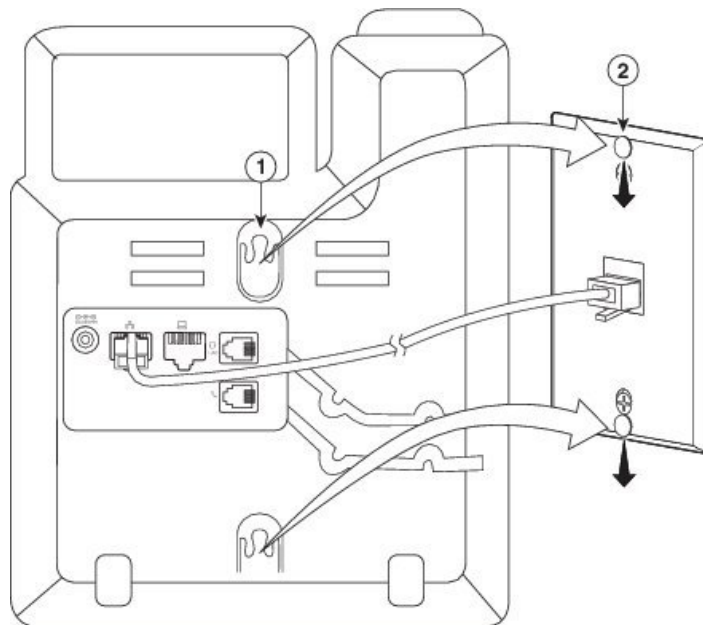
Install a Cisco IP Phone 6841, 6851, or 6861 with the Wall Mount Kit

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

Before you begin

You need these tools:

- #2 Phillips-head screwdriver
- Level
- Pencil

You must also install an Ethernet jack for the phone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular phone jack.

If the phone is a Cisco IP Phone 6841 or 6861, you need a power outlet close to the phone. If the phone is a Cisco IP Phone 6851, you require either a power outlet close to the phone or you need the LAN to provide Power over Ethernet (PoE).

Procedure

Step 1	Hold the bracket against the wall, with the notches at the bottom.
Step 2	Use the level to ensure that the bracket is level.
Step 3	Use a pencil to mark the screw holes.
Step 4	Center the anchor over the pencil mark and use a #2 Phillips-head screwdriver to press the anchor into the wall. Screw the anchor clockwise into the wall until it is seated flush.
Step 5	Use the M4-25L screws provided and the #2 Phillips-head screwdriver to attach the bracket to the wall through the anchors.

You should tighten the screws so that the bracket is held to the wall, but can be slipped off.

The following graphic shows steps 1 to 5.
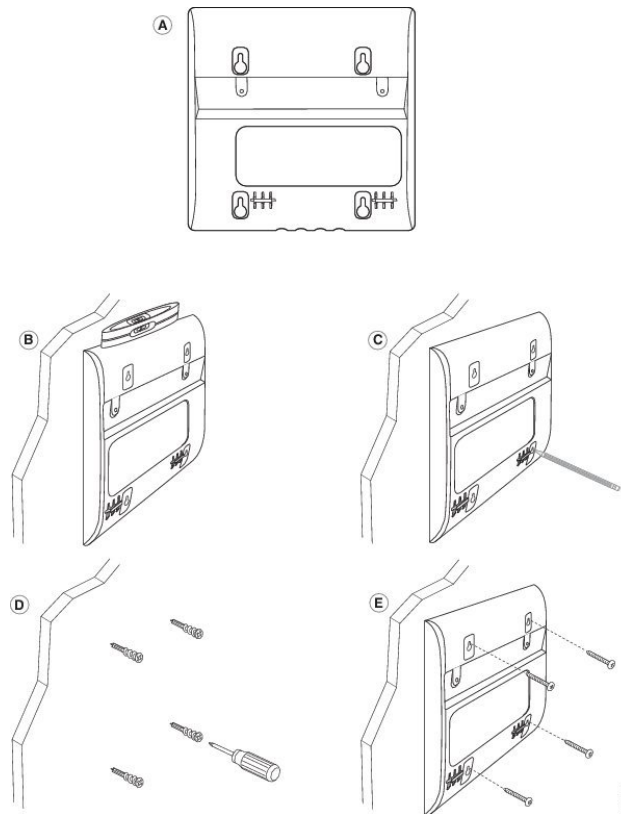
Step 6   If the phone is in use, unplug the LAN and power cables from the phone.

The handset cable needs to be connected to the phone and seated in the cable channel.

Step 7   Remove the wall bracket from the wall and place it on the back of the phone so that the bracket fits in the indentations in the back of the phone.
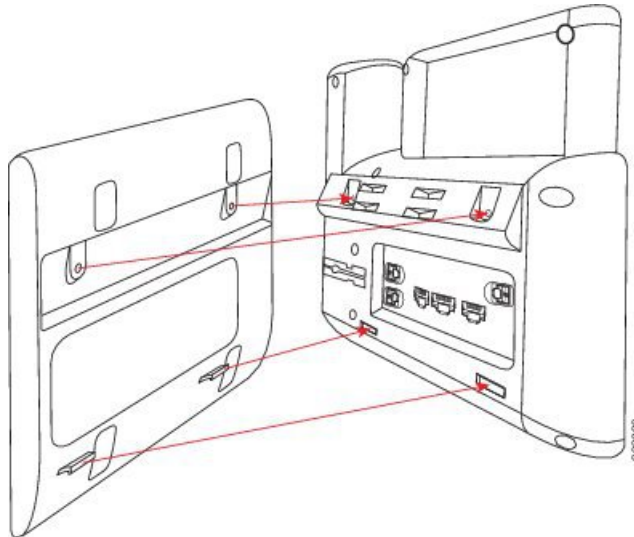
Make sure that the handset cable is between the phone and the bracket, as shown below.
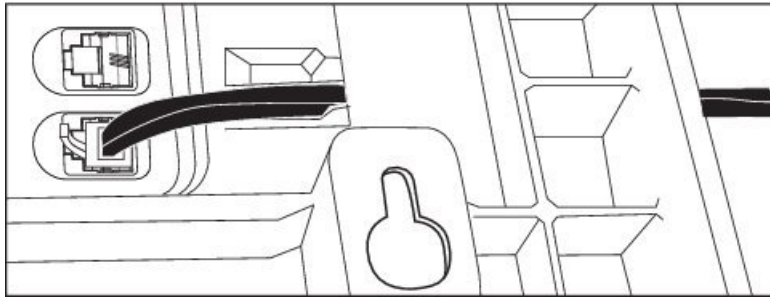
Step 8   Attach the bracket to the phone with the M3-7L screws provided.

Step 9   If you use the power adapter, plug the adapter into the phone and thread the cable through the closest notch in the bottom of the bracket.
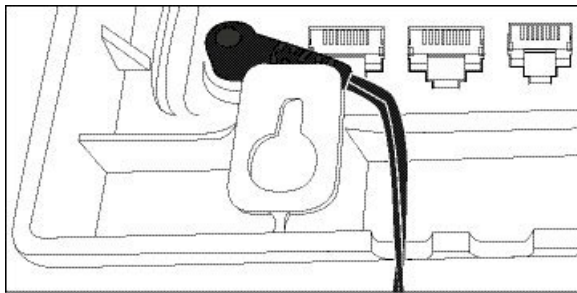
Step 10   Plug the LAN cable into the phone and thread the cable through a notch in the bottom of the bracket.
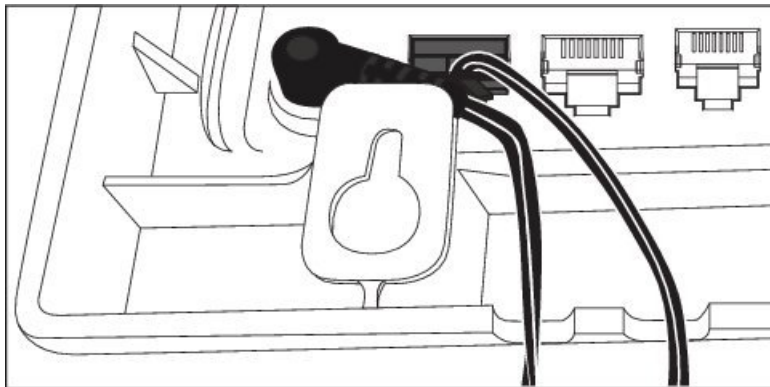
Step 11   Place the bracket over the wall screws and pull the phone down until it is seated securely. You may need to remove the phone and loosen or tighten the wall screws to make the phone and bracket stable.
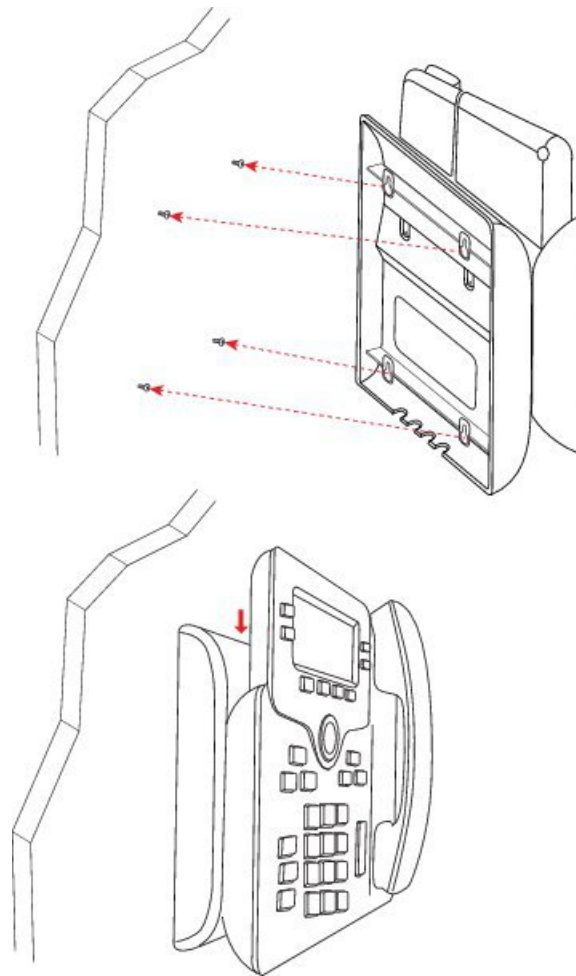
Step 12   Plug the LAN cable into the LAN jack.

Step 13   If you use external power, plug the power adapter into the electrical outlet.

What to do next

You can adjust the phone so that the handset doesn't fall out of the handset rest. See Adjust the Handset Rest, on page 117.

Adjust the Handset Rest

If your phone is wall-mounted or if the handset slips out of the cradle too easily, you may need to adjust the handset rest to ensure that the receiver does not slip out of the cradle.

Figure 11: Adjust the Handset Rest
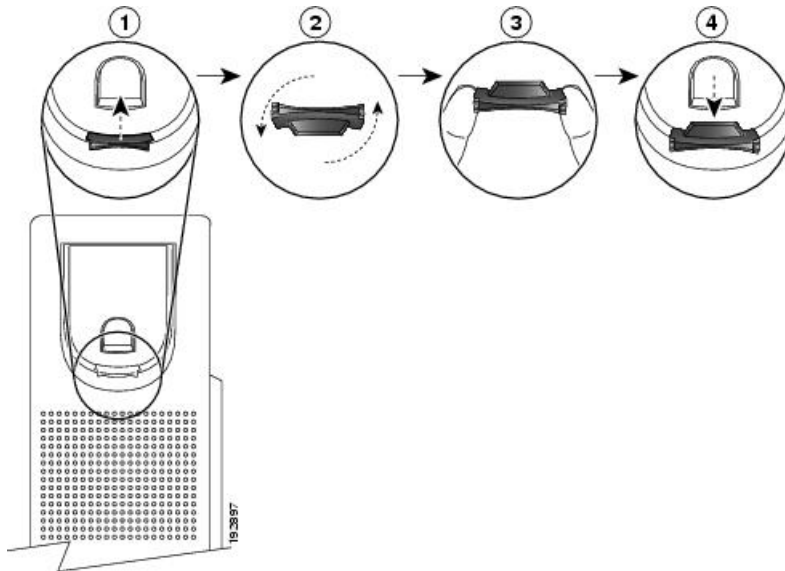
Procedure

Step 1   Remove the handset from the cradle and pull the plastic tab from the handset rest.

Step 2   Rotate the tab 180 degrees.

Step 3   Hold the tab between two fingers, with the corner notches facing you.

Step 4   Line up the tab with the slot in the cradle and press the tab evenly into the slot. An extension protrudes from the top of the rotated tab.

Step 5   Return the handset to the handset rest.

PART IV

Phone Administration

Cisco IP Phone Security

Security Features

Security features ensure that calls are secure and authenticated.

Domain and Internet Setting

Configure Restricted Access Domains

If you enter domains, the Cisco IP Phone responds only to SIP messages only from the identified servers.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **System**.

Step 2   In the **System Configuration** section, in the **Restricted Access Domains** field, enter fully qualified domain names (FQDNs) for each SIP server that you want the phone to respond to. Separate FQDNs with commas.

Example:

```
voiceip.com, voiceip1.com
```

Step 3   Click **Submit All Changes**.

Configure the Internet Connection Type

You can set the connection type to one of the following:

• Dynamic Host Configuration Protocol (DHCP)—Enables the phone to receive an IP address from the network DHCP server. The Cisco IP phone typically operates in a network where a DHCP server assigns

IP addresses to devices. Because IP addresses are a limited resource, the DHCP server periodically renews the device lease on the IP address. If a phone loses the IP address for any reason, or if some other device on the network is assigned the same IP address, the communication between the SIP proxy and the phone is either severed or degraded. Whenever an expected SIP response is not received within a programmable amount of time after the corresponding SIP command is sent, the DHCP Timeout on Renewal parameter causes the device to request a renewal of its IP address. If the DHCP server returns the IP address that it originally assigned to the phone, the DHCP assignment is presumed to be operating correctly. Otherwise, the phone resets to try to fix the issue.

- Static IP—A static IP address for the phone.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **System**.

Step 2   In the **IPv4 Settings** section, use the **Connection Type** drop-down list box to choose the connection type:

- Dynamic Host Configuration Protocol (DHCP)

- Static IP

Step 3   In the **IPv6 Settings** section, use the **Connection Type** drop-down list box to choose the connection type:

- Dynamic Host Configuration Protocol (DHCP)

- Static IP

Step 4   If you choose Static IP, configure these settings in the **Static IP Settings** section:

- **Static IP**—Static IP address of the phone

- **NetMask**—Netmask of the phone

- **Gateway**—Gateway IP address

Step 5   Click **Submit All Changes**.

DHCP Option Support

The following table lists the DHCP options that are supported on the Cisco IP Phone.

Network Standard	Description
DHCP option 1	Subnet mask
DHCP option 2	Time offset
DHCP option 3	Router

Network Standard	Description
DHCP option 6	Domain name server
DHCP option 15	Domain name
DHCP option 41	IP address lease time
DHCP option 42	NTP server
DHCP option 43	Vendor-specific information Can be used for TR.69 Auto Configurations Server (ACS) discovery.
DHCP option 56	NTP server NTP server configuration with IPv6
DHCP option 60	Vendor class identifier
DHCP option 66	TFTP server name
DHCP option 125	Vendor-identifying vendor-specific information Can be used for TR.69 Auto Configurations Server (ACS) discovery.
DHCP option 150	TFTP server
DHCP option 159	Provisioning server IP
DHCP option 160	Provisioning URL

Configure the Challenge for the SIP INVITE Messages

The phone can challenge the SIP INVITE (initial) message in a session. The challenge restricts the SIP servers that are permitted to interact with the devices on a service provider network. This practice significantly increases the security of the VoIP network through prevention of malicious attacks against the device.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **SIP Settings** section, choose **Yes** from the **Auth INVITE** drop-down list box.

Step 3 Click **Submit All Changes**.

Transport Layer Security

Transport Layer Security (TLS) is a standard protocol for securing and authenticating communications over the Internet. SIP over TLS encrypts the SIP messages between the service provider SIP proxy and the end user. SIP over TLS encrypts only the signaling messages, not the media.

TLS has two layers:

- TLS Record Protocol—Layered on a reliable transport protocol, such as SIP or TCH, this layer ensures that the connection is private through use of symmetric data encryption and it ensures that the connection is reliable.

- TLS Handshake Protocol—Authenticates the server and client, and negotiates the encryption algorithm and cryptographic keys before the application protocol transmits or receives data.

The Cisco IP Phone uses UDP as the standard for SIP transport, but the phone also supports SIP over TLS for added security.

Configure SIP Over TLS Signaling Encryption

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2   In the **SIP Settings** section, select **TLS** from the **SIP Transport** drop-down list box.

Step 3   Click **Submit All Changes**.

Configure LDAP over TLS

You can configure LDAP over TLS (LDAPS) to enable secure data transmission between the server and a specific phone.

⚠️

Attention   Cisco recommends leaving the authentication method to the default value of **None**. Next to the server field is an authentication field that uses the values **None**, **Simple**, or **DIGEST-MD5**. There is no **TLS** value for authentication. The software determines the authentication method from the ldaps protocol in the server string.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **LDAP** section, enter a server address in the **Server** field.

For example, enter `ldaps://<ldaps_server>[:port]` .

where:

- `ldaps://`= The server string starts with `ldaps://` before you enter the IP address or domain name

- `ldaps_server` = IP address or domain name

- `port` = Port number. Default: 636

Step 3   Click **Submit All Changes**.

Cisco Product Security Overview

This product contains cryptographic features and is subject to U.S. and local country laws that govern import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations can be found at https://www.bis.doc.gov/policiesandregulations/ear/index.htm.

Cisco IP Phone Customization

Phone Information and Display Settings

The phone web user interface allows you to customize settings such as the phone name, background picture, logo, and screen saver.

Configure the Phone Name

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 Under **General**, enter the phone name in the **Station Display Name** field.

This name displays on the phone LCD in the top left corner.

Step 3 Click **Submit All Changes**.

Change Wallpaper from the Phone Page

Your administrator can allow you to change the default wallpaper on your phone to one of the wallpapers available.

Procedure

Step 1   On the phone web page, select **User Login** > **Voice** > **User**.

Step 2   In the **Phone Background** field of the **Screen** section, select any of the options as a phone wallpaper.

- **Default**: Phone does not have any wallpaper. If no wallpaper is added to the phone screen, the phone screen displays monochrome wallpaper.

- **Logo**: In the phone web page you can select **Logo** as your phone background option. The logo that you add in the **Logo URL** is used as the wallpaper.

    Caution   Do not exceed a maximum length of 255 characters for the **Logo URL** or **Picture Download URL**.

    The logo display area is the center of the phone screen. The logo display area size of the phone is 128x128 pixels. If original logo size does not fit display area, the logo scales to fit the display area.

Step 3   Click **Submit All Changes**.

Add a Logo as the Boot Display

If you want your user to see a logo icon when the phone restarts, enable this feature from the phone web page.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **User**.

Step 2   In the **Screen** section, select **Logo** from the **Boot Display** field. In the **Logo URL** field, enter a URL or path for the location where the logo image is saved.

You can also download a picture and add it as a boot display: select **Download Picture** from the **Boot Display** field. In the **Picture Download URL** field, enter a URL or path for the location where the picture is saved.

The logo must be a .jpg or a .png file. The phone has a fixed display area. So, if the original logo size doesn't fit into the display area, you need to scale it to fit the screen. The logo display area is at the mid-center of the phone screen. The display area size of the Cisco IP Phone 6841 and 6851 Multiplatform Phones is 64x64. The display area size of the Cisco IP Phone 6821 Multiplatform Phones is 48x48.

Step 3   Click **Submit All Changes**.

Adjust Backlight Timer from Configuration Utility

You can save energy by disabling the backlight on each phone at a preset time. The phone's desktop remains visible, even with the backlight off.

User can select **User Login** > **Advanced** > **Voice** > **User** and can adjust the backlight timer.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **User**.

Step 2 Under Screen, select a setting for the **Back Light Timer** parameter.

Step 3 In the **LCD Contrast** field, enter a number for the desired contrast.

Configure the Number of Call Appearances Per Line

Phones that support multiple call appearances on a line can be configured to specify the number of calls to allow on the line.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 In the **Miscellaneous Line Key Settings** section, use the **Call Appearances Per Line** drop-down list box to specify the number of calls per line to allow.

Step 3 Click **Submit All Changes**.

Reverse Name Lookup for Incoming and Outgoing Calls

Reverse name lookup searches for the name of a number in an incoming, outgoing, conference, or transfer call. The reverse name lookup acts when the phone cannot find a name using the service provider directory, Call History, or your contacts. Reverse name lookup needs a valid LDAP Directory or XML Directory configuration.

The reverse name lookup searches the phone's external directories. When a search succeeds, the name is placed in the call session and in the call history. For simultaneous, multiple phone calls, reverse name lookup searches for a name to match the first call number. When the second call connects or is placed on hold, reverse name lookup searches for a name to match the second call.

Reverse name lookup is enabled by default.

Reverse name lookup searches the directories in the following order:

1. Phone contacts

2. Call History

3. LDAP Directory

4. XML Directory

> **Note** The phone searches the XML directory using this format: `directory_url?n=incoming_call_number`.
>
> Example: For a multiplatform phone using a third-party service, the phone number (1234) search query has this format, `http://your-service.com/dir.xml?n=1234`.

Enable and Disable Reverse Name Lookup

Before you begin

- Configure one of these directories before you can enable or disable the reverse name lookup:

    - LDAP Corporate Directory

    - XML Directory

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 In the **Supplementary Services** area, set the **Reverse Phone Lookup Serv** to:

- **Yes**–Enable the reverse name lookup feature.
- **No**–Disable the reverse name lookup feature.

Step 3 Click **Submit All Changes**.

Step 4 Alternative method is to use the `config.xml` file to provision the reverse name lookup feature.

`<Reverse_Phone_Lookup_Serv ua="na">Yes</Reverse_Phone_Lookup_Serv>`

Call Features Configuration

Enable Call Transfer

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   Under **Supplementary Services**, choose **Yes** for each of the transfer services that you want to enable:

- **Attn Transfer Serv**—Attended call transfer service. The user answers the call before transferring it.

- **Blind Transfer Serv**—Blind call transfer service. The user transfers the call without speaking to the caller.

Step 3   To disable a transfer service, set the field to **No**.

Step 4   Click **Submit All Changes**.

Call Forward

To enable call forwarding, you can enable the feature in two places: on the Voice tab and the User tab of the phone web page.

Enable Call Forwarding on Voice Tab

Perform this task if you want to enable call forward for a user.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   Under **Supplementary Services**, choose **Yes** for each of the call forwarding services that you want to enable:

- **Cfwd All Serv**—Forwards all calls.

- **Cfwd Busy Serv**—Forwards calls only if the line is busy.

- **Cfwd No Ans Serv**—Forwards calls only if the line is not answered.

Step 3   Click **Submit All Changes**.

Related Topics

Enable Call Forwarding on User Tab

Perform the following task if you want to give a user the ability to modify the call forward settings from the Configuration Utility page.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **User**.

Step 2   Under **Call Forward**, choose **Yes** for CFWD Setting.

Step 3   Click **Submit All Changes**.

Enable Conferencing

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   Under **Supplementary Services**, choose **Yes** in the **Conference Serv** drop-down list box.

Step 3   Click **Submit All Changes**.

Configure Missed Call Indication with the Configuration Utility

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **User**.
	The user can select **User Login** > **Voice** > **User**.
Step 2	In the **Supplementary Services** section, choose **Voicemail, Missed Call** in the **Handset LED Alert** field.
Step 3	Click **Submit All Changes**.

Enable Do Not Disturb

You can allow persons to turn the Do not disturb feature on or off. The caller receives a message that the person is unavailable. A person can press the **Ignore** softkey on the phone to divert an incoming call to another destination.

If the feature is enabled for the phone, users can turn the feature on or off with the DND softkey.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Choose **Voice** > **User**.
Step 2	In the **Supplementary Services** area, select **Yes** in the **DND Setting** drop-down list.
Step 3	Click **Submit All Changes**.

When you select a line (multiline phone), a Do Not Disturb banner displays at the top of the phone screen.

What to do next

Change another setting to ensure that multiline phones correctly display the Do not disturb (currently, a steady, green color) status for each selected or unselected line. See DND and Call Forwarding Status Sync, on page 192.

Users can enable or turn off the DND feature for each phone line if you configure star codes for DND. See Configure Star Codes for DND, on page 133.

Related Topics

Configure Star Codes for DND

You can configure star codes that a user dials to turn on or off the do not disturb (DND) feature on a phone.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Regional**.

Step 2   In the **Vertical Service Activation Codes** area, enter *78 in the **DND Act Code** field.

Step 3   In the **Vertical Service Activation Codes** area, enter *79 in the **DND Deact Code** field.

Step 4   Click **Submit All Changes**.

Shared Lines

A shared line is a directory number that appears on more than one phone. You can create a shared line by assigning the same directory number to different phones.

Incoming calls display on all phones that share a line, and anyone can answer the call. Only one call remains active at a time on a phone.

Call information displays on all phones that are sharing a line. If somebody turns on the privacy feature, you do not see the outbound calls made from the phone. However, you see inbound calls to the shared line.

All phones with a shared line ring when a call is made to the line. If you place the shared call on hold, anyone can resume the call by pressing the corresponding line key from a phone that shares the line. You can also press the **Select** button if the Resume icon is displayed.

The following shared line features are supported:

- Line Seizure

- Public Hold

- Private Hold

- Silent Barge (only through enabled programmable softkey)

The following features are supported as for a private line

- Transfer

- Conference

- Call Park / Call Retrieve

- Call Pickup

- Do Not Disturb

- Call Forward

You can configure each phone independently. Account information is usually the same for all IP phones, but settings such as the dial plan or preferred codec information can vary.

Configure a Shared Line

You can create a shared line by assigning the same directory number to different phones on the phone web page.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Ext(n)**, where **(n)** is the number of an extension to share.
Step 2	In the **General** section, set **Line Enable** to **Yes**.
Step 3	In the **Share Line Appearance** section, set **Share Ext** to **Yes**.
	If you set set **Share Ext** to **No**, this extension is private and doesn't share calls, regardless of the **Share Call Appearance** setting on the **Phone** tab. If you set this extension shared, calls follow the **Share Call Appearance** setting on the **Phone** tab.
Step 4	In the **Shared User ID field**, enter the user ID of the phone with the extension that is being shared.
Step 5	In the **Subscription Expires** field, enter the number of seconds before the SIP subscription expires. The default is 3600 seconds.
	Until the subscription expires, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension.
Step 6	In the **Restrict MWI** field, set the message waiting indicator:
	• **Yes**—Lights only for messages on private lines (SIP).
	• **No**—Lights for all messages.
Step 7	In the **Proxy and Registration** section, enter the IP address of the proxy server in the **Proxy** field.
Step 8	In the **Subscriber Information** section, enter the **Display Name** and **User ID** (extension number) for the shared extension.
Step 9	In the **Miscellaneous Line Key Settings** section, set **SCA Barge-In Enable** to:
	• **Yes**—Allows users to take over the call on a shared line.
	• **No**—Prevents users from taking over the call on a shared line.
Step 10	Click **Submit All Changes.**

Configure Voice Mail

You can configure the internal or external phone number or URL for the voice mail system. If you are using an external voice mail service, the number must include any digits required to dial out and any required area code

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 Under **General**, enter the **Voice Mail Number**.

Step 3 Click **Submit All Changes**. The phone reboots.

Configure Voice Mail for each Extension

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Ext(n)**, where **(n)** is the number of an extension.

Step 2 In the **Call Feature Settings** section, enter the **Voice Mail Server**.

Step 3 (Optional) Enter the **Voice Mail Subscribe Interval**; the expiration time in seconds, of a subscription to a voice mail server.

Step 4 Click **Submit All Changes**.

The phone reboots.

Configure the Message Waiting Indicator

You can configure the Message Waiting Indicator for separate extensions on the phone. The Message Waiting Indicator lights based on the presence of new voicemail messages in the mailbox.

You can enable the indicator at the top of your IP phone to light when voice mail is left, or display a seeing message waiting notification.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Ext(n)**, where **(n)** is the number of an extension.

Step 2 In the **Call Feature Settings** section, set the **Message Waiting** field to **Yes** to enable it.

Step 3   Click **Submit All Changes**.

Assign a Ringtone to an Extension

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Ext(n)**, where **(n)** is the number of an extension.

Step 2   Under **Call Feature Settings**, use the **Default Ring (n)** drop-down list box to specify one of the following:

- No Ring

- Choose one of the available 12 ringtones.

Step 3   Click **Submit All Changes**.

Configure the Audio Settings

The user can modify volume settings by pressing the volume control button on the phone, then pressing the **Save** softkey.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **User**.

Step 2   In the **Audio Volume** section, configure a volume level of 1 (quiet) through 10 (loudest):

- **Ringer Volume**—Sets the ringer volume.

- **Speaker Volume**—Sets the volume for the full-duplex speakerphone.

- **Headset Volume**—Sets the headset volume.

- **Handset Volume**—Sets the handset volume.

Only the Cisco IP Phone 6851 Multiplatform Phones support the Electronic Hookswitch feature.

Step 3   Click **Submit All Changes**.

Specify Audio Compliance Standard

You can specify a compliance standard for the audio tuning for the phone. When a compliance standard is specified, the acoustic parameters that conform to the specified standard are loaded to the phone.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Go to **Voice** > **User**.

Step 2   In the **Audio Compliance** section, choose an option from the **Compliant Standard** drop-down list as described in .

Step 3   Click **Submit All Changes**.

User Access Control

The Cisco IP Phone respects only the "ua" user access attribute. For a specific parameter, the "ua" attribute defines access by the user account to the administration web server. If the "ua" attribute is not specified, the phone applies the factory default user access for the corresponding parameter. This attribute does not affect access by the admin account.

Note   The value of the element attribute encloses within double quotes.

The "ua" attribute must have one of the following values:

- na – no access

- ro – read-only

- rw – read/write

Phone Web Server

The web server allows administrators and users to log in to the phone by using a phone web user interface. Administrators and users have different privileges and see different options for the phone based on their role.

Configure the Web Server from the Phone Screen Interface

Use this procedure to enable the phone web user interface from the phone screen.

Procedure

Step 1   Press **Applications** ⚙.

Step 2   Select **Network configuration** > **Web Server**.

Step 3   Select **On** to enable or **Off** to disable.

Step 4   Press **Set**.

Direct Action URL

If the Enable Direct Action URL setting is set to "Yes ", these Direct action URLs are accessible only for the admin. If Admin user is password protected, the client provides a login prompt before these are accessed. The Direct Action URLs are accessible via the phone web page via the path `/admin/<direct_action>`. The syntax is:

`http[s]://<ip_or_hostname>/admin/<direct_action>[?<url>]`

For example, `http://10.1.1.1/admin/resync?http://server_path/config.xml`

The following table provides a list of the different direct action URLs that are supported.

direct_action	Description
resync	Initiates a one-time resync of the config file specified by URL. The URL to resync is provided by appending ? followed by the URL. The URL specified here will not be saved anywhere in the phone settings. **Example** http://10.1.1.1/admin/resync?http://my_provision_server.com/cfg/device.cfg
upgrade	Initiates an upgrade of a phone to the specified load. The load is specified via the upgrade rule. the rule is specified by appending ? followed by URL path to the load. The upgrade rule specified is one time only and will not be saved in any property setting. **Example** http://10.1.1.1/admin/upgrade?http://my_upgrade_server.com/loads/sip88xx.11.0.0MP2.123.loads
updateca	Initiates a one-time install of the Custom Certificate Authority (Custom CA) specified by the URL. The URL to download is provided by appending ? followed by the URL. The URL specified here will not be saved anywhere in the phone settings. **Example** http://10.1.1.1/admin/updateca?http://my_cert_server.com/certs/myCompanyCA.pem

direct_action	Description
reboot	Initiates a reboot of the phone. Does not take any parameter with ? **Example** http://10.1.1.1/admin/reboot
cfg.xml	Downloads a snapshot of the phone configuration in XML format. The passwords are hidden for security. Most of the information here corresponds to the properties on the phone web page under **Voice** tab. **Example** http://10.1.1.1/admin/cfg.xml
status.xml	Downloads a snapshot of the phone status in XML format. Most of the information here corresponds to the **Status** tab in the phone web page. **Example** http://10.1.1.1/admin/status.xml
screendump.bmp	Downloads a screenshot of the phone LCD UI at the time when this action is initiated. **Example** http://10.1.1.1/admin/screendump.bmp
log.tar	Downloads a set of archived logs stored on the phone. **Example** http://10.1.1.1/admin/log.tar

Enable Access to Phone Web Interface

Before you begin

Access the phone administration web page. See .

Procedure

Step 1 Select **Voice** > **System**.

Step 2 Under the **System Configuration** section, choose **Yes** from the **Enable Web Server** drop-down list box.

Step 3 In the **Enable Protocol** drop-down list box, choose Http or Https.

Step 4 In the **Web Server Port** field, enter the port to access the web server. The default is port 80 for HTTP or port 443 for HTTPS.

Step 5 In the **Enable Web Admin Access** drop-down list box, you can enable or disable local access to the **Admin Login** of the phone web user interface. Defaults to **Yes** (enabled).

Step 6 In the **Admin Password** field, enter a password if you want the system administrator to log in to the phone web user interface with a password. The password prompt appears when an administrator clicks **Admin Login**. The minimum password length can be 4 characters or the maximum password length is 127 characters.

Note   The password can contain any character except the Space key.

Step 7   In the **User Password** field, enter a password if you want users to log in to the phone web user interface with a password. The password prompt appears when users click **User Login**. The minimum password length can be 4 characters or the maximum password length is 127 characters.

Note   The password can contain any character except the Space key.

Step 8   Click **Submit All Changes**.

XML Services

The phones provide support for XML services, such as an XML Directory Service or other XML applications. For XML services, only HTTP and HTTPS support is available.

The following Cisco XML objects are supported:

- CiscoIPPhoneMenu
- CiscoIPPhoneText
- CiscoIPPhoneInput
- CiscoIPPhoneDirectory
- CiscoIPPhoneIconMenu
- CiscoIPPhoneStatus
- CiscoIPPhoneExecute
- CiscoIPPhoneImage
- CiscoIPPhoneImageFile
- CiscoIPPhoneGraphicMenu
- CiscoIPPhoneFileMenu
- CiscoIPPhoneStatusFile
- CiscoIPPhoneResponse
- CiscoIPPhoneError
- CiscoIPPhoneGraphicFileMenu
- Init:CallHistory
- Key:Headset
- EditDial:n

The full list of supported URIs is contained in *Cisco Unified IP Phone Services Application Development Notes for Cisco Unified Communications Manager and Multiplatform Phones*, located here:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/products-programming-reference-guides-list.html

XML Directory Service

When an XML URL requires authentication, use the parameters **XML UserName** and **XML Password**.

The parameter **XML UserName** in XML URL is replaced by $XML UserName.

For example:

The parameter XML UserName is **cisco**. The XML Directory Service URL is
http://www.sipurash.compath?username=$XML_User_Name.

This results in the request URL: `http://www.sipurash.com/path?username=cisco.`

XML Applications

When authentication is required for CGI/Execute URL via Post from an external application (for example, a web application) to the phones, the parameter `CISCO XML EXE Auth Mode` is used in 3 different scenarios:

- Trusted—No authentication is performed (local user password is set or not). This is the default.

- Local Credential—Authentication is based on digest authentication using the local user password, if the local user password is set. If not set, then no authentication is performed.

- Remote Credential—Authentication is based on digest authentication using the remote username/password as set in the XML application on the web page (to access an XML application server).

Macro Variables

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2 to UIDn

- Display name—DISPLAYNAME1, DISPLAYNAME2 to DISPLAYNAMEn

- Auth ID—AUTHID1, AUTHID2 to AUTHIDn

- Proxy—PROXY1, PROXY2 to PROXYn

- MAC Address using lowercase hex digits—MA

- Product Name—PN

- Product Series Number—PSN

- Serial Number—SERIAL_NUMBER

The following table shows the list of macros supported on the phones:

Macro Name	Macro Expansion
$	The form $$ expands to a single $ character.
A through P	Replaced by general-purpose parameters GPP_A through GPP_P.

Macro Name	Macro Expansion
SA through SD	Replaced by special purpose parameters GPP_SA through GPP_SD. These parameters hold keys or passwords used in provisioning. **Note** $SA through $SD are recognized as arguments to the optional resync URL qualifier, --key.
MA	MAC address using lowercase hex digits (000e08aabbcc).
MAU	MAC address using uppercase hex digits (000E08AABBCC).
MAC	MAC address using lowercase hex digits with a colon to separate hex digit pairs (00:0e:08:aa:bb:cc).
PN	Product Name; for example, IP Phone 6841.
PSN	Product Series Number; for example, 6841.
SN	Serial Number string; for example, 88012BA01234.
CCERT	SSL Client Certificate status, installed or not installed.
IP	IP address of the phone within its local subnet; for example, 192.168.1.100.
EXTIP	External IP of the phone, as seen on the internet; for example, 66.43.16.52.
SWVER	Software version string; for example, 2.0.6(b). Use the software version string to compare against the current phone's firmware load, with one of the following methods: • **With quotes, "$SWVER"**–Variable acts as a string in firmware load name comparisons. For `"$SWVER" eq "sip8845_65.1-0129-18-0356dev.loads"`, the phone model number and load number are part of the comparison. • **Without quotes, $SWVER**–Variable is parsed to determine a build number, plus major, minor, and micro revision numbers. For example, when the `sip88xx.11-1-1MSR-1dev.loads` and `sip8845_65.11-1-1MSR-1dev.loads` firmware names are parsed, the result ignores the model number and load number. The result for both firmware names yields a major revision=1, minor revision=1, micro revision=1MSR, and build number=1.
HWVER	Hardware version string; for example, 1.88.1.
PRVST	Provisioning State (a numeric string): • -1 = explicit resync request • 0 = power-up resync • 1 = periodic resync • 2 = resync failed, retry attempted

Macro Name	Macro Expansion
UPGST	Upgrade State (a numeric string): • 1 = first upgrade attempt • 2 = upgrade failed, retry attempt
UPGERR	Result message (ERR) of previous upgrade attempt; for example, http_get failed.
PRVTMR	Seconds since last resync attempt.
UPGTMR	Seconds since last upgrade attempt.
REGTMR1	Seconds since Line 1 lost registration with SIP server.
REGTMR2	Seconds since Line 2 lost registration with SIP server.
UPGCOND	Legacy macro name.
SCHEME	File access scheme (TFTP, HTTP, or HTTPS, obtained after parsing resync or upgrade URL).
METH	Deprecated alias for SCHEME, do not use.
SERV	Request target server hostname.
SERVIP	Request target server IP address (following DNS lookup).
PORT	Request target UDP/TCP port.
PATH	Request target file path.
ERR	Result message of resync or upgrade attempt.
UIDn	The contents of the Line n UserID configuration parameter.
ISCUST	If unit is customized, value=1, otherwise 0. **Note** Customization status viewable on Web UI Info page.
INCOMINGNAME	Name associated with first connected, ringing, or inbound call.
REMOTENUMBER	Phone number of first connected, ringing, or inbound call. If there are multiple calls, the data associated with the first call found is provided.
DISPLAYNAMEn	The contents of the Line N Display Name configuration parameter.
AUTHIDn	The contents of the Line N auth ID configuration parameter.

Configure a Phone to Connect to an XML Application

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 Enter this information:

- XML Application Service Name—Name of the XML application. Displays on the user's phone as a menu item.

- XML Application Service URL—URL where the XML application is located.

If you configure an unused line button to connect to an XML application, the button connects to the URL configured above. If this is not what you want, you need to enter a different URL when you configure the line button.

Step 3 Click **Submit All Changes**.

Configure a Phone to Connect to an XML Directory Service

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 Enter this information:

- XML Directory Service Name—Name of the XML Directory. Displays on the user's phone as a directory choice.

- XML Directory Service URL—URL where the XML Directory is located.

Step 3 Click **Submit All Changes**.

C H A P T E R 10

Phone Features and Setup

Phone Features and Setup Overview

After you install Cisco IP Phones in your network, configure their network settings, and add them to Third-Party Call Control System, you must use the Third-Party Call Control System to configure telephony features, optionally modify phone templates, set up services, and assign users.

You can modify additional settings for the Cisco IP Phone from Third-Party Call Control Configuration Utility. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks.

Cisco IP Phone User Support

If you are a system administrator, you are likely the primary source of information for Cisco IP Phone users in your network or company. It is important to provide current and thorough information to end users.

To successfully use some of the features on the Cisco IP Phone (including Services and voice message system options), users must receive information from you or from your network team or must be able to contact you for assistance. Make sure to provide users with the names of people to contact for assistance and with instructions for contacting those people.

We recommend that you create a web page on your internal support site that provides end users with important information about their Cisco IP Phones.

Consider including the following types of information on this site:

- User guides for all Cisco IP Phone models that you support

- List of features supported

- User guide or quick reference for your voicemail system

Telephony Features for Cisco IP Phone

After you add Cisco IP Phones to Third-Party Call Control system, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure by using Third-Party Call Control system.

> **Note** The Third-Party Call Control system also provides several service parameters that you can use to configure various telephony functions.

Feature	Description and More Information
AES 256 Encryption Support for Phones	Enhances security by supporting TLS 1.2 and new ciphers.
Alphanumeric Dialing	Allows users to place a call with alphanumeric characters. You can use these characters for alphanumeric dialing: a-z, A-Z, 0-9, -, _, ., and +.
Any Call Pickup	Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone.
Assisted Directed Call Park	Enables users to park a call by pressing only one button using the Direct Park feature. Administrators must configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button.
Audio Settings	Configures audio settings for the phone speaker, the handset, and the headsets that are connected to the phone.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset.
Blind Transfer	Blind Transfer: This transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Blind Transfer does not initiate a consultation call and does not put the active call on hold. Some JTAPI/TAPI applications are not compatible with the Join and Blind Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Busy Lamp Field (BLF)	Allows user to monitor call state of a directory number.
Busy Lamp Field (BLF) Pickup	Allows user to pick up incoming calls to the directory number monitored through BLF.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. RPID and PAID caller id handling are supported.
Call Forward	Allows users to redirect incoming calls to another number. Call Forward options include Call Forward All, Call Forward Busy, Call Forward No Answer.
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.

Feature	Description and More Information
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature: • Logs missed calls for a shared line. • Logs all answered and placed calls for a shared line.
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone.
Call Pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display.
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display.
Caller ID Blocking	Allows a user to block their phone number or name from phones that have caller identification enabled.
Calling Party Normalization	Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book.
Cisco Extension Mobility	Allows users to temporarily access their Cisco IP Phone configuration such as line appearances, services, and speed dials from shared Cisco IP Phone by logging into the Cisco Extension Mobility service on that phone when they log into the Cisco Extension Mobility service on that phone. Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.
Cisco Extension Mobility Cross Cluster (EMCC)	Enables a user configured in one cluster to log into a Cisco IP Phone in another cluster. Users from a home cluster log into a Cisco IP Phone at a visiting cluster. **Note** Configure Cisco Extension Mobility on Cisco IP Phones before you configure EMCC.
Cisco Unified Video Advantage (CUVA)	Allows users to make video calls by using a Cisco IP Phone, a personal computer, and an external video camera. **Note** Configure the Video Capabilities parameter in the Product Specific Configuration Layout section in Phone Configuration. See the Cisco Unified Video Advantage documentation.

Feature	Description and More Information
Cisco WebDialer	Allows users to make calls from web and desktop applications.
Classic Ringtone	Supports narrowband and wideband ringtones. The feature makes the available ringtones common with other Cisco IP Phones.
Client Matter Code (CMC)	Enables a user to specify that a call relates to a specific client matter.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually.
	Allows a noninitiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line.
	Note Be sure to inform your users whether these features are activated.
Configurable RTP/sRTP Port Range	Provides a configurable port range (2048 to 65535) for Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP).
	The default RTP and sRTP port range is 16384 to 16538.
	You configure the RTP and sRTP port range in the SIP Profile.
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.
Device Invoked Recording	Provides end users with the ability to record their telephone calls via a softkey.
	In addition administrators may continue to record telephone calls via the CTI User Interface.
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number.
	Note If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.
Directed Call Pickup	Allows a user to pick up a ringing call on a DN directly by pressing the GPickUp softkey and entering the directory number of the device that is ringing.
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls.
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur.
DND and Call Forward Indication on Non-selected Line Key	Displays the DND and call forward icons next the to the line key label. The line key should be enabled with feature key sync. The line key should also be enabled with DND or call forward.
Emergency Calls	Enables users to make emergency calls. The emergency services receive the phone's location and a call-back number, to use when the emergency call unexpectedly disconnects.

Feature	Description and More Information
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings.
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC).
Extension Mobility Size Safe and Feature Safe	With Feature Safe, your phone can use any phone button template that has the same number of line buttons that the phone model supports. Size Safe allows your phone to use any phone button template that is configured on the system.
Forced Authorization Code (FAC)	Controls the types of calls that certain users can place.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.
Hold/Resume	Allows the user to move a connected call from an active state to a held state. • No configurations are required unless you want to use Music On Hold. See "Music On Hold" in this table. • See "Hold Reversion" in this table.
HTTP Download	Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download.
HTTPS for Phone Services	Increases security by requiring communication using HTTPS. **Note** When the web is in HTTPS mode, the phone is an HTTPS server.
Improve Caller Name and Number Display	Improves the display of caller names and numbers. If the Caller Name is known, then the Caller Number is displayed instead of Unknown.
IPv6 Support	Provides support for expanded IP addressing on Cisco IP Phones. IPv6 support is provided in standalone or in dual-stack configurations. In dual-stack mode, the phone is able to communicate using IPv4 and IPv6 simultaneously, independent of the content.
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.
Join Across Lines	Allows users to combine calls that are on multiple phone lines to create a conference call. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.

Feature	Description and More Information
Join	Allows users to combine two calls that are on one line to create a conference call and remain on the call.
Line Display Enhancement	Improves Call Display by removing the central dividing line when it is not required. This feature applies to the Cisco IP Phone 7841 only.
Log out of hunt groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent nonhunt group calls from ringing their phone.
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.
Meet Me Conference	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.
Message Waiting	Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message system uses the specified directory number to set or to clear a message waiting indication for a particular Cisco IP Phone.
Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages.
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone.
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desk phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day.
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device such as a cellular phone.
Monitoring and Recording	Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear a monitoring audible alert tone during a call when it is being monitored. When a call is secured, the security status of the call is displayed as a lock icon on Cisco IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being monitored. **Note** When an active call is being monitored or recorded, the use can receive or place intercom calls; however, if the user place an intercom call, the active call will be put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call.
Multicasting Paging	Enables users to page some or all phones. If the phone is on an active call while a group page starts, the incoming page is ignored.

Feature	Description and More Information
Multiple Calls Per Line Appearance	Each line can support multiple calls. By default, the phone supports two active calls per line, and a maximum of ten active calls per line. Only one call can be connected at any time; other calls are automatically placed on hold.
	The system allows you to configure maximum calls/busy trigger not more than 10/6. Any configuration more than 10/6 is not officially supported.
Music On Hold	Plays music while callers are on hold.
Mute	Mutes the handset or headset microphone.
No Alert Name	Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.
Onhook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.
Other Group Pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.
Pause in Speed Dial	Users can set up the speed-dial feature to reach destinations that require Forced Authorization Code (FAC) or Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination and inserts the necessary dialing pauses.
Peer Firmware Sharing (PFS)	Allows IP Phones located at remote sites to share the firmware files amongst them, which saves bandwidth when the upgrade process takes place. This feature uses Cisco Peer-to-Peer-Distribution Protocol (CPPDP) which is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. CPPDP is also used to copy firmware or other files from peer devices to the neighbouring devices.
	PFS aids in firmware upgrades in branch/remote office deployment scenarios that run over bandwidth-limited WAN links.
	Provides the following advantages over the traditional upgrade method:
	• Limits congestion on TFTP transfers to centralized remote TFTP servers
	• Eliminates the need to manually control firmware upgrades
	• Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously
	The more the number of IP phones, the better it's performance compared to the traditional firmware upgrade method.
PLK Support for Queue Statistics	The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.

Feature	Description and More Information
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a plus (+) sign.
	To dial the + sign, the user needs to press and hold the star (*) key for at least 1 second. This applies to dialing the first digit for an on-hook (including edit mode) or off-hook call.
Power Negotiation over LLDP	Allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).
Problem Reporting Tool	Submits phone logs or reports problems to an administrator.
Programmable Feature Buttons	You can assign features, such as New Call, Call Back, and Forward All to line buttons.
Quality Reporting Tool (QRT)	Allows users to submit information about problem phone calls by pressing a button. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.
Redial	Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.
Remote Customization (RC)	Allows a service provider to customize the phone remotely. There is no need for either the service provider to physically touch the phone or a user to configure the phone. The service provider can work with a sales engineer at the time of ordering to set this up.
Ringtone Setting	Identifies ring type used for a line when a phone has another active call.
Reverse Name Lookup	Identifies the caller name using the incoming or outgoing call number. You must configure either the LDAP Directory or the XML directory. You can enable or disable the reverse name lookup using the phone administration web page.
RTCP Hold For SIP	Ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.
Secure Conference	Allows secure phones to place conference calls using a secured conference bridge. As new participants are added by using Confrn, Join, cBarge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones.
	The Conference List displays the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.
Serviceability for SIP Endpoints	Enables administrators to quickly and easily gather debug information from phones.
	This feature uses SSH to remotely access each IP phone. SSH must be enabled on each phone for this feature to function.
Shared Line	Allows a user with multiple phones to share the same phone number or allows a user to share a phone number with a coworker.

Feature	Description and More Information
Show Calling ID and Calling Number	The phones can display both the calling ID and calling number for incoming calls. The IP phone LCD display size limits the length of the calling ID and the calling number that display.
	The Show Calling ID and Calling Number feature applies to the incoming call alert only and does not change the function of the Call Forward and Hunt Group features.
	See "Caller ID" in this table.
Show Duration for Call History	Displays the time duration of placed and received calls in the Call History details.
	If the duration is greater than or equal to one hour, the time is displayed in the Hour, Minute, Second (HH:MM:SS) format.
	If the duration is less than one hour, the time is displayed in the Minute, Second (MM:SS) format.
	If the duration is less than one minute, the time is displayed in the Second (SS) format.
Silence Incoming Call	Allows you to silence an incoming call by pressing **Ignore** softkey or by pressing the volume button down.
Speed Dial	Dials a specified number that has been previously stored.
Time Zone Update	Updates the Cisco IP Phone with time zone changes.
Transfer	Allows users to redirect connected calls from their phones to another number.
	Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Voice Message System	Enables callers to leave messages if calls are unanswered.
Web Access Enable by Default	Web services are enabled by default.
XSI call logs display	Allows you to configure a phone to display recent call logs from either the BroadWorks server or the local phone. After you enable the feature, the **Recents** screen has a **Display recents from** menu and the user can choose the XSI call logs or the local call logs.

Feature Buttons and Softkeys

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. An "X" in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco IP Phone administration.

Note The Cisco IP Phone 6821 does not have programmable feature buttons. Supported features display on softkeys.

Table 15: Features with Corresponding Buttons and Softkeys

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Answer		X	X
Call Forward All		X	X
Call Park		X	X
Call Park Line Status		X	
Call Pickup (Pick Up)		X	X
Call Pickup Line Status		X	
Conference	X		X (only displayed during connected call conference scenario)
Divert			X
Do Not Disturb		X	X
Hold	X		X
Intercom		X	
Mute	X		
Redial		X	X
Speed Dial		X	X
Speed Dial Line Status		X	
Transfer	X		X (only displayed during connected call transfer scenario)

Enable Users to Configure Features on Line Keys

You can enable users to configure these features on line keys:

• Speed dial

• Busy Lamp Field (BLF) to monitor a coworker's line, with the following options:

• Speed dial to the monitored line

• Call pickup from the monitored line

Users can select any available line keys to configure features. They can also select a line key that is functioning as a speed-dial key or as a BLF key. The user's configuration will override any existing configuration for the line key. Users cannot select line keys on which you have configured other features. If a user selects a BLF list key, the phone adjusts the positions of the BLF list keys using the next available line keys.

For the BLF feature options, the phone subscribes to the BLF list URI that you specify (XML parameter `BLF_List_URI`), to be notified of changes in the status of the monitored lines. If you do not specify a BLF list URI, the phone subscribes to `$USER@$PROXY`.

Procedure

Step 1 On the phone administration web page, go to **Admin Login** > **Advanced**, **Voice** tab.

Step 2 To allow features, go to **Att Console** > **General**, and configure **Customizable PLK Options** as described in General, on page 297.

When this step is complete, users can configure features on Key Expansion Module keys.

Step 3 To enable feature configuration on a line key on the phone, do one of the following:

• Disable the extension function for the line key:

1. Go to **Voice** > **Phone**.

2. Set **Extension** to **Disabled** in the corresponding **Line Key** *number* section.

• Disable service on the corresponding line:

1. Go to **Voice**.

2. Go to the corresponding **Ext** *number* tab.

3. In the **General** section, set **Line Enable** to **No**.

Configure a Speed Dial on a Line Key

You can configure speed dial on an idle line of a user phone. The user can then use that line key to speed-dial a number. When you enable the speed dial on the line key, the user sees the speed-dial icon a name for the speed dial line key. The user presses the line key to dial the assigned extension.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Phone**.
Step 2	Select a Line Key on which to configure speed-dial.
Step 3	From the Extension pulldown menu, select **Disabled** to disable the extension.
Step 4	In the **Extended Function** field, enter a string in this format:

`fnc=sd;ext=9999@$PROXY;nme=xxxx`

If you configure a phone with alphanumeric dialing feature in which the phone can place a call with alphanumeric characters instead of the traditional digits, you can enter a string in this format:

`fnc=sd;ext=xxxx.yyyy@$PROXY;vid=n;nme=xxxx`

where:

- fnc= sd means function=speed dial
- ext= 9999 is the phone that the line key calls. Replace 9999 with appropriate phone number.

  ext= xxxx.yyyy is the phone that the line key calls. Replace xxxx.yyyy with alphanumeric characters. You can use these characters for alphanumeric dialing: a-z, A-Z, 0-9, -, _, ., and +.

- vid=n is the line index of the phone.

- nme= XXXX is the name displayed on the phone for the speed-dial line key. Replace XXXX with a name.

You can also configure XML service with line key. Enter a string in this format:

`fnc=xml;url=http://xml.service.url;nme=name`

Step 5	Click **Submit All Changes**.

Configure a Speed Dial with the Configuration Utility Page

You can configure speed dials on the phone with the web interface.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **User**.
Step 2	In the **Speed Dial** section, enter a name and number that corresponds to the speed dial entry.
Step 3	Click **Submit All Changes**.

Related Topics

Enable Conference Button with a Star Code

You can add a star code to the Conference button so that your user can press the button only once to add many active calls to a conference. You can enable this feature from the phone web page.

Before you begin

- The phone server must suppport this feature.

- Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2   In the **Call Features Settings** section, select **Yes** for the **Conference Single Hardkey** field, enter a star code in the **Conference Bridge URL**, and press **Submit All Changes**. For example, you can enter *55 to represent the conference bridge URL of a telecom service provider.

You can also enable the conference button with a xml file. Enter a string in this format:

```
<Conference_Bridge_URL_1_ ua="na">*55</Conference_Bridge_URL_1_>
<Conference_Single_Hardkey_1_ ua="na">Yes</Conference_Single_Hardkey_1_>
```

Set up Extra Line Keys

Enable this feature if you want to use the buttons on both sides of the phone screen as line keys.

Procedure

Step 1   On the Configuration Utility page, click **Admin Login** > **Voice** > **Phone**.

Step 2   Choose a line key and select an extension to enable it.

Step 3   Click **Submit All Changes**.

Configure the Screen Saver with the Phone Web Page

You can configure a screen saver for the phone. When the phone is idle for a specified time, it enters screen saver mode.

Any button press returns the phone to normal mode.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 On the phone web page, select **Voice** > **User**.

The user can select **User Login** > **Voice** > **User** to add screen saver to the phone.

Step 2 In the **Screen** section, set up the fields as described in the following table.

Parameter	Description
Screen Saver Enable	Select **Yes** to enable a screen saver on the phone. When the phone is idle for a specified time, it enters screen saver mode. Default: No
Screen Saver Type	Types of screen saver. Options you can choose: • **Clock**—Displays a digital clock on a plain background. • **Download Picture**—Displays a picture pushed from the phone webpage. • **Logo**: Displays a logo on the phone screen. Add a logo image in the **Logo URL** field.
Screen Saver Wait	Amount of idle time before screen saver displays. Enter the number of seconds of idle time to elapse before the screen saver starts. Default: 300
Picture Download URL	URL locating the (.png) file to display on the phone screen background. If you select picture as as screensaver type, this image displays as a screensaver on the phone screen. When you enter an incorrect URL to download a new wallpaper, the phone fails to upgrade to the newer wallpaper and displays the existing downloaded wallpaper. If the phone does not have any wallpaper downloaded earlier, it displays a gray screen.
Logo URL	Enter a URL or path for the location where the logo image is saved. If you select logo as as screensaver type, this image displays as a screensaver on the phone screen.

Step 3   Click **Submit All Changes**.

Phone Configuration for Monitoring Other Phones

You can configure the phone to monitor the status of lines on other phones. This feature is useful if users routinely handle calls for colleagues and need to see if they are available to answer calls. The phone monitors each line on a separate line key. The monitoring line keys function as Busy Lamp Field (BLF) keys. A BLF is an LED that changes color to indicate the status of the monitored line:

Table 16: BLF Key LED Status

LED Color	Meaning
Green	The monitored line is available.
Red	The monitored line is busy.
Blinking red	The monitored line is ringing.
Amber	Error in BLF key configuration.

If the phone is registered to a BroadSoft server, you can set up the phone to monitor multiple users, with a single set of configurations.

Configure the Phone to Monitor Multiple Users' Lines

If the phone is registered to a BroadSoft server, you can configure the phone to monitor the entire BLF list. The phone assigns available line keys in sequence to monitor the BLF list entries, and starts showing the status of the monitored lines on the BLF keys.

Before you begin

- Make sure that the phone is registered to a BroadSoft server.

- You set up a BLF list for a user of the phone on the BroadSoft server.

Procedure

Step 1   On the phone administration web page, go to **Admin Login** > **Advanced**, **Voice** > **Att Console** > **General**.

Step 2   Configure **BLF List URI**, **BLF List**, and **Use Line Keys For BLF List** as described in General, on page 297.

If you allow users to configure individual BLF keys (see Enable Users to Configure Features on Line Keys, on page 157), we recommend setting **BLF List** to **Hide**.

Step 3   Click **Submit All Changes**.

Configure the Busy Lamp Field in the Phone Configuration File

If the phone is registered to a BroadSoft server, you can use the phone configuration file to configure the busy lamp field.

Procedure

Step 1 Edit the BLF_List_URI parameter of the phone configuration file that is available in the BroadSoft server.

Step 2 Add the List URI: sip: parameter @ domain name.

The List URI must match the one defined in the BroadSoft server.

Step 3 Save the changes.

Configure a Line Key on the Phone to Monitor a Single User's Line

You can configure busy lamp field on a phone line when a user needs to monitor a coworker's availability to handle calls.

You can configure the busy lamp field to work with any combination of speed dial or call pickup. For example, busy lamp field alone, busy lamp field and speed dial, busy lamp field and call pickup, or busy lamp field, speed dial, and call pickup can all be configured to work together. But speed dial alone requires a different configuration.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 Select a line key on which to configure a busy lamp field.

Step 3 Select **Disabled** to disable the extension.

Step 4 In the **Extended Function** field, enter a string in this format:

fnc=blf;sub=xxxx@$PROXY;usr=yyyy@$PROXY

fnc=blf;sub=xxxx@$PROXY;ext=yyyy@$PROXY

Where:

- fnc=blf means function=busy lamp field

- sub=the URI to which the SUBSCRIBE message should be sent. For a BroadSoft server, this name must be identical to the name defined in the **List URI: sip:** parameter. xxxx is the name that is defined in **List URI: sip**: parameter. Replace xxxx with the exact defined name. $PROXY is the server. Replace $PROXY with the server address or name.

> • usr/ext=the user that the busy lamp field monitors. yyyy is user id of the phone that the busy lamp field monitors. Replace yyyy with the exact user id of the monitored phone. $PROXY is the server. Replace $PROXY with the server address or name.

Step 5   (Optional) You can configure the busy lamp field to work with any combination of speed dial or call pickup. To enable the busy lamp field to work with speed dial or call pickup, enter a string in the following format in the Extended Function field:

`fnc=blf+sd+cp;sub=xxxx@$PROXY;usr=yyyy@$PROXY.`

Where:

sd= speed dial

cp= call pickup

Step 6   Click **Submit All Changes**.

Configure Busy Lamp Field with Other Features

You can configure busy lamp field to work with other features on your key expansion module, such as speed dial, and call pickup. Use the information in the following table as a guide when selecting the correct string format.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Att Console**.

Step 2   Select a key expansion module line key.

Step 3   Enter a string in the appropriate format.

Feature	String Format
Busy Lamp Field and Speed Dial	`fnc=blf+sd;sub=xxx@proxy;ext=monitored userID@proxy.`
Busy Lamp Field, Speed Dial, and Call Pickup	`fnc=blf+sd+cp;sub=xxx@proxy;ext=monitored userID@proxy.`
Busy Lamp Field, Speed Dial, and Park Notification	`fnc=blf+sd;sub=xxx@proxy;ext=monitored userID@proxy.` This combination cannot be configured using the extended function. This combination is supported on Broadsoft servers only and it is configured using the BLF List and related configuration on the server.

Feature	String Format
Busy Lamp Field, Speed Dial, Park Notification, and Call Pickup	`fnc=blf+sd+cp;sub=xxx@proxy;ext=monitored userID@proxy.` This combination cannot be configured using the extended function. This combination is supported on Broadsoft servers only and it is configured using the BLF List and related configuration on the server.
Busy Lamp Field and Park Notification	`fnc=blf;sub=xxx@proxy;ext=monitored userID@proxy.` This combination cannot be configured using the extended function. This combination is supported on Broadsoft servers only and it is configured using the BLF List and related configuration on the server.
Busy Lamp Field, Park Notification, and Call Pickup	`fnc=blf+cp;sub=xxx@proxy;ext=monitored userID@proxy.` This combination cannot be configured using the extended function. This combination is supported on Broadsoft servers only and it is configured using the BLF List and related configuration on the server.
Busy Lamp Field and Call Pickup	`fnc=blf+cp;sub=xxx@proxy;ext=monitored userID@proxy`

Step 4   Click **Submit All Changes**.

Configure Alphanumeric Dialing

You can configure a phone so that the user of the phone can make a call by dialing alphanumeric characters instead of dialing only digits. In the phone web page, you can configure alphanumeric dialing with speed-dial, blf, and call pickup.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Ext**.

Step 2   In the **Enable URI Dialing 1**, select **Yes** to enable alphanumeric dialing.

In the phone page, you can add a string on a line key in this format to enable speed dial with alphanumeric dialing capability:

`fnc=sd;ext=xxxx.yyyy@$PROXY;nme=yyyy,xxxx`

For example:

`fnc=sd;ext=first.last@$PROXY;nme=Last,First`

The above example will enable the user to dial "first.dial" to make a call.

Note   The supported characters that you can use for alphanumeric dialing are a-z, A-Z, 0-9, -, _, ., and +.

Step 3   Click **Submit All Changes**.

Configure a Paging Group (Multicast Paging)

You can configure multicast paging so that users can page all the phones at once or page a group of phones without involving a server. On the Configuration Utility page, you configure a phone as a part of a paging group and can subscribe them to the same multicast address. This enables users to direct pages to specific groups of phones. When you assign each paging group with a unique number, the user dials the paging group number to start paging. All phones that are subscribed to the same multicast address (also configured on the Configuration Utility page) receive the page. The user hears a paging tone of three short beeps when there is an incoming paging call.

Keep these things in mind:

- Your network must support multicasting so that all devices in the same paging group are able to join the corresponding multicast group.

- Paging groups must use even-numbered port numbers.

- If the phone is on an active call when a group page starts, the incoming page is ignored.

- Group paging is one way and uses the G711 codec. The paged phone can only listen to the call from the originator.

- Incoming pages are ignored when DND is enabled.

- When paging occurs, the speaker on the paged phones automatically powers on unless the handset or the headset is in use.

- If the phone is on an active call when a group page starts, the incoming page is ignored. When the call ends, the page is answered, if the page is active.

- When multiple pages occur, the pages are answered in chronological order. Until the active page ends, the next page is not answered.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **Multiple Paging Group Parameters** section, enter a string in the **Group Paging Script** field in this format:

`pggrp=multicast-address:port;[name=xxxx;]num=yyy;[listen={yes|no}]];`

where:

- multicast-address = Multicast IP address of the phone that listens for and receives pages.

- port = Port on which to page; you must use different, even-number ports for each paging group.

Multicast paging doesn't work with odd-numbered ports.

- name (optional) = xxxx is the name of the paging group. Replace *xxxx* with a name. The name can consist maximum of 64 characters.

- num= yyy is a unique number that the user dials to access the paging group. Replace *yyy* with a number. The number can consist maximum of 64 characters and the allowed range is 1024 to 32767.

- listen = Indicates whether the phone listens on the page group. Only the first two groups with listen set to **yes** listen to group pages. If the field is not defined, the default value is **no**, so you must set this field to listen to the group pages.

You can add more paging groups by appending to the configuration string. Here is an example of several paging groups.

```
pggrp=224.168.168.168:34560;name=All;num=500;listen=yes;
pggrp=224.168.168.168:34562;name=GroupA;num=501;listen=yes;
pggrp=224.168.168.168:34564;name=GroupB;num=502;
pggrp=224.168.168.168:34566;name=GroupC;num=503;
```

This example creates four paging groups: **All**, **GroupA**, **GroupB**, and **GroupC**. Users dial 500 to send pages to all phones, 501 to send pages to phones configured as part of the **GroupA** group, 502 to send pages to phones configured as part of the **GroupB** group, and 503 to send pages to phones configured as part of the **GroupC** group. The configured phone receives pages directed to the **All** and **GroupA** groups.

Step 3   Click **Submit All Changes**.

Call Park

With call park, a call can be parked and then retrieved either from your phone or from another phone. The following LED colors display on the line key when this feature is configured:

- Green LED—Call park is successfully configured.

- Amber LED—Call park is not configured.

- Red slow blinking LED—A call is parked.

Configure Call Park with Star Codes

You can configure call park so that the user can put a call on hold and then retrieve the call from either the user's phone or another phone.

When configuring call park, the Call Park Code and the Call Unpark Code must match the Feature Access Code configured on the server.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Regional**.
Step 2	Enter ***68** in the **Call Park Code** field.
Step 3	Enter ***88** in the **Call Unpark Code** field.
Step 4	Click **Submit All Changes**.

Add Call Park to a Programmable Line Key

You can add call park to a line key to enable the user to temporarily store and retrieve calls. Call park is supported on private lines and shared lines.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Phone**.
Step 2	Select a line key.
Step 3	Select **Disabled** to disable the extension.
Step 4	In the **Extended Function** field, enter a string in this format:

For a private line, enter `fnc=prk;sub=$USER@$PROXY;nme=CallPark-Slot1`.

For a shared line, enter `fnc=prk;sub=$USER@$PROXY;nme=Call-Park1;orbit=<DN of primary line>`.

where:

- fnc= prk means function=call park

- sub= 999999 is the phone to which the call parks. Replace 999999 with a numbers.

- nme= XXXX is the name displayed on the phone for the call park line key. Replace XXXX with a name.

Step 5	Click **Submit All Changes**.

Configuring Programmable Softkeys

You can customize the softkeys displayed on the phone. The default softkeys (when the phone is in an idle state) are Redial, Directory, Call Forward, and Do Not Disturb. Other softkeys are available during specific call states (for example, if a call is on hold, the Resume softkey displays).

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   Under **Programmable Softkeys**, edit the softkeys depending on the call state that you want the softkey to display. For more information, see Programmable Softkeys, on page 171.

In the Programmable Softkeys section, each phone state is displayed and the softkeys that are available to display during that state are listed. Each softkey is separated by a semicolon. Softkeys are shown in the format:

```
softkeyname |[ position ]
```

where softkeyname is the name of the key and position is where the key is displayed on the IP phone screen. Positions are numbered, with position one displayed on the lower left of the IP phone screen, followed by positions two through four. Additional positions (over four) are accessed by pressing the right arrow key on the phone. If no position is given for a softkey, the key will float and appears in the first available empty position on the IP phone screen.

Step 3   Click **Submit All Changes**.

Customize a Programmable Softkey

The phone provides sixteen programmable softkeys (fields PSK1 through PSK16). You can define the fields by a speed-dial script.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.

Step 3   Select a programmable softkey number field on which to configure a phone feature.

Step 4   Enter the string for the programmable soft key. See the different types of programmable softkeys described in Configure Speed Dial on a Programmable Softkey, on page 169.

Step 5   Click **Submit All Changes**.

Configure Speed Dial on a Programmable Softkey

You can configure programmable softkeys as speed dials. The speed dials can be extensions or phone numbers. You can also configure programmable softkeys with speed dials that perform an action that a vertical service

activation code (or a star [*] code) defines. For example, if you configure a programmable softkey with a speed dial for *67, the call is placed on hold.

Before you begin

Access the phone administration web page. See

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.

Step 3   To configure a speed dial PSK, enter the following in the PSK **number** field:

```
fnc=sd;ext=extensionname/starcode@$PROXY;vid=n;nme=name
```

Where:

- fnc= function of the key (speed dial)

- extensionname=extension being dialed or the star code action to perform

- vid= n is the extension that the speed dial will dial out

- name is the name of the speed dial being configured

Note   The **name** field displays on the softkey on the IP phone screen. We recommend a maximum of 10 characters for a phone. If more characters are used, the label might be truncated on the phone screen.

Step 4   Edit the following:

- **Idle Key List:** Edit the field as described in the following example:

```
redial|1;newcall|2;dnd;psk1
```

If the user incorrectly configures the programmable softkey list features on the phone, the key list on the phone LCD does not update. For example:

- If a user enters **rdeial;newcall;cfwd** (redial has been misspelt), the key list is not updated and the user does not see any change on the LCD.

- If a user enters **redial;newcall;cfwd;delchar**, the user will not see a change on the LCD, as the delchar softkey is not allowed in the **Idle Key List**. Hence, this is an incorrect configuration of the programmable softkey list.

- **PSK1:**

```
fnc=sd;ext=5014@$PROXY;nme=sktest1
```

Note   In this example, we are configuring a softkey on a phone as a speed dial number for extension 5014 (sktest1).

You can also configure an XML service on the programmable soft key. Enter the string in this format:

```
fnc=xml;url=http://xml.service.url;nme=name
```

Step 5   Click **Submit All Changes**.

Programmable Softkeys

Keyword	Key Label	Definition	Available Phone Status
acd_login	Agt signin	Logs user in to Automatic Call Distribution (ACD).	Idle
acd_logout	AgtSignOut	Logs user out of ACD.	Idle
answer	Answer	Answers an incoming call.	Ringing
astate	Agt Status	Checks the ACD status.	Idle
avail	Avail	Denotes that a user who is logged in to an ACD server has set his status as available.	Idle
barge	Barge	Allows another user to interrupt a shared call.	Shared-Active, Shared-Held
bargesilent	BargeSilent or BargeSlnt	Allows another user to interrupt a shared call with the mic disabled.	Shared-Active
bxfer	BlindXfer	Performs a blind call transfer (transfers a call without speaking to the party to whom the call is transferred). Requires that Blind Xfer Serv is enabled.	Connected
call (or dial)	Call	Calls the selected item in a list.	Dialing Input
call info	Call Info	Show call information	Progressing
cancel	Cancel	Cancels a call (for example, when conferencing a call and the second party is not answering.	Off-Hook
cfwd	Forward / Clr fwd	Forwards all calls to a specified number.	Idle, Off-Hook, Shared-Active, Hold, Shared-Held
crdpause	PauseRec	Pause recording	Connected, Conferencing
crdresume	ResumeRec	Resume recording	Connected, Conferencing
crdstart	Record	Start a recording	Connected, Conferencing
crdstop	StopRec	Stop recording	Connected, Conferencing

Keyword	Key Label	Definition	Available Phone Status
conf	Conference	Initiates a conference call. Requires that Conf Server is enabled and there are two or more calls that are active or on hold.	Connected
confLx	Conf line	Conferences active lines on the phone. Requires that Conf Serv is enabled and there are two or more calls that are active or on hold.	Connected
delchar	delChar - backspace Icon	Deletes a character when entering text.	Dialing Input
dir	Dir	Provides access to phone directories.	Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held
disp_code	DispCode	Enter Disposition Code	Idle, Connected, Conferencing, Hold
dnd	DND / Clr Dnd	Sets Do Not Disturb to prevent calls from ringing the phone.	Idle, Off-Hook, Hold, Shared-Active, Shared-Held, Conferencing, Start-Conf, Start-Xfer
emergency	Emergency	Enter emergency number	Connected
em_login (or signin)	Sign in	Logs user in to Extension Mobility.	Idle
em_logout (or signout)	Sign out	Logs user out of Extension Mobility.	Idle
endcall	End call	Ends a call.	Connected, Start-Xfer, Start-Conf, Conferencing, Hold
favorites	Favorites	Provides access to "Speed Dials".	Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held
gpickup	GrPickup	Allows user to answer a call ringing on an extension by discovering the number of the ringing extension.	Idle, Off-Hook
hold	Hold	Put a call on Hold.	Connected, Start-Xfer, Start-Conf, Conferencing
ignore	Decline	Ignores an incoming call.	Ringing

Keyword	Key Label	Definition	Available Phone Status
ignoresilent	Ignore	Silences an incoming call	Ringing
join	Join	Connects a conference call. If the conference host is user A and users B & C are participants, when A presses "Join", A will drop off and users B & C will be connected.	Conferencing
lcr	Call Rtn/lcr	Returns the last missed call.	Idle, Missed-Call,Off-Hook (no input)
left	Left arrow icon	Moves the cursor to the left.	Dialing Input
messages	Messages	Provides access to voicemail.	Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held
miss	Miss	Displays the list of missed calls.	Missed-Call
newcall	New Call	Begins a new call.	Idle, Hold, Shared-Active, Shared-Held
option	Option	Opens a menu of input options.	Off-Hook
park	Park	Puts a call on hold at a designated "park" number.	Connected
phold	PrivHold	Puts a call on hold on an active shared line.	Connected
pickup	PickUp	Allows a user to answer a call ringing on another extension by entering the extension number.	Idle, Off-Hook
recents	Recents	Displays the All calls list from call history.	Idle, Off-Hook, Shared-Active, Shared-Held
redial	Redial	Displays the redial list.	Idle, Connected, Start-Conf, Start-Xfer, Off-Hook (no input), Hold
resume	Resume	Resumes a call that is on hold.	Hold, Shared-Held
right	Right arrow icon	Moves the cursor to the right.	Dialing (input)
settings	Settings	Provides access to "Information and Settings".	All
starcode	Input Star Code/*code	Displays a list of star codes that can be selected.	Off-Hook, Dialing (input)

Keyword	Key Label	Definition	Available Phone Status
trace	Trace	Trigger trace	Idle, Connected, Conferencing, Hold
unavail	Unavail	Denotes that a user who is logged in to an ACD server has set his status as unavailable.	Idle
unpark	Unpark	Resumes a parked call.	Idle, Off-Hook, Connected, Shared-Active
xfer	Transfer	Performs a call transfer. Requires that Attn Xfer Serv is enabled and there is at least one connected call and one idle call.	Connected, Start-Xfer, Start-Conf
xferlx	Xfer line	Transfers an active line on the phone to a called number. Requires that Attn Xfer Serv is enabled and there are two or more calls that are active or on hold.	Connected

Configure Provisioning Authority

You can set up provisioning authority so that users can access their personalized phone settings from other phones. For example, people who work different shifts or who work at different desks during the week can share an extension, yet have their own personalized settings.

The **Sign in** softkey appears on the phone when you enable provisioning authority on the phone. Users enter their usernames and passwords to access their personal phone settings. Users can also ignore the sign-in and use the phone as a guest. After users sign in, they have access to their personal directory numbers on the phone. When the user signs out, the phone reverts to a basic profile with limited features.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Provisioning**.

Step 2   In the **Configuration Profile** section, set the **Profile Rule** field to the phone configuration file's URL.

Example:

http://192.0.2.1:80/dms/CP-MMxx-MPP/MMxxSystem.xml

where,

MM– Cisco IP Phone MM Series with Multiplatform Firmware (68, 78, or 88)

MMxx– Cisco specific phone model (for example, 7841,7861, 8845, 8865 or 7832)

Step 3 Select **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 4 Fill in the **EM Enable** and **EM User Domain** fields in the **Extension Mobility** section, based on the information provided in the phone configuration file.

Step 5 Set the amount of time (in minutes) that the phone session will last for in the **Session Timer(m)** field. The phone signs out when the session times out.

Step 6 Set the amount of time (in seconds) that the user has to cancel the sign-out in **Countdown Timer(s)**.

Step 7 Choose input type of the password from the **Preferred Password Input Mode** field.

For information on Extension Mobility fields, see Extension Mobility, on page 267.

Your user can also change the password input type from the phone.

Step 8 (Optional) If the **Programmable Softkey Enable** field in the **Programmable Softkeys** section is set to **Yes**, add `signin` to **Idle Key List**.

Example:

newcall|1;signin|2

Step 9 Click **Submit All Changes**.

Configure Provisioning Authority in the Phone Configuration File

You can enable provisioning authority in the default configuration file for your phones, so that you don't need to set up the feature manually for each phone.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 In the phone configuration file, set the following parameters:

a) Set the Provisioning Authority profile rules in the **Profile_Rule** parameters.

Example:
```
<Profile_Rule ua="na">("$EMS" eq "mobile" and "$MUID" ne "" and "$MPWD" ne "")?[--uid
$MUID$PDOM --pwd $MPWD]
http://10.74.121.51:80/dms/CP-8851-3PCC/8851System.xml|http://10.74.121.51:80/dms/CP-8851-3PCC/8851System.xml</Profile_Rule>
```

b) Set the **EM_Enable** parameter to **Yes**.

Example:
```
<EM_Enable ua="na">Yes</EM_Enable>
```

c) Enter the enter the domain for the phone, or the authentication server in the **EM_User_Domain** parameter.

Example:
```
<EM_User_Domain ua="na">@10.74.121.51</EM_User_Domain>
```

Step 2 Save the configuration file and upload it to your provisioning server.

Step 3 Select **Voice** > **Provisioning**.

Step 4   Enter the filepath to the configuration file in one of the **Profile Rule** fields.

Example:

http://<SERVER IP ADDRESS>:80/dms/td_8861/8861System.xml

Step 5   Click **Submit All Changes**.

Enable Hoteling on a Phone

Set up the hotel feature on Broadworks and set the phone as a host or a guest.

Procedure

Step 1   Select **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2   In the **Call Feature Settings** section, set **Enable Broadsoft Hoteling** to **Yes**.

Step 3   Set the amount of time (in seconds) that the user can be signed in as a guest on the phone in **Hoteling Subscription Expires**.

Step 4   Click **Submit All Changes**.

Set the User Password

Users can set their own password on their phones, or you can set a password for them.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **System**.

Step 2   Set a password in the **User Password** field.

Step 3   Click **Submit All Changes**.

Download Problem Reporting Tool Logs

Users submit problem reports to you with the Problem Reporting Tool.

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue.

To issue a problem report, users access the Problem Reporting Tool and provide the date and time that the problem occurred, and a description of the problem. You need to download the problem report from the Configuration Utility page.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Info** > **Debug Info** > **Device Logs**.
Step 2	In the **Problem Reports** area, click the problem report file to download.
Step 3	Save the file to your local system and open the file to access the problem reporting logs.

Configure PRT Upload

You must use a server with an upload script to receive the problem reports that the user sends from the phone.

- If the URL specified in the **PRT Upload Rule** field is valid, users get a notification alert on the phone UI saying that they have successfully submitted the problem report.

- If the **PRT Upload Rule** field is empty or has an invalid URL, users get a notification alert on the phone UI saying that the data upload failed.

The phone uses an HTTP/HTTPS POST mechanism, with parameters similar to an HTTP form-based upload. The following parameters are included in the upload (utilizing multipart MIME encoding):

- devicename (example: "SEP001122334455")

- serialno (example: "FCH12345ABC")

- username (The user name is either the **Station Display Name** or the **User ID** of the extension. The **Station Display Name** is first considered. If this field is empty, then the **User ID** is chosen.)

- prt_file (example: "probrep-20141021-162840.tar.gz")

You can generate PRT automatically at specific intervals and can define the PRT file name.

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```php
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
```

```
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Before you begin

Access the phone administration web page. See .

Procedure

Step 1	Select **Voice** > **Provisioning**.
Step 2	In the **Problem Report Tool** section, set the fields as described in the .

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. Enter the string in this format:

```
<PRT_Upload_Rule ua="na">

http://64.101.234.132:8000//Users/abcd/uploads/prt/test-prt.tar.gz

</PRT_Upload_Rule>

<PRT_Upload_Method ua="na">POST</PRT_Upload_Method>

<PRT_Max_Timer ua="na">20</PRT_Max_Timer>
```

Step 3	Click **Submit All Changes**.

Configure a Phone to Accept Pages Automatically

The Single Paging or Intercom feature enables a user to directly contact another user by phone. If the phone of the person being paged has been configured to accept pages automatically, the phone does not ring. Instead, a direct connection between the two phones is automatically established when paging is initiated.

Before you begin

Access the phone administration web page. See .

Step 1   Select **Voice** > **User**.

Step 2   In the **Supplementary Services** section, choose **Yes** for the **Auto Answer Page** field.

Step 3   Click **Submit All Changes**.

Server-Configured Paging

You can configure a paging group on a server so that users can page a group of phones. For more details, refer to your server documentation.

Manage Phones with TR-069

You can use the protocols and standards defined in Technical Report 069 (TR-069) to manage phones. TR-069 explains the common platform for management of all phones and other customer-premises equipment (CPE) in large-scale deployments. The platform is independent of phone types and manufacturers.

As a bidirectional SOAP/HTTP-based protocol, TR-069 provides the communication between CPEs and Auto Configuration Servers (ACS).

For TR-069 Enhancements, see TR-069 Parameter Comparison, on page 327.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **TR-069**.

Step 2   Set up the fields as described in TR-069, on page 300.

Step 3   Click **Submit All Changes**.

View TR-069 Status

When you enable TR-069 on a user phone, you can view status of TR-069 parameters on the Configuration page.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Select **Info** > **Status** > **TR-069 Status**.

You can view status of TR-069 parameters in .

Enable Electronic Hookswitch

The Electronic Hookswitch feature enables users to use headsets that electronically connect a wireless headset to a phone. Typically, the headset requires a base that plugs into the phone and communicates with the headset. Here are the supported headsets:

- Plantronics Savi 740

- Jabra PRO920

- Jabra PRO9400

- Sennheiser DW Pro1

Only the Cisco IP Phone 6851 Multiplatform Phones and Cisco IP Phone 6861 Multiplatform Phones support the Electronic Hookswitch feature.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **User**.

Step 2   Set up the fields as described in .

Step 3   Click **Submit All Changes**.

Enable Remote Call Recording with SIP REC

You can enable call recording on a phone so that your user can record an active call. The recording mode configured on the server controls the display of the recording softkeys for each phone.

Table 17: Recording Mode and Recording Softkeys

Recording Mode in Server	Recording Softkeys Available on the Phone
Always	No softkeys available. Your user can't control recording from the phone. Recording starts automatically when a call is connected.
Always with Pause/Resume	PauseRec ResumeRec When a call is connected, recording starts automatically and your user can control the recording.
On Demand	Record PauseRec ResumeRec When a call is connected, recording starts automatically but the recording is not saved until the user presses the **Record** softkey. Your user sees a message when recording state changes.
On Demand with User Initiated Start	Record PauseRec StopRec ResumeRec The recording only starts when your user presses the **Record** softkey. Your user sees a message when recording state changes.

During a recording, your user sees different icons which depend on the recording state. The icons are displayed on the Calls screen and also on the line key on which the user is recording a call.

Table 18: Recording Icons

Icon	Meaning
◉	Recording in progress.
◉	Recording paused

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2 In the **Supplementary Services** section, click **Yes** or click **No** to enable or to disable call recording in the **Call Recording Serv** field.

Step 3 (Optional) In the **Programmable Softkeys** section, to enable softkeys, add a string in this format in the **Connected Key List** and **Conferencing Key List** fields.

```
crdstart;crdstop;crdpause;crdresume
```

Step 4 In the phone web page, click the **Ext(n)** tab that requires call recording.

Step 5 In the **SIP Settings** section, in the **Call Recording Protocol**, select **SIPREC** as the call recording protocol.

For details on the **SIP Settings** fields, see SIP Settings, on page 277.

Step 6 Click **Submit All Changes**.

Enable Remote Call Recording with SIP INFO

You can enable call recording on a phone so that your user can record an active call.

During a recording, your user sees different icons which depend on the recording state. The icons are displayed on the Calls screen and also on the line key on which the user is recording a call.

Your user presses the following softkeys to control the phone recording:

- **Record**

- **StopRec**

The recording only starts when your user presses the **Record** softkey. Your user sees a message when recording state changes and the recording icon displays on the call screen.

Once a phone recording starts, the **StopRec** softkey can work. The recording stops when your user presses the **StopRec** softkey. Your user sees a message when the recording state changes.

Table 19: Recording Icons

Icon	Meaning
◉	Recording in progress.

Before you begin

- You need to set up call recording on the call control system.

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 In the **Supplementary Services** section, click **Yes** or click **No** to enable or to disable call recording in the **Call Recording Serv** field.

Step 3 (Optional) In the **Programmable Softkeys** section, to enable softkeys, add a string in this format in the **Connected Key List** and **Conferencing Key List** fields.

```
crdstart;crdstop;crdpause;crdresume
```

Step 4 In the phone web page, click the **Ext(n)** tab that requires call recording.

Step 5 In the **SIP Settings** section, in the **Call Recording Protocol**, select **SIPINFO** as the call recording protocol.

For details on **SIP Settings** fields, see SIP Settings, on page 277.

Step 6 Click **Submit All Changes**.

Set Up a Phone for Presence

Before you begin

- Set up the Broadsoft server for XMPP.

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 In the **Broadsoft XMPP** section, set the fields as described in Broadsoft XMPP, on page 269.

Step 3 Click **Submit All Changes**.

Set Up a Call Center Agent Phone

You can enable a phone with Automatic Call Distribution (ACD) features. This phone acts as a call center agent's phone and can be used to trace a customer call, to escalate any customer call to a supervisor in emergency, to categorize contact numbers using disposition codes, and to view customer call details.

Before you begin

- Set up the phone as a call center phone on the BroadSoft server.

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Ext(n)**.

Step 2 In the **ACD Settings** section, set up the fields as described in ACD Settings, on page 282.

Step 3   Click **Submit All Changes**.

Emergency Calls

Emergency Call Support Background

Emergency call service providers can register a phone's location for each IP-based phone in a company. The location information server (LIS) transfers the emergency response location (ERL) to the phone. The phone stores its location during registration, after the phone restarts, and when a person signs in to the phone. The location entry can specify the street address, building number, floor, room, and other office location information.

When you place an emergency call, the phone transfers the location to the call server. The call server forwards the call and the location to the emergency call service provider. The emergency call service provider forwards the call and a unique call-back number (ELIN) to the emergency services. The emergency service or public safety answering point (PSAP) receives the phone location. The PSAP also receives a number to call you back, if the call disconnects.

See for the terms used to describe emergency calls from the phone.

You insert the following parameters to obtain the phone's location for any phone extension number:

  • Company Identifier–A Unique number (UUID) assigned to your company by the NG9-1-1 service provider.

  • Primary Request URL–The HTTPS address of the primary server used to obtain the phone location.

  • Secondary Request URL–The HTTPS address of a secondary server (backup) used to obtain the phone location.

  • Emergency Number–A sequence of digits that identify an emergency call. You can specify multiple emergency numbers, by separating each emergency number with a comma.

    Common emergency service numbers include:

      • North America–911

      • European countries–112

      • Hong Kong–999

The phone requests new location information for the following activities:

  • You register the phone with the call server.

  • A person restarts the phone and the phone was previously registered with the call server.

  • A guest signs in to the phone.

  • You change the network interface used in the SIP registration. For example, change Wi-Fi to Ethernet.

  • You change the IP address of the phone.

If all of the location servers do not send a location response, the phone re-sends the location request every two minutes.

Emergency Call Support Terminology

The following terms describe emergency call support for the Cisco Multiplatform Phones.

- Emergency Location ID Number (ELIN)–A number used to represent one or more phone extensions that locate the person who dialed emergency services.

- Emergency Response Location (ERL)–A logical location that groups a set of phone extensions.

- HTTP Enabled Location Delivery (HELD)–An encrypted protocol that obtains the PIDF-LO location for a phone from a location information server (LIS).

- Location Information Server (LIS)–A server that responds to a SIP-based phone HELD request and provides the phone location using a HELD XML response.

- Emergency Call Service Provider–The company that responds to a phone HELD request with the phone's location. When you make an emergency call (which carries the phone's location), a call server routes the call to this company The emergency call service provider adds an ELIN and routes the call to the emergency services (PSAP). If the call is disconnected, the PSAP uses the ELIN to reconnect with the phone used to make the emergency call.

- Public Safety Answering Point (PSAP)–Any emergency service (for example, fire, police, or ambulance) joined to the Emergency Services IP Network.

- Universally Unique Identifier (UUID)–A 128-bit number used to uniquely identify a company using emergency call support.

Configure a Phone to Make Emergency Calls

Before you begin

- Obtain the E911 Geolocation Configuration URLs and the company identifier for the phone from your emergency call services provider. You can use the same Geolocation URLs and company identifier for multiple phone extensions in the same office area.

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Click the **Voice** > **Ext *n***, where *n* is the phone extension number (1-10) of the phone web dialog.
Step 2	In the **Dial Plan** area, set the **Emergency Number** to the digits that correspond to the customer emergency service numbers.
	To specify multiple emergency numbers, separate each emergency number with a comma.
Step 3	In the **E911 Geolocation Configuration** area, set the **Company UUID** to the unique customer identifier obtained from your emergency call service provider.
	For example:

```
07072db6-2dd5-4aa1-b2ff-6d588822dd46
```

Step 4   Specify the encrypted **Primary Request URL** to the main georedundant server. This location information server returns the location for this phone.

For example:

```
https://prod.blueearth.com/e911Locate/held/held_request.action
```

Step 5   Specify the encrypted **Secondary Request URL** for the backup server that can return location information.

For example:

```
https://prod2.blueearth.com/e911Locate/held/held_request.action
```

Step 6   Click **Submit All Changes**.

Configure the SIP Transport

For SIP messages, you can either specify the transport protocol of your choice, or, you can let the phone select the appropriate protocol automatically, for each extension.

When you set up automatic selection, the phone determines the transport protocol based on the Name Authority Pointer (NAPTR) records on the DNS server. The phone uses the protocol specified in the record that has the lowest order and preference. When there are multiple records with the same order and preference, the phone looks for a protocol within the records, in the following order of preference: 1. UDP, 2. TCP, and 3. TLS. The phone uses the first protocol that it finds, in that order of preference.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2   In the **SIP Settings** section, set the **SIP Transport** parameter as described in SIP Settings, on page 277.

Step 3   Click **Submit All Changes**.

Block Non-Proxy SIP Messages to a Phone

You can disable the ability of the phone to receive incoming SIP messages from a non-proxy server. When you enable this feature, the phone only accepts SIP messages from:

- proxy server
- outbound proxy server
- alternative proxy server

> • alternative outbound proxy server
>
> • IN-Dialog message from proxy server and non-proxy server. For example: Call Session dialog and Subscribe dialog

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **System**.
Step 2	In the **System Configuration** section, set the **Block Nonproxy SIP** field as described in the System Configuration, on page 222.
Step 3	Click **Submit All Changes**.

Configure a Privacy Header

A user privacy header in the SIP message sets user privacy needs from the trusted network.

You can set the user privacy header value for each line extension using the phone web page.

The privacy header options are:

> • Disabled (default)
>
> • none—The user requests that a privacy service applies no privacy functions to this SIP message.
>
> • header—The user needs a privacy service to obscure headers which cannot be purged of identifying information.
>
> • session—The user requests that a privacy service provide anonymity for the sessions.
>
> • user—The user requests a privacy level only by intermediaries.
>
> • id—The user requests that the system substitute an id that doesn't reveal the IP address or host name.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Extension**.
Step 2	In the **SIP Settings** section, set the **Privacy Header** field as described in the SIP Settings, on page 277.
Step 3	Click **Submit All Changes**.

Enable P-Early-Media Support

You can determine whether to include the P-Early-Media header in the SIP message of outgoing calls. The P-Early-Media header contains the status of the early media stream. If the status indicates that the network is blocking the early media stream, the phone plays the local ringback tone. Otherwise, the phone plays the early media while waiting for the call to be connected.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Voice** > **Ext (n)**.

Step 2 In the SIP Settings section, set the **P-Early-Media Support** field as described in SIP Settings, on page 277.

Step 3 Click **Submit All Changes**.

Peer Firmware Sharing

Peer Firmware Sharing (PFS) is a firmware distribution model which allows a Cisco IP phone to find other phones of the same model or series on the subnet and share updated firmware files when you need to upgrade multiple phones all at the same time. PFS uses Cisco Peer-to-Peer-Distribution Protocol (CPPDP) which is a Cisco proprietary protocol. With CPPDP, all the devices in the subnet form a peer-to-peer hierarchy, and then copy the firmware or the other files from peer devices to the neighboring devices. To optimize firmware upgrades, a root phone downloads the firmware image from the load server and then transfers the firmware to other phones on the subnet using TCP connections.

Peer firmware sharing:

- Limits congestion on TFTP transfers to centralized remove load servers.

- Eliminates the need to manually control firmware upgrades.

- Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously.

Note

- Peer firmware sharing does not function unless multiple phones are set to upgrade at the same time. When a NOTIFY is sent with Event:resync, it initiates a resync on the phone. Example of an xml that can contain the configurations to initiate the upgrade:

  "Event:resync;profile="http://10.77.10.141/profile.xml

- When you set the Peer Firmware Sharing Log server to an IP address and port, the PFS specific logs are sent to that server as UDP messages. This setting must be done on each phone. You can then use the log messages when troubleshooting issues related to PFS.

Peer_Firmware_Sharing_Log_Server specifies UDP Remote syslog server hostname and the port. The port defaults to the default syslog 514.

For example:

```
<Peer_Firmware_Sharing_Log_Server>192.168.5.5</ Peer_Firmware_Sharing_Log_Server>
```

To use this feature, enable PFS on the phones.

Enable Peer Firmware Sharing

You can enable Peer Firmware Sharing (PFS) when you want a phone to find other phones of the same model or series on the subnet and share updated firmware files. The phones are organized into a hierarchy and one of the phones in that hierarchy acts as a root phone. After the hierarchy formation, the root phone downloads the firmware image from the load server and then transfers the firmware to other phones in the hierarchy.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Provisioning**.

Step 2   In the **Firmware Upgrade** section, set the **Peer Firmware Sharing** and the **Peer Firmware Sharing Log Server** fields as described in Firmware Upgrade, on page 249.

Step 3   Click **Submit All Changes**.

Profile Authentication

Profile Authentication allows phone users to resynchronize the provisioning profile onto the phone. Authentication information is required while the phone tries to resynchronize and download configuration file for the first time and gets an HTTP or HTTPS 401 authentication error. When you enable this feature, the **Profile account setup** screen is displayed on the phone for the following situations:

- When the HTTP or HTTPs 401 authentication error occurs during first-time provisioning after the phone reboots

- When the profile account username and password are empty

- When there are no username and password in the Profile Rule

If the **Profile account setup** screen is missed or ignored, the user can also access the setup screen through the phone screen menu, or the **Setup** softkey, which displays only when no line on the phone is registered.

When you disable the feature, the **Profile account setup** screen doesn't display on the phone.

The username and password in the **Profile Rule** field have a higher priority than the profile account.

- When you provide a correct URL in the **Profile Rule** field without a username and password, the phone requires authentication or digest to resynchronize the profile. With the correct profile account, authentication passes. With an incorrect profile account, authentication fails.

- When you provide a correct URL in the **Profile Rule** field with a correct username and password, the phone requires authentication or digest to resynchronize the profile. The profile account is not used for phone resynchronization. Sign-in is successful.

- When you provide a correct URL in the **Profile Rule** field with an incorrect username and password, the phone requires authentication or digest to resynchronize the profile. The profile account isn't used for phone resynchronization. Sign-in always fails.

- When you provide an incorrect URL in the **Profile Rule** field, sign-in always fails.

Specify the Profile Authentication Type

You can specify the profile authentication type from the phone administration web page.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Provisioning**.

Step 2   In the **Configuration Profile** section, set the **Profile Authentication Type** field as described in the .

Step 3   Click **Submit All Changes**.

Add Ignore Programmable Soft Key to Silence an Incoming Call

You can add the **Ignore** softkey on the phone. User can press this softkey to silence an incoming call when busy and don't want to be disturbed. When the user presses the softkey, the phone stops ringing, but the user gets a visual alert, and, can answer the phone call.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.

Step 3   Enter the following values in the **Ringing Key List** field:

```
answer|1;ignore|2;ignoresilent|3;
```

Step 4   Click **Submit All Changes**.

Enable BroadWorks Anywhere

You can configure a phone to allow a call to seamlessly be moved from one desk phone(location) to another mobile phone or desk phone(location).

When you enable this feature, the **Anywhere** menu is added into the phone screen. The user can use this menu to add multiple phones as locations to the extension. When there is an incoming call in that extension, all the added phones will ring and the user can answer the incoming call from any location. The locations list also gets saved to the BroadWorks XSI server.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Ext(n)**.

Step 2   In the **XSI Line Service** section, set the **XSI Host Server**, **XSI Authentication Type**, **Login User ID**, **Login Password**, and **Anywhere Enable** field as described in the XSI Line Service, on page 287.

If you select **SIP Credentials** for **XSI Authentication Type**, you need to enter subsriber **Auth ID** and **Password** in the **Subscriber Information** section.

Step 3   Click **Submit All Changes**.

Sync the Block Caller ID Feature with the Phone and the BroadWords XSI Server

You can sync the **Block caller id** status on the phone and the **Line ID Blocking** status on the BroadWorks XSI server. When you enable the synchronization, the changes that the user makes in the **Block caller id** settings also changes the BroadWorks server settings.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Voice** > **Ext(n)**.

Step 2   In the **XSI Line Service** section, set the **Block CID Enable** field as described in the XSI Line Service, on page 287.

Step 3   Click **Submit All Changes**.

Enable Viewing BroadWorks XSI Call Logs on a Line

You can configure a phone to display recent call logs from either the BroadWorks server or the local phone. After you enable the feature, the Recents screen has a **Display recents from** menu and the user can choose the XSI call logs or the local call logs.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **XSI Phone Service** section, set the **XSI Host Server**, **XSI Authentication Type**, **Login User ID**, **Login Password**, and **Directory Enable** fields as described in .

If you select **SIP Credentials** for **XSI Authentication Type**, you need to enter **SIP Auth ID** and **SIP Password** in this section.

Step 3   Set the **CallLog Associated Line** and **Display Recents From** fields as described in .

Note   The **Display recents from** menu doesn't appear in the **Recents** phone screen when you set the value of the **CallLog Enable** field to **No**,

Step 4   Click **Submit All Changes**.

DND and Call Forwarding Status Sync

You can configure the settings on the phone administration web page to enable status synchronization of do not disturb (DND) and call forwarding between the phone and the server.

There are two ways to synchronize the feature status:

- Feature Key Synchronization (FKS)
- XSI Synchronization

FKS uses SIP messages to communicate the feature status. XSI Synchronization uses HTTP messages. If both FKS and XSI synchronization are enabled, FKS takes precedent over XSI synchronization. See the table below for how FKS interacts with XSI synchronization.

Table 20: Interaction Between FKS and XSI Synchronization

Feature Key Sync	DND Enabled	CFWD Enabled	DND Sync	CFWD Sync
Yes	Yes	Yes	Yes (SIP)	Yes (SIP)

Feature Key Sync	DND Enabled	CFWD Enabled	DND Sync	CFWD Sync
Yes	No	No	Yes (SIP)	Yes (SIP)
Yes	No	Yes	Yes (SIP)	Yes (SIP)
Yes	No	No	Yes (SIP)	Yes (SIP)
No	Yes	Yes	Yes (HTTP)	Yes (HTTP)
No	No	Yes	No	Yes (HTTP)
No	Yes	No	Yes (HTTP)	No
No	No	No	No	No

If a line key is configured with FKS or XSI synchronization and is also enabled with DND or call forwarding, the respective DND ⊘ icon or the call forwarding ⌣ icon is displayed next to the line key label. If the line key has a missed call, a voice message, or an urgent voicemail alert, the DND icon or the call forwarding icon is also displayed with the alert notification.

Related Topics

Enable Feature Key Sync, on page 193

Enable Call Forwarding Status Sync via XSI Service, on page 194

Enable DND Status Sync via XSI Service, on page 194

Enable Feature Key Sync

When you enable the Feature Key Synchronization (FKS), the settings of call forwarding and do not disturb (DND) on the server are synchronized to the phone. The changes in DND and call forwarding settings made on the phone will also be synchronized to the server.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Voice** > **Ext [n]** (where [n] is the extension number).
Step 2	In the **Call Feature Settings** section, set the **Feature Key Sync** field to **Yes**.
Step 3	Click **Submit All Changes**.

Related Topics

DND and Call Forwarding Status Sync, on page 192

Enable Call Forwarding Status Sync via XSI Service, on page 194

Enable DND Status Sync via XSI Service, on page 194

Enable Call Forwarding Status Sync via XSI Service

When call forwarding sync is enabled, the settings related to call forwarding on the server are synchronized to the phone. The changes in call forwarding settings made on the phone will also be synchronized to the server.

Note   If XSI sync for call forwarding is enabled and the XSI host server or XSI account is not configured correctly, the phone user can't forward calls on the phone.

Before you begin

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

- Configure the XSI host server and the corresponding credentials on the **Voice** > **Ext (n)** tab.

  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.

  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.

- Disable Feature Key Sync (FKS) in **Call Feature Settings** section from **Voice** > **Ext (n)** .

Procedure

Step 1   Select **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2   Set the **CFWD Enable** field to **Yes**.

Step 3   Click **Submit All Changes**.

Related Topics
DND and Call Forwarding Status Sync, on page 192
Enable Feature Key Sync, on page 193

Enable DND Status Sync via XSI Service

When do not disturb (DND) sync is enabled, the DND setting on the server is synchronized to the phone. The changes in DND setting made on the phone will also be synchronized to the server.

Note   If XSI sync for DND is enabled and the XSI host server or XSI account is not configured correctly, the phone user can't turn on DND mode on the phone.

Before you begin

- Access the phone administration web page. See Access the Phone Web Page, on page 92.

- Configure the XSI host server and the corresponding credentials on the **Voice** > **Ext (n)** tab.

  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.

  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.

- Disable Feature Key Synchronization (FKS) in **Call Feature Settings** section from **Voice** > **Ext (n)**.

Procedure

Step 1	Select **Voice** > **Ext [n]** (where [n] is the extension number).
Step 2	Set the **DND Enable** field to **Yes**.
Step 3	Click **Submit All Changes**.

Related Topics

DND and Call Forwarding Status Sync, on page 192
Enable Feature Key Sync, on page 193

Capture Packets

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1	Select **Info** > **Debug Info**.
Step 2	In the **Problem Report Tool** section, click the **Start Packet Capture** button in the **Packet Capture** field.
Step 3	Choose **Al** to capture all packets that the phone receives and select **Host IP Address** to capture packets only when source or destination is the IP address of the phone.
Step 4	Make phone calls to and from the selected phone.
Step 5	When you want to stop the packet capture, click **Stop Packet Capture**.
Step 6	Click **Submit**. You see a file in the **Capture File** field. This file contains the filtered packets.

Factory Reset the Phone with the Web UI Button

You can factory reset the phone from the phone web page. The reset only happens if the phone is idle. If the phone is not idle, the phone web page shows a message that the phone is busy and that you need to try again.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1   Select **Admin Login** > **advanced** > **Info** > **Debug Info**.

Step 2   In the **Factory Reset** section, click **Factory Reset**.

Step 3   Click **Confirm factory reset**.

CHAPTER 11

Corporate and Personal Directory Setup

Personal Directory Setup

The Personal Directory allows a user to store a set of personal numbers.

Personal Directory consists of the following feature:

- Personal Address Book (PAB)

Users can use these methods to access Personal Directory features:

- From a web browser—Users can access the PAB and Speed Dials features from the Configuration Utility web page.

- From the Cisco IP Phone—Choose Contacts to search the corporate directory or the user personal directory.

To configure Personal Directory from a web browser, users must access their Configuration Utility. You must provide users with a URL and sign-in information.

LDAP Configuration

The Cisco IP Phone supports Lightweight Directory Access Protocol (LDAP) v3. LDAP Corporate Directory Search allows a user to search a specified LDAP directory for a name, phone number, or both. LDAP-based directories, such as Microsoft Active Directory 2003 and OpenLDAP-based databases, are supported.

Users access LDAP from the **Directory** menu on their IP phone. An LDAP search returns up to 20 records.

The instructions in this section assume that you have the following equipment and services:

- An LDAP server, such as OpenLDAP or Microsoft Active Directory Server 2003.

Prepare the LDAP Corporate Directory Search

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 In the **IPv4 Settings** section, in the **Primary DNS** field, enter the IP address of the DNS server.

This step is required only if you are using Active Directory with authentication set to MD5.

Step 3 In the **Optional Network Configuration** section, in the **Domain** field, enter the LDAP domain.

This step is required only if you are using Active Directory with authentication set to MD5.

Some sites might not deploy DNS internally and instead use Active Directory 2003. In this case, it is not necessary to enter a Primary DNS address and an LDAP Domain. However, with Active Directory 2003, the authentication method is restricted to Simple.

Step 4 Click the **Phone** tab.

Step 5 In the **LDAP** section, use the **LDAP Dir Enable** drop-down list box to choose **Yes**.

This action enables LDAP and causes the name that is defined in the **Corp Dir Name** field to appear in the phone directory.

Step 6 Configure the LDAP fields as described in LDAP, on page 271 .

Step 7 Click **Submit All Changes**.

Configure BroadSoft Settings

The BroadSoft directory service enables users to search and view their personal, group, or enterprise contacts. This application feature uses BroadSoft's Extended Services Interface (XSI).

To improve security, the phone firmware places access restrictions on the host server and directory name entry fields.

The phone uses two types of XSI authentication methods:

- User login credentials: The phone uses the XSI user id and password.

- SIP credentials: The register name and password of the SIP account registered on the phone. For this method, the phone can use the XSI user ID along with the SIP authentication credentials for the authentication.

Procedure

Step 1 In the phone web page, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 In the **XSI Service** section, choose **Yes** from the **Directory Enable** drop down list box.

Step 3 Set up the fields as described in XSI Phone Service, on page 268.

Step 4   Click **Submit All Changes**.

Configure the XML Directory Service

Procedure

Step 1   In the Phone Web page, click **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2   In the **XML Directory Service Name** field, enter the name of XML directory.

Step 3   In the **XML Directory Service URL** field, enter the url where XML directory is located.

Step 4   In the **XML User Name** field, enter the username of XML service.

Step 5   In the **XML Password** field, enter the password of XML service.

Step 6   Click **Submit All Changes**.

PART V

Phone Troubleshooting

Monitoring Phone Systems

Monitoring Phone Systems Overview

You can view a variety of information about the phone using the phone status menu on the phone and the phone web pages. This information includes:

• Device information

• Network setup information

• Network statistics

• Device logs

• Streaming statistics

This chapter describes the information that you can obtain from the phone web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

Include a Device Identifier in Uploaded Syslog Messages

You can choose to include a device identifier in syslog messages that are uploaded to the syslog server. While the IP address of a phone may change over time, the device identifier does not change. This can ease the process of identifying the source of each message in a stream of incoming messages from multiple phones. The device identifier appears after the timestamp in each message.

Before you begin

Configure a syslog sever for the phone to upload syslog messages. See **Syslog Server** in Optional Network Configuration, on page 225 for details.

Procedure

Step 1 On the phone administration web page, go to **Voice** > **System** > **Optional Network Configuration**.

Step 2 Configure the **Syslog Identifier** parameter as described in .

Cisco IP Phone Status

The following sections describes how to view model information, status messages, and network statistics on the Cisco IP Phone.

- Model Information: Displays hardware and software information about the phone.

- Status menu: Provides access to screens that display the status messages, network statistics, and statistics for the current call.

You can use the information that displays on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone web page.

Display the Phone Information Window

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Status** > **Product Information**.

If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.

Step 3 To exit the Model Information screen, press **Back**.

View the Phone Status

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Status** > **Phone Status** > **Phone Status**.

You can view the following information:

- **Elapsed time**—Total time elapsed since the last reboot of the system

- **Tx (Packets)**—Transmitted packets from the phone.

- **Rx (Packets)**—Received packets from the phone.

View the Status Messages on the Phone

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Status** > **Status messages**.

You can view a log of the various phone statuses since provisioning was last done.

Note Status messages reflect UTC time and are not affected by the timezone settings on the phone.

Step 3 Press **Back**.

View the Network Status

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Status** > **Network Status**.

You can view the following information:

- **Network type**—Indicates the type of Local Area Netwrok (LAN) connection that the phone uses.

- **Network status**—Indicates if the phone is connected to a network.

- **IPv4 status**—IP address of the phone. You can see information on IP address, Addressing type, IP status, Subnet mask, Default router, Domain Name Server (DNS) 1, DNS 2 of the phone.

- **IPv6 status** —IP address of the phone. You can see information on IP address, Addressing type, IP status, Subnet mask, Default router, Domain Name Server (DNS) 1, DNS 2 of the phone.

- **VLAN ID**—VLAN ID of the phone.

- **MAC address**—Unique Media Access Control (MAC) address of the phone.

- **Host name**—Displays the current host name assigned to the phone.

- **Domain**—Displays the network domain name of the phone. Default: cisco.com

- **Switch port link**—Status of the switch port.

- **Switch port config**—Indicates speed and duplex of the network port.

- **PC port config**—Indicates speed and duplex of the PC port.

- **PC port link**—Indicates speed and duplex of the PC port.

Display Call Statistics Window

You can access the Call Statistics screen on the phone to display counters, statistics, and voice-quality metrics of the most recent call.

Note You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics that are not available on the phone.

A single call can use multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

To display the Call Statistics screen for information about the latest voice stream, follow these steps:

Procedure

Step 1	Press **Applications** ⚙.
Step 2	Select **Status** > **Phone Status** > **Call Statistics**.
Step 3	Press **Back**.

Call Statistics Fields

The following table describes the items on the Call Statistics screen.

Table 21: Call Statistics Items for the Cisco IP Phone

Item	Description
Receiver Codec	Type of received voice stream (RTP streaming audio from codec): • G.729 • G.722 • G.711 mu-law • G.711 A-law • OPUS • iLBC
Sender Codec	Type of transmitted voice stream (RTP streaming audio from codec): • G.729 • G.722 • G.711 mu-law • G.711 A-law • OPUS • iLBC
Receiver Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets that were received since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP voice packets that were transmitted since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were transmitted since the call began because the call might have been placed on hold.

Item	Description
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, that was observed since the receiving voice stream opened.
Max Jitter	Maximum jitter, in milliseconds, that was observed since the receiving voice stream opened.
Receiver Discarded	Number of RTP packets in the receiving voice stream that were discarded (bad packets, too late, and so on). **Note** The phone discards payload type 19 comfort noise packets that Cisco Gateways generate, because they increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice-Quality Metrics	
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Seconds	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Seconds	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

View the Customization State in the Configuration Utility

After the RC download from the EDOS server completes, you can view the customization state of a phone using the web interface.

Here are the descriptions of the remote customization states:

- Open—The phone has booted for the first time and is not configured.

- Aborted—Remote customization is aborted due to other Provisioning like DHCP options.

- Pending—The profile has been downloaded from the EDOS server.

- Custom-Pending—The phone has downloaded a redirect URL from the EDOS server.

- Acquired—In the profile downloaded from the EDOS server, there is a redirect URL for provision configuration. If the redirect URL download from the provisioning server is successful, this state is displayed.

- Unavailable—Remote customization has stopped because the EDOS server responded with an empty provisioning file and the HTTP response was `200 OK`.

Procedure

Step 1 On the Phone Web page, select **Admin Login** > **Info** > **Status**.

Step 2 In the **Product Information** section, you can view the customization state of the phone in the **Customization** field.

If any provisioning is failing, you can view the details in the **Provisioning Status** section on the same page.

Cisco IP Phone Web Page

This section describes the information that you can obtain from the phone web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

Related Topics

Info

The fields on this tab are read-only and cannot be edited.

Status

System Information

Parameter	Description
Host Name	Displays the current host name assigned to the phone.
Domain	Displays the network domain name of the phone. Default: cisco.com

Parameter	Description
Primary NTP Server	Displays the primary NTP server assigned to the phone.
Secondary NTP Server	Displays the secondary NTP server assigned to the phone.

IPv4 Information

Parameter	Description
IP Status	Indicates that the connection is established.
Connection Type	Indicates the type of internet connection for the phone: • DHCP • Static IP
Current IP	Displays the current IP address assigned to the IP phone.
Current Netmask	Displays the network mask assigned to the phone.
Current Gateway	Displays the default router assigned to the phone.
Primary DNS	Displays the primary DNS server assigned to the phone.
Secondary DNS	Displays the secondary DNS server assigned to the phone.

IPv6 Information

Parameter	Description
IP Status	Indicates that the connection is established.
Connection Type	Indicates the type of internet connection for the phone: • Static IP • DHCP
Current IP	Displays the current IPv6 address assigned to the IP phone.
Prefix Length	Identifies number of bits of a global unicast IPv6 address that are part of the network. For example, if the IPv6 address is 2001:0DB8:0000:000b::/64, the number 64 identifies that the first 64 bits are part of the network.

Parameter	Description
Current Gateway	Displays the default router assigned to the phone.
Primary DNS	Displays the primary DNS server assigned to the phone.
Secondary DNS	Displays the secondary DNS server assigned to the phone.

Reboot History

For information about reboot history, see Reboot Reasons, on page 324.

Product Information

Parameter	Description
Product Name	Name that represents the Cisco IP phone.
Software Version	Version number of the phone firmware.
MAC Address	Hardware address of the phone.
Customization	For an RC unit, this field indicates whether the unit has been customized or not. Pending indicates a new RC unit that is ready for provisioning. If the unit has already retrieved its customized profile, this field displays the name of the company that provisioned the unit.
Serial Number	Serial number of the phone.
Hardware Version	Version number of the phone hardware.
Client Certificate	Status of the client certificate, which authenticates the phone for use in the ITSP network. This field indicates if the client certificate is properly installed in the phone.

Downloaded Locale Package

Parameter	Description
Locale download status	Displays the downloaded locale package status.
Locale download URL	Displays the location from where the local package is downloaded.
Font download status	Displays the downloaded font file status.
Font download URL	Displays the location from where the font file is downloaded.

Phone Status

Parameter	Description
Current Time	Current date and time of the system; for example, 08/06/14 1:42:56 a.m.
Elapsed Time	Total time elapsed since the last reboot of the system; for example, 7 days, 02:13:02.
SIP Messages Sent	Total number of SIP messages sent (including retransmissions).
SIP Bytes Sent	Total number of SIP messages received (including retransmissions).
SIP Messages Recv	Total number of bytes of SIP messages sent which includes retransmissions.
SIP Bytes Recv	Total number of bytes of SIP messages received (including retransmissions).
Network Packets Sent	Total number of network packets sent.
Network Packets Recv	Total number of network packets received.
External IP	External IP of the phone.
Operational VLAN ID	ID of the VLAN currently in use if applicable.
SW Port	Displays the type of Ethernet connection from the IP phone to the switch.
PC Port	Displays the type of Ethernet connection from PC Port.
Upgrade Status	Displays status of the last phone upgrade.
SW Port Config	Displays the type of SW port configuration.
PC Port Config	Displays the type of PC port configuration.
Last Successful Login	Displays the time when the phone has last successful log in.
Last Failed Login	Displays the time when the phone has last failed log in.

Dot1x Authentication

Parameter	Description
Transaction status	Indicates if the phone is authenticated.
Protocol	Displays the protocol of the registered phone.

Ext Status

Parameter	Description
Registration State	Shows "Registered" if the phone is registered, or "Not Registered" if the phone is not registered to the ITSP.
Last Registration At	Last date and time the line was registered.
Next Registration In Seconds	Number of seconds before the next registration renewal.
Message Waiting	Indicates whether message waiting is enabled or disabled.
Mapped SIP Port	Port number of the SIP port mapped by NAT.
Hoteling State	Indicates whether Hoteling is enabled or disabled.
Extended Function Status	Indicates whether extended function is enabled.

Line Call Status

Parameter	Description
Call State	Status of the call.
Tone	Type of tone that the call uses.
Encoder	Codec used for encoding.
Decoder	Codec used for decoding.
Type	Direction of the call.
Remote Hold	Indicates whether the far end placed the call on hold.
Callback	Indicates whether the call was triggered by a call back request.
Mapped RTP Port	The port mapped for Real Time Protocol traffic for the call.
Peer Name	Name of the internal phone.
Peer Phone	Phone number of the internal phone.
Duration	Duration of the call.
Packets Sent	Number of packets sent.
Packets Recv	Number of packets received.
Bytes Sent	Number of bytes sent.
Bytes Recv	Number of bytes received.

Parameter	Description
Decode Latency	Number of milliseconds for decoder latency.
Jitter	Number of milliseconds for receiver jitter.
Round Trip Delay	Number of milliseconds for delay in the RTP-to-RTP interface round trip.
Packets Lost	Number of packets lost.
Loss Rate	The fraction of RTP data packets from the source lost since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Packet Discarded	The fraction of RTP data packets from the source lost since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Discard Rate	The fraction of RTP data packets from the source that have been discarded since the beginning of reception, due to late or early arrival, under-run or overflow at the receiving jitter buffer. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Burst Duration	The mean duration, expressed in milliseconds, of the burst periods that have occurred since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Gap Duration	The mean duration, expressed in milliseconds, of the gap periods that have occurred since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
R-Factor	Voice quality metric that describes the segment of the call that is carried over this RTP session. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-LQ	The estimated mean opinion score for listening quality (MOS-LQ) is a voice quality metric on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-CQ	The estimated mean opinion score for conversational quality (MOS-CQ) is defined as including the effects of delay and other effects that affect conversational quality. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).

Paging Status

Parameter	Description
Multicast Rx Pkts	Indicates Rx packets during a multicast paging.
Multicast Tx Pkts	Indicates Tx packets during a multicast paging.

TR-069 Status

Parameter	Description
TR-069 Feature	Indicates if TR-069 function is enabled or disabled.
Periodic Inform Time	Displays the inform time interval from CPE to ACS.
Last Inform Time	Indicates the last inform time.
Last Transaction Status	Displays the success or the failure status.
Last Session	Indicates the start and end time of the session.
ParameterKey	Displays the key for reference checkpoint for parameter set configured.

PRT Status

Parameter	Description
PRT Generation Status	The location of initiation and status of generation of the most recently initiated problem report. Problem reports may be initiated from the phone LCD user interface, from the phone administration web page, or remotely. See Report All Phone Issues from the Phone Web Page, on page 315 and Report a Phone Problem Remotely, on page 316 for details. XML tag in `status.xml`: `PRT_Generation_Status`
PRT Upload Status	The status of upload of the most recently initiated problem report. See Configure PRT Upload, on page 177 for information on configuring an upload rule for problem reports. XML tag in `status.xml`: `PRT_Upload_Status`

Debug Info

Console Logs

Displays the syslog output of the phone in the reverse order, where messages is the latest one. The display includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone and the time stamp reflects UTC time, regardless of the time zone settings.

Parameter	Description
Debug Message	Displays debug messages when you click **messages** link.

Problem Reports

Parameter	Description
Report Problem	Displays the tab Generate PRT.
Prt file	Displays the file name of the PRT logs.
Packet Capture	Displays the tab **Start Packet Capture**. Click this tab to initiate capture packets. Click **All** to capture all packets that the phone receives or click **Host IP Address** to capture packets only when src/dest is the IP address of the phone. You can also stop the capture process after initiating it.
Capture File	Displays the file that contains the captured packets. Download the file to see the packet details.

Factory Reset

Parameter	Description
Factory Reset	Resets the phone when you click **Factory Reset** tab when the phone is idle.

Download Status

Firmware Upgrade Status

Parameter	Description
Firmware Upgrade Status 1	Displays the upgrade status (failed or succeeded) with reason for the same.
Firmware Upgrade Status 2	
Firmware Upgrade Status 3	

Provisioning Status

Parameter	Description
Provisioning Status 1	Displays the provisioning status (resync) of the phone.
Provisioning Status 2	
Provisioning Status 3	

Custom CA Status

Parameter	Description
Custom CA Provisioning Status	Indicates whether provisioning using a custom CA succeeded or failed: • Last provisioning succeeded on mm/dd/yyyy HH:MM:SS; • Last provisioning failed on mm/dd/yyyy HH:MM:SS
Custom CA Info	Displays information about the custom CA: • Installed—Displays the "CN Value", where "CN Value" is the value of the CN parameter for the Subject field in the first certificate. • Not Installed—Displays if no custom CA certificate is installed.

Network Statistics

Ethernet Information

Parameter	Description
TxFrames	Total number of packets that the phone transmitted.
TxBroadcasts	Total number of broadcast packets that the phone transmitted.
TxMulticasts	Total number of multicast packets that the phone transmitted.
TxUnicasts	Total number of unicast packets that the phone transmitted.
RxFrames	Total number of packets received by the phone.
RxBroadcasts	Total number of broadcast packets that the phone received.

Parameter	Description
RxMulticasts	Total number of multicast packets that the phone received.
RxUnicasts	Total number of unicast packets that the phone received.

Network Port Information

Parameter	Description
RxtotalPkt	Total number of packets that the phone received.
Rxunicast	Total number of unicast packets that the phone received.
Rxbroadcast	Total number of broadcast packets that the phone received.
Rxmulticast	Total number of multicast packets that the phone received.
RxDropPkts	Total number of packets dropped.
RxUndersizePkts	The total number of packets received that are less than 64 octets long, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxOversizePkts	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxJabbers	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but incudes FCS octets, and do not end with an even number of octets (alignment error), or had an FCS error.
RxAlignErr	Total number of packets between 64 and 1522 bytes in length that were received and that had a bad Frame Check Sequence (FCS).
Rxsize64	Total number of received packets, including bad packets, that were between 0 and 64 bytes in size.
Rxsize65to127	Total number of received packets, including bad packets, that were between 65 and 127 bytes in size.
Rxsize128to255	Total number of received packets, including bad packets, that were between 128 and 255 bytes in size.
Rxsize256to511	Total number of received packets, including bad packets, that were between 256 and 511 bytes in size.

Parameter	Description
Rxsize512to1023	Total number of received packets, including bad packets, that were between 512 and 1023 bytes in size.
Rxsize1024to1518	Total number of received packets, including bad packets, that were between 1024 and 1518 bytes in size.
TxtotalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
lldpFramesOutTotal	Total number of LLDP frames that the phone sent out.
lldpAgeoutsTotal	Total number of LLDP frames that timed out in the cache.
lldpFramesDiscardedTotal	Total number of LLDP frames that were discarded when any of the mandatory TLVs is missing, out of order, or contains out of range string length.
lldpFramesInErrorsTotal	Total number of LLDP frames that were received with one or more detectable errors.
lldpFramesInTotal	Total number of LLDP frames that the phone received.
lldpTLVDiscardedTotal	Total number of LLDP TLVs that were discarded.
lldpTLVUnrecognizedTotal	Total number of LLDP TLVs that were not recognized on the phone.
CDPNeighborDeviceId	Identifier of a device connected to this port that CDP discovered.
CDPNeighborIP	IP address of the neighbor device discovered that CDP discovered.
CDPNeighborIPv6	IPV6 address of the neighbor device discovered that CDP discovered.
CDPNeighborPort	Neighbor device port to which the phone is connected discovered by CDP.
LLDPNeighborDeviceId	Identifier of a device connected to this port discovered by LLDP discovered.
LLDPNeighborIP	IP address of the neighbor device that LLDP discovered.
LLDPNeighborIPv6	IPV6 address of the neighbor device that LLDP discovered.
LLDPNeighborPort	Neighbor device port to which the phone connects that LLDP discovered.

Parameter	Description
PortSpeed	Speed and duplex information.

Access Port Information

Parameter	Description
RxtotalPkt	Total number of packets that the phone received.
Rxunicast	Total number of unicast packets that the phone received.
Rxbroadcast	Total number of broadcast packets that the phone received.
Rxmulticast	Total number of multicast packets that the phone received.
RxDropPkts	Total number of packets dropped.
RxUndersizePkts	The total number of packets received that are less than 64 octets long, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxOversizePkts	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxJabbers	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but incudes FCS octets, and do not end with an even number of octets (alignment error), or had an FCS error.
RxAlignErr	Total number of packets between 64 and 1522 bytes in length that were received and that had a bad Frame Check Sequence (FCS).
Rxsize64	Total number of received packets, including bad packets, that were between 0 and 64 bytes in size.
Rxsize65to127	Total number of received packets, including bad packets, that were between 65 and 127 bytes in size.
Rxsize128to255	Total number of received packets, including bad packets, that were between 128 and 255 bytes in size.
Rxsize256to511	Total number of received packets, including bad packets, that were between 256 and 511 bytes in size.
Rxsize512to1023	Total number of received packets, including bad packets, that were between 512 and 1023 bytes in size.

Parameter	Description
Rxsize1024to1518	Total number of received packets, including bad packets, that were between 1024 and 1518 bytes in size.
TxtotalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
lldpFramesOutTotal	Total number of LLDP frames that the phone sent out.
lldpAgeoutsTotal	Total number of LLDP frames that timed out in the cache.
lldpFramesDiscardedTotal	Total number of LLDP frames that were discarded when any of the mandatory TLVs is missing, out of order, or contains out of range string length.
lldpFramesInErrorsTotal	Total number of LLDP frames that were received with one or more detectable errors.
lldpFramesInTotal	Total number of LLDP frames that the phone received.
lldpTLVDiscardedTotal	Total number of LLDP TLVs that were discarded.
lldpTLVUnrecognizedTotal	Total number of LLDP TLVs that were not recognized on the phone.
CDPNeighborDeviceId	Identifier of a device connected to this port that CDP discovered.
CDPNeighborIP	IP address of the neighbor device discovered that CDP discovered.
CDPNeighborIPv6	IPV6 address of the neighbor device discovered that CDP discovered.
CDPNeighborPort	Neighbor device port to which the phone is connected discovered by CDP.
LLDPNeighborDeviceId	Identifier of a device connected to this port discovered by LLDP discovered.
LLDPNeighborIP	IP address of the neighbor device that LLDP discovered.
LLDPNeighborIPv6	IPV6 address of the neighbor device that LLDP discovered.
LLDPNeighborPort	Neighbor device port to which the phone connects that LLDP discovered.
PortSpeed	Speed and duplex information.

Voice

System

System Configuration

Parameter	Description
Restricted Access Domains	This feature is used when implementing software customization.
Enable Web Server	Enable/disable web server of the IP phone. Default: Yes
Enable Protocol	Choose the type of protocol: • Http • Https If you specify the HTTPS protocol, you must include **https:** in the URL. Default: Http
Enable Direct Action Url	Enables the direct action of the URL. Default: Yes
Session Max Timeout	Allows you to enter maximum timeout of the session. Default: 3600
Session Idle Timeout	Allows you to enter idle timeout of the session. Default: 3600
Web Server Port	Allows you to enter port number of the phone web user interface. Default: 80 • 80 for protocol HTTP. • 443 for protocol HTTPS. If you specify a port number other than the default value for that protocol, you must include the nondefault port number in the server URL. Example: **https://192.0.2.1:999/admin/advanced**
Enable Web Admin Access	Allows you to enable or disable local access to the phone web user interface. Select Yes or No from the drop-down menu. Default: Yes

Parameter	Description
Admin Password	Allows you to enter password for the administrator. Default: Blank
User Password	Allows you to enter password for the user. Default: Blank
Phone-UI-readonly	Allows you to make the phone menus and options that the phone users see as read-only fields. Default: No
Phone-UI-User-Mode	Allows you to restrict the menus and options that phone users see when they use the phone interface. Choose yes to enable this parameter and restrict access. Default: No Specific parameters are then designated as "na", "ro", or "rw" using provisioning files. Parameters designated as "na" don't appear on the phone screen. Parameters designated as "ro" aren't editable by the user. Parameters designated as "rw" are editable by the user.
Block Nonproxy SIP	Enables or disables the phone receiving SIP messages from non-proxy server. If you choose **Yes**, the phone blocks any incoming non-proxy SIP messages except IN-dialog message. If you choose **No**, the phone does not block any incoming non-proxy SIP messages. Set **Block Nonproxy SIP** to No for phones that use TCP or TLS to transport SIP messages. Nonproxy SIP messages transported over TCP or TLS are blocked by default. Default: No

Network Settings

Parameter	Description
IP Mode	Allows you to select the internet protocol mode in which the phone operates. Options are: IPv4 Only, IPv6 Only, and Dual Mode. In dual mode, the phone can have both IPv4 and IPv6 addresses. Default: Dual Mode

IPv4 Settings

Parameter	Description
Connection Type	Internet connection type that is configured for the phone. Options are DHCP and Static IP. Default: DHCP
NetMask	Subnet mask of the phone.
Static IP	IP address of the phone.
Gateway	IP address of the gateway.
Primary DNS	Primary Domain Name Server (DNS) assigned to the phone.
Secondary DNS	Secondary Domain Name Server (DNS) if assigned to the phone.

IPv6 Settings

Parameter	Description
Connection Type	Internet connection type that is configured for the phone. Options are DHCP and Static IP. Default: DHCP
Static IP	IPv6 address of the phone.
Prefix Length	Identifies number of bits of a global unicast IPv6 address that are part of the network. For example, if the IPv6 address is 2001:0DB8:0000:000b::/64, the number 64 identifies that the first 64 bits are part of the network.
Gateway	IP address of the gateway.
Primary DNS	Primary Domain Name Server (DNS) assigned to the phone.
Secondary DNS	Secondary Domain Name Server (DNS) if assigned to the phone.
Broadcast Echo	Options are Disabled and Enabled. Default: Disabled
Auto Config	When enabled, phone generates an IPv6 address by default with the prefix length sent from the router. Options are Disabled and Enabled. Default: Enabled

802.1X Authentication

Parameter	Description
Enable 802.1X Authentication	Enables/disables 802.1X Default: No

Optional Network Configuration

Parameter	Description
Host Name	The hostname of the Cisco IP Phone.
Domain	The network domain of the Cisco IP Phone. If you are using LDAP, see LDAP Configuration, on page 197.
DNS Server Order	Specifies the method for selecting the DNS server: • Manual, DHCP • Manual • DHCP,Manual
DNS Query Mode	Specified mode of DNS query. • Parallel • Sequential
DNS Caching Enable	When set to Yes, the DNS query results are not cached. Default: Yes
Switch Port Config	Allows you to select speed and duplex of the network port. Values are: • Auto • 10MB half • 10MB full • 100 MB half • 100MB full • 100 half • 1000 full

Parameter	Description
PC Port Config	Allows you to select Speed and duplex of the Computer (access) port. • Auto • 10MB half • 10MB full • 100 MB half • 100MB full • 100 half • 1000 full
PC PORT Enable	Specifies if PC port is enabled. Options are Yes or No.
Enable PC Port Mirror	Adds the ability to port mirror on the PC port. When enabled, you can see the packets on the phone. Select **Yes** to enable PC port mirroring and select **No** to disable it.
Syslog Server	Specify the syslog server name and port. This feature specifies the server for logging IP phone system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.

Parameter	Description
Syslog Identifier	Select the device identifier to include in syslog messages that are uploaded to the syslog server. The device identifier appears after the timestamp in each message. • None: No device identifier. • $MA: The MAC address of the phone, expressed as continuous lower case letters and digits. Example: `c4b9cd811e29` • $MAU: The MAC address of the phone, expressed as continuous upper case letters and digits. Example: `C4B9CD811E29` • $MAC: The MAC address of the phone in the standard colon-separated format. Example: `c4:b9:cd:81:1e:29` • $SN: The product serial number of the phone. Default: None Example XML configuration: `<Syslog_Identifier ua="na">$MAC</Syslog_Identifier>`
Debug Level	The debug level from 0 to 2. The higher the level, the more debug information is generated. Zero (0) means that no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Default: 0
Primary NTP Server	IP address or name of the primary NTP server used to synchronize its time. Default: Blank
Secondary NTP Server	IP address or name of the secondary NTP server used to synchronize its time. Default: Blank
Enable SSLv3	Choose Yes to enable SSLv3. Choose No to disable. Default: No

VLAN Settings

Parameter	Description
Enable VLAN	Choose **Yes** to enable VLAN. Choose **No** to disable.

Parameter	Description
Enable CDP	Enable CDP only if you are using a switch that has Cisco Discovery Protocol. CDP is negotiation based and determines which VLAN the IP phone resides in.
Enable LLDP-MED	Choose **Yes** to enable LLDP-MED for the phone to advertise itself to devices that use that discovery protocol. When the LLDP-MED feature is enabled, after the phone has initialized and Layer 2 connectivity is established, the phone sends out LLDP-MED PDU frames. If the phone receives no acknowledgment, the manually configured VLAN or default VLAN will be used if applicable. If the CDP is used concurrently, the waiting period of 6 seconds is used. The waiting period will increase the overall startup time for the phone.
Network Startup Delay	Setting this value causes a delay for the switch to get to the forwarding state before the phone will send out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use Spanning Tree Protocol.
VLAN ID	If you use a VLAN without CDP (VLAN enabled and CDP disabled), enter a VLAN ID for the IP phone. Note that only voice packets are tagged with the VLAN ID. Do not use 1 for the VLAN ID.
PC Port VLAN ID	VLAN ID for the PC port.
DHCP VLAN Option	A predefined DHCP VLAN option to learn the voice VLAN ID. You can use the feature only when no voice VLAN information is available by CDP/LLDP and manual VLAN methods. CDP/LLDP and manual VLAN are all disabled. Valid values are: • Null • 128 to 149 • 151 to 158 • 161 to 254 Set the value to Null to disable DHCP VLAN option. Cisco recommends that you use DHCP Option 132.

Wi-Fi Settings

Parameter	Description
Phone-wifi-on	Allows you to turn on or off the Wi-Fi on your phone. Select **Yes** if you want to turn on the Wi-Fi and **No** if you want to turn it off. Default: Yes
Phone-wifi-type	Allows you to select a way to connect the phone to a wireless network. The options are: • **WLAN**: This option requires the user to enter the credentials on the phone to connect to a protected wireless network. • **WPS**: The user can connect the phone to a wireless network using either the WPS button on the access point or the PIN code.

Wi-Fi Profile (n)

Parameter	Description
Network Name	Allows you to enter a name for the SSID. This name displays on the phone. Multiple profiles can have the same network name with different security mode.
Security Mode	Allows you to select the authentication method that is used to secure access to the Wi-Fi network. Depending on the method you choose, a password, passphrase, or key field appears so that you can provide the credentials that are required to join this Wi-Fi network. Options are: • Auto • EAP-FAST • PEAP-GTC • PEAP-MSCHAPV2 • PSK • WEP • None Default: None

Parameter	Description
Wi-Fi User ID	Allows you to enter a user ID for the network profile.
	This field is available when you set the security mode to Auto, EAP-FAST, PEAP-GTC, or PEAP (MSCHAPV2). This is a mandatory field and it allows maximum length of 32 alphanumeric characters.
Wi-Fi Password	Allows you to enter the password for the specified Wi-Fi User ID.
WEP Key	Allows you to enter password for the network profile that you create. You need to enter this value when the security mode is WEP.
PSK Passphrase	Allows you to enter password for the network profile that you create. You need to enter this value when the security mode is PSK.
Frequency Band	Allows you to select the wireless signal frequency band that is the WLAN uses. Options are: • Auto • 2.4 GHz • 5 GHz Default: Auto

The following table defines the function and usage of each parameter in the **Wi-Fi Profile(n)** section under the **System** tab in the phone web page. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Inventory Settings

Parameter	Description
Asset ID	Provides the ability to enter an asset ID for inventory management when using LLDP-MED. The default value for Asset ID is empty. Enter a string of less than 32 characters if you are using this field.
	The Asset ID can be provisioned only by using the web management interface or remote provisioning. The Asset ID is not displayed on the phone screen.
	Changing the Asset ID field causes the phone to reboot.

SIP

SIP Parameters

Parameter	Description
Max Forward	SIP Max Forward value, which can range from 1 to 255. Default: 70
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. Default: 5
Max Auth	Maximum number of times (from 0 to 255) a request can be challenged. Default: 2
SIP User Agent Name	Used in outbound REGISTER requests. Default: $VERSION If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed
SIP Server Name	Server header used in responses to inbound responses. Default: $VERSION
SIP Reg User Agent Name	User-Agent name to be used in a REGISTER request. If this is not specified, the SIP User Agent Name is also used for the REGISTER request. Default: Blank
SIP Accept Language	Accept-Language header used. To access, click the SIP tab, and fill in the SIP Accept Language field. There is no default. If empty, the header is not included.
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. This field must match that of the Service Provider. Default: application/dtmf-relay
Hook Flash MIME Type	MIME Type used in a SIPINFO message to signal a hook flash event.
Remove Last Reg	Enables you to remove the last registration before registering a new one if the value is different. Select yes or no from the drop-down menu.

Parameter	Description
Use Compact Header	If set to yes, the phone uses compact SIP headers in outbound SIP messages. If inbound SIP requests contain normal headers, the phone substitutes incoming headers with compact headers. If set to no, the phones use normal SIP headers. If inbound SIP requests contain compact headers, the phones reuse the same compact headers when generating the response, regardless of this setting. Default: No
Escape Display Name	Enables you to keep the Display Name private. Select Yes if you want the IP phone to enclose the string (configured in the Display Name) in a pair of double quotes for outbound SIP messages. Default: Yes.
Talk Package	Enables support for the BroadSoft Talk Package that lets users answer or resume a call by clicking a button in an external application. Default: No
Hold Package	Enables support for the BroadSoft Hold Package, which lets users place a call on hold by clicking a button in an external application. Default: No
Conference Package	Enables support for the BroadSoft Conference Package that enables users to start a conference call by clicking a button in an external application. Default: No
RFC 2543 Call Hold	If set to yes, unit includes c=0.0.0.0 syntax in SDP when sending a SIP re-INVITE to the peer to hold the call. If set to no, unit will not include the c=0.0.0.0 syntax in the SDP. The unit will always include a=sendonly syntax in the SDP in either case. Default: Yes
Random REG CID on Reboot	If set to yes, the phone uses a different random call-ID for registration after the next software reboot. If set to no, the Cisco IP phone tries to use the same call-ID for registration after the next software reboot. The Cisco IP phone always uses a new random Call-ID for registration after a power-cycle, regardless of this setting. Default: No.

Parameter	Description
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. Default: 5060
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. Default: 5080
Caller ID Header	Provides the option to take the caller ID from PAID-RPID-FROM, PAID-FROM, RPID-PAID-FROM, RPID-FROM, or FROM header. Default: PAID-RPID-FROM
Hold Target Before Refer	Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered). Default: No
Dialog SDP Enable	When enabled and the Notify message body is too big causing fragmentation, the Notify message xml dialog is simplified; Session Description Protocol (SDP) is not included in the dialog xml content.
Keep Referee When Refer Failed	If set to yes, it configures the phone to immediately handle NOTIFY sipfrag messages.
Display Diversion Info	Display the Diversion info included in SIP message on LCD or not.
Display Anonymous From Header	Show the caller ID from the SIP INVITE message "From" header when set to Yes, even if the call is an anonymous call. When the parameter is set to no, the phone displays "Anonymous Caller" as the caller ID.
Sip Accept Encoding	Supports the content-encoding gzip feature. The options are none and gzip. If gzip is selected, the SIP message header contains the string "Accept-Encoding: gzip", and the phone is able to process the SIP message body, which is encoded with the gzip format.
Disable Local Name To Header	The options are No and Yes. If No is selected, no changes are made. The default value is No. If Yes is selected, it disables the display name in "Directory", "Call History", and in the "To" header during an outgoing call.

Parameter	Description
SIP IP Preference	Sets if the phone uses IPv4 or IPv6. Default: IPv4.

SIP Timer Values (sec)

Parameter	Description
SIP T1	RFC 3261 T1 value (RTT estimate) that can range from 0 to 64 seconds. Default: 0.5 seconds
SIP T2	RFC 3261 T2 value (maximum retransmit interval for non-INVITE requests and INVITE responses) that can range from 0 to 64 seconds. Default: 4 seconds
SIP T4	RFC 3261 T4 value (maximum duration a message remains in the network), which can range from 0 to 64 seconds. Default: 5 seconds.
SIP Timer B	INVITE time-out value, which can range from 0 to 64 seconds. Default: 16 seconds.
SIP Timer F	Non-INVITE time-out value, which can range from 0 to 64 seconds. Default: 16 seconds.
SIP Timer H	INVITE final response, time-out value, which can from 0 to 64 seconds. Default: 16 seconds.
SIP Timer D	ACK hang-around time, which can range from 0 to 64 seconds. Default: 16 seconds.
SIP Timer J	Non-INVITE response hang-around time, which can range from 0 to 64 seconds. Default: 16 seconds.
INVITE Expires	INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 2000000. Default: 240 seconds

Parameter	Description
ReINVITE Expires	ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 2000000. Default: 30
Reg Min Expires	Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the minimum value is used.
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is larger than this setting, the maximum value is used.
Reg Retry Intv	Interval to wait before the Cisco IP Phone retries registration after failing during the last registration.The range is from 1 to 2147483647 Default: 30 See the note below for additional details.
Reg Retry Long Intvl	When registration fails with a SIP response code that does not match<Retry Reg RSC>, the Cisco IP Phone waits for the specified length of time before retrying. If this interval is 0, the phone stops trying. This value should be much larger than the Reg Retry Intvl value, which should not be 0. Default: 1200 See the note below for additional details.
Reg Retry Random Delay	Random delay range (in seconds) to add to <Register Retry Intvl> when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the short timer. The range is from 0 to 2147483647. Default: 0
Reg Retry Long Random Delay	Random delay range (in seconds) to add to <Register Retry Long Intvl> when retrying REGISTER after a failure. Default: 0

Parameter	Description
Reg Retry Intvl Cap	Maximum value of the exponential delay. The maximum value to cap the exponential backoff retry delay (which starts at the Register Retry Intvl and doubles every retry). Defaults to 0, which disables the exponential backoff (that is, the error retry interval is always at the Register Retry Intvl). When this feature is enabled, the Reg Retry Random Delay is added to the exponential backoff delay value. The range is from 0 to 2147483647. Default: 0
Sub Min Expires	Sets the lower limit of the REGISTER expires value returned from the Proxy server.
Sub Max Expires	Sets the upper limit of the REGISTER minexpires value returned from the Proxy server in the Min-Expires header. Default: 7200.
Sub Retry Intvl	This value (in seconds) determines the retry interval when the last Subscribe request fails. Default: 10.

Note The phone can use a RETRY-AFTER value when it is received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the specified length of time before to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the Reg Retry Interval or the Reg Retry Long Interval.

Response Status Code Handling

Parameter	Description
Try Backup RSC	This parameter may be set to invoke failover upon receiving specified response codes. Default: Blank For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??

Parameter	Description
Retry Reg RSC	Interval to wait before the phone retries registration after failing during the last registration.
	Default: Blank
	For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??

RTP Parameters

Parameter	Description
RTP Port Min	Minimum port number for RTP transmission and reception. Minimum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16538.
	Default: 16384
RTP Port Max	Maximum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16538.
	The maximum value for the RTP port must be lesser than 49152.
	Default: 16538
RTP Packet Size	Packet size in seconds, which can range from 0.01 to 0.13. Valid values must be a multiple of 0.01 seconds.
	Default: 0.02
Max RTP ICMP Err	Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the phone terminates the call. If value is set to 0, the phone ignores the limit on ICMP errors.
RTCP Tx Interval	Interval for sending out RTCP sender reports on an active connection. It can range from 0 to 255 seconds.
	Default: 0

Parameter	Description
SDP IP Preferences	Select IPv4 or IPv6.
	Default: IPv4
	If the phone is in dual-mode and has both ipv4 and ipv6 addresses, it will always include both addresses in SDP by attributes "a=altc …
	If IPv4 address is selected, then ipv4 address has higher priority than ipv6 address in SDP and indicates that phone prefers using ipv4 RTP address.
	If the phone has only ipv4 address or ipv6 address, SDP does not have ALTC attributes and RTP address is specified in "c=" line.

SDP Payload Types

Parameter	Description
G722.2 Dynamic Payload	G722 Dynamic Payload type.
	Default: 96
iLBC Dynamic Payload	iLBC Dynamic Payload type.
	Default: 97
OPUS Dynamic Payload	OPUS Dynamic Payload type.
	Default: 99
AVT Dynamic Payload	AVT dynamic payload type. Ranges from 96-127.
	Default: 101
INFOREQ Dynamic Payload	INFOREQ Dynamic Payload type.
H264 BP0 Dynamic Payload	H264 BPO Dynamic Payload type.
	Default: 110
H264 HP Dynamic Payload	H264 HP Dynamic Payload type.
	Default: 110
G711u Codec Name	G711u codec name used in SDP.
	Default: PCMU
G711a Codec Name	G711a codec name used in SDP.
	Default: PCMA
G729a Codec Name	G729a codec name used in SDP.
	Default: G729a

Parameter	Description
G729b Codec Name	G729b codec name used in SDP. Default: G729b
G722 Codec Name	G722 codec name used in SDP. Default: G722
G722.2 Codec Name	G722.2 codec name used in SDP. Default: G722.2
iLBC Codec Name	iLBC codec name used in SDP. Default: iLBC
OPUS Codec Name	OPUS codec name used in SDP. Default: OPUS
AVT Codec Name	AVT codec name used in SDP. Default: telephone-event

NAT Support Parameters

Parameter	Description
Handle VIA received	Enables the phone to process the received parameter in the VIA header. Default: No
Handle VIA rport	Enables the phone to process the rport parameter in the VIA header. Default: No
Insert VIA received	Enables to insert the received parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Default: No
Insert VIA rport	Enables to insert the rport parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Default: No
Substitute VIA Addr	Enables the user to use NAT-mapped IP:port values in the VIA header. Default: No

Parameter	Description
Send Resp To Src Port	Enables to send responses to the request source port instead of the VIA sent-by port.
	Default: No
STUN Enable	Enables the use of STUN to discover NAT mapping.
	Default: No
STUN Test Enable	If the STUN Enable feature is enabled and a valid STUN server is available, the phone can perform a NAT-type discovery operation when it powers on. It contacts the configured STUN server, and the result of the discovery is reported in a Warning header in all subsequent REGISTER requests. If the phone detects symmetric NAT or a symmetric firewall, NAT mapping is disabled.
	Default: No
STUN Server	IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery. You can use a public STUN server or set up your own STUN server.
	Default: Blank
EXT IP	External IP address to substitute for the actual IP address of phone in all outgoing SIP messages. If 0.0.0.0 is specified, no IP address substitution is performed.
	If this parameter is specified, phone assumes this IP address when generating SIP messages and SDP (if NAT Mapping is enabled for that line).
	Default: Blank
EXT RTP Port Min	External port mapping number of the RTP Port Minimum number. If this value is not zero, the RTP port number in all outgoing SIP messages is substituted for the corresponding port value in the external RTP port range.
	Default: 0
NAT Keep Alive Intvl	Interval between NAT-mapping keep alive messages.
	Default: 15
Redirect Keep Alive	If enabled, the IP phone redirects the keepalive message when SIP_301_MOVED_PERMANENTLY is received as the registration response.

Provisioning

Configuration Profile

Parameter	Description
Provision Enable	Allows or denies resync actions. Default: Yes
Resync On Reset	The device performs a resync operation after power-up and after each upgrade attempt when set to **Yes**. Default: Yes
Resync Random Delay	A random delay following the boot-up sequence before performing the reset, specified in seconds. In a pool of IP Telephony devices that are scheduled to simultaneously power up, this introduces a spread in the times at which each unit sends a resync request to the provisioning server. This feature can be useful in a large residential deployment, in the case of a regional power failure. The value for this field must be an integer ranging between 0 and 65535. The default value is 2.
Resync At (HHmm)	The time (HHmm) that the device resynchronizes with the provisioning server. The value for this field must be a four-digit number ranging from 0000 to 2400 to indicate the time in HHmm format. For example, 0959 indicates 09:59. The default value is empty. If the value is invalid, the parameter is ignored. If this parameter is set with a valid value, the Resync Periodic parameter is ignored.
Resync At Random Delay	Prevents an overload of the provisioning server when a large number of devices power-on simultaneously. To avoid flooding resync requests to the server from multiple phones, the phone resynchronizes in the range between the hours and minutes, and the hours and minutes plus the random delay (hhmm, hhmm+random_delay). For example, if the random delay = (Resync At Random Delay + 30)/60 minutes, the input value in seconds is converted to minutes, rounding up to the next minute to calculate the final random_delay interval. The valid value ranges between 0 and 65535. This feature is disabled when this parameter is set to zero. The default value is 600 seconds (10 minutes).

Parameter	Description
Resync Periodic	The time interval between periodic resynchronizes with the provisioning server. The associated resync timer is active only after the first successful sync with the server. The valid formats are as follows: • An integer Example: An input of **3000** indicates that the next resync occurs in 3000 seconds. • Multiple integers Example: An input of **600,1200,300** indicates that the first resync occurs in 600 seconds, the second resync occurs in 1200 seconds after the first one, and the third resync occurs in 300 seconds after the second one. • A time range Example, an input of **2400+30** indicates that the next resync occurs in between 2400 and 2430 seconds after a successful resync. Set this parameter to zero to disable periodic resynchronization. The default value is 3600 seconds.

Parameter	Description
Resync Error Retry Delay	If a resync operation fails because the IP Telephony device was unable to retrieve a profile from the server, or the downloaded file is corrupt, or an internal error occurs, the device tries to resync again after a time specified in seconds.
	The valid formats are as follows:
	• An integer
	Example: An input of **300** indicates that the next retry for resync occurs in 300 seconds.
	• Multiple integers
	Example: An input of **600,1200,300** indicates that the first retry occurs in 600 seconds after the failure, the second retry occurs in 1200 seconds after the failure of the first retry, and the third retry occurs in 300 seconds after the failure of the second retry.
	• A time range
	Example, an input of **2400+30** indicates that the next retry occurs in between 2400 and 2430 seconds after a resync failure.
	If the delay is set to 0, the device does not try to resync again following a failed resync attempt.
Forced Resync Delay	Maximum delay (in seconds) the phone waits before performing a resynchronization.
	The device does not resync while one of its phone lines is active. Because a resync can take several seconds, it is desirable to wait until the device has been idle for an extended period before resynchronizing. This allows a user to make calls in succession without interruption.
	The device has a timer that begins counting down when all of its lines become idle. This parameter is the initial value of the counter. Resync events are delayed until this counter decrements to zero.
	The valid value ranges between 0 and 65535.
	The default value is 14,400 seconds.

Parameter	Description
Resync From SIP	Controls requests for resync operations via a SIP NOTIFY event sent from the service provider proxy server to the IP Telephony device. If enabled, the proxy can request a resync by sending a SIP NOTIFY message containing the Event: resync header to the device.
	Default: Yes
Resync After Upgrade Attempt	Enables or disables the resync operation after any upgrade occurs. If Yes is selected, sync is triggered.
	Default: Yes
Resync Trigger 1 Resync Trigger 2	If the logical equation in these parameters evaluates to FALSE, Resync is not triggered even when Resync On Reset is set to TRUE. Only Resync via direct action URL and SIP notify ignores these Resync Trigger.
	Default: Blank
Resync Fails On FNF	A resync is considered unsuccessful if a requested profile is not received from the server. This can be overridden by this parameter. When it is set to **No**, the device accepts a `file-not-found` response from the server as a successful resync.
	Default: Yes

Parameter	Description

Profile Authentication Type	Specifies the credentials to use for profile account authentication. The available options are:
	
	  • **Disabled**: Disables the profile account feature. When this feature is disabled, the **Profile account setup** menu doesn't display on the phone screen.
	
	  • **Basic HTTP Authentication**: The HTTP login credentials are used to authenticate the profile account.
	
	  • **XSI Authentication**: XSI login credentials or XSI SIP credentials are used to authenticate the profile account. The authentication credentials depend on the **XSI Authentication Type** for the phone:
	
	    • When the **XSI Authentication Type** for the phone is set to **Login Credentials**, the XSI login credentials are used.
	
	    • When the **XSI Authentication Type** for the phone is set to **SIP Credentials**, the XSI SIP credentials are used.
	
	Default: Basic HTTP Authentication

Profile Rule Profile Rule B Profile Rule C Profile Rule D	Each profile rule informs the phone of a source from which to obtain a profile (configuration file). During every resync operation, the phone applies all the profiles in sequence. Default: **/$PSN.xml** If you are applying AES-256-CBC encryption to the configuration files, specify the encryption key with the **--key** keyword as follows: **[--key <encryption key>]** You can enclose the encryption key in double-quotes (") optionally.
DHCP Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles. Default: 66,160,159,150,60,43,125
DHCPv6 Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles. Default: 17,160,159

Parameter	Description
Log Request Msg	The message sent to the syslog server at the start of a resync attempt. Default: `$PN $MAC -Requesting % $SCHEME://$SERVIP:$PORT$PATH`

Log Success Msg	The syslog message issued upon successful completion of a resync attempt.
	
	Default:
	
	`$PN $MAC -Successful Resync  %`
	
	`$SCHEME://$SERVIP:$PORT$PATH`

Log Failure Msg	The syslog message that is issued after a failed download attempt. Default: `$PN $MAC -- Resync failed: $ERR`
User Configurable Resync	Allows a user to resync the phone from the phone screen. Default: Yes

Upload Configuration Options

Field	Description

Report Rule	Specifies how the phone reports its current internal configuration to the provisioning server. The URLs in this field specify the destination for a report and can include an encryption key.
	
	You can use the following keywords, encryption key, and file locations and names to control how you store the phone configuration information:
	
	• No keywords and *only* an XML file reports the *entire* configuration data to server.
	
	• **[--status]** keyword reports the *status data* to server.
	
	• **[--delta]** keyword reports the *changed* configuration to server.
	
	• **[--key <encryption key>]** keyword tells the phone to apply AES-256-CBC encryption with the specified encryption key to the configuration report, before sending it to the server.
	
	You can enclose the encryption key in double-quotes (") optionally.
	
	Note If you have provisioned the phone with Input Keying Material (IKM) and want the phone to apply RFC 8188-based encryption to the file, do not specify a AES-256-CBC encryption key.
	
	• Two rules used together as:
	
	`[--delta]http://my_http_server/config-mpp-delta.xml`
	`[--status]http://my_http_server/config-mpp-status.xml`
	
	Caution If you need to use the [--delta]xml-delta file rule and the [--status]xml-status file rule together, you must separate the two rules with a **space**.

HTTP Report method:	Specifies whether the HTTP Request that the phone sends should be an *HTTP PUT* or an *HTTP POST*. • **PUT Method**–To create a new report or overwrite an existing report at a known location on the server. For example, you may want to keep overwriting each report that you send and only store the most *current* configuration on the server. • **POST Method**–To send the report data to the server for processing, such as, by a PHP script. This approach provides more flexibility for storing the configuration information. For example, you may want to send a series of phone status reports and store *all* the reports on the server.

Field	Description
Report to Server:	Defines when the phone reports its configuration to the provisioning servers. • **On Request**: The phone reports its configuration only when an administrator sends a sip notify event, or the phone restarts. • **On Local Change**: The phone reports its configuration when any configuration parameter changes by an action on the phone or on the phone administration web page. The phone waits for a few seconds after a change is made, and then reports the configuration. This delay ensures that changes are reported to the web server in batches, rather than reporting a single change at a time. • **Periodically**: The phone reports its configuration at regular intervals. The interval is expressed in seconds. Example XML configuration: **\<Report_to_Server ua="na">** Periodically **\</Report_to_Server>**
Periodic Upload to Server:	Defines the interval (in seconds) that the phone reports its configuration to the provisioning servers. This field is used only when **Report to Server** is set to **Periodically**. Default: 3600 Minimum: 600 Maximum: 2592000 (30 days) Example XML configuration: **\<Report_to_Server ua="na">** Periodically **\</Report_to_Server>** \<!available options: On Request | On Local Change| Periodically--> **\<periodic_upload_to_server ua="na">** 3600 **\</periodic_upload_to_server>\<User_Configurable_Resync ua="na">** Yes **\</User_Configurable_Resync_**

Field	Description
Upload Delay On Local Change:	Defines the delay (in seconds) that the phone waits after a change is made, and then reports the configuration. This field is used only when **Report to Server** is set to **On Local Change**. Default: 60 Minimum: 10 Maximum: 900 Example XML configuration: **`<Upload_Delay_On_Local_Change ua="na">`** 60 **`</Upload_Delay_On_Local_Change>`**

Firmware Upgrade

Parameter	Description
Upgrade Enable	Allows firmware update operations independent of resync actions. Default: Yes

Parameter	Description
Upgrade Rule	A firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule.
	Use the following format to enter the upgrade rule:
	`protocol://server[:port]/profile_pathname`
	For example:
	`tftp://192.168.1.5/image/sip88xx.11-1-1MPP-221.loads`
	If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as the server name. If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).
	You can also include the credentials that are used to access the server. Then, the upgrade rule is:
	`[--uid $userID --pwd $password]protocol://server[:port]/profile_pathname`
	For example,
	`[--uid TEST --pwd TestAbC123]tftp://192.168.1.5/image/sip88xx.11-1-1MPP-221.loads`
	If the user ID or the password contains special characters (/ [& } (*) # , etc.), you need to quote them in the upgrade rule. There are two options for quoting special characters:
	• Put the user ID or the password that contains special characters into double quotation marks (" "). This option doesn't work for some of the special characters, such as " " [ ].
	For example,
	`[--uid TEST --pwd "Test#\AbC123"]tftp://192.168.1.5/image/sip88xx.11-1-1MPP-221.loads`
	• Use the octal encoding of the special characters.
	For example, escape the pond (#) with "\043" and the backslash with "\057" for the password "Test#\AbC123" in the following rule:
	`[--uid TEST --pwd Test\043\057AbC123]tftp://192.168.1.5/image/sip88xx.11-1-1MPP-221.loads`
	Default: Blank

Parameter	Description
Log Upgrade Request Msg	Syslog message issued at the start of a firmware upgrade attempt.
	Default: $PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH
Log Upgrade Success Msg	Syslog message issued after a firmware upgrade attempt completes successfully.
	Default: $PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR
Log Upgrade Failure Msg	Syslog message issued after a failed firmware upgrade attempt.
	Default: $PN $MAC -- Upgrade failed: $ERR
Peer Firmware Sharing	Enables or disables the Peer Firmware Sharing feature. Select **Yes** or **No** to enable or to disable the feature.
	Default: Yes
Peer Firmware Sharing Log Server	Indicates the IP address and the port to which the UDP message is sent.
	For example: 10.98.76.123:514 where, 10.98.76.123 is the IP address and 514 is the port number.

For more information about the Provisioning page, see the *Cisco IP Phone 6800 Series Multiplatform Phones Provisioning Guide*.

CA Settings

Parameter	Description
Custom CA Rule	The URL to download Custom CA.
	Default: Blank

HTTP Settings

Parameter	Description
HTTP User Agent Name	Allows you to enter a name for HTTP user.
	Default: Blank

Problem Report Tool

Parameter	Description

PRT Upload Rule	Specifies the path to the PRT upload script. You can enter the path in the format:
	
	`https://proxy.example.com/prt_upload.php`
	
	or
	
	`http://proxy.example.com/prt_upload.php`
	
	If **PRT Max Timer** and **PRT Upload Rule** fields are empty, problem reports are not generated.

PRT Upload Method	Determines the method used to upload PRT logs to the remote server. Options are: HTTP POST and PUT. Default: POST
PRT Max Timer	Determines at what interval (minutes) the phone starts generating problem report automatically. The interval range that you can set is 15 minutes to 1440 minutes. Default: Empty If **PRT Max Timer** and **PRT Upload Rule** fields are empty, problem reports are not generated. a
PRT Name	Defines a name for the generated PRT file. Enter the name in the format: **prt-string1-$MACRO**

General Purpose Parameters

Parameter	Description
GPP A - GPP P	The general purpose parameters GPP_* are used as free string, registers when configuring the Cisco IP phones to interact with a particular provisioning server solution. They can be configured to contain diverse values, including the following: • Encryption keys • URLs • Multistage provisioning status information • Post request templates • Parameter name alias maps • Partial string values, eventually combined into complete parameter values Default: Blank

Regional

Call Progress Tones

Parameter	Description
Dial Tone	Prompts the user to enter a phone number.
Outside Dial Tone	Alternative to the Dial Tone. It prompts the user to enter an external phone number, as opposed to an internal extension. It is triggered by a, (comma) character encountered in the dial plan.
Prompt Tone	Prompts the user to enter a call forwarding phone number.
Busy Tone	Played when a 486 RSC is received for an outbound call.
Reorder Tone	Played when an outbound call has failed or after the far end hangs up during an established call. Reorder Tone is played automatically when <Dial Tone> or any of its alternatives times out.
Off Hook Warning Tone	Played when the phone receiver has been off hook after a period of time.
Ring Back Tone	Played during an outbound call when the far end is ringing.

Parameter	Description
Call Waiting Tone	Played when a call is waiting.
Confirm Tone	Brief tone to notify the user that the last input value has been accepted.
MWI Dial Tone	Played instead of the Dial Tone when there are unheard messages in the caller's mailbox.
Cfwd Dial Tone	Played when all calls are forwarded.
Holding Tone	Informs the local caller that the far end has placed the call on hold.
Conference Tone	Played to all parties when a three-way conference call is in progress.
Secure Call Indication Tone	Played when a call has been successfully switched tosecure mode. It should be played only for a short while (less than 30 seconds) and at a reduced level (less than -19 dBm) so it does not interfere with the conversation.
Page Tone	Specifies the tone transmitted when the paging feature is enabled.
Alert Tone	Played when an alert occurs.
Mute Tone	Played when the **Mute** button is pressed to mute the phone.
Unmute Tone	Played when the **Mute** button is pressed to unmute the phone.
System Beep	Audible notification tone played when a system error occurs.
Call Pickup Tone	Provides the ability to configure an audio indication for call pickup.

Distinctive Ring Patterns

Parameter	Description
Cadence 1	Cadence script for distinctive ring 1. Defaults to 60(2/4).
Cadence 2	Cadence script for distinctive ring 2. Defaults to 60(.3/.2, 1/.2,.3/4).
Cadence 3	Cadence script for distinctive ring 3. Defaults to 60(.8/.4,.8/4).

Parameter	Description
Cadence 4	Cadence script for distinctive ring 4. Defaults to 60(.4/.2,.3/.2,.8/4).
Cadence 5	Cadence script for distinctive ring 5. Defaults to 60(.2/.2,.2/.2,.2/.2,1/4).
Cadence 6	Cadence script for distinctive ring 6. Defaults to 60(.2/.4,.2/.4,.2/4).
Cadence 7	Cadence script for distinctive ring 7. Defaults to 60(4.5/4).
Cadence 8	Cadence script for distinctive ring 8. Defaults to 60(0.25/9.75)
Cadence 9	Cadence script for distinctive ring 9. Defaults to 60(.4/.2,.4/2).

Control Timer Values (sec)

Parameter	Description
Reorder Delay	Delay after far end hangs up before reorder (busy) tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds. Set to 255 to return the phone immediately to on-hook status and to not play the tone.
Interdigit Long Timer	Long timeout between entering digits when dialing. The interdigit timer values are used as defaults when dialing. The Interdigit_Long_Timer is used after any one digit, if all valid matching sequences in the dial plan are incomplete as dialed. Range: 0–64 seconds. Default: 10
Interdigit Short Timer	Short timeout between entering digits when dialing. The Interdigit_Short_Timer is used after any one digit, if at least one matching sequence is complete as dialed, but more dialed digits would match other as yet incomplete sequences. Range: 0–64 seconds. Default: 3

Vertical Service Activation Codes

Parameter	Description
Call Return Code	This code calls the last caller. Defaults to *69.
Blind Transfer Code	Begins a blind transfer of the current call to the extension specified after the activation code. Defaults to *95.
Cfwd All Act Code	Forwards all calls to the extension specified after the activation code. Defaults to *72.
Cfwd All Deact Code	Cancels call forwarding of all calls. Defaults to *73.
Cfwd Busy Act Code	Forwards busy calls to the extension specified after the activation code. Defaults to *90.
Cfwd Busy Deact Code	Cancels call forwarding of busy calls. Defaults to *91.
Cfwd No Ans Act Code	Forwards no-answer calls to the extension specified after the activation code. Defaults to *92.
Cfwd No Ans Deact Code	Cancels call forwarding of no-answer calls. Defaults to *93.
CW Act Code	Enables call waiting on all calls. Defaults to *56.
CW Deact Code	Disables call waiting on all calls. Defaults to *57.
CW Per Call Act Code	Enables call waiting for the next call. Defaults to *71.
CW Per Call Deact Code	Disables call waiting for the next call. Defaults to *70.
Block CID Act Code	Blocks caller ID on all outbound calls. Defaults to *61.

Parameter	Description
Block CID Deact Code	Removes caller ID blocking on all outbound calls. Defaults to *62.
Block CID Per Call Act Code	Removes caller ID blocking on the next inbound call. Defaults to *81.
Block CID Per Call Deact Code	Removes caller ID blocking on the next inbound call. Defaults to *82.
Block ANC Act Code	Blocks all anonymous calls. Defaults to *77.
Block ANC Deact Code	Removes blocking of all anonymous calls. Defaults to *87.
DND Act Code	Enables the do not disturb feature. Defaults to *78.
DND Deact Code	Disables the do not disturb feature. Defaults to *79.
Secure All Call Act Code	Makes all outbound calls secure. Defaults to *16.
Secure No Call Act Code	Makes all outbound calls not secure. Defaults to *17.
Secure One Call Act Code	Makes a secure call. Default: *18.
Secure One Call Deact Code	Disables secure call feature. Default: *19.
Paging Code	The star code used for paging the other clients in the group. Defaults to *96.
Call Park Code	The star code used for parking the current call. Defaults to *68.
Call Pickup Code	The star code used for picking up a ringing call. Defaults to *97.

Parameter	Description
Call Unpark Code	The star code used for picking up a call from the call park. Defaults to *88.
Group Call Pickup Code	The star code used for picking up a group call. Defaults to *98.
Referral Services Codes	These codes tell the IP phone what to do when the user places the current call on hold and is listening to the second dial tone. One or more *code can be configured into this parameter, such as *98, or *97|*98|*123, and so on. Max total length is 79 chars. This parameter applies when the user places the current call on hold (by Hook Flash) and is listening to second dial tone. Each *code (and the following valid target number according to current dial plan) entered on the second dial-tone triggers the phone to perform a blind transfer to a target number that is prepended by the service *code. For example, after the user dials *98, the IP phone plays a special dial tone called the Prompt Tone while waiting for the user the enter a target number (which is checked according to dial plan as in normal dialing). When a complete number is entered, the phone sends a blind REFER to the holding party with the Refer-To target equals to *98<target_number>. This feature allows the phone to hand off a call to an application server to perform further processing, such as call park. The *codes should not conflict with any of the other vertical service codes internally processed by the IP phone. You can empty the corresponding *code that you do not want to the phone to process.

Parameter	Description
Feature Dial Services Codes	These codes tell the phone what to do when the user is listening to the first or second dial tone.
	One or more *code can be configured into this parameter, such as *72, or *72|*74|*67|*82, and so forth. The maximum total length is 79 characters. This parameter applies when the user has a dial tone (first or second dial tone). Enter *code (and the following target number according to current dial plan) entered at the dial tone triggers the phone to call the target number prepended by the *code. For example, after user dials *72, the phone plays a prompt tone awaiting the user to enter a valid target number. When a complete number is entered, the phone sends a INVITE to *72\<target_number\> as in a normal call. This feature allows the proxy to process features like call forward (*72) or BLock Caller ID (*67).
	The *codes should not conflict with any of the other vertical service codes internally processed by the phone. You can empty the corresponding *code that you do not want to the phone to process.
	You can add a parameter to each *code in Features Dial Services Codes to indicate what tone to play after the *code is entered, such as *72'c'|*67'p'. Below are a list of allowed tone parameters (note the use of back quotes surrounding the parameter without spaces)
	• c = Cfwd Dial Tone
	• d = Dial Tone
	• m = MWI Dial Tone
	• o = Outside Dial Tone
	• p = Prompt Dial Tone
	• s = Second Dial Tone
	• x = No tones are place, x is any digit not used above
	If no tone parameter is specified, the phone plays Prompt tone by default.
	If the *code is not to be followed by a phone number, such as *73 to cancel call forwarding, do not include it in this parameter. In that case, simple add that *code in the dial plan and the phone sends INVITE *73@..... as usual when user dials *73.

Vertical Service Announcement Codes

Parameter	Description
Service Annc Base Number	Defaults to blank.
Service Annc Extension Codes	Defaults to blank.

Outbound Call Codec Selection Codes

Parameter	Description
Prefer G711u Code	Makes this codec the preferred codec for the associated call. Defaults to *017110.
Force G711u Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027110.
Prefer G711a Code	Makes this codec the preferred codec for the associated call. Defaults to *017111
Force G711a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027111.
Prefer G722 Code	Makes this codec the preferred codec for the associated call. Defaults to *01722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio.
Force G722 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio.
Prefer G722.2 Code	Makes this codec the preferred codec for the associated call.
Force G722.2 Code	Makes this codec the only codec that can be used for the associated call.

Parameter	Description
Prefer G729a Code	Makes this codec the preferred codec for the associated call. Defaults to *01729.
Force G729a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02729.
Prefer iLBC Code	Makes this codec the preferred codec for the associated call.
Force iLBC Code	Makes this codec the only codec that can be used for the associated call.
Prefer OPUS Code	Makes this codec the preferred codec for the associated call.
Force OPUS Code	Makes this codec the only codec that can be used for the associated call.

Time

Parameter	Description
Set Local Date (mm/dd/yyyy)	Sets the local date (mm represents the month and dd represents the day). The year is optional and uses two or four digits. Default: Blank
Set Local Time (HH/mm)	Sets the local time (hh represents hours and mm represents minutes). Seconds are optional. Default: Blank
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,…, GMT, GMT+01:00, GMT+02:00, …, GMT+13:00. Default: GMT-08:00
Time Offset (HH/mm)	This specifies the offset from GMT to use for the local system time. Default: 00/00

Parameter	Description
Ignore DHCP Time Offset	When used with some routers that have DHCP with time offset values configured, the IP phone uses the router settings and ignores the IP phone time zone and offset settings. To ignore the router DHCP time offset value, and use the local time zone and offset settings, choose yes for this option. Choosing no causes the IP phone to use the router's DHCP time offset value. Default: Yes.
Daylight Saving Time Rule	Enter the rule for calculating daylight saving time; it should include the start, end, and save values. This rule is comprised of three fields. Each field is separated by ; (a semicolon) as shown below. Optional values inside [ ] (the brackets) are assumed to be 0 if they are not specified. Midnight is represented by 0:0:0 of the given date. This is the format of the rule: Start = <start-time>; end=<end-time>; save = <save-time>. The <start-time> and <end-time> values specify the start and end dates and times of daylight saving time. Each value is in this format: <month> /<day> / <weekday>[/HH:[mm[:ss]]] The <save-time> value is the number of hours, minutes, and/or seconds to add to the current time during daylight saving time. The <save-time> value can be preceded by a negative (-) sign if subtraction is desired instead of addition. The <save-time> value is in this format: [/[+|-]HH:[mm[:ss]]] The <month> value equals any value in the range 1-12 (January-December). The <day> value equals [+|-] any value in the range 1-31. If <day> is 1, it means the <weekday> on or before the end of the month (in other words the last occurrence of < weekday> in that month).

Parameter	Description
Daylight Saving Time Rule (continued)	The <weekday> value equals any value in the range 1-7 (Monday-Sunday). It can also equal 0. If the <weekday> value is 0, this means that the date to start or end daylight saving is exactly the date given. In that case, the <day> value must not be negative. If the <weekday> value is not 0 and the <day> value is positive, then daylight saving starts or ends on the <weekday> value on or after the date given. If the <weekday> value is not 0 and the <day> value is negative, then daylight saving starts or ends on the <weekday> value on or before the date given. Where: • HH stands for hours (0-23). • mm stands for minutes (0-59). • ss stands for seconds (0-59). Default: 3/-1/7/2;end=10/-1/7/2;save=1.
Daylight Saving Time Enable	Enables Daylight Saving Time. Default: Yes

Language

Parameter	Description
Dictionary Server Script	Use this field to specify the language options for the phone display, and the dictionary and font files required for each language. See Set Up Dictionaries and Fonts, on page 85. Default: Blank
Language Selection	Use this field to specify the default language. The value must match one of the languages supported by the dictionary server. See Specify a Language for the Phone Display, on page 87. You can configure the language through the XML Configuration file. For example: `<Language_Selection ua="na"> Spanish </Language_Selection>` The language name can have up to 512 characters.
Locale	Use this drop-down list box to see the supported languages. See Supported Languages for the Phone Display, on page 85.

Phone

General

Parameter	Description
Station Name	Name of the phone.
Station Display Name	Name to identify the phone; appears on the phone screen. You can use spaces in this field and the name does not have to be unique.
Voice Mail Number	A phone number or URL to check voice mail. Default: None
WideBand Handset Enable	This field is available for Cisco IP Phone 6841 Multiplatform Phones and Cisco IP Phone 6851 Multiplatform Phones. Enables or disables the phone to use the wideband handset. By default, the system configures the setting of this field against the phone's hardware version. You can also change the setting as needed. Default: The default setting depends upon the phone's hardware version. • Hardware version 00 and 01: **No** • Hardware version 02: **Yes**

Line Key

Each line key has a set of settings.

Parameter	Description
Extension	Specifies the n extension to be assigned to Line Key n. Default: n XML configuration examples: To set the line key 1 to extension 1: **<Extension_1_ ua="na">1</Extension_1_>** To disable the extension function for line key 2: **<Extension_2_ ua="na">Disabled</Extension_2_>**

Parameter	Description
Short Name	Specifies the user name for Line Key. Default: $USER
Share Call Appearance	Specifies whether the incoming call appearance is shared with other phones or it is private.
Extended Function	Use to assign any of the following features or functions to unused line keys on the phone: • Busy Lamp Field • Call Pickup • Speed Dial

Miscellaneous Line Key Settings

Parameter	Description
Line ID Mapping	Specifies the shared call appearance line ID mapping. If Vertical First is set, the second call makes the next available line ID LED flash. If Horizontal first is set, the second call will make the same LED flash on which the first call is received. Also, the behavior is same for both outgoing and incoming calls. Default: Horizontal First
SCA Barge-In Enable	Enables the SCA Barge-In. Default: No
SCA Sticky Auto Line Seize	If enabled, restricts to automatically pick up an incoming call on a shared line when you take the phone off-hook.
Call Appearances Per Line	This parameter allows you to choose the number of calls per line button. You can choose a value from 2 to 10. Default: 2

Supplementary Services

Parameter	Description
Conference Serv	Enable or disable three-way conference service. Default: Yes
Attn Transfer Serv	Enable or disable attended-call-transfer service. Default: Yes

Parameter	Description
Blind Transfer Serv	Enable or disable blind-call-transfer service. Default: Yes
DND Serv	Enable or disable do not disturb service. Default: Yes
Block ANC Serv	Enable or disable block-anonymous-call service. Default: Yes
Block CID Serv	Enable or disable blocking outbound Caller-ID service. Default: Yes
Secure Call Serv	Enable or disable secured call services. Default: Yes
Cfwd All Serv	Enable or disable call-forward-all service. Default: Yes
Cfwd Busy Serv	Enable or disable call-forward-on-busy service. Default: Yes
Cfwd No Ans Serv	Enable or disable call-forward-no-answer service. Default: Yes
Paging Serv	Enable or disable paging service on the phone. Default: Yes
Call Park Serv	Enable or disable call park services on the phone. Default: Yes
Call Pick Up Serv	Enable or disable call pick up services on the phone. Default: Yes
ACD Login Serv	Enable or disable ACD login services on the phone. Default: Yes
Group Call Pick Up Serv	Enable or disable group call pick up services on the phone. Default: Yes
Service Annc Serv	Enable or disable the vertical service announcement services on the phone. Default: No

Parameter	Description
Call Recording Serv	Enable or disable the call recording services on the phone.
	Default: No
Reverse Phone Lookup Serv	Enable or disable reverse name lookup for the phone.
	When enabled, the phone can searches the personal address book and call history, server directory, and either the configured LDAP or XML directory.
	Default: Yes

Ringtone

Parameter	Description
Ring1 to Ring12	Ring tone scripts for different rings.
Silent Ring Duration	Controls the duration of the silent ring.
	For example, if the parameter is set to 20 seconds, the phone plays the silent ring for 20 seconds then sends 480 response to INVITE message.

Extension Mobility

Parameter	Description
EM Enable	Options to enable or to disable the extension mobility support for the phone.
	Default: No
EM User Domain	Name of the domain for the phone or the authentication server.
	Default: Blank
Session Timer(m)	Specifies the duration of the phone session.
Countdown Timer(s)	Specifies the duration for which it waits before it logs out.
	Default: 10
Preferred Password Input Mode	Options to specify the password input method of extension mobility PIN. Options are: Alpha-numeric and Numeric.
	Default: Alphanumeric

XSI Phone Service

Parameter	Description
XSI Host Server	Enter the name of the server; for example, xsi.iop1.broadworks.net. **Note** XSI Host Server uses http protocol by default. To enable XSI over HTTPS, you can specify `https://` in the server. Default: Blank
XSI Authentication Type	Determines the XSI authentication type. Select **Login Credentials** to authenticate access with XSI id and password. Select **SIP Credentials** to authenticate access with the register user ID and password of the SIP account registered on the phone. Default: Login Credentials
Login User ID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com. Enter SIP Auth ID when you select **Login Credentials** or **SIP Credentials** for XSI authentication type. When you choose SIP Auth ID as **SIP Credentials**, you must enter Login User ID. Without Login User ID, the BroadSoft directory will not appear under the phone Directory list. Default: Blank
Login Password	Alphanumeric password associated with the User ID. Enter login password, when you select **Login Credentials** for XSI authentication type. Default: Blank
SIP Auth ID	The registered user ID of the SIP account registered on the phone. Enter SIP Auth ID when you select **SIP Credentials** for XSI authentication type.
SIP Password	The password of the SIP account registered on the phone. Enter SIP password when you select **SIP Credentials** for XSI authentication type.
Directory Enable	Enables BroadSoft directory for the phone user. Select **Yes** to enable the directory and select **No** to disable it. Default: No

Parameter	**Description**
Directory Name	Name of the directory. Displays on the phone as a directory choice. Default: Blank
Directory Type	Select the type of BroadSoft directory: Enterprise: Allows users to search on last name, first name, user or group ID, phone number, extension, department, or email address. Group: Allows users to search on last name, first name, user ID, phone number, extension, department, or email address. Personal: Allows users to search on last name, first name, or telephone number. Default: Enterprise
CallLog Enable	Enables to log XSI calls. Select **Yes** to log XSI calls and select **No** to disable it. Default: No
CallLog Associated Line	Allows you to select a phone line for which you want to display the recent call logs. You can select line numbers ranges from 1 to 10.
Display Recents From	Allows you to set which type of recent call logs the phone will display. Choose **Server** to display BroadSoft XSI recent call logs and select **Phone** to display local recent call logs. **Note** The **Display recents from** is added to the **Recents** screen of the phone only when you set **CallLog Enable** to **Yes** and **Display Recents From** type to **Server**.

Broadsoft XMPP

Parameter	**Description**
XMPP Enable	Set to Yes to enable the BroadSoft XMPP directory for the phone user. Default: No
Server	Enter the name of the XMPP server; for example, xsi.iop1.broadworks.net. Default: Blank

Parameter	Description
Port	Server port for the directory. Default: Blank
User ID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com. Default: Blank
Password	Alphanumeric password associated with the User ID. Default: Blank
Login Invisible	When enabled, the user's presence information is not published when the user signs in. Default: No
Retry Intvl	Interval, in seconds, to allow a reconnect without a log in after the client disconnects from the server. After this interval, the client needs to reauthenticate. Default: 30

XML Service

Parameter	Description
XML Directory Service Name	Name of the XML Directory. Displays on the user's phone as a directory choice Default: Blank
XML Directory Service URL	URL where the XML Directory is located. Default: Blank
XML Application Service Name	Name of the XML application. Displays on the user's phone as a web application choice.
XML Application Service URL	URL where the XML application is located.
XML User Name	XML service username for authentication purposes Default: Blank
XML Password	XML service password for authentication purposes Default: Blank
CISCO XML EXE Enable	Enables or disables Cisco XML EXE authentication. Default: No

Parameter	Description
CISCO XML EXE Auth Mode	Specifies the authentication mode for Cisco XML EXE. The available options are: • Trusted—No authentication is performed (local user password is set or not). • Local Credential—Authentication is based on digest authentication using the local user password, if the local user password is set. If not set, then no authentication is performed. • Remote Credential—Authentication is based on digest authentication using the remote username/password as set in the XML application on the web page (to access an XML application server). Default: Trusted

Multiple Paging Group Parameters

Feature	Description
Group Paging Script	Enter a string to configure group paging.

LDAP

Parameter	Description
LDAP Dir Enable	Choose Yes to enable LDAP. Default: No
Corp Dir Name	Enter a free-form text name, such as "Corporate Directory." Default: Blank
Server	Enter a fully qualified domain name or IP address of an LDAP server in the following format: nnn.nnn.nnn.nnn Enter the host name of the LDAP server if the MD5 authentication method is used. Default: Blank
Search Base	Specify a starting point in the directory tree from which to search. Separate domain components [dc] with a comma. For example: dc=cv2bu,dc=com Default: Blank

Parameter	Description
Client DN	Enter the distinguished name domain components [dc]; for example:
	dc=cv2bu,dc=com
	If you are using the default Active Directory schema (Name(cn)->Users->Domain), an example of the client DN follows:
	cn="David Lee",dc=users,dc=cv2bu,dc=com
	cn="David Lee",dc=cv2bu,dc=com
	username@domain is the client DN format for a Windows server
	For example, DavidLee@cv2bu.com
	Default: Blank
User Name	Enter the username for a credentialed user on the LDAP server.
	Default: Blank
Password	Enter the password for the LDAP username.
	Default: Blank
Auth Method	Select the authentication method that the LDAP server requires. Choices are:
	None—No authentication is used between the client and the server.
	Simple—The client sends its fully-qualified domain name and password to the LDAP server. Might present security issues.
	Digest-MD5—The LDAP server sends authentication options and a token to the client. The client returns an encrypted response that is decrypted and verified by the server.
	Default: None
Last Name Filter	Use this field to specify how the phone must perform searches based on the last name or surname (sn), when users search for contacts.
	Examples:
	`sn:(sn=$VALUE*)` instructs the phone to find all last names that begin with the entered search string.
	`sn:(sn=*$VALUE*)` instructs the phone to find all last names in which the entered search string appears anywhere in the last name. This method is more inclusive and retrieves more search results. This method is consistent with the search method in other directories such as the Broadsoft directories and the user's personal address book on the phone.
	Default: Blank

Parameter	Description
First Name Filter	Use this field to specify how the phone must perform searches based on the first name or common name (cn), when users search for contacts.
	Examples:
	`cn:(cn=$VALUE*)` instructs the phone to find all first names that begin with the entered search string.
	`cn:(cn=*$VALUE*)` instructs the phone to find all first names in which the entered search string appears anywhere in the first name. This method is more inclusive and retrieves more search results. This method is consistent with the search method in other directories such as the Broadsoft directories and the user's personal address book on the phone.
	Default: Blank
Search Item 3	Additional customized search item. Can be blank if not needed.
	Default: Blank
Search Item 3 Filter	Customized filter for the searched item. Can be blank if not needed.
	Default: Blank
Search Item 4	Additional customized search item. Can be blank if not needed.
	Default: Blank
Search Item 4 Filter	Customized filter for the searched item. Can be blank if not needed.
	Default: Blank

Parameter	Description
Display Attrs	Format of LDAP results displayed on phone, where:
	• a—Attribute name
	• cn—Common name
	• sn—Surname (last name)
	• telephoneNumber—Phone number
	• n—Display name
	For example, n=Phone causes "Phone:" to be displayed in front of the phone number of an LDAP query result when the detail soft button is pressed.
	• t—type
	When t=p, that is, t is of type phone number, the retrieved number can be dialed. Only one number can be made dialable. If two numbers are defined as dialable, only the first number is used. For example, a=ipPhone, t=p; a=mobile, t=p;
	This example results in only the IP Phone number being dialable and the mobile number is ignored.
	• p—phone number
	When p is assigned to a type attribute, example t=p, the retrieved number is dialable by the phone.
	For example, a=givenName,n=firstname;a=sn,n=lastname;a=cn,n=cn;a=telephoneNumber,n=tele,t=p
	Default: Blank
Number Mapping	Can be blank if not needed.
	Note With the LDAP number mapping, you can manipulate the number that was retrieved from the LDAP server. For example, you can append 9 to the number if your dial plan requires a user to enter 9 before dialing. Add the 9 prefix by adding (<:9xx.>) to the LDAP Number Mapping field. For example, 555 1212 would become 9555 1212.
	If you do not manipulate the number in this fashion, a user can use the Edit Dial feature to edit the number before dialing out.
	Default: Blank

Programmable Softkeys

Parameter	Description
Programmable Softkey Enable	Enables programmable softkeys.
Idle Key List	Softkeys that display when the phone is idle.
Off Hook Key List	Softkeys that display when the phone is off-hook.
Dialing Input Key List	Softkeys that display when the user must enter dialing data.
Progressing Key List	Softkeys that display when a call is attempting to connect.
Connected Key List	Softkeys that display when a call is connected.
Start-Xfer Key List	Softkeys that display when a call transfer has been initiated.
Start-Conf Key List	Softkeys that display when a conference call has been initiated.
Conferencing Key List	Softkeys that display when a conference call is in progress.
Releasing Key List	Softkeys that display when a call is released.
Hold Key List	Softkeys that display when one or more calls are on hold.
Ringing Key List	Softkeys that display when a call is incoming. To silence an incoming call, you can add **Ignore** softkey.
Shared Active Key List	Softkeys that display when a call is active on a shared line.
Shared Held Key List	Softkeys that display when a call is on hold on a shared line.
PSK 1 through PSK 16	Programmable softkey fields. Enter a string in these fields to configure softkeys that display on the phone screen. You can create softkeys for speed dials to numbers or extensions, vertical service activation codes (* codes), or XML scripts.

Extension

Extension

In a configuration profile, the Line parameters must be appended with the appropriate numeral to indicate the line to which the setting applies. For example:

```
[1] to specify line one
[2] to specify line two
```

General

Parameter	Description
Line Enable	To enable this line for service, select yes. Otherwise, select No.
	Default: Yes
	Example XML configuration:
	To disable service on the line associated with extension 2:
	<Line_Enable_2_ ua="na">No</Line_Enable_2_>

Share Line Appearance

Parameter	Description
Share Ext	Indicates whether this extension is to be shared with other Cisco IP phones or private.
	Default: Yes
Shared User ID	The user identified assigned to the shared line appearance.
	Default: Blank
Subscription Expires	Number of seconds before the SIP subscription expires. Before the subscription expiration, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension.
	Default: 3600
Restrict MWI	When enabled, the message waiting indicator lights only for messages on private lines.
	Default: No

NAT Settings

Parameter	Description
NAT Mapping Enable	To use externally mapped IP addresses and SIP/ RTP ports in SIP messages, select yes. Otherwise, select no.
	Default: No

Parameter	Description
NAT Keep Alive Enable	To send the configured NAT keep alive message periodically, select yes. Otherwise, select no. Default: No
NAT Keep Alive Msg	Enter the keep alive message that should be sent periodically to maintain the current NAT mapping. If the value is $NOTIFY, a NOTIFY message is sent. If the value is $REGISTER, a REGISTER message without contact is sent. Default: $NOTIFY
NAT Keep Alive Dest	Destination that should receive NAT keep alive messages. If the value is $PROXY, the messages are sent to the current or outbound proxy.

Network Settings

Parameter	Description
SIP TOS/DiffServ Value	Time of service (ToS)/differentiated services (DiffServ) field value in UDP IP packets carrying a SIP message. Default: 0x68.
RTP ToS/DiffServ Value	Value for the ToS field of voice data packets. Sets the priority for voice packets in data traffic. Default: 0xb8.

SIP Settings

Parameter	Description
SIP Transport	Select the transport protocol for SIP messages: • UDP • TCP • TLS • AUTO **AUTO** allows the phone to select the appropriate protocol automatically, based on the NAPTR records on the DNS server. See Configure the SIP Transport, on page 186 for more details. Default: UDP

Parameter	Description
SIP Port	The phone's port number for SIP message listening and transmission.
	Specify the port number here only when you are using UDP as the SIP transport protocol.
	If you are using TCP, the system uses a random port within the range specified in **SIP TCP Port Min** and **SIP TCP Port Max** on the **Voice** > **SIP** tab.
	If you need to specify a port of SIP proxy server, you can specify it using the **Proxy** field (Proxy and Registration, on page 283) or the **XSI Host Server** field (XSI Line Service, on page 287).
	Default: 5060
SIP 100REL Enable	Support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests. Select **Yes** to enable.
	Default: No
EXT SIP Port	The external SIP port number.
Auth Resync-Reboot	The Cisco IP Phone authenticates the sender when it receives a NOTIFY message with the following requests:
	• resync
	• reboot
	• report
	• restart
	• XML-service
	Select **Yes** to enable.
	Default: Yes
SIP Proxy-Require	The SIP proxy can support a specific extension or behavior when it sees this header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported. Enter the appropriate header in the field provided.
SIP Remote-Party-ID	The Remote-Party-ID header to use instead of the From header. Select **Yes** to enable.
	Default: Yes

Parameter	Description
Referor Bye Delay	Controls when the phone sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target) are configured on this screen. For the Referror Bye Delay, enter the appropriate period of time in seconds. Default: 4
Refer-To Target Contact	Indicates the refer-to target. Select **Yes** to send the **SIP Refer** to the contact. Default: No
Referee Bye Delay	For the Referee Bye Delay, enter the appropriate period of time in seconds. Default: 0
Refer Target Bye Delay	For the Refer Target Bye Delay, enter the appropriate period of time in seconds. Default: 0
Sticky 183	When enabled, the IP telephony ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE. To enable this feature, select **Yes**. Otherwise, select **No**. Default: No
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy. To enable this feature, select **Yes**. Default: No
Ntfy Refer On 1xx-To-Inv	If set to **Yes**, as a transferee, the phone will send a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg. If set to **No**, the phone will only send a NOTIFY for final responses (200 and higher).
Set G729 annexb	Configure G.729 Annex B settings.

Parameter	Description
User Equal Phone	When a tel URL is converted to a SIP URL and the phone number is represented by the user portion of the URL, the SIP URL includes the optional : user=phone parameter (RFC3261). For example: To: sip:+12325551234@example.com; user=phone To enable this optional parameter, select **Yes**. Default: No
Call Recording Protocol	Determines the type of recording protocol that the phone uses. Options are: • SIPINFO • SIPREC Default: SIPREC
Privacy Header	Sets user privacy in the SIP message in the trusted network. The privacy header options are: • Disabled (default) • none—The user requests that a privacy service applies no privacy functions to this SIP message. • header—The user needs a privacy service to obscure headers which cannot be purged of identifying information. • session—The user requests that a privacy service provide anonymity for the sessions. • user—The user requests a privacy level only by intermediaries. • id—The user requests that the system substitute an id that doesn't reveal the IP address or host name. Default: Disabled
P-Early-Media Support	Controls whether the P-Early-Media header is included in the SIP message for an outgoing call. To include the P-Early-Media header, select **Yes**. Otherwise, select **No**. Default: No

Call Feature Settings

Parameter	Description
Blind Attn-Xfer Enable	Enables the phone to perform an attended transfer operation by ending the current call leg and performing a blind transfer of the other call leg. If this feature is disabled, the phone performs an attended transfer operation by referring the other call leg to the current call leg while maintaining both call legs. To use this feature, select Yes. Otherwise, select No. Default: No
Message Waiting	Indicates whether the Message Waiting Indicator on the phone is lit. This parameter toggles a message from the SIP proxy to indicate if a message is waiting.
Auth Page	Specifies whether to authenticate the invite before auto answering a page. Default: No
Default Ring	Type of ring heard. Choose from No Ring or 1 through 10. Ring options are Sunlight, Chirp 1, Chirp 2, Delight, Evolve, Mellow, Mischief, Reflections, Ringer, Ascent, Are you there, and Chime.
Auth Page Realm	Identifies the Realm part of the Auth that is accepted when the Auth Page parameter is set to Yes. This parameter accepts alphanumeric characters.
Conference Bridge URL	URL used to join a conference call, generally in the form of the word conference or user@IPaddress:port.
Auth Page Password	Identifies the password used when the Auth Page parameter is set to Yes. This parameter accepts alphanumeric characters.
Mailbox ID	Identifies the voice mailbox number/ID for the phone.
Voice Mail Server	Identifies the SpecVM server for the phone, generally the IP address, and port number of the VM server.
Voice Mail Subscribe Interval	The expiration time, in seconds, of a subscription to a voice mail server.
Auto Ans Page On Active Call	Determines the behavior of the phone when a page call arrives.

Parameter	Description
Feature Key Sync	Enable the synchronization of settings between the line and the server if necessary.
	Feature Key Sync must be enabled for lines that are configured for the following functions or users:
	• Call forward all
	• DND
Call Park Monitor Enable	BroadSoft server-only feature. If call park is enabled on the server or on any of the programmable line keys, you need to enable this field for call park notification to work.
	Default: No
Enable Broadsoft Hoteling	When this parameter is set to yes, the phone sends out subscription messages (without body) to the server.
	Default: No
Hoteling Subscription Expires	An expiration value that is added in the subscription message. Default value is 3600.
Secure Call Option	The secure call feature works only when the **SIP Transport** on the **Ext (n)** tab is set to **TLS**.
	Enables secured calls on an extension. Options are:
	• Optional: The phone maintains the current behavior for secure calls.
	• Required: The phone rejects nonsecure calls from other phones.
	Default: Optional

ACD Settings

Parameter	Description
Broadsoft ACD	Enables the phone for Automatic Call Distribuion (ACD). Select **Yes** to enable or **No** to disable.
	Default: No
Call Information Enable	Enables the phone to display details of a call center call. Select **Yes** to enable or **No** to disable.
	Default: No

Parameter	Description
Disposition Code Enable	Enables the user to add a disposition code. Select **Yes** to enable or **No** to disable. Default: No
Trace Enable	Enables the user to trace the last incoming call. Select **Yes** to enable or **No** to disable. Default: No
Emergency Escalation Enable	Enables the user to escalate a call to a supervisor in case of emergency. Select **Yes** to enable or **No** to disable. Default: No
Queue Status Notification Enable	Displays the call center status and the agent status. Select **Yes** to enable or **No** to disable. Default: No

Proxy and Registration

Parameter	Description
Proxy	SIP proxy server and port number set by the service provider for all outbound requests. For example: 192.168.2.100:6060. The port number is optional. If you don't specify a port, the default port 5060 is used for UDP, and the default port 5061 is used for TLS. When you need to refer to this proxy in another setting, for example, the speed dial line key configuration, use the `$PROXY` macro variable.
Outbound Proxy	All outbound requests are sent as the first hop. Enter an IP address or domain name.

Parameter	Description
Alternate Proxy Alternate Outbound Proxy	This feature provides fast fall back when there is network partition at the Internet or when the primary proxy (or primary outbound proxy) is not responsive or available. The feature works well in a Verizon deployment environment as the alternate proxy is the Integrated Service Router (ISR) with analog outbound phone connection. Enter the proxy server addresses and port numbers in these fields. After the phone is registered to the primary proxy and the alternate proxy (or primary outbound proxy and alternate outbound proxy), the phone always sends out INVITE and Non-INVITE SIP messages (except registration) via the primary proxy. The phone always registers to both the primary and alternate proxies. If there is no response from the primary proxy after timeout (per the SIP RFC spec) for a new INVITE, the phone attempts to connect with the alternate proxy. The phone always tries the primary proxy first, and immediately tries the alternate proxy if the primary is unreachable. Active transactions (calls) never fall back between the primary and alternate proxies. If there is fall back for a new INVITE, the subscribe/notify transaction will fall back accordingly so that the phone's state can be maintained properly. You must also set Dual Registration in the Proxy and Registration section to Yes.
Use OB Proxy In Dialog	Determines whether to force SIP requests to be sent to the outbound proxy within a dialog. Ignored if the **Use Outbound Proxy** field is set to **No** or if the **Outbound Proxy** field is empty. Default: Yes
Register	Enables periodic registration with the proxy. This parameter is ignored if a proxy is not specified. To enable this feature, select **Yes**. Default: Yes
Make Call Without Reg	Enables making outbound calls without successful (dynamic) registration by the phone. If set to No, the dial tone plays only when registration is successful. To enable this feature, select **Yes**. Default: No

Parameter	**Description**
Register Expires	Defines how often the phone renews registration with the proxy. If the proxy responds to a REGISTER with a lower expires value, the phone renews registration based on that lower value instead of the configured value.
	If registration fails with an "Expires too brief" error response, the phone retries with the value specified in the Min-Expires header of the error.
	The range is from 32 to 2000000.
	Default: 3600 seconds
Ans Call Without Reg	If enabled, the user does not have to be registered with the proxy to answer calls.
	Default: No
Use DNS SRV	Enables DNS SRV lookup for the proxy and outbound proxy. To enable this feature, select **Yes**. Otherwise, select **No**.
	Default: No
DNS SRV Auto Prefix	Enables the phone to automatically prepend the proxy or outbound proxy name with _sip._udp when performing a DNS SRV lookup on that name.
	Default: No
Proxy Fallback Intvl	Sets the delay after which the phone retries from the highest priority proxy (or outbound proxy) after it has failed over to a lower priority server.
	The phone should have the primary and backup proxy server list from a DNS SRV record lookup on the server name. It needs to know the proxy priority; otherwise, it does not retry.
	The range is from 0 to 65535.
	Default: 3600 seconds
Proxy Redundancy Method	Select **Normal** or **Based on SRV Port**. The phone creates an internal list of proxies returned in the DNS SRV records.
	If you select Normal, the list contains proxies ranked by weight and priority.
	If you select Based on SRV Port, the phone uses normal, then inspects the port number based on the first-listed proxy port.
	Default: Normal

Parameter	Description
Dual Registration	Set to **Yes** to enable the Dual registration/Fast Fall back feature. To enable the feature you must also configure the alternate proxy/alternate outbound proxy fields in the Proxy and Registration section.
Auto Register When Failover	If set to No, the fallback happens immediately and automatically. If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to the primary proxy.
	If set to Yes, the fallback happens only when current registration expires, which means only a REGISTER message can trigger fallback.
	For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback is triggered 3600 seconds later and not 600 seconds later. When the value for Register Expires is 600 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback is triggered at 1200 seconds. After successfully registering back to primary server, all the SIP messages go to primary server.

Subscriber Information

Parameter	Description
Display Name	Name displayed as the caller ID.
User ID	Extension number for this line.
	When you need to refer to this user ID in another setting, for example, the short name for a line key, use the `$USER` macro variable.
Password	Password for this line.
	Default: Blank (no password required)
Auth ID	Authentication ID for SIP authentication.
	Default: Blank
Reversed Auth Realm	The IP address for an authentication realm other than the proxy IP address. The default value is blank; the proxy IP address is used as the authentication realm.
	The parameter for extension 1 appears as follows in the phone configuration file:
	`<Reversed_Auth_Realm_1_ ua="na">` `</Reversed_Auth_Realm_1_>`

Parameter	Description
SIP URI	The parameter by which the user agent will identify itself for this line. If this field is blank, the actual URI used in the SIP signaling should be automatically formed as:
	sip:UserName@Domain
	where UserName is the username given for this line in the User ID, and Domain is the domain given for this profile in the User Agent Domain. If the User Agent Domain is an empty string, then the IP address of the phone should be used for the domain.
	If the URI field is not empty, but if a SIP or SIPS URI contains no @ character, the actual URI used in the SIP signaling should be automatically formed by appending this parameter with an @ character followed by the IP address of the device.

XSI Line Service

Parameter	Description
XSI Host Server	Enter the name of the server; for example, .
	xsi.iop1.broadworks.net
	Note XSI Host Server uses http protocol by default. To enable XSI over HTTPS, you can specify `https://` in the server.
	For example:
	https://xsi.iop1.broadworks.net
	You can also specify a port for the server.
	For example:
	https://xsi.iop1.broadworks.net:5061
	If you don't specify a port. The default port for the specified protocol is used.
	Default: Blank
XSI Authentication Type	Determines the XSI authentication type. Select **Login Credentials** to authenticate access with Login User ID and Login Password. Select **SIP Credentials** to authenticate access with the register Auth ID and Password of the SIP account registered on the phone.
	Default: Login Credentials

Parameter	Description
Login User ID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.
	For any XSI Authentication Type, you must enter **Login User ID**. Without **Login User ID**, the BroadWorks Anywhere feature does not work.
	Default: Blank
Login Password	Alphanumeric password associated with the Login User ID.
	Enter Login Password, when you select **Login Credentials** for XSI authentication type.
	Default: Blank
Anywhere Enable	Enables BroadWorks Anywhere feature on an extension.
	If you choose **Yes**, Anywhere is enabled on this line, and the user can use the phone menu to add multiple locations to this specific line.
	Default: Yes
Block CID Enable	Enables XSI Caller ID blocking on a line.
	Choose **Yes** to enable the synchronization of blocking caller id status with the server using XSI interface. Choose **No** to use the phone's local blocking caller id settings.
CFWD Enable	Enables or disables call forwarding status sync on a line via XSI service.
	Choose **Yes** to enable the phone to synchronize the call forwarding status with the server using the XSI service. Choose **No** to disable this feature.
	Note • When **Feature Key Sync** is set to **Yes**, FKS takes precedent over XSI synchronization. • If XSI host server and credentials are not entered and the **CFWD Enable** field is set to **Yes**, the phone user can't forward calls on the phone.

Parameter	Description
DND Enable	Enables or disables DND status sync on a line via XSI service.
	Choose **Yes** to enable the phone to synchronize DND status with the server using the XSI service. Choose **No** to disable this feature.
	Note • When **Feature Key Sync** is set to **Yes**, FKS takes precedent over XSI synchronization. • If XSI host server and credentials are not entered and the **DND Enable** field is set to **Yes**, the phone user can't turn on DND mode on the phone.

Audio Configuration

Parameter	Description
Preferred Codec	Preferred codec for all calls. The actual codec used in a call still depends on the outcome of the codec negotiation protocol.
	Select one of the following:
	• G711u
	• G711a
	• G729a
	• G722
	• G722.2
	• iLBC
	Default: G711u
Use Pref Codec Only	Select **No** to use any code. Select **Yes** to use only the preferred codes. When you select Yes, calls fail if the far end does not support the preferred codecs.
	Default: No
Second Preferred Codec	Codec to use if the first codec fails.
	Default: Unspecified
Third Preferred Codec	Codec to use if the second codec fails.
	Default: Unspecified

Parameter	Description
G711u Enable	Enables use of the G.711u codec. Default: Yes
G711a Enable	Enables use of the G.711a codec. Default: Yes
G729a Enable	To enable use of the G.729a codec at 8 kbps, select **Yes**. Otherwise, select **No**. Default: Yes
G722 Enable	Enables use of the G.722 codec. Default: Yes
G722.2 Enable	Enables use of the G.722.2 codec. Default: No
iLBC Enable	Enables use of the iLBC codec. Default: Yes
OPUS Enable	Enables the use of OPUS codec. Default: Yes
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select **Yes**. Otherwise, select **No**. Default: No
DTMF Tx Method	The method for transmitting DTMF signals to the far end. The options are: • AVT—Audio video transport. Sends DTMF as AVT events. • InBand—Sends DTMF by using the audio path. • Auto—Uses InBand or AVT based on the outcome of codec negotiation. • INFO—Uses the SIP INFO method.
Codec Negotiation	When set to Default, the Cisco IP phone responds to an Invite with a 200 OK response advertising the preferred codec only. When set to List All, the Cisco IP phone responds listing all the codecs that the phone supports. The default value is Default, or to respond with the preferred codec only.

Parameter	Description
Encryption Method	Encryption method to be used during secured call. Options are AES 128 and AES 256 GCM Default: 128.

Dial Plan

Parameter	Description
Dial Plan	Dial plan script for the selected extension. The dial plan syntax allows the designation of three parameters for use with a specific gateway: • uid – The authentication user-id • pwd – The authentication password • nat – If this parameter is present, use NAT mapping. Separate each parameter with a semi-colon (;).
Caller ID Map	Inbound caller ID numbers can be mapped to a different string. For example, a number that begins with +44xxxxxx can be mapped to 0xxxxxx. This feature has the same syntax as the Dial Plan parameter. With this parameter, you can specify how to map a caller ID number for display on screen and recorded into call logs.
Enable URI Dialing	Enables or disables URI dialing.
Emergency Number	Enter a comma-separated list of emergency numbers. When one of these numbers is dialed, the unit disables processing of CONF, HOLD, and other similar softkeys or buttons to avoid accidentally putting the current call on hold. The phone also disables hook flash event handling. Only the far end can terminate an emergency call. The phone is restored to normalcy after the call is terminated and the receiver is back on-hook. Maximum number length is 63 characters. Defaults to blank (no emergency number).

E911 Geolocation Configuration

E911 Geolocation Configuration

Parameter	Description
Company UUID	The Universally Unique Identifier (UUID) assigned to the customer by the emergency call services provider. Maximum identifier length is 128 characters. Defaults to blank.
Primary Request URL	Encrypted HTTPS phone location request. The request uses the phone IP addresses, MAC address, Network Access Identifier (NAI), and chassis ID and port ID assigned by the network switch manufacturer. The request also includes the location server name and the customer identifier. The server used by the emergency call services provider responds with an Emergency Response Location (ERL) that has a location Uniform Resource Identifier (URI) tied to the user phone IP address. Defaults to blank.
Secondary Request URL	Encrypted HTTPS request sent to the emergency call services provider's backup server to obtain the user's phone location. Defaults to blank.

See for terms that describe emergency call support for phones.

User

Hold Reminder

Parameter	Description
Hold Reminder Timer	Specifies the time delay (in seconds), that a ring splash is heard on an active call when another call was placed on hold. Default: 0
Hold Reminder Ringtone	Specifies the volume of the timer ringtone.

Call Forward

Parameter	Description
Cfwd Setting	Select **Yes** to enable call forwarding.

Parameter	Description
Cfwd All Dest	Enter the extensions to which the call is forwarded.
Cfwd Busy Dest	Enter the extensions to forward calls to when the line is busy. Default: voicemail
Cfwd No Ans Dest	Enter the extension to forward calls to when the call is not answered. Default: voicemail
Cfwd No Ans Delay	Enter the delay in time (in seconds) to wait before forwarding a call that is unanswered. Default: 20 seconds

Speed Dial

Parameter	Description
Speed Dial Name (2 to 9)	Name assigned to a specific speed dial number. Default: Blank
Speed Dial Number 2 to 9)	Target phone number (or URL) assigned to speed dial 2, 3, 4, 5, 6, 7, 8, or 9. Press the digit key (2-9) to dial out the assigned number. Default: Blank

Supplementary Services

Parameter	Description
CW Setting	Enables or disables the Call Waiting service. Default: Yes
Block CID Setting	Enables or disables the Block CID service. Default: No
Block ANC Setting	Enables or disables the Block ANC service. Default: No
DND Setting	Enables or disables the DND settings options for a user.
Handset LED Alert	Enables or disables LED alert on the handset. Options are: Voicemail and Voicemail, Missed Call. Default: Voicemail

Parameter	Description
Secure Call Setting	Enables or disables Secure Call.
	Default: No
Dial Assistance	Enables or disables the dial assistance feature.
	Default: No
Auto Answer Page	Enables or disables automatic answering of paged calls.
	Default: Yes
Preferred Audio Device	Choose the type of audio that the phone will use. Options are: Speaker and Headset.
	Choose the type of audio that the phone will use. Options are: Speaker and Headset.
	Default: None
Time Format	Choose the time format for the phone (12 or 24 hour).
	Default: 12hr
Date Format	Choose the date format for the phone (month/day or day/month).
	Default: month/day
Miss Call Shortcut	Enables or disables the option for creating a missed call shortcut.
Alert Tone Off	Enables or disables the alert tone.
Log Missed Calls for EXT (n)	Enables or disables the missed calls logs for a specific extension.
Shared Line DND Cfwd Enable	Enable/disable the Shared Line DND Call Forward.

Audio Volume

Parameter	Description
Ringer Volume	Sets the default volume for the ringer.
	Default: 9
Speaker Volume	Sets the default volume for the speakerphone.
	Default: 8
Handset Volume	Sets the default volume for the handset.
	Default: 10

Parameter	Description
Headset Volume	Sets the default volume for the headset. Default: 10
Electronic Hookswitch Control	Enables or disables the Electronic HookSwitch (EHS) feature. After EHS is enabled, the AUX port does not output phone logs.

Audio Compliance

Parameter	Description
Compliant Standard	Specifies the compliance standard for the phone audio. The available options are: • **ETSI**: A set of standards for speech and multimedia transmission for the narrowband and wideband terminals from European Telecommunications Standards Institute (ETSI). • **TIA**: A set of standards from US Telecommunications Industry Association (TIA). The standards are for narrowband and wideband audio transmission via wired telephones. Default: TIA

Screen

Parameter	Description
Screen Saver Enable	Enables a screen saver on the phone. When the phone is idle for a specified time, it enters screen saver mode. Default: No
Screen Saver Wait	Amount of idle time before screen saver displays. enter the number of seconds of idle time to elapse before the screen saver starts. Default: 300
Screen Saver Type	Types of screen saver. Options you can choose: • **Clock**: Displays a digital clock on a plain background. • **Download Picture**: Displays a picture pushed from the phone webpage. • **Logo**: Enables to add logo as phone background.

Parameter	Description
Screen Saver Refresh Period	Number of seconds before the screen saver should refresh (if, for example, you chose a rotation of pictures).
Back Light Timer	Number of seconds for which the back light timer will be on.
LCD Contrast	Value for desired contrast.
Boot Display	Type of display on the phone screen when the phone boots up. Options you can choose: • Default • Download Picutre • Logo • Text

Text Display	Text to display when the phone boots up. A service provider, for example, can enter logo text as follows:
	
	• Up to 2 lines of text
	
	• Each line must be fewer than 32 characters
	
	• Insert a new line character (\n) between lines
	
	• Insert escape code %0a
	
	For example,
	
	`Super\n%0aTelecom`
	
	displays:
	
	`Super`
	
	`Telecom`
	
	Use the + character to add spaces for formatting. For example, you can add multiple + characters before and after the text to center it.

Phone Background Type	If set to Download Picture, enables you to download a picture to customize the background on the phone screen.
Picture Download URL	URL locating the (.png) file to display on the phone screen background. For more information, see the Phone Information and Display Settings, on page 127.

Parameter	Description
Logo URL	URL locating the (.png) file to display the logo on the phone screen.

Att Console

General

✎

Note   The attendant console tab, labeled **Att Console**, is only available in **Admin Login** > **advanced** mode.

Parameter	Description
Subscribe Expires	Specifies how long the subscription remains valid. After the specified period of time elapses, the Cisco Attendant Console initiates a new subscription. Default: 1800
Subscribe Retry Interval	Specifies the length of time to wait to try again if the subscription fails. Default: 30
Number of Units	Specifies the number of Cisco Attendant Console units. Default: 0
Subscribe Delay	Length of delay before attempting to subscribe. Default: 1
Server Type	Specifies the server type with which the phone is connected. Options available: • BroadSoft • SPA9000 • Asterisk • RFC3265_4235 • Sylantro

Parameter	Description
BLF List URI	The Uniform Resource Identifier (URI) of the Busy Lamp Field (BLF) list that you have set up for a user of the phone, on the BroadSoft server.
	This field is only applicable if the phone is registered to a BroadSoft server. The BLF list is the list of users whose lines the phone is allowed to monitor. See Phone Configuration for Monitoring Other Phones, on page 162 for details.
	The BLF List URI must be specified in the format **<URI name>@<server>**. The BLF List URI specified must be the same as the value configured for the **List URI: sip** parameter on the BroadSoft server.
	Default: Blank
	Example XML configuration:
	`<BLF_List_URI ua="na">MonitoredUsersList@sipurash22.com</BLF_List_URI>`
Use Line Keys For BLF List	Controls whether the phone uses its line keys to monitor the BLF list, when monitoring of the BLF list is active.
	When set to **No**, the phone uses only the Key Expansion Module keys to monitor the BLF list.
	This setting only has significance when **BLF List** is set to **Show**.
	Default: No
	Example XML configuration:
	`<Use_Line_Keys_For_BLF_List ua="na">Yes</Use_Line_Keys_For_BLF_List>`

Parameter	Description
Customizable PLK Options	Features that users are allowed to configure on line keys.
	To allow a feature, add the corresponding option as shown below. Separate options with the semi-colon (;).
	• Speed dial: `sd`
	• Busy Lamp Field (BLF) key to monitor a user: `blf`
	• Call pickup from a monitored line: `cp`
	Note This option is only effective when the `blf` option is added.
	Default: `sd;`
	Note Adding the `sd` option automatically allows users to configure speed dial to a monitored line (speed dial with BLF) when the `blf` option is added.
	Example, to allow all features:
	`sd;blf;cp`
	Example XML configuration:
	`<Customizable_PLK_options ua="na">sd;</Customizable_PLK_options>`
BLF List	Activates or deactivates monitoring of the BLF list.
	When set to **Show**, the phone assigns available line keys in sequence, to monitor the BLF list entries. The labels of the BLF list keys show the names of the monitored users and the status of the monitored lines.
	This setting only has significance when **BLF List URI** is configured.
	Example XML configuration:
	`<BLF_List ua="rw">Show</BLF_List>`
Attendant Console LCD Brightness	The contrast between the text, lines, and background on the attendant console display. Enter a number value from 1 to 30. The higher the number, the greater the contrast on the display.
	Default: 12

Parameter	Description
BXfer to Starcode Enable	When set to **Yes**, the phone performs a blind transfer when the *code is defined in a speed dial extended function,. If set to **No**, the current call is held and a new call is started to the speed dial destination. Default: No
BXfer On Speed Dial Enable	When set to **Yes**, the phone performs a blind transfer when the speed dial function key is selected. When set to no, the current connected call is held and a new call to the speed dial destination is started. For example, when a user parks a call using the speed dial function, if the parameter is enabled, a blind transfer is performed to the parking lot. If the parameter is not enabled, an attended transfer is performed to the parking lot. Default: No
BXfer To Remote Party Number Enable	When set to **Yes**, the phone performs a blind transfer to a remote number. When set to no, blind transfer to remote number is disabled.
BLF Label Display Mode	Options to select a mode which displays on the phone screen for BLF. Default: Blank

TR-069

TR-069

Parameter	Description
Enable TR-069	Settings that enables or disables the TR-069 function. Default: Disabled
ACS URL	URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when it uses SSL or TLS.
ACS Username	Username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE. If the user name is not configured, admin is used as default.

Parameter	Description
ACS Password	Password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE. If the password is not configured, admin is used as default.
ACS URL In Use	URL of the ACS that is currently in use. This is a read-only field.
Connection Request URL	URL of the ACS that makes the connection request to the CPE.
Connection Request Username	Username that authenticates the ACS that makes the connection request to the CPE.
Connection Request Password	Password used to authenticate the ACS that makes a connection request to the CPE.
Periodic Inform Interval	Duration in seconds of the interval between CPE attempts to connect to the ACS when Periodic Inform Enable is set to yes. Default value is 20 seconds.
Periodic Inform Enable	Settings that enables or disables the CPE connection requests. Default value is Yes.
TR-069 Traceability	Settings that enables or disables TR-069 transaction logs. The default value is No.
CWMP V1.2 Support	Settings that enables or disables CPE WAN Management Protocol (CWMP) support. If set to disable, the phone does not send any Inform messages to the ACS nor accept any connection requests from the ACS. Default value is Yes.
TR-069 VoiceObject Init	Settings to modify voice objects. Select Yes to initialize all voice objects to factory default values or select No to retain the current values.
TR-069 DHCPOption Init	Settings to modify DHCP settings. Select Yes to initialize the DHCP settings from the ACS or select No to retain the current DHCP settings.
TR-069 Fallback Support	Settings that enables or disables the TR-069 fallback support. If the phone attempts to discover the ACS with DHCP and is unsuccessful, the phone next uses DNS to resolve the ACS IP address.
BACKUP ACS URL	Backup URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when it uses SSL or TLS.
BACKUP ACS User	Backup username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
BACKUP ACS Password	Backup password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE.

Parameter	Description
Note	If you do not configure the above parameters, you can also fetch them through DHCP options 60,43, and 125.

Call History

Displays the call history for the phone. To change the information displayed, select the type of call history from the following tabs:

- All Calls
- Missed
- Received
- Placed

Select **Add to Directory** to add the call information to your Personal Directory.

Personal Directory

The Personal Directory allows a user to store a set of personal numbers. Directory entries can include the following contact information:

- No. (the directory number)
- Name
- Work
- Mobile
- Home
- Speed Dials

To edit contact information, click **Edit Contacts**.

Troubleshooting

General Troubleshooting Information

The following table provides general troubleshooting information for the Cisco IP Phone.

Table 22: Cisco IP Phone Troubleshooting

Summary	Explanation
Connecting a Cisco IP Phone to another Cisco IP Phone	Cisco does not support connecting an IP phone to another IP Phone through the PC port. Each IP Phone should connect directly to a switch port. If phones are connected together in a line by using the PC port, the phones do not work.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.

Summary	Explanation
Moving a network connection from the phone to a workstation	If you power your phone through the network connection, you must be careful if you decide to unplug the network connection of the phone and plug the cable into a desktop computer. **Caution** The network card in the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration	By default, the administrator password settings are locked to prevent users from making changes that could impact their network connectivity. You must unlock the administrator password settings before you can configure them. **Note** If the administrator password is not set in common phone profile, then user can modify the network settings.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service. See Display Call Statistics Window, on page 206 for details.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. See Display Call Statistics Window, on page 206 for details.

Summary	Explanation
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option on the phone is set to 10 Half (10-BaseT/half duplex). • The phone receives power from an external power supply. • The phone is powered down (the power supply is disconnected). In this case, the switch port on the phone can become disabled and the following message appears in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, reenable the port from the switch.

Startup Problems

After you install a phone into your network and you can access the phone web page (phone Configuration Utility), the phone should start up as described in the related topic below.

If the phone does not start up properly, see the following sections for troubleshooting information.

Cisco IP Phone Does Not Go Through the Normal Startup Process

Problem

When you connect a Cisco IP Phone to the network port, the phone does not go through the normal startup process as described in the related topic and the phone screen does not display information.

Cause

If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, or the phone may not be functional.

Solution

To determine whether the phone is functional, use the following suggestions to eliminate other potential problems.

• Verify that the network port is functional:

   • Exchange the Ethernet cables with cables that you know are functional.

   • Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify that the port is active.

- Connect the Cisco IP Phone that does not start up to a different network port that is known to be good.

- Connect the Cisco IP Phone that does not start up directly to the port on the switch, eliminating the patch panel connection in the office.

- Verify that the phone is receiving power:

  - If you are using external power, verify that the electrical outlet is functional.

  - If you are using in-line power, use the external power supply instead.

  - If you are using the external power supply, switch with a unit that you know to be functional.

- If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.

- If the phone still does not start up properly, perform a factory reset of the phone.

- After you attempt these solutions, if the phone screen on the Cisco IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Phone Displays Error Messages

Problem

Status messages display errors during startup.

Solution

While the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the "Display Status Messages Window" section for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Phone Cannot Connect Using DNS

Problem

The DNS settings may be incorrect.

Solution

If you use DNS to access the TFTP server or Third-Party Call Control Manager, you must ensure that you specify a DNS server.

Configuration File Corruption

Problem

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

Solution

Get a new configuration file remotely from the provisioning server using `resync.`

Cisco IP Phone Cannot Obtain IP Address

Problem

If a phone cannot obtain an IP address when it starts up, the phone may not be on the same network or VLAN as the DHCP server, or the switch port to which the phone connects may be disabled.

Solution

Ensure that the network or VLAN to which the phone connects has access to the DHCP server, and ensure that the switch port is enabled.

Phone Reset Problems

If users report that their phones are resetting during calls or while the phones are idle on their desk, you should investigate the cause. If the network connection and Third Party Call Control connection are stable, a Cisco IP Phone should not reset.

Typically, a phone resets if it has problems in connecting to the Ethernet network or to Third Party Call Control.

Phone Resets Due to Intermittent Network Outages

Problem

Your network may be experiencing intermittent outages.

Solution

Intermittent network outages affect data and voice traffic differently. Your network might be experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect to the network. Contact the system administrator for information on known problems in the voice network.

Phone Resets Due to DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

Verify that you have properly configured the phone to use DHCP. Verify that the DHCP server is set up properly. Verify the DHCP lease duration. We recommend that you set the lease duration to 8 days.

Phone Resets Due to Incorrect Static IP Address

Problem

The static IP address assigned to the phone may be incorrect.

Solution

If the phone is assigned a static IP address, verify that you have entered the correct settings.

Phone Resets During Heavy Network Usage

Problem

If the phone appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured.

Solution

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

Phone Does Not Power Up

Problem

The phone does not appear to be powered up.

Solution

In most cases, a phone restarts if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then connects to an external power supply.

Phone Cannot Connect to LAN

Problem

The physical connection to the LAN may be broken.

Solution

Verify that the Ethernet connection to which the Cisco IP Phone connects is up. For example, check whether the particular port or switch to which the phone connects is down and that the switch is not rebooting. Also ensure that no cable breaks exist.

Audio Problems

The following sections describe how to resolve audio problems.

No Speech Path

Problem

One or more people on a call do not hear any audio.

Solution

When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configuration of routers and switches to ensure that IP connectivity is properly configured.

Choppy Speech

Problem

A user complains of choppy speech on a call.

Cause

There may be a mismatch in the jitter configuration.

Solution

Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity.

General Telephone Call Problems

The following sections help troubleshoot general telephone call problems.

Phone Call Cannot Be Established

Problem

A user complains about not being able to make a call.

Cause

The phone does not have a DHCP IP address. The phones display the message `Configuring IP` or `Registering.`

Solution

1. Verify the following:

   1. The Ethernet cable is attached.
   2. The Third-Party Call Control system is active.

2. Enable audio server debug and capture logs on both phones, then examine the logs.

Phone Does Not Recognize DTMF Digits or Digits Are Delayed

Problem

The user complains that numbers are missed or delayed when the keypad is used.

Cause

Pressing the keys too quickly can result in missed or delayed digits.

Solution

Keys should not be pressed rapidly.

Feature Troubleshooting

Here is troubleshooting information related to some of the phone features.

ACD Call Information Missing

Problem

A call center phone does not see call information during a call.

Solution

- Check the phone configuration to determine if **Call Information Enable** is set to yes.

- Check the Broadsoft server configuration to determine if the user's Device Profile is configured with "Support Call Center MIME Type".

Phone Doesn't Show ACD Softkeys

Problem

The phone doesn't display the Agent Sign In or Agent Sign Out softkeys.

Solution

- Check Broadsoft server configuration to determine if that user has been configured as a call center agent.

- Enable the programmable softkeys (PSK) and add the ACD softkeys to the softkey list. For more information, see Configuring Programmable Softkeys, on page 168.

- Check the phone configuration to determine if **BroadSoft ACD** is set to yes.

Call Doesn't Record

Problem

When a user tries to record a call, the recording doesn't takes place.

Cause

This is often due to configuration issues.

Solution

1. Set the phone to always record a call.

2. Make a call.

If the recording doesn't start, there are configuration problems. Check the configuration of the BroadWorks and third-party recorder.

If the recording does start:

1. Set the phone to record on demand.

2. Set up Wireshark to capture a trace of the network traffic between the phone and Broadworks when the problem occurs. When you have the trace, contact TAC for further assistance.

An Emergency Call Doesn't Connect to Emergency Services

Problem

A user tries to place an emergency call, but the call doesn't connect to the emergency services (fire, police, or emergency services operator).

Solution

Check the emergency call configuration:

- Company Identifier or location request URL setup is incorrect. See Configure a Phone to Make Emergency Calls, on page 185.

- An incorrect or blank emergency number exists in the Dial Plan setup. See Dial Plan, on page 291

The location request servers (emergency call service provider) did not respond with a phone location, after multiple attempts.

Presence Status Doesn't Work

Problem

The phone doesn't show presence information.

Solution

Use UC Communicator as a reference to verify that the account works.

Phone Presence Message: Disconnected from Server

Problem

Instead of presence information, the user sees the message `Disconnected from server`.

Solution

- Check the Broadsoft server configuration to determine if IM&P service is enabled and assigned to that user.

- Check the phone configuration to determine if the phone can connect to the internet and get the XMPP messages.

- Check the XMPP Incoming and Outgoing messages printed in the syslog to make sure it can login successfully.

Phone Cannot Access BroadSoft Directory for XSI

Problem

The phone displays XSI directory access error.

Solution

1. Check Broadsoft server configuration for the user login and SIP credentials.

2. Check error messages in syslog.

3. Check information on the error on the phone screen.

4. If HTTPS connection fails, check the error message on the phone screen and in the syslog.

5. Install custom CA for HTTPS connection if the BroadSoft certificate is not signed from phone built-in root CA.

Cannot Access DND or Call Forwarding Settings on the Phone

Problem

The **DND** or **Forward all** softkey is grayed on the phone. Meanwhile, phone user can't access the settings of **Do not disturb** or **Call forwarding** from **Applications** > **User preferences** > **Call preferences**.

- *"Fail to get XSI settings"* message appears when accessing the **Call preferences** menu on the phone screen.

- *"Access Fail. Please check config and network"* message appears when accessing the **Call forwarding** menu on the phone screen.

Cause

Feature Key Sync is disabled and XSI account is not properly configured on the phone administration web page when XSI sync for DND or call forwarding is enabled.

Solution

Follow one of the following possible solutions as needed.

- Check the settings of XSI host server and the credentials in the **XSI Line Service** section from **Voice** > **Ext (n)** on the phone administration web page.

- If you don't want to use XSI synchronization to sync DND or call forwarding status between the phone and the server, set **DND Enable** or **CFWD Enable** to **No** in the **XSI Line Service** section from **Voice** > **Ext (n)**. Otherwise, ensure that the XSI account settings are correctly configured.

- Enable **Feature Key Sync** in **Phone Feature Settings** section from **Voice** > **Ext (n)**. This enables the phone to synchronize DND and call forwarding status with the server using SIP messages.

Phone Display Problems

Your users may see unusual screen displays. Use the following sections to troubleshoot the problem.

The Font is Too Small or Has Unusual Characters

Problem

The phone screen has smaller fonts than expected or there are unusual characters displayed. Examples of unusual characters are letters from a different alphabet from the characters that the locale uses.

Cause

Possible causes are:

- TFTP server does not have the correct set of locale and font files

- XML files or other files are specified as a font file

- The font and locale files did not download successfully.

Solution

- Font files and locale files must be in the same directory.

- Do not add or change files in the locale and font folder structure.

- On the phone web page, select **Admin Login** > **Advanced** > **Info** > **Status** and scroll to the **Locale Download Package** section to verify that the locale and font files downloaded successfully. If they did not, try the download again.

Phone Screen Displays Boxes Instead of Asian Characters

Problem

The phone is set for an Asian language, but the phone shows square boxes instead of Asian characters.

Cause

Possible causes are:

- TFTP server does not have the correct set of locale and font files.

- The font and locale files did not download successfully.

Solution

- Font files and locale files must be in the same directory.

- On the phone web page, select **Admin Login** > **Advanced** > **Info** > **Status** and scroll to the **Locale Download Package** section to verify that the locale and font files downloaded successfully. If they did not, try the download again.

Softkey Labels are Truncated

Problem

The softkey labels appear to be truncated.

Cause

The phone has the wrong version of files in the TFTP server.

Solution

Check that the file version is correct for the phone model. Each phone model has its own files.

Phone Locale is Not Displayed

Problem

The phone is set to use a different language from the one that is displayed.

Cause

TFTP server does not have the correct set of locale and font files.

Solution

Font files and locale files must be in the same directory.

Report All Phone Issues from the Phone Web Page

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue. You can generate PRT logs using the phone web page and upload them to a remote log server.

Before you begin

Access the phone administration web page. See .

Procedure

Step 1 Select **Info** > **Debug Info**.

Step 2 In the **Problem Reports** section, click **Generate PRT**.

Step 3 Enter the following information in the **Report Problem** screen:

    a) Enter the date that you experienced the problem in the **Date** field. The current date appears in this field by default.

    b) Enter the time that you experienced the problem in the **Time** field. The current time appears in this field by default.

    c) In the **Select Problem** drop-down list box, choose the description of the problem from the available options.

Step 4 Click **Submit** in the **Report Problem** screen.

The Submit button is enabled only if you select a value in the **Select Problem** drop-down list box.

You get a notification alert on the Phone Web page that indicates if the PRT upload was successful or not.

Report a Phone Problem Remotely

You can initiate a phone problem report remotely. The phone generates a problem report using the Cisco Problem Report Tool (PRT), with the problem description "Remote PRT Trigger". If you have configured an upload rule for problem reports, the phone uploads the problem report according to the upload rule.

You can see the status of the problem report generation and upload on the phone administration web page. When a problem report is successfully generated, you can download the problem report from the phone administration web page.

Procedure

To initiate a phone problem report remotely, initiate a `SIP-NOTIFY` message from the server to the phone, with the Event specified as `prt-gen`.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Check DHCP Settings

Procedure

Step 1 On the phone, press **Applications** ⚙.

Step 2 Select **Admin Settings** > **Network Setup** > **IPv4 Setup**.

Step 3 Check the DHCP server field.

Check the DHCP option for enabled or disabled.

Step 4 Check the IP Address, Subnet Mask, and Default Router fields.

If you assign a static IP address to the phone, you must manually enter settings for these options.

Step 5 If you are using DHCP, check the IP addresses that your DHCP server distributes.

See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Verify DNS Settings

Procedure

Step 1   On the phone, press **Applications** ⚙.

Step 2   Select **Admin Settings** > **Network Setup** > **IPv4 Setup**

Step 3   Check that the DNS Server 1 field is set correctly.

Step 4   You should also verify that a CNAME entry was made in the DNS server for the TFTP server and for the Third-Party Call Control.

You must also ensure that DNS is configured to do reverse lookups.

Additional Troubleshooting Information

If you have additional questions about troubleshooting your phone, go to the following Cisco website and navigate to the desired phone model:

https://www.cisco.com/cisco/web/psa/troubleshoot.html

CHAPTER **14**

Maintenance

Basic Reset

Performing a basic reset of a Cisco IP Phone provides a way to recover when the phone experiences an error.
The reset provides a way to reset or restore various configuration and security settings.

Note When you set up emergency calls, the phone requests an updated location whenever a person performs a
phone restart.

The following table describes the ways to perform a basic reset. You can reset a phone with any of these
operations after the phone has started up. Choose the operation that is applicable for your situation.

Table 23: Basic Reset Methods

Operation	Action	Explanation
Restart phone	Press **Applications** and choose **Admin Settings** > **Restart**.	Resets any user and network setup changes that you have made, to the previously saved settings that the phone has not written to its flash memory. The phone then restarts.
Reset settings	To reset settings, press **Applications** and choose **Admin Settings** > **Factory Reset**.	Restores the phone configuration or settings to factory default.

Note   When an administrator has set up emergency calls, the phone requests an updated location whenever the administrator does the following actions:

- Registers the phone with the call server.

- Restarts the phone (phone is registered).

- Changes the network interface that is used for the SIP registration.

- Changes the IP address of the phone.

Perform a Factory Reset with the Phone Keypad

Use these steps to reset the phone to factory default settings using the phone keypad.

Procedure

Step 1   Unplug the phone:

- If using PoE, unplug the LAN cable.
- If using the power cube, unplug the power cube.

Step 2   Wait 5 seconds.

Step 3   Press and hold **#** and plug the phone back in.

When the phone boots up:

- For Cisco IP Phone 6821 Multiplatform Phones, the lights on the light strip and the line keys light up.

- For Cisco IP Phone 6841 and 6851 Multiplatform Phones, the lights on the headset button, the speaker button, and the handset flash.

Step 4   Press the **123456789*0#** keys in sequence.

For Cisco IP Phone 6821 Multiplatform Phones, when you press a key, the lights on the line keys and the light strip flash.

For Cisco IP Phone 6841 and 6851 Multiplatform Phones, when you press **1**, the handset light and the light on the speaker button turn off.

After you press these buttons, the phone goes through the factory reset process.

If you press the buttons out of sequence, the phone powers on normally.

Caution   Do not power down the phone until it completes the factory reset process, and the main screen appears.

Perform Factory Reset from Phone Menu

Procedure

Step 1 Press **Applications** ⚙.

Step 2 Select **Device administration** > **Factory reset**.

Step 3 To restore phone configuration or settings to factory default, press **OK**.

Factory Reset the Phone with the Web UI Button

You can factory reset the phone from the phone web page. The reset only happens if the phone is idle. If the phone is not idle, the phone web page shows a message that the phone is busy and that you need to try again.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 92.

Procedure

Step 1 Select **Admin Login** > **advanced** > **Info** > **Debug Info**.

Step 2 In the **Factory Reset** section, click **Factory Reset**.

Step 3 Click **Confirm factory reset**.

Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.

- Concealed Second metrics—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely "concealed second" is a second in which the DSP plays more than five percent concealment frames.

✎

Note Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics from the Cisco IP Phone using the Call Statistics screen or remotely by using Streaming Statistics.

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

Table 24: Changes to Voice Quality Metrics

Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter levels: • Average MOS LQK decreases may indicate widespread and uniform impairment. • Individual MOS LQK decreases may indicate bursty impairment. Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.
MOS LQK scores increase significantly	• Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

Note   Voice quality metrics do not account for noise or distortion, only frame loss.

Voice Quality Reporting

You can capture voice quality metrics for Voice over Internet Protocol (VoIP) sessions with a Session Initiation Protocol (SIP) event package. Voice call quality information derived from RTP and call information from SIP is conveyed from a User Agent (UA) in a session (reporter) to a third party (collector).

The Cisco IP phone uses User Datagram Protocol (UDP) to send a SIP PUBLISH message to a collector server.

Supported Scenarios for Voice Quality Reporting

Currently, only the basic call scenario supports voice quality reporting. A basic call can be a peer to peer incoming or outgoing call. The phone sends the SIP Publish message when a call ends.

Mean Opinion Scores and Codecs

The voice quality metrics use Mean Opinion Score (MOS) to rate the quality. A MOS rating of 1 is the lowest quality; a MOS rating of 5 is the highest quality. The following table gives a description of the codecs and MOS scores. For other codecs, the phone does not send the SIP Publish message.

Codec	Complexity and Description	MOS	Minimum Call Duration for Valid MOS Value
G.711 (A-law and u-law)	Very low complexity. Supports uncompressed 64 kbps digitized voice transmission at one to ten 5 ms voice frames-per-packet. This codec provides the highest voice quality and uses the most bandwidth of any of the available codecs.	A minimum value of 4.1 indicates good voice quality.	10 seconds
G.729A	Low to medium complexity.	A minimum value of 3.5 indicates good voice quality.	30 seconds
G.729AB	Contains the same reduced complexity modifications present in the G.729A.	A minimum value of 3.5 indicates good voice quality.	30 seconds

Configure Voice Quality Reporting

You can enable voice quality reporting on the phone with the web interface. Each extension on a phone has a separate voice quality report. For each extension on the phone, use the corresponding **Voice Quality Report Address** field to configure the generation of voice quality report.

Procedure

Step 1 On the Phone Web page, select **Admin Login** > **advanced** > **Voice** > **Ext x**.

Where:

- Ext x = the extension number on the phone

Step 2 In **SIP Settings**, enter a value in the **Voice Quality Report Address x** field. You can enter either a domain name or an IP address in this field.

You can also add a port number along with the domain name or an IP address in this field. If you do not enter a port number, the value of the **SIP UDP Port** (5060) is used by default. If the collector server URL parameter is blank, a SIP PUBLISH message is not sent out.

Step 3 Click **Submit All Changes**.

Cisco IP Phone Cleaning

To clean your Cisco IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all non-weatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the screen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning.

View Phone Information

Procedure

To check the current status of the Cisco IP Phone, click the **Info** tab.

The Info tab shows information about all phone extensions, including phone statistics and the registration status.

Reboot Reasons

The phone stores the most recent five reasons that the phone was refreshed or rebooted. When the phone is reset to factory defaults, this information is deleted.

The following table describes the reboot and refresh reasons for the Cisco IP Phone.

Reason	Description
Upgrade	The reboot was a result of an upgrade operation (regardless whether the upgrade completed or failed).
Provisioning	The reboot was the result of changes made to parameter values by using the IP phone screen or phone web user interface, or as a result of synchronization.
SIP Triggered	The reboot was triggered by a SIP request.
RC	The reboot was triggered as a result of remote customization.
User Triggered	The user manually triggered a cold reboot.
IP Changed	The reboot was triggered after the phone IP address changed.

You can view the reboot history as follows:

- From the phone web user interface

- From the IP phone screen

- From the phone Status Dump file (http://*phoneIP*/status.xml or http://*phoneIP*/admin/status.xml)

Reboot History on the Phone Web User Interface

On the **Info** > **System Status** page, the **Reboot History** section displays the device reboot history, the five most recent reboot dates and times, and a reason for the reboot. Each field displays the reason for the reboot and a time stamp that indicates when the reboot took place.

For example:

```
Reboot Reason 1: [08/13/14 06:12:38] User Triggered
Reboot Reason 2: [08/10/14 10:30:10] Provisioning
Reboot Reason 3: [08/10/14 10:28:20] Upgrade
```

The reboot history displays in reverse chronological order; the reason for the most recent reboot displays in **Reboot Reason 1**.

Reboot History on the Cisco IP Phone Screen

Reboot History is located under **Apps** > **Admin Settings** > **Status** menu. In the Reboot History window, the reboot entries displays in reverse chronological order, similar to the sequence that displays on the phone web user interface.

Reboot History in the Status Dump File

The reboot history is stored in the Status Dump file (http://*<phone_IP_address>*/admin/status.xml).

In this file, tags **Reboot_Reason_1** to **Reboot_Reason_3** store the reboot history, as shown in this example:

```
<Reboot_History>
<Reboot_Reason_1>[08/10/14 14:03:43]Provisioning</Reboot_Reason_1>
<Reboot_Reason_2>[08/10/14 13:58:15]Provisioning</Reboot_Reason_2>
<Reboot_Reason_3>[08/10/14 12:08:58]Provisioning</Reboot_Reason_3>
<Reboot_Reason_4>
<Reboot_Reason_5>
<Reboot_History/>
```

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco IP Phone voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan

- Attacks that occur on your network, such as a Denial of Service attack

To reduce or eliminate any adverse effects to the phones, schedule administrative network tasks during a time when the phones are not being used or exclude the phones from testing.

TR-069 Parameter Comparison

XML and TR-069 Parameter Comparison

This table shows the XML parameters that the phones use, with their TR-069 counterpart.

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.	N/A
Device.Services.VoiceService.{i}.	N/A
Device.Services.VoiceService.{i}.Capabilities.	N/A
Device.Services.VoiceService.{i}.Capabilities.ButtonMap	N/A
Device.Services.VoiceService.{i}.Capabilities.Codecs.	N/A
Device.Services.VoiceService.{i}.Capabilities.Codecs.{i}.	N/A
Device.Services.VoiceService.{i}.Capabilities.Codecs.{i}.BitRate	N/A
Device.Services.VoiceService.{i}.Capabilities.Codecs.{i}.Codec	N/A
Device.Services.VoiceService.{i}.Capabilities.Codecs.{i}.EntryID	N/A
Device.Services.VoiceService.{i}.Capabilities.Codecs.{i}.PacketizationPeriod	N/A
Device.Services.VoiceService.{i}.Capabilities.Codecs.{i}.SilenceSuppression	N/A
Device.Services.VoiceService.{i}.Capabilities.DigitMap	N/A
Device.Services.VoiceService.{i}.Capabilities.DSCPCoupled	N/A
Device.Services.VoiceService.{i}.Capabilities.EthernetTaggingCoupled	N/A
Device.Services.VoiceService.{i}.Capabilities.FaxPassThrough	N/A
Device.Services.VoiceService.{i}.Capabilities.FaxT38	N/A
Device.Services.VoiceService.{i}.Capabilities.FileBasedRingGeneration	N/A
Device.Services.VoiceService.{i}.Capabilities.FileBasedToneGeneration	N/A
Device.Services.VoiceService.{i}.Capabilities.MaxLineCount	N/A

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.Capabilities.MaxProfileCount	N/A
Device.Services.VoiceService.{i}.Capabilities.MaxSessionCount	N/A
Device.Services.VoiceService.{i}.Capabilities.MaxSessionsPerLine	N/A
Device.Services.VoiceService.{i}.Capabilities.ModemPassThrough	N/A
Device.Services.VoiceService.{i}.Capabilities.NumberingPlan	N/A
Device.Services.VoiceService.{i}.Capabilities.PatternBasedRingGeneration	N/A
Device.Services.VoiceService.{i}.Capabilities.PatternBasedToneGeneration	N/A
Device.Services.VoiceService.{i}.Capabilities.PSTNSoftSwitchOver	N/A
Device.Services.VoiceService.{i}.Capabilities.Regions	N/A
Device.Services.VoiceService.{i}.Capabilities.RingDescriptionsEditable	N/A
Device.Services.VoiceService.{i}.Capabilities.RingFileFormats	N/A
Device.Services.VoiceService.{i}.Capabilities.RingGeneration	N/A
Device.Services.VoiceService.{i}.Capabilities.RingPatternEditable	N/A
Device.Services.VoiceService.{i}.Capabilities.RTCP	N/A
Device.Services.VoiceService.{i}.Capabilities.RTPRedundancy	N/A
Device.Services.VoiceService.{i}.Capabilities.SignalingProtocols	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.EventSubscription	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.Extensions	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.ResponseMap	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.Role	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.TLSAuthenticationKeySizes	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.TLSAuthenticationProtocols	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.TLSEncryptionKeySizes	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.TLSEncryptionProtocols	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.TLSKeyExchangeProtocols	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.Transports	N/A
Device.Services.VoiceService.{i}.Capabilities.SIP.URISchemes	N/A
Device.Services.VoiceService.{i}.Capabilities.SRTP	N/A
Device.Services.VoiceService.{i}.Capabilities.SRTPEncryptionKeySizes	N/A
Device.Services.VoiceService.{i}.Capabilities.SRTPKeyingMethods	N/A
Device.Services.VoiceService.{i}.Capabilities.ToneDescriptionsEditable	N/A

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.Capabilities.ToneFileFormats	N/A
Device.Services.VoiceService.{i}.Capabilities.ToneGeneration	N/A
Device.Services.VoiceService.{i}.Capabilities.VoicePortTests	N/A
Device.Services.VoiceService.{i}.VoiceProfile.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.DTMFMethod	DTMF_Tx_Method_\<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Enable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.AnonymousCalEnable	Block_CID_Setting
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.AnonymousCallBlockEnable	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallerIDEnable	Block_CID_Setting
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallerIDName	Display_Name_\<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallForwardOnBusyNumber	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallForwardOnNoAnswerNumber	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallForwardOnNoAnswerRingCount	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallForwardUnconditionalEnable	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallForwardUnconditionalNumber	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallReturnEnable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallTransferEnable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallWaitingEnable	CW_Setting
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.ConferenceCallingSessionCount	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.ConferenceCallingStatus	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.DoNotDisturbEnable	DND_Setting
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.MaxSessions	Call_Appearances_Per_Line
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.MessageWaiting	Message_Waiting_\<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.MWIEnable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.RepeatDialEnable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.X_CISCO_SharedLineDNDCfwdEnable	Shared_Line_DND_Cfwd_Enable
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallState	N/A

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.BitRate	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.Codec	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.Enable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.EntryID	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.PacketizationPeriod	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.Priority	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.SilenceSuppression	Silence_Supp_Enable_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.ReceiveBitRate	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.ReceiveCodec	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.ReceiveSilenceSuppression	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.TransmitBitRate	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.TransmitCodec	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.TransmitPacketizationPeriod	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.TransmitSilenceSuppression	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.X_CISCO_PreferredCodec	Preferred_Codec_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.X_CISCO_PreferredCodec2	Second_Preferred_Codec_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.X_CISCO_PreferredCodec3	Third_Preferred_Codec_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.X_CISCO_UsePrefCodecOnly	Use_Pref_Codec_Only_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.X_CISCO_CodecNegotiation	Codec_Negotiation_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.DirectoryNumber	User_ID_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Enable	Line_Enable_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.PhyReferenceList	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.RingMuteStatus	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.RingVolumeStatus	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Session.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Session.{i}.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Session.{i}.FarEndIPAddress	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Session.{i}.FarEndUDPPort	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Session.{i}.LocalUDPPort	

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Session.{i}.SessionDuration	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Session.{i}.SessionStartTime	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.AuthPassword	Password_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.AuthUserName	User_ID_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.SIPEventSubscribeNumberOfElements	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.URI	SIP_URI_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_AuthID	Auth_ID_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_DisplayName	Display_Name_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_UseDNSSRV	Use_DNS_SRV_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_UserEqualPhone	User_Equal_Phone_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_SetG729annexb	Set_G729_annexb_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_BlindAttnXferEnable	Blind_Attn-Xfer_Enable_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_FeatureKeySync	Feature_Key_Sync_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.X_CISCO_DNSSRVAutoPrefix	DNS_SRV_Auto_Prefix_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Status	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.VoiceProcessing.	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.VoiceProcessing.EchoCancellationEnable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.VoiceProcessing.EchoCancellationInUse	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.VoiceProcessing.EchoCancellationTail	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.X_CISCO_DialPlan	Dial_Plan_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.X_CISCO_DefaultRing	Default_Ring_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.MaxSessions	Call_Appearances_Per_Line
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Name	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.NumberOfLines	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Region	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Reset	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.DSCPMark	RTP_TOS_DiffServ_Value_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.LocalPortMax	RTP_Port_Max
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.LocalPortMin	RTP_Port_Min
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.RTCP.	

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.RTCP.Enable	RTCP_Tx_Interval
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.RTCP.TxRepeatInterval	RTCP_Tx_Interval
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.SRTP.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.SRTP.Enable	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.SRTP.EncryptionKeySizes	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.SRTP.KeyingMethods	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.TelephoneEventPayloadType	AVT_Dynamic_Payload
Device.Services.VoiceService.{i}.VoiceProfile.{i}.RTP.X_CISCO_RTPPacketSize	RTP_Packet_Size
Device.Services.VoiceService.{i}.VoiceProfile.{i}.ServiceProviderInfo.	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.ServiceProviderInfo.ContactPhoneNumber	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.ServiceProviderInfo.EmailAddress	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.ServiceProviderInfo.Name	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.ServiceProviderInfo.URL	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SignalingProtocol	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.	
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.DSCPMark	SIP_TOS_DiffServ_Value_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.InviteExpires	INVITE_Expires
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.Organization	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.OutboundProxy	Outbound_Proxy_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.OutboundProxyPort	Outbound_Proxy_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.ProxyServer	Proxy_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.ProxyServerPort	Proxy_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.ProxyServerTransport	SIP_Transport_<1>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.RegisterExpires	Register_Expires_<i>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.RegisterRetryInterval	Reg_Retry_Intvl
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.RegistersMinExpires	Reg_Min_Expires
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.ReInviteExpires	ReINVITE_Expires
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.SIPEventSubscribeNumberOfElements	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.SIPResponseMapNumberOfElements	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerB	SIP_Timer_B
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerD	SIP_Timer_D
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerF	SIP_Timer_F

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerH	SIP_Timer_H
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerJ	SIP_Timer_J
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerT1	SIP_T1
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerT2	SIP_T2
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.TimerT4	SIP_T4
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.UserAgentDomain	N/A
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.UserAgentPort	SIP_Port_<1>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.UserAgentTransport	SIP_Transport_<1>_
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.X_CISCO_SubMinExpires	Sub_Min_Expires
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.X_CISCO_SubMaxExpires	Sub_Max_Expires
Device.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.X_CISCO_SubRetryIntvl	Sub_Retry_Intvl
Device.Services.VoiceService.{i}.VoiceProfile.{i}.STUNEnable	STUN_Enable
Device.Services.VoiceService.{i}.VoiceProfileNumberOfEntries	N/A
Device.Services.VoiceService.{i}.X_CISCO_SIP.	
Device.Services.VoiceService.{i}.X_CISCO_SIP.G711uCodecName	G711u_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.G711aCodecName	G711a_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.G729aCodecName	G729a_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.G729bCodecName	G729b_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.G722CodecName	G722_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.G7222CodecName	G722.2_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.iLBCCodecName	iLBC_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.OPUSCodecName	OPUS_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.AVTCodecName	AVT_Codec_Name
Device.Services.VoiceService.{i}.X_CISCO_SIP.G7222BEDynamicPayload	G722.2_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.G7222OADynamicPayload	G722.2_OA_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.iLBC20msDynamicPayload	iLBC_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.iLBC30msDynamicPayload	iLBC_30ms_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.OPUSDynamicPayload	OPUS_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.AVTDynamicPayload	AVT_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.AVT16kHzDynamicPayload	AVT_16kHz_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.AVT48kHzDynamicPayload	AVT_48kHz_Dynamic_Payload
Device.Services.VoiceService.{i}.X_CISCO_SIP.INFOREQDynamicPayload	INFOREQ_Dynamic_Payload

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.X_CISCO_SIP.DisplayAnonymousFromHeader	Display_Anonymous_From_Header
Device.Services.VoiceService.{i}.X_CISCO_SIP.RedirectKeepAlive	Redirect_Keep_Alive
Device.Services.VoiceService.{i}.X_CISCO_Regional.	
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.	
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.DialTone	Dial_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.OutsideDialTone	Outside_Dial_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.PromptTone	Prompt_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.BusyTone	Busy_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.ReorderTone	Reorder_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.OffHookWarningTone	Off_Hook_Warning_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.RingBackTone	Ring_Back_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.CallWaitingTone	Call_Waiting_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.ConfirmTone	Confirm_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.MWIDialTone	MWI_Dial_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.CfwdDialTone	Cfwd_Dial_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.HoldingTone	Holding_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.ConferenceTone	Conference_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.SecureCallIndicationTone	Secure_Call_Indication_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.PageTone	Page_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.AlertTone	Alert_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.MuteTone	Mute_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.UnmuteTone	Unmute_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.SystemBeep	System_Beep
Device.Services.VoiceService.{i}.X_CISCO_Regional.Tones.CallPickupTone	Call Pickup_Tone
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.	
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence1	Cadence_1
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence2	Cadence_2
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence3	Cadence_3
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence4	Cadence_4
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence5	Cadence_5
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence6	Cadence_6
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence7	Cadence_7

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence8	Cadence_8
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.Cadence9	Cadence_9
Device.Services.VoiceService.{i}.X_CISCO_Regional.Cadences.	
Device.Services.VoiceService.{i}.X_CISCO_Regional.ControlTimer.ReorderDelay	Reorder_Delay
Device.Services.VoiceService.{i}.X_CISCO_Regional.ControlTimer.InterdigitLongTimer	Interdigit_Long_Timer
Device.Services.VoiceService.{i}.X_CISCO_Regional.ControlTimer.InterdigitShortTimer	Interdigit_Short_Timer
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.	
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.NumberOfUnits	Number_of_Units
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.ServerType	
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.SubscribeRetryInterval	Subscribe_Retry_Interval
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.BXferOnSpeedDialEnable	Bxfer_On_Speed_Dial_Enable
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.AttendantConsoleLCDContrast	Attendant_Console_LCD_Brightness
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.BXferToStarcodeEnable	Bxfer_To_Starcode_Enable
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.Unit.	N/A
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.Unit.{i}.	N/A
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.Unit.{i}.Key.	N/A
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.Unit.{i}.Key.{i}.	N/A
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.Unit.{i}.Key.{i}.Config	Unit_<i>_Key_<i>_
Device.Services.VoiceService.{i}.X_CISCO_AttConsole.Unit.{i}.NumberOfKey	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LineKey.	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LineKey.{i}.	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LineKey.{i}.ExtendedFunction	Extended_Function_<i>_
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LineKey.{i}.Extension	Extension_<i>_
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LineKey.{i}.ShareCallApparence	Share_Call_Appearance_<i>_
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LineKey.{i}.ShortName	Short_Name_<i>_
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.NumberOfLineKey	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.StationName	Station_Name
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.GroupPagingScript	Group_Paging_Script
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.VoiceMailNumber	Voice_Mail_Number
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.BluetoothMode	Bluetooth_Mode
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Line	Line

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring1	Ring1
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring2	Ring2
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring3	Ring3
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring4	Ring4
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring5	Ring5
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring6	Ring6
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring7	Ring7
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring8	Ring8
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring9	Ring9
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring10	Ring10
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring11	Ring11
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.Ringtone.Ring12	Ring12
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.ConferenceServ	Coference_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.AttnTransferServ	Attn_Transfer_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.BlindTransferServ	Blind_Transfer_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.DNDServ	DND_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.BlockANCServ	Block_ANC_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.BlockCIDServ	Block_CID_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.SecureCallServ	Secure_Call_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.CfwdAllServ	Cfwd_All_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.CfwdBusyServ	Cfwd_Busy_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.CfwdNoAnsServ	Cfwd_No_Ans_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.PagingServ	Paging_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.CallParkServ	Call_Park_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.CallPickUpServ	Call_Pick_Up_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.ACDLoginServ	ACD_Login_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.GroupCallPickUpServ	Group_Call_Pick_Up_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.ServiceAnncServ	Service_Annc_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.CallRecordingServ	Call_Recording_Serv
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.SuppServices.ReversePhoneLookupServ	Reverse_Phone_Lookup_Serv

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ProgrammableSoftkeyEnable	Programmable_Softkey_Enable
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.IdleKeyList	Idle_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.MissedCallKeyList	Missed_Call_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.OffHookKeyList	Off_Hook_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.DialingInputKeyList	Dialing_Input_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ProgressingKeyList	Progressing_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ConnectedKeyList	Connected_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.StartXferKeyList	Start-Xfer_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.StartConfKeyList	Start-Conf_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ConferencingKeyList	Conferencing_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ReleasingKeyList	Releasing_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.HoldKeyList	Hold_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.RingingKeyList	Ringing_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.SharedActiveKeyList	Shared_Active_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.SharedHeldKeyList	Shared_Held_Key_List
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK1	PSK_1
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK2	PSK_2
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK3	PSK_3
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK4	PSK_4
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK5	PSK_5
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK6	PSK_6
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK7	PSK_7
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK8	PSK_8
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK9	PSK_9
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK10	PSK_10
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK11	PSK_11
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK12	PSK_12
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK13	PSK_13
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK14	PSK_14
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK15	PSK_15
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK16	PSK_16

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.	N/A
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.LDAPDirEnable	LDAP_Dir_Enable
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.CorpDirName	LDAP_Corp_Dir_Name
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.Server	LDAP_Server
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.SearchBase	LDAP_Search_Base
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.ClientDN	LDAP_Client_DN
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.UserName	LDAP_User_Name
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.Password	LDAP_Password
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.AuthMethod	LDAP_Auth_Method
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.LastNameFilter	LDAP_Last_Name_Filter
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.FirstNameFilter	LDAP_First_Name_Filter
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.SearchItem3	LDAP_Search_Item_3
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.SearchItem3Filter	LDAP_Item_3_Filter
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.SearchItem4	LDAP_Search_Item_4
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.SearchItem4Filter	LDAP_Item_4_Filter
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.DisplayAttrs	LDAP_Display_Attrs
Device.Services.VoiceService.{i}.X_CISCO_PhoneSetting.LDAP.NumberMapping	LDAP_Number_Mapping
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.	N/A
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.RingerVolume	Ringer_Volume
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.SpeakerVolume	Speaker_Volume
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.HandsetVolume	Handset_Volume
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.HeadsetVolume	Headset_Volume
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.PhoneBackground	Phone_Background
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.PictureDownloadURL	Picture_Download URL
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.ElectronicHookSwitchControl	Ehook_Enable
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.ScreenSaverEnable	Screen_Saver_Enable
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.ScreenSaverType	Screen_Saver_Type
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.MissCallShortcut	Miss_Call_Shortcut
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.AlertToneOff	Alert_Tone_Off
Device.Services.VoiceService.{i}.X_CISCO_UserSetting.LogoURL	Logo_URL
Device.Services.VoiceService.{i}.X_CISCO_StarCode.	N/A
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateBlockAnonymousCall	Block_ANC_Act_Code

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateBlockCallerId	Block_CID_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateBlockCallerIdNextCall	Block_CID_Per_Call_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateCallForwardAll	Cfwd_All_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateCallForwardBusy	Cfwd_Busy_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateCallForwardNoAnswer	Cfwd_No_Ans_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateCallWaiting	CW_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateCallWaitingNextCall	CW_Per_Call_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateDoNotDisturb	DND_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateSecureCall	Secure_All_Call_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.ActivateSecureCallNextCall	Secure_One_Call_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.BlindTransfer	Blind_Transfer_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.CallPark	Call_Park_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.CallPickup	Call_Pickup_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.CallReturn	Call_Return_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.CallUnpark	Call_Unpark_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateBlockAnonymousCall	Block_ANC_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateBlockCallerId	Block_CID_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateBlockCallerIdNextCall	Block_CID_Per_Call_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateCallForwardAll	Cfwd_All_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateCallForwardBusy	Cfwd_Busy_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateCallForwardNoAnswer	Cfwd_No_Ans_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateCallWaiting	CW_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateCallWaitingNextCall	CW_Per_Call_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateDoNotDisturb	DND_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateSecureCal	Secure_No_Call_Act_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.DeactivateSecureCallNextCall	Secure_One_Call_Deact_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.GroupCallPickup	Group_Call_Pickup_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PagingCode	Paging_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PreferCodecG711a	Prefer_G711a_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PreferCodecG711u	Prefer_G711u_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PreferCodecG722	Prefer_G722_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PreferCodecG7222	Prefer_G722.2_Code

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PreferCodecG729a	Prefer_G729a_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PreferCodeciLBC	Prefer_iLBC_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.PreferCodecOPUS	Prefer_OPUS_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.UseOnlyCodecG711a	Force_G711a_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.UseOnlyCodecG711u	Force_G711u_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.UseOnlyCodecG722	Force_G722_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.UseOnlyCodecG7222	Force_G722.2_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.UseOnlyCodecG729a	Force_G729a_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.UseOnlyCodeciLBC	Force_iLBC_Code
Device.Services.VoiceService.{i}.X_CISCO_StarCode.UseOnlyCodecOPUS	Force_OPUS_Code
	N/A
	N/A
*(1) We support such TR-069 configuration, but no corresponding parameter on Web/GUI	N/A
*(2) We support such TR-069 configuration, but can only be set to 'Yes"	N/A
*(3) i=0 G.711MuLaw i=1 G.711ALaw i=2 G.729a i=3 G.722 i=4 G.722.2 i=5 iLBC i=6 (88xx iSAC) (78xx OPUS) i=7 OPUS (88xx)	N/A
*(4) Only available on 8851/8861/8865	N/A
*(5) This parameter is for global setting, not per extension	N/A
*(6) This will leads to codec <i> on line <i> enable/disable, for codec <i>, please refer to *(4)	N/A
*(7) Only with sidecar. On mountlake it is named Attendant Console LCD Contrast	N/A
Device.	N/A
Device.DeviceSummary	N/A
Device.Services.	N/A
Device.Services.VoiceServiceNumberOfEntries	
Device.DeviceInfo.	N/A
Device.DeviceInfo.Manufacturer	N/A
Device.DeviceInfo.ManufacturerOUI	N/A
Device.DeviceInfo.ModelName	N/A
Device.DeviceInfo.Description	N/A
Device.DeviceInfo.ProductClass	N/A
Device.DeviceInfo.SerialNumber	N/A

TR-069 Parameter	XML Parameter
Device.DeviceInfo.HardwareVersion	N/A
Device.DeviceInfo.SoftwareVersion	N/A
Device.DeviceInfo.EnabledOptions	N/A
Device.DeviceInfo.AdditionalHardwareVersion	N/A
Device.DeviceInfo.AdditionalSoftwareVersion	N/A
Device.DeviceInfo.ProvisioningCode	N/A
Device.DeviceInfo.DeviceStatus	N/A
Device.DeviceInfo.UpTime	N/A
Device.ManagementServer.	N/A
Device.ManagementServer.URL	N/A
Device.ManagementServer.Username	N/A
Device.ManagementServer.Password	N/A
Device.ManagementServer.PeriodicInformEnable	N/A
Device.ManagementServer.PeriodicInformInterval	N/A
Device.ManagementServer.PeriodicInformTime	N/A
Device.ManagementServer.ParameterKey	N/A
Device.ManagementServer.ConnectionRequestURL	N/A
Device.ManagementServer.ConnectionRequestUsername	N/A
Device.ManagementServer.ConnectionRequestPassword	N/A
Device.GatewayInfo.	N/A
Device.GatewayInfo.ManufacturerOUI	N/A
Device.GatewayInfo.ProductClass	N/A
Device.GatewayInfo.SerialNumber	N/A
Device.Time.	N/A
Device.Time.NTPServer1	Primary_NTP_Server
Device.Time.NTPServer2	Secondary_NTP_Server
Device.Time.CurrentLocalTime	N/A
Device.Time.LocalTimeZone	Time_Zone
Device.Time.X_CISCO_TimeFormat	Time_Format
Device.Time.X_CISCO_DateFormat	Date_Format
Device.LAN.	N/A
Device.LAN.X_CISCO_IPMode	IP_Mode

TR-069 Parameter	XML Parameter
Device.LAN.AddressingType	Connection_Type
Device.LAN.IPAddress	Static_IP
Device.LAN.SubnetMask	NetMask
Device.LAN.DefaultGateway	Gateway
Device.LAN.DNSServers	Primary_DNS
Device.LAN.MACAddress	N/A
Device.LAN.DHCPOptionNumberOfEntries	N/A
Device.LAN.DHCPOption.	N/A
Device.LAN.DHCPOption.{i}.	N/A
Device.LAN.DHCPOption.{i}.Request	DHCP_Option_To_Use
Device.LAN.DHCPOption.{i}.Tag	DHCP_Option_To_Use
Device.LAN.DHCPOption.{i}.Value	DHCP_Option_To_Use
Device.Ethernet.	N/A
Device.Ethernet.X_CISCO_CDP	Enable_CDP
Device.Ethernet.X_CISCO_LLDP	Enable_LLDP-MED
Device.Ethernet.X_CISCO_EnableVLAN	Enable_VLAN
Device.Ethernet.X_CISCO_VLANID	VLAN_ID
Device.X_CISCO_Language.	N/A
Device.X_CISCO_Language.DictionaryServerScript	Dictionary_Server_Script
Device.X_CISCO_Language.LanguageSelection	Language_Selection
Device.X_CISCO_Language.Locale	Locale
Device.X_CISCO_XmlService.	N/A
Device.X_CISCO_XmlService.Password	XML_Password
Device.X_CISCO_XmlService.UserName	XML_User_Name
Device.X_CISCO_XmlService.XMLAppServiceName	XML_Application_Service_Name
Device.X_CISCO_XmlService.XMLAppServiceURL	XML_Application_Service_URL
Device.X_CISCO_XmlService.XMLDirServiceName	XML_Directory_Service_Name
Device.X_CISCO_XmlService.XMLDirServiceURL	XML_Directory_Service_URL
Device.X_CISCO_XmlService.CISCOXMLEXEEnable	CISCO_XML_EXE_Enable
Device.X_CISCO_XmlService.CISCOXMLEXEAuthMode	CISCO_XML_EXE_AUTH_MODE
Device.X_CISCO_RestrictedAccessDomains	Restricted_Access_Domains
Device.X_CISCO_EnableWebServer	Enable_Web_Server

TR-069 Parameter	XML Parameter
Device.X_CISCO_WebProtocol	Enable_Protocol
Device.X_CISCO_EnableDirectActionUrl	Enable_Direct_Action_Url
Device.X_CISCO_SessionMaxTimeout	Session_Max_Timeout
Device.X_CISCO_SessionIdleTimeout	Session_Idle_Timeout
Device.X_CISCO_WebServerPort	Web_Server_Port
Device.X_CISCO_EnableWebAdminAccess	Enable_Web_Admin_Access
Device.X_CISCO_HostName	Host_Name
Device.X_CISCO_Domain	Domain
Device.X_CISCO_UpgradeErrorRetryDelay	Upgrade_Error_Retry_Delay
Device.X_CISCO_UpgradeRule	Upgrade_Rule
Device.X_CISCO_ProfileRule	Profile_Rule
Device.X_CISCO_UserConfigurableResync	User_Configurable_Resync
Device.X_CISCO_HTTPReportMethod	HTTP_Report_Method
Device.X_CISCO_CWMPV1dot2Support	CWMP_V1.2_Support