Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Administration Guide, Release 9.3(4)

December 4, 2014
Revised: October 10, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

About This Document ix

Purpose ix

Document Audience ix

Organization ix

Document Conventions x

Get Started 1-1

Overview of the Conference Phone 1-1

Network Configurations 1-1

Other SIP IP PBX Call Control Systems 1-1

Use the Web-Based Configuration Utility 1-2

Determine the IP Address of the Phone 1-2

Allow Web Access to the Conference Phone 1-2

Save the Configuration Profile 1-2

Understand Administrator and User Views 1-3

Restrict User Access to the Phone Interface Menus 1-3

Access Administrative Options 1-3

Use the Web Administration Tabs 1-3

View Phone Information 1-4

View Reboot Reasons 1-4

View the Reboot History on the Phone Web User Interface 1-4

View the Reboot History on the Phone Screen 1-5

View the Reboot History in the Status Dump File 1-5

Wireless Microphone Region Setting 1-5

Customize Standard Features 2-1

Configure Phone Information and Display Settings 2-1

Configure the Phone Name 2-1

Customize the Startup Screen 2-1

Change the Display Background Picture 2-2

Configure the Screen Saver 2-3

Configure the LCD Contrast 2-4

Configure Back Light Settings 2-4

Call Appearances Per Line 2-4

Enable Call Features 2-4
Enable Call Transfer and Call Forwarding Services 2-4
Enable Conferencing 2-5
Enable Do Not Disturb 2-5
Configure Ring Tones 2-5
Assign a Ring Tone to an Extension 2-5
Configure Audio Settings 2-6
Configure the User Access Control 2-6
Enable and Configure the Phone Web Server 2-6
Configure the Web Server from the Phone Web Interface 2-6
Configure the Web Server from the Phone Screen Interface 2-7
Configure LDAP for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control 2-7
Configure BroadSoft Settings 2-10

Configure SIP and NAT 3-1

SIP and Cisco Unified IP Conference Phone 8831 for Third-Party Call Control 3-1
SIP Over TCP 3-2
SIP Proxy Redundancy 3-2
Dual Registration 3-2
Limitations for Dual Registration and DNS SRV Redundancy 3-3
Alternate Proxy and Dual Registration 3-3
Register Upon Failover/Recovery 3-3
Fallback Behavior 3-3
RFC3261 Support 3-3
Support for SIP NOTIFY XML-Service 3-3
Configure SIP 3-4
Configure Basic SIP Parameters 3-4
Configure SIP Timer Values 3-5
Configure Response Status Code Handling 3-6
Configure RTP Parameters 3-6
Configure SDP Payload Types 3-7
Configure SIP Settings for Extensions 3-7
Configure a SIP Proxy Server 3-8
Configure Subscriber Information Parameters 3-10
Configure NAT Support Parameters 3-10

Configure Security, Quality, and Network Features 4-1

Set Security Features 4-1
Configure Domain and Internet Settings 4-1
Configure Restricted Access Domains 4-1

Configure DHCP and Static IP Connection Type 4-1
Challenge SIP Initial INVITE Messages 4-2
Encrypt Signaling with SIP Over TLS 4-3
Configure Voice Codecs 4-3
Set Optional Network Servers 4-5
Configure VLAN Settings 4-5
Configure Cisco Discovery Protocol (CDP) 4-6
Configure LLDP-MED 4-6
TLV Information 4-7
Configure the VLAN Settings 4-12

Provisioning 5-1
Redundant Provisioning Servers 5-1
Retail Provisioning 5-2
Automatic In-House Preprovisioning 5-2
Use HTTPS 5-3
Server Certificates 5-3
Client Certificates 5-3
Obtain a Server Certificate 5-3
Manually Provision a Phone from the Keypad 5-4
Sample Configuration File 5-4
Update Profiles and Firmware 5-5
Allow and Configure Profile Updates 5-5
Allow and Configure Firmware Updates 5-7
Firmware Upgrade 5-7
Firmware Upgrade With a Browser Command 5-8
Configure a Custom Certificate Authority 5-8
General Purpose Parameters 5-9

Configure Dial Plan 6-1
About Dial Plan 6-1
Digit Sequences 6-1
Digit Sequence Examples 6-3
Acceptance and Transmission of the Dialed Digits 6-4
Dial Plan Timer (Off-Hook Timer) 6-5
Syntax for the Dial Plan Timer 6-5
Interdigit Long Timer (Incomplete Entry Timer) 6-5
Syntax for the Interdigit Long Timer 6-6
Interdigit Short Timer (Complete Entry Timer) 6-6

Syntax for the Interdigit Short Timer 6-6
Edit Dial Plan on the IP Phone 6-7
Reset the Control Timers 6-7

Configure Regional Parameters and Supplementary Services 7-1
Control Timer Values (sec) 7-1
Localize Your Conference Phone 7-2
Manage the Time and Date 7-3
Configure Daylight Saving Time 7-3
Daylight Saving Time Examples 7-4
Select a Display Language 7-4
Create a Dictionary Server Script 7-5
Localization Configuration Example 7-6

Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Field Reference A-1
Info A-1
System Status A-1
System Information A-1
Reboot History A-2
Product Information A-3
Phone Status A-3
Call Status A-3
Ext Status A-3
Call 1 Status/Call 2 Status A-4
Download Status A-6
Downloaded Ring Tone A-6
Downloaded Locale Package A-6
Firmware Upgrade Status A-6
Provisioning Status A-6
Custom CA Status A-7
Debug Info A-7
Console Logs A-7
Browser Info A-8
Voice A-8
System A-8
System Configuration A-8
Internet Connection Type A-9
Static IP Settings A-9
Optional Network Configuration A-9
VLAN Settings A-10

Inventory Settings A-11
SIP A-11
SIP Parameters A-11
SIP Timer Values A-12
Response Status Code Handling A-13
RTP Parameters A-14
SDP Payload Types A-14
NAT Support Parameters A-14
Provisioning A-14
Regional A-15
Control Timer Values (sec) A-15
Time A-15
Localization A-17
Phone A-17
QoS Settings A-17
General A-18
Miscellaneous Line Key Settings A-19
Supplementary Services A-19
BroadSoft Settings A-19
LDAP Corporate Directory Search A-20
XML Service A-22
User A-22
Call Forward A-22
Speed Dial A-22
Supplementary Services A-23
Audio A-23
LCD A-23
Extension A-23
General A-23
NAT Settings A-24
Call Feature Settings A-24
Call History A-24

Related Documentation B-1

Cisco IP Phone 8800 Series Documentation B-1
Cisco IP Phone Firmware Support Policy B-1
Documentation, Service Requests, and Additional Information B-1

About This Document

This guide describes the administration of the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control:

- Purpose, page ix
- Document Audience, page ix
- Organization, page ix
- Document Conventions, page x

Purpose

The document describes the administration of Cisco Unified IP Conference Phone 8831 for Third-Party Call Control devices.

Document Audience

This document is written for administrative staff responsible for administration of Cisco Unified IP Conference Phone 8831 for Third-Party Call Control devices.

Organization

This document is divided into the following chapters and appendices.

Chapter/Appendix	Contents
Chapter 1, “Get Started”	Contains basic information on Cisco Unified IP Conference Phone 8831 for Third-Party Call Control.
Chapter 2, “Customize Standard Features”	Describes customization of the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control. Includes the following topics: display settings, call features, ring tones, audio settings.

Chapter/Appendix	Contents
Chapter 3, “Configure SIP and NAT”	Describes configuration of the Session Initiation Protocol (SIP) phone protocol and Network Address Translation (NAT) support parameters.
Chapter 4, “Configure Security, Quality, and Network Features”	Describes how to configure security, voice quality, and optional network features for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control.
Chapter 5, “Provisioning”	Provides an overview of provisioning the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control. Details of provisioning are found in the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.
Chapter 6, “Configure Dial Plan”	Includes information about dial plans and procedures for configuring dial plans.
Chapter 7, “Configure Regional Parameters and Supplementary Services”	Describes use of the **Regional** tab to configure regional and local settings, such as control timer parameters, dictionary server script, language Selection, and locale to change localization.
Appendix A, “Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Field Reference”	This appendix describes the fields in the following sections (tabs) of the phone web user interface: Info, Voice, Call History.
Appendix B, “Related Documentation”	Provides links to resources for information and support.

Document Conventions

The following typographic conventions are used in this document.

Typographic Element	Meaning
Boldface	An option on a menu or a literal value to be entered in a field.
<parameter>	Angle brackets (<>) identify parameters that appear on the configuration pages of the administration web server.
Italic	A variable that should be replaced with a literal value.
`Monospaced Font`	A code sample or system output.

Get Started

This chapter contains basic information on Cisco Unified IP Conference Phone 8831 for Third-Party Call Control. This chapter contains the following sections:

- Overview of the Conference Phone, page 1-1
- Network Configurations, page 1-1
- Use the Web-Based Configuration Utility, page 1-2
- View Phone Information, page 1-4
- Wireless Microphone Region Setting, page 1-5

Overview of the Conference Phone

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control is a full-featured VoIP (Voice-over-Internet Protocol) phone that provides voice communication over an IP network. It provides all the features of traditional business phones, such as call forwarding, redialing, speed dialing, transferring calls, and conference calling. The Conference Phone is targeted for solutions centered on 3rd-Party SIP-based IP PBX.

For more information on phone features, see the data sheets for this product.

Network Configurations

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control is used as a part of a SIP network as it supports Session Initiation Protocol (SIP).

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

Other SIP IP PBX Call Control Systems

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control are 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 Unified IP Conference Phone 8831 for Third-Party Call Control.

Use the Web-Based Configuration Utility

Your phone system administrator can allow you to view the phone statistics and modify some or all of the parameters by using the phone web user interface. The features of the conference phone that can be modified by the user by using the phone web user interface are described in this document.

To access the IP phone configuration utility, launch a web browser on a computer that can reach the phone on the subnetwork and enter the IP address of the phone in your web browser address bar. For example, `http://192.168.1.8`. If you are connected to a VPN, you must first exit the VPN.

Note If your service provider disabled access to the configuration utility, you must contact the service provider to proceed.

Determine the IP Address of the Phone

The IP address is assigned by a DHCP server, so the phone must be booted up and connected to the subnetwork.

To display your IP address:

Step 1 Click **Admin Login > advanced > Info > System Status**.

Step 2 Scroll to **System Information**. The IP Address is displayed under Current IP.

Allow Web Access to the Conference Phone

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

For more information, see the provisioning guide for the conference phone.

To allow or disallow from the phone viewing of the phone web user interface:

Step 1 Click **Admin login > Advanced > Voice Tab > System**.

Step 2 Scroll to **System Configuration**.

Step 3 Set **Enable Web Server** to **Yes**.

Save the Configuration Profile

Click **Submit All Changes** when you have finished modifying the fields in the phone web user interface to update the configuration profile. The phone is rebooted and the changes are applied.

Click **Undo All Changes** if you want to clear all changes made this session and return to the parameter values set before the session began or since the last time you clicked **Submit All Changes**.

Understand Administrator and User Views

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control firmware provides specific privileges for login to a user account and an administrator account. The Administrator account name is **admin**, and the User account name is **user**. These account names cannot be changed. The Admin account is designed to give the service provider or VAR configuration access to the Cisco IP phone, while the User account is designed to give limited and configurable control to the end user of the device.

The User and Admin accounts can be independently password protected. If the service provider set an Administrator account password, you are prompted for it when you click **Admin Login**. If it does not yet exist, the screen is refreshed, displaying the administration parameters. No default passwords are assigned to either the Administrator or the User accounts. Only the Administrator account can assign or change passwords.

The Administrator account can view and modify all web profile parameters, including web parameters available to the user login. The phone system administrator can further restrict the parameters that a User account can view and modify by using a *provisioning profile*.

The configuration parameters that are available to the User account are configurable in the conference phone. User access to the conference phone web user interface can be disabled.

Restrict User Access to the Phone Interface Menus

The Admin account can set the phone web user interface to allow or disable access by the User account. Allowing User account access gives a user the option of setting parameters, such as speed dial numbers and caller ID blocking through the phone web user interface.

The ability to configure individual parameters can be restricted by using phone profile provisioning. For more information on provisioning, see the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide* on cisco.com.

To change the user account access to the phone LCD GUI setup menu:

Step 1 Click **Admin Login > advanced > Voice > System**.

Step 2 Under **System Configuration** in the Phone-UI-user-mode field, choose **Yes**.

Access Administrative Options

To access administrative options, either:

- Log in to the configuration utility, then click **Admin Login**.
- Enter the IP address of the phone in a Web browser and include the **admin/** extension. For example: `http://192.168.1.220/admin/`

Use the Web Administration Tabs

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

Appendix A, "Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Field Reference," briefly describes each parameter available on the phone web user interface.

View Phone Information

You can check the current status of the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control by clicking the **Info** tab. The Info tab shows information about all phone extensions, including phone statistics and the registration status.

View Reboot Reasons

The phone stores the most recent five reasons the phone was refreshed or rebooted. When the phone is reset to factory defaults, this information is deleted.

The list describes the reboot and refresh reasons for Cisco Unified IP Conference Phone 8831 for Third-Party Call Control.

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 was changed.

You can view the reboot history from the phone web user interface, the IP phone screen, and the phone Status Dump file (http://*phoneIP*/status.xml or http://*phoneIP*/admin/status.xml).

View the Reboot History on the Phone Web User Interface

The **Info > System Information > Reboot History** page 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 indicating 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 is displayed in reverse chronological order; the reason for the most recent reboot is displayed in **Reboot Reason 1**.

View the Reboot History on the Phone Screen

Reboot History is located under **Apps > Admin Settings > Status** menu. In the Reboot History window, the reboot entries are displayed in reverse chronological order, similar to the sequence that is displayed on the phone web user interface.

View the 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/>
```

Wireless Microphone Region Setting

The Wireless Microphone Frequency Lock enhancement provides a secure Digital Enhanced Cordless Telecommunications (DECT) frequency for wireless microphones by locking the wireless region setting.

When the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control is shipped from the manufacturer, the mask and the Wireless Microphone Region setting are already configured for a particular region. For all devices, no matter the firmware release, no wireless region setting is available to the user.

If your Cisco Unified IP Conference Phone 8831 for Third-Party Call Control is operating with an earlier firmware release, you must upgrade to firmware release 9.3(4) so that the Wireless Microphone Region can be locked. Six new firmware versions lock this setting for customers who are running firmware versions earlier than firmware release 9.3(4).

If a device is shipped with firmware release 9.3(4) or later, its wireless region setting is set during manufacturing to one of the following values:

- NA – North America
- EU – Europe
- JP – Japan
- BR– Brazil
- TW– Taiwan
- LA – Latin America

Note For devices that are shipped with firmware release 9.3(4) and later, the wireless region cannot be changed.

If a device is shipped with firmware release 9.3(3), only one wireless region, NA (North America), exists.

Note Although you cannot change the value of the Wireless Microphone Region setting, you can check its value. To do so, execute **Info > System Status > Product Information** and check the Wireless Microphone Region value on the webpage.

Refer to the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Release Notes for Firmware Release 9.3(4)* if you need to upgrade a device from firmware release 9.3(3) to 9.3(4).

Customize Standard Features

This chapter describes customizing the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control and contains the following sections:

- Configure Phone Information and Display Settings, page 2-1
- Enable Call Features, page 2-4
- Configure Ring Tones, page 2-5
- Configure Audio Settings, page 2-6
- Enable and Configure the Phone Web Server, page 2-6
- Configure LDAP for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control, page 2-7
- Configure BroadSoft Settings, page 2-10

Configure 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

Navigate to **Admin Login > advanced > Voice > Phone**.

Under **General**, enter the Station Display Name for the phone. This name displays on the phone LCD GUI in the top left corner.

Customize the Startup Screen

You can create a text or 128-by-48 pixel by 1-bit deep image logo to display when the conference phone boots up. A logo displays during the boot sequence for a short period after the Cisco logo displays.

To configure a custom logo:

Step 1 Click **Admin Login > advanced > Voice > Phone**.

To display a text logo, in the Text Logo field enter text as follows:

- Up to two lines of text
- Each line must be less than 32 characters
- Insert a new line character (\n) and escape code (%0a) between the two lines

  For example, `Super\n%0aTelecom` displays:

  ```
  Super
  Telecom
  ```

- Use the **+** character to add spaces for formatting. You can add multiple **+** characters before and after the text to center it.

Step 2 To display a picture logo:

a. In the PNG Picture Download URL field, enter the path, for example:

`http://192.168.2.244/pictures/image04_128x48.png`

(you can also use a TFTP server)

b. Change **Select Logo** to **PNG Picture.**

Step 3 Click **Submit All Changes**. The phone reboots, retrieves the .png file, and displays the picture when it next boots.

Note The phone image file types supported are:

- Bitmap format, 1 bit-per-pixel color, size 128-by-48 pixels.

Change the Display Background Picture

You can use a picture to customize the background on the phone screen.

When the *PNG Picture Download URL* is changed, the phone compares the URL to the previous image URL. (If the URLs are the same, the phone does not perform the download.) If the URLs are different, the phone downloads the new image and displays it (providing the *Select Background Picture* field is set to **PNG Picture**).

The phone does not reboot after you change the background image URL.

A background image is displayed while the phone is running. To display a logo during the phone boot sequence.

Step 1 Copy the image to a TFTP or HTTP server that is accessible from the phone.

Step 2 Click **Admin Login > advanced > Voice > Phone**.

Step 3 Select the background picture in the Select Background Picture menu:

- None–Does not display a background picture.

- PNG Picture–Displays the **PNG Picture Download URL** picture.
- Text Logo–Displays the text string in the Text Logo field.

Step 4 If you selected None, in Step 3, go to Step 6. If you selected **Text Logo** in Step 3, go to Otherwise, enter the URL of the image file you want in **PNG Picture Download URL**. The URL must include the TFTP or HTTP server name (or IP address), directory, and filename, for example:

`tftp://myserver.mydomain.com/images/downloadablepicture.png`

or

`http://myserver.mydomain.com/images/downloadablepicture.png`

If the HTTP Refresh Timer is set in the server response to **PNG Picture Download URL**, the phone downloads the picture from the link and displays it on the phone scree. The phone automatically retrieves the picture after the specified number of seconds.

Step 5 If you selected **Text Logo**, enter a text string in the Text Logo field.

Step 6 Click **Submit All Changes**.

Configure the Screen Saver

You can configure a screen saver for the IP conference phone. When the phone is idle for a specified time, it enters screen saver mode.

Any button press returns the phone to normal mode. If a user password is set, the user must enter it to exit screen saver mode.

To configure the screen saver:

Step 1 Click **Admin Login > advanced > Voice > Phone**.

In the General section, in the **Screen Saver Enable** field, choose **Yes** to enable.

Step 2 In the **Screen Saver Wait** field, enter the number of seconds of idle time to elapse before the screen saver starts.

Step 3 In the **Screen Saver Icon** field, choose the display type:

- A background picture.
- The station time in the middle of the IP phone screen.
- A moving padlock icon. When the phone is locked, the status line displays a scrolling message “Press any key to unlock your phone.”
- Cisco logo.
- The station date and time on the IP phone screen.

Step 4 Click **Submit All Changes**.

Configure the LCD Contrast

You can configure the LCD contrast on the IP conference phone.

To configure the contrast for the IP phone screen on the phone:

Step 1 Click **Admin Login > advanced > User**.

Step 2 Under **LCD**, in the **LCD Contrast** field, enter a number value from 1 to 30. The higher the number, the greater the contrast on the IP phone screen.

Step 3 Click **Submit All Changes**.

Configure Back Light Settings

To configure the back light settings for the IP phone screen on the phone:

Step 1 Click **Admin Login > advanced > Voice > User**.

Step 2 Under **LCD** in the **Back Light Timer** field, enter the number of seconds of idle time that can elapse before the back light turns off.

Step 3 Click **Submit All Changes**.

Call Appearances Per Line

The IP conference phone is a single-line conference phone.

To expand the call appearances per line:

Step 1 Click **Admin Login > advanced > Voice > Phone**.

Step 2 In the **Miscellaneous Line Key Settings** section in the **Call Appearance Per Line** field, choose how many calls per line to allow from the drop-down.

Enable Call Features

This section describes how to enable and disable call features on the IP conference phone.

Enable Call Transfer and Call Forwarding Services

You can transfer or forward a call when the service is enabled.

Step 1 Click **Admin Login > advanced > Voice > Phone**.

Step 2 Under **Supplementary Services**, under the transfer type you want to enable, choose **Yes**:

- **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.

You can also enable or disable call forwarding:

- **Cfwd All**—Forwards all calls.
- **Cfwd Busy**—Forwards calls only if the line is busy.
- **Cfwd No Ans**—Forwards calls only if the line is not answered.

Step 3 Click **Submit All Changes**.

Enable Conferencing

To allow the user to perform call conferencing, navigate to **Admin Login > advanced > Voice > Phone**. Under **Supplementary Services** in the Conference Serv field, choose **Yes** to enable.

Enable Do Not Disturb

You can allow users to turn the Do Not Disturb feature on or off. This feature plays a message to the caller saying the user is unavailable. On the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control, the users can press the **Ignore** softkey to divert a ringing call to another destination.

This feature is not configurable on web page, and only applicable using the LCD soft key.

Configure Ring Tones

Click **Admin Login > advanced >Info > Download Status** and scroll to the **Downloaded Ring Tone** section to see the status of the ringtone download.

Assign a Ring Tone to an Extension

To assign a ring tone to an extension:

Step 1 Click **Admin Login > advanced > Voice > Extension** tab.

Step 2 Under **Call Feature Settings** in the **Default Ring** field, choose from the following:

- No Ring
- 1 through 10

Step 3 Click **Submit All Changes**.

Configure Audio Settings

You can configure default audio settings for the phone. The volume settings can be modified by the user by pressing the volume control button on the phone, then pressing the **Save** soft button.

To configure the audio volume settings:

Step 1 Click **Admin Login > advanced > Voice > User**.

Step 2 In the Audio Volume section, configure a volume level between 1 and 10, with 1 being the lowest level:

Parameter	Description
Ringer Volume	Sets the volume for the ringer.
Speaker Volume	Sets the volume for the full-duplex speakerphone.

Step 3 Click **Submit All Changes**.

Configure the User Access Control

Only the user access attribute “ua” is respected by the conference phone device. For a specific parameter, the “ua” attribute defines access by the user account to the administration web server. If “ua” attribute is not specified, the factory default user access is applied for the corresponding parameter. Access by the Admin account is unaffected by this attribute.

Note The value of the element attributes must be enclosed by double quotes.

The “ua” attribute must have one of the following values:

- na – no access
- ro – read-only
- rw – read/write

Enable and Configure the 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 Web Interface

To enable the web server:

Step 1 Click **Admin Login > advanced > System**.

Step 2 Under the **System Configuration** section in the **Enable Web Server** field, verify that the parameter is set to **Yes** to enable the web administration server.

Step 3 In the **Web Server Port** field, enter the port to access the web server. The default is port 80.

Step 4 In the **Enable Web Admin Access** field, you can enable or disable local access to the **Admin Login** of the phone web user interface. Defaults to Yes (enabled.)

Step 5 In the **Admin Passwd** 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 maximum password length is 32 characters.

Step 6 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 maximum password length is 32 characters

Step 7 Click **Submit All Changes**.

Configure the Web Server from the Phone Screen Interface

To enable the phone web user interface from the **Phone** tab:

Step 1 Press menu.

Step 2 Select **Network** and **Enable Web Server**.

Step 3 Select **Edit**.

Step 4 Press y/n to toggle the selection to **Yes** and enable.

Step 5 Click **OK > Save**.

Configure LDAP for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control 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. There is a limit of 20 records returned from a LDAP search.

The instructions in this section assume you have the following equipment and services:

- A LDAP server, such as OpenLDAP or Microsoft Active Directory Server 2003

To prepare the LDAP Corporate Directory Search:

Step 1 Click **Admin Login > advanced > System**.

Step 2 In the **Optional Network Configuration** section, under **Primary DNS**, enter the IP address of the DNS server. (Only required if using Active Directory with authentication set to MD5.)

Step 3 In the **Optional Network Configuration** section, under **Domain**, enter the LDAP domain. (Only required if 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 Under **LDAP**, in the **LDAP Dir Enable** field, choose **Yes** to enable LDAP and cause the name defined in **LDAP Corp Dir Name** to appear in the phone directory.

Step 6 Configure values for the fields in the following table and click **Submit All Changes**.

Parameter	Description
LDAP Corp Dir Name	Enter a free-form text name, such as *Corporate Directory*.
LDAP Server	Enter a fully qualified domain name or IP address of LDAP server, in the format `nnn.nnn.nnn.nnn`. Enter the host name of the LDAP server if the MD5 authentication method is used.
LDAP Auth Method	Select the authentication method that the LDAP server requires: 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 create 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.
LDAP Client DN	Enter the distinguished name domain components [dc] ; for example: `dc=cv2bu,dc=com` If using the default Active Directory schema (Name(cn)->Users->Domain), example of the client DN: `cn="David Lee",dc=users,dc=cv2bu,dc=com`
LDAP Username	Enter the username for a credentialed user on the LDAP server.
LDAP Password	Enter the password for the LDAP username.
LDAP 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`
LDAP Last Name Filter	Define the search for surnames [sn], known as last name in some parts of the world. For example, `sn:(sn=*$VALUE*)`. This searches for the text string anywhere in the beginning, middle, or at the end of a name. You must enter a value in both the last name and first name fields so that the LDAP corporate directory option displays on the phone. If both fields are empty, the directory does not display.

Parameter	Description
LDAP First Name Filter	Define the search for the common name `[cn]`. For example, `cn:(cn=*$VALUE*)`. This searches for the text string anywhere in the beginning, middle, or at the end of a name. You must enter a value in both the last name and first name fields so that the LDAP corporate directory option displays on the phone. If both fields are empty, the directory does not display.
LDAP Search Item 3	Enter a customized search item. Can be blank if not needed.
LDAP Item 3 Filter	Enter a customized filter for the searched item. Can be blank if not needed.
LDAP Search Item 4	Enter a customized search item. Can be blank if not needed.
LDAP Item 4 Filter	Enter a customized filter for the searched item. Can be blank if not needed.
LDAP Display Attrs	Enter the format of LDAP results display 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`, **t** is of type phone number and 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 `ipPhone` number being dialable and the mobile number is ignored. • p—phone number When **p** is assigned to a type attribute, example `t=p`, the the retrieved number is dialable.
LDAP Number Mapping	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 `(<:9>xx.>)` to the LDAP Number Mapping field. For example, 555 1212 will become 9555 1212. Can be blank if not needed. 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.

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 configure the BroadSoft Directory service:

Step 1 Click **Admin Login > advanced > Voice > Phone**.

Step 2 Under **Broadsoft Settings**, configure the following:

- Directory Enable: Set to **Yes**.
- XSI Host Server: Enter the name of the server; for example, `xsp.xdp.com`.
- Directory Name: Name of the directory. Displays on the user phone as a directory choice (for example, **John's Personal Directory**).
- Directory Type: Select the type of BroadSoft directory:
  - Enterprise (default): 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.
- Directory UserID: BroadSoft User ID of the phone user; for example, johndoe@xdp.com.
- Directory Password: Alphanumeric password associated with the User ID.

To improve security, the phone firmware places access restrictions on the host server and directory name entry fields.

Field	Access Restriction
Dir. Name	Admin password required (if set)
Host Server	Admin password required (if set)
Type	None
User ID	None
Password	None

Step 3 Click **Submit All Changes**.

Configure SIP and NAT

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control uses the following protocol:

- Session Initiation Protocol (SIP)

This chapter describes how to configure the SIP phone protocol:

- SIP and Cisco Unified IP Conference Phone 8831 for Third-Party Call Control, page 3-1
- Configure SIP, page 3-4
- Configure NAT Support Parameters, page 3-10

SIP and Cisco Unified IP Conference Phone 8831 for Third-Party Call Control

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control 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 requesting phone is called the SIP user agent server (UAS), while the receiving 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 is routed back to the UAS, and a direct peer-to-peer session is established between the two UAs. Voice traffic is transmitted between UAs over dynamically-assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; it 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, Cisco conference 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 UDP ports have of being blocked by corporate firewalls. With TCP, new ports do not need to be opened 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 agents are served by different domains, for example, you would 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 conference 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 host names, priority, listening ports, and so forth. The Cisco conference phone tries to contact the hosts in the order of their priority.

If the Cisco conference 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 via primary proxy first. If there is no response for the new INVITE from the primary proxy, after timeout, the phone should attempt with the alternate proxy.

Dual registration is supported per line basis. Three new parameters are added which can be configured via Web GUI and remote provisioning:

- Alternate Proxy—Default is empty
- Alternate Outbound Proxy—Default is empty
- Dual Registration—Default is NO (turned off)

Upon configuring the parameters, reboot the phone for the feature to take effect.

Note The administrator should specify a value for primary proxy (or primary outbound proxy) and alternate proxy (or alternate outbound proxy) for the feature to function properly.

Limitations for Dual Registration and DNS SRV Redundancy

The limitations for Dual Registration and DNS SRV redundancy are as follows:

- When Dual Registration is enabled, DNS SRV Proxy Fallback/Recovery must be disabled.
- Do not use Dual Registration in conjunction with other Fallback/Recovery mechanisms. For example: Broadsoft mechanism.
- There is no recovery mechanism for feature request. However, the administrator can adjust the re-registration time for a prompt update of the registration state for primary and alternate proxy.

Alternate Proxy and Dual Registration

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

Register Upon Failover/Recovery

- Failover—The phone performs a failover to secondary proxy when the SIP request gets no response from primary proxy.
- Recovery—The phone attempts to re-register with the primary proxy while registered or actively connected to the secondary proxy.

Fallback Behavior

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

If the Proxy Fallback Intvl exceeds, 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 is triggered 600 seconds later.

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

After successfully registering back to primary server, all the SIP messages go to primary server.

RFC3261 Support

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control supports RFC-3261, the SIP UPDATE Method.

Support for SIP NOTIFY XML-Service

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control support 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 be 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
```

Configure SIP

SIP settings for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control are configured for the phone in general and for the extensions.

Configure Basic SIP Parameters

To configure general SIP parameters, navigate to **Admin Login > advanced > Voice > SIP**. Under **SIP Parameters**, make these changes:

Parameter	Description
Max Forward	The number of proxies or gateways that can forward the request to the next downstream server. The Max-Forwards value is an integer in the range of 0 to 255 indicating the remaining number of times the request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The initial value is 70.
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. The default is 5.
SIP User Agent Name	User-Agent header used in outbound requests. The default is $VERSION. If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed.
SIP Server Name	Server header used in responses to inbound responses. The default is **$VERSION**.
SIP Reg User Agent Name	User-Agent name used in a REGISTER request. If not specified, the SIP User Agent Name is used for the REGISTER request.
SIP Accept Language	The preferred languages for reason phrases, session descriptions, or status responses carried as message bodies in the response. If blank, the header is not included and the server assumes that all languages are acceptable to the client. Defaults to blank.
RFC 2543 Call Hold	If set to **Yes**, the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control includes Session Description Protocol (SDP) syntax c=0.0.0.0 when sending a SIP re-INVITE to a peer to hold the call. If set to No, the phone does not include the c=0.0.0.0 syntax in the SDP. With either setting, the phone includes a=sendonly syntax in the SDP. Defaults to Yes.
SIP TCP Port Min	Lowest TCP port number that can be used for SIP sessions. Defaults to 5060.

Parameter	Description
SIP TCP Port Max	Highest TCP port number that can be used for SIP sessions. Defaults to 5080.
Caller ID Header	Select from where the IP phone gets the caller ID: PAID-RPID-FROM PAID-FROM RPID-PAID-FROM RPID-FROM FROM header Defaults to PAID-RPID-FROM.
Max INVITE Retry Attempts	Maximum number of INVITE retry attempts by the phone. Defaults to 6.
Max NON-INVITE Retry Attempts	Maximum number of NON-INVITE retry attempts by the phone. Defaults to 6.

Configure SIP Timer Values

All SIP timer values are in seconds. To configure SIP timer values, navigate to **Admin Login > advanced > Voice > SIP.** Under **SIP Timer Values** (sec), make these changes:

Parameter	Description
SIP T1	RFC-3261 T1 value (RTT estimate). Ranges from 0 to 64 seconds. Defaults to 0.5 seconds.
SIP T2	RFC-3261 T2 value, the maximum retransmit interval for non-INVITE requests and INVITE responses. Ranges from 0 to 64 seconds. Defaults to 4 seconds.
INVITE Expires	The length of time the INVITE is valid. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 2000000. Defaults to 240 seconds.
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. Defaults to 30
Reg Retry Intvl[1]	Interval to wait before the phone retries registration after failing during the previous registration. The range is from 1 to 2147483647. Do not enter 0. Defaults to 30 seconds.
Reg Retry Long Intvl	When registration fails with a SIP response code that does not match the Retry Reg response status code (RSC) value (see next table), the phone waits for this 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. The range is from 0 to 2147483647. Defaults to 1200 seconds.

Parameter	Description
Reg Retry Random Delay	Random delay added to the Register Retry Intvl value 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. Defaults to 0, which disables this feature.
Reg Retry Long Random Delay	Random delay added to Register Retry Long Intvl value when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the long timer. Random delay range (in seconds) to add to the Register Retry Long Intvl when retrying REGISTER after a failure. Defaults to 0, which disables this feature.
Reg Retry Intvl Cap	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.

1. 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.

Configure Response Status Code Handling

To configure response status code handling , under **Response Status Code Handling** make these changes:

- **Try Backup RSC**—SIP response code that retries a backup server for the current request. Defaults to blank.
- **Retry Reg RSC**—Interval the device waits before re-trying registration after a failed registration. Defaults to blank.

Configure RTP Parameters

To configure Real-time Transport Protocol (RTP), navigate to **Admin Login > advanced > Voice > SIP**. Under **RTP Parameters**, configure these fields:

- **RTP Port Min**—Minimum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> defines a range that contains at least 10 even number ports (twice the number of lines); for example, 100–106. Defaults to 16384.
- **RTP Port Max**—Maximum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> should define a range that contains at least 10 even number ports (twice the number of lines); for example, 100–106. Defaults to 16482.
- **RTP Packet Size**—Packet size in seconds. The range is from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. Defaults to 0.02.
- **RTCP Tx Enable**—To enable Real-Time Transport Control Protocol (RTCP) sender report on an active connection. Defaults to no.

During an active connection, the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control sends out compound RTCP packets. Each compound RTP packet, except the last one, contains a sender report (SR) and a source description (SDES). The last RTCP packet contains an additional BYE packet. Each SR, except the last one, contains one receiver report (RR); the last SR carries no RR.

The SDES contains CNAME, NAME, and TOOL identifiers:

- **CNAME**—*User ID@Proxy*
- **NAME**—*Display Name* (or *Anonymous* if user blocks caller ID)
- **TOOL**—Vendor/Hardware-platform-software-version.

Configure SDP Payload Types

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

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

To configure SDP payload types, navigate to **Admin Login > advanced > Voice > SIP**. Under **SDP Payload Types**, configure these parameters:

Parameter	Description
AVT Dynamic Payload	Any non-standard data. Both sender and receiver must agree on a number. Ranges from 96 to 127. Defaults to 101.

Configure SIP Settings for Extensions

To configure SIP settings, navigate to **Admin Login > advanced > Voice > Extension**. Under **SIP Settings**, configure the following fields:

Parameter	Description
SIP Transport	Select from **UDP**, **TCP** or **TLS**. Defaults to UDP.
SIP Port	Port number of the SIP message listening and transmission port. Defaults to 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. Defaults to No.

Parameter	Description
Auth Resync-Reboot	The Cisco Unified IP Conference Phone 8831 authenticates the sender when it receives a NOTIFY message with the following requests: • resync • reboot • report • restart • XML-service Select **Yes** to enable. Defaults to Yes.
SIP Remote-Party-ID	The Remote-Party-ID header to use instead of the From header. Select **Yes** to enable. Defaults to Yes.
Refer-To Target Contact	Indicates the refer-to target. Select **Yes** to send the **SIP Refer** to the contact. Defaults to No.
SIP Debug Option	How SIP messages are received at or sent from the proxy listen port to the log. Select: • Default—No messages. • Current—Logs all the current SIP messages in full text • Full—Logs all SIP messages in full text.
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**. Defaults to No.
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy. To enable this feature, select **Yes**. Defaults to No.
User Equal Phone	When a tel URL is converted to a SIP URL and the telephone 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**. The default value is No.

Configure a SIP Proxy Server

To configure SIP proxy and registration parameters, navigate to **Admin Login > advanced > Voice > Extension**. Under **Proxy and Registration**, configure the following fields:

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. The default is port 5060.
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 fallback when there is network partition at he 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 fallback 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.
Register	Enables periodic registration with the proxy. This parameter is ignored if a proxy is not specified. To enable this feature, select **Yes**. Defaults to 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**. Defaults to No.
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. Defaults to 3600 seconds.
Use DNS SRV	Enables DNS SRV lookup for the proxy and outbound proxy. To enable this feature, select **Yes**. Otherwise, select **No**. Defaults to No.

Parameter	Description
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. Defaults to 3600 seconds.
Dual Registration	Set to **Yes** to enable the Dual registration/Fast Fallback feature. To enable the feature you must also configure the alternate proxy/alternate outbound proxy fields in the Proxy and Registration section.

Configure Subscriber Information Parameters

To configure subscriber information parameters for each extension, navigate to **Admin Login > advanced > Voice > Extension**. Under **Subscriber Information**, configure the following fields:

Parameter	Description
Display Name	Name displayed as the caller ID.
User ID	Extension number for this line.
Password	Password for this line. Defaults to blank (no password required).
Auth ID	Authentication ID for SIP authentication. Defaults to 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_>`

Configure NAT Support Parameters

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.

To configure NAT support parameters on the phone:

Step 1 Click **Voice > SIP** and navigate to **NAT Support Parameters**.

Step 2 Set a value to the parameter **NAT Keep Alive Intvl**.

Step 3 Enter the public IP address for your router.

Step 4 Click the **Extension** tab and navigate to **NAT Settings**.

Step 5 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 6 Click **Submit All Changes**.

Step 7 Configure the firewall settings on your router to allow SIP traffic. See the "Configure SIP" section on page 3-4.

Configure Security, Quality, and Network Features

This chapter describes how to configure security, voice quality, and optional network features for the phone:

- Set Security Features, page 4-1
- Configure Voice Codecs, page 4-3
- Set Optional Network Servers, page 4-5
- Configure VLAN Settings, page 4-5

Set Security Features

The security features ensure that calls are secure and authenticated.

Configure Domain and Internet Settings

Configure Restricted Access Domains

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

To configure restricted access domains, navigate to **Admin Login > advanced > Voice > System**. Under **System Configuration** in the Restricted Access Domains field. Enter fully-qualified domain names (FQDNs) for each SIP server you want the phone to respond to. Separate FQDNs with semicolons. For example, `voiceip.com;voiceip1.com`.

Configure DHCP and Static IP Connection Type

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

- Dynamic Host Configuration Protocol (DHCP) receives an IP address from the network DHCP server. The IP conference phones typically operate in a network where a DHCP server assigns the devices their IP addresses. Because IP addresses are a limited resource, the DHCP server periodically renews the device lease on the IP address. If a phone loses its IP address for any reason, or if some other device on the network is assigned its 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.

To set the connection type, navigate to **Admin Login > advanced > Voice > System**. Under **Internet Connection Type** choose the Connection Type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP, and configure the following:
  - **Static IP Address** of the phone.
  - **Netmask** of the phone.
  - **Gateway** IP address

DHCP Option Support

The table shows the DHCP options that are supported on the conference phones:

Network Standard	
DHCP option 1	Subnet mask
DHCP option 2	Time Offset
DHCP option 3	Router
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
DHCP option 60	Vendor class identifier
DHCP option 66	TFTP server name
DHCP option 125	Vendor-Identifying Vendor-Specific Information
DHCP option 150	TFTP server
DHCP option 158	
DHCP option 159	
DHCP option 160	

Challenge SIP Initial INVITE Messages

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

To configure SIP INVITE challenge, navigate to **Admin Login > advanced > Voice > Extension**. Under **SIP Settings** in the Auth INVITE field, choose **Yes**.

Encrypt Signaling with SIP Over TLS

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, it ensures that the connection is private by using 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 IP conference phone uses UDP as a standard for SIP transport, but they also support SIP over TLS for added security.

To enable TLS for the phone, navigate to **Admin Login > advanced > Voice > Extension**. Under **SIP Settings**, select **TLS** from the SIP Transport list.

Configure 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. If the G.729a codec is enabled and included in the codec list, that resource is tied up until the end of the call whether or not the call actually uses G.729a. If the G729a resource is already allocated (and since only one G.729a resource is allowed per IP phone), no other low-bit-rate codec can be allocated for subsequent calls. The only choices are G711a and G711u.

Negotiation of the optimal voice codec sometimes depends on the ability of the conference 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.

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

To configure the voice codecs on each extension, navigate to **Admin Login > advanced > Voice > Extension**. Under **Audio Configuration**, configure the following parameters:

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 • G729ab • G722 • iLBC Defaults to G711u.
Use Pref Codec Only	To use only the preferred codecs for all calls, select **Yes**. (The call fails if the far end does not support these codecs.) Otherwise, select **No**. Defaults to No.
Second Preferred Codec	If the first codec fails, this codec is tried. Defaults to **unspecified**.
Third Preferred Codec	If the second codec fails, this codec is tried. Defaults to **unspecified**.
G711u Enable	Enables use of the G.711u codec. Defaults to Yes.
G711a Enable	Enables use of the G.711a codec. Defaults to Yes.
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select **Yes**. Otherwise, select **No**. Defaults to Yes.
G722 Enable	Enables use of the G.722 codec. Defaults to Yes.
iLBC Enable	Enables use of the iLBC codec. Defaults to Yes.
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select **Yes**. Otherwise, select **No**. Defaults to No.
DTMF Tx Method	The method for transmitting DTMF signals to the far end. The options are: InBand, audio video transport (AVT), INFO, Auto, InBand+INFO, or AVT+INFO. • InBand sends DTMF by using the audio path. • AVT sends DTMF as AVT events. • INFO uses the SIP INFO method. • Auto uses InBand or AVT based on the outcome of codec negotiation. Defaults to Auto.

Set Optional Network Servers

Optional network servers provide resources such as DNS lookup, network time, logging, and device discovery.

To configure the (PoE) requirements, navigate to **Admin Login > advanced > Voice > System.** Under **Optional Network Configuration** configure the following fields:

- Host Name—The host name of the phone.
- Domain—The network domain of the phone. If using LDAP see the "Configure LDAP for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control" section on page 2-7.
- Primary DNS—DNS server used by the phone in addition to the DHCP-supplied DNS servers (if DHCP is enabled), When DHCP is disabled, this is the primary DNS server. Defaults to 0.0.0.0. If using LDAP see the "Configure LDAP for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control" section on page 2-7.
- Secondary DNS—DNS server used by the phone in addition to the DHCP-supplied DNS servers (if DHCP is enabled), When DHCP is disabled, this is the secondary DNS server. Defaults to 0.0.0.0.
- Syslog Server—Syslog server name and port for logging system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.
- Debug Level—The debug level ranges from 0 to 3. The higher the level, the more debug information is generated. Zero (0) means no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Defaults to 0.
- Primary NTP Server—IP address or name of the primary NTP server used to synchronize its time. Defaults to blank.
- Secondary NTP Server—IP address or name of the secondary NTP server used to synchronize its time. Defaults to blank.
- DNS Cache TTL Ignore—When set to Yes, the DNS query results are not cached. When set to No, the phone will cache the A/AAAA/SRV/CNAME record according to the TTL responses. Defaults to Yes.
- SSH Access— The administrator can be configure this parameter to control the SSH console. Defaults to No.
- SSH User ID—The administrator can set the User ID for SSH login. Defaults to blank.
- SSH Password—The administrator can set the Password for SSH login. Defaults to blank.

Configure VLAN Settings

If you use a VLAN, your phone voice packets are tagged with the VLAN ID.

Configure Cisco Discovery Protocol (CDP)

CDP is negotiation-based and determines which VLAN the IP phone resides in. If you are using a Cisco switch, Cisco discovery protocol (CDP) is available and is enabled by default. CDP:

- 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 IP conference phone.

Configure LLDP-MED

The IP conference phones support 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 IP conference phone operates as LLDP-MED Media End Point Class III devices 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 IP conference phone supports only the following limited set of TLVs as 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 above TLVs when 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 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 is not supported.
- SNMP and corresponding MIBs are not supported.
- Recording and retrieval of statistical counters are not supported.
- There is no full validation of all TLVs; TLVs that do not apply to the phones are ignored.
- Protocol state machines as stated in the standards are only used for reference.

TLV Information

These sections provide the TLV information.

Chassis ID TLV

For the outgoing LLDPDU, the TLV supports sub-type=5 (Network Address). When IP address is known, the value of 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 Chassis ID is `0.0.0.0`. The only INAN address family supported is IPv4. Currently, IPv6 address for the Chassis ID is not supported. For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form MSAP identifier. The value is not validated against its sub-type. 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 sub-type=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID in wired or wireless mode. 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 sub-type. 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 is different from 120 seconds as recommended by the standard. 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 Unified IP Conference Phone 8831 for Third-Party Call Control, 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 field 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's description.

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

System description—This field contains an alpha-numeric string that is the textual description of the network entity. The system description includes the full name and version identification of the system's 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 auto-negotiation, 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 auto-negotiation support/status should be:

- Bit 0—Set to 1 to indicate the auto-negotiation support feature is supported.
- Bit 1—Set to 1 to indicate auto-negotiation status is enabled.
- Bit 2-7—Set to 0.

The bit values for the 2 octets PMD auto-negotiation 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, in most cases, 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 will send out this TLV only when in wired mode. When the phone is not set for auto-negotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value auto-negotiation support/status should be clear (0) to indicate auto-negotiation is disabled. The 2 octets PMD auto-negotiation 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) and 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

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.

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 “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 conference 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 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 firmware version. For the incoming LLDPDU, the TLVs are all ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

Final Network Policy Resolution and QoS For the Phone

The following sections describe network policy and QoS for the IP phones.

Special VLANs

VLAN=0, VLAN=1 and VLAN=4095 are treated the same way as an untagged VLAN. As the VLAN is untagged, 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. 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. 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 will be used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on value used for extension 1. If CoS is applicable and if CoS != 0, CoS will be used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP=0, the default will be 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 will be 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 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 voice application from LLDP-MED PDU and if the tagged flag is not set, only the DPSC (mapped to ToS) is applicable.

The conference phone reboots and restarts the fast start sequence.

Co-Existence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN is determined by 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 both CDP and LLDP-MED PDUs at the same time.

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

LLDP-MED and Multiple Network Devices

If the same application type is used for 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.

LLDP-MED and IEEE 802.X

The phones do not support IEEE 802.X and will not work in a 802.1X wired environment. However, IEEE 802.1X or Spanning Tree Protocols on network devices could result in delay of fast start response from switches.

Configure the VLAN Settings

To configure VLAN settings, navigate to **Admin Login > advanced > Voice > System**. Under **VLAN Settings**, configure the following parameters:

Parameter	Description
VLAN ID	If you use a VLAN without Cisco Discovery Protocol (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.
Enable CDP	Enable CDP only if you are using a switch that has CDP. CDP is negotiation-based and determines on which VLAN the IP phone resides.
Enable LLDP-MED	Choose **Yes** to enable LLDP-MED for the phone to advertise itself to devices that use that discovery protocol. (By default, this setting is enabled.) 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 is used if applicable. If CDP is used concurrently, a waiting period of 6 seconds is used. The waiting period increases the overall startup time for the phone.
Network Startup Delay	Enter the delay in seconds for the switch to get to the forwarding state before the phone sends out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, it might be necessary 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.

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 limited to service providers. Configuration profiles or updated firmware are transferred to the device by using TFTP, HTTP, or HTTPS.

The conference phone accepts configuration profiles in XML format, or in a proprietary binary format generated by the SIP Profile Compiler (SPC) available from Cisco. The conference phone supports 256-bit symmetric key encryption to secure the XML content of the profiles. SPC compiled binary profiles can be encrypted when they are complied. Since firmware does not contain sensitive personal information, typically it is not encrypted.

Provisioning is described in detail in the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.

This chapter describes:

- Redundant Provisioning Servers, page 5-1
- Retail Provisioning, page 5-2
- Automatic In-House Preprovisioning, page 5-2
- Use HTTPS, page 5-3
- Manually Provision a Phone from the Keypad, page 5-4
- Update Profiles and Firmware, page 5-5
- Firmware Upgrade, page 5-7
- Configure a Custom Certificate Authority, page 5-8
- General Purpose Parameters, page 5-9

Redundant Provisioning Servers

The provisioning server may be specified as an IP address or as a fully qualified domain name (FQDN). The use of a FQDN facilitates the deployment of redundant provisioning servers. When the provisioning server is identified through a FQDN, the Cisco IP phone attempts to resolve the FQDN to an IP address through DNS. Only DNS A-records are supported for provisioning; DNS SRV address resolution is not available for provisioning. The Cisco conference phone continues to process A-records until the first server responds. If no server associated with the A-records responds, the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control logs an error to the syslog server.

Retail Provisioning

The conference phone includes the web-based configuration utility that displays internal configuration and accepts new configuration parameter values. The server also accepts a special URL command syntax for performing remote profile resync and firmware upgrade operations.

In a retail distribution model, a customer purchases a Cisco voice endpoint device, and subsequently subscribes to a particular service. The customer first signs on to the service and establishes a VoIP account, possibly through an online portal. Subsequently, the customer binds the particular device to the assigned service account.

To do so, the unprovisioned Cisco Unified IP Conference Phone 8831 for Third-Party Call Control is instructed to resync with a specific provisioning server through a resync URL command. The URL command typically includes an account PIN number or alphanumeric code to associate the device with the new account.

In the following example, a device at the DHCP-assigned IP address 192.168.1.102 is instructed to provision itself to the SuperVoIP service:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

In this example, 1234abcd is the PIN number of the new account. The remote provisioning server is configured to associate the phone that is performing the resync request with the new account, based on the URL and the supplied PIN. Through this initial resync operation, the phone is configured in a single step, and is automatically directed to resync thereafter to a permanent URL on the server. For example:

```
https://prov.supervoip.com/cisco-init
```

For both initial and permanent access, the provisioning server relies on the Cisco IP phone client certificate for authentication and supplies correct configuration parameter values based on the associated service account.

Automatic In-House Preprovisioning

Using the phone web user interface and issuing a resync URL is convenient for a customer in the retail deployment model, but it is not as convenient for preprovisioning a large number of units.

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control supports a more convenient mechanism for in-house preprovisioning. With the factory default configuration, the phone automatically tries to resync to a specific file on a TFTP server, whose IP address is offered as one of the DHCP-provided parameters. This lets a service provider connect each new Cisco IP phone to a LAN environment configured to preprovision phones. Any new Cisco IP phone connected to this LAN automatically resyncs to the local TFTP server, initializing its internal state in preparation for deployment. Among other parameters, this preprovisioning step configures the URL of the Cisco IP phone provisioning server.

Subsequently, when a new customer signs up for service, the preprovisioned Cisco Unified IP Conference Phone 8831 for Third-Party Call Control can be simply bar-code scanned, to record its MAC address or serial number, before being shipped to the customer. Upon receiving the unit, the customer connects the unit to the broadband link. On power-up the Cisco IP phone already knows the server to contact for its periodic resync update.

Use HTTPS

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control provides a reliable and secure provisioning strategy based on HTTPS requests from the phone to the provisioning server, using both server and client certificates for authenticating the client to the server and the server to the client.

To use HTTPS with the phone, you must generate a Certificate Signing Request (CSR) and submit it to Cisco. The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control generates a certificate for installation on the provisioning server that is accepted by the conference phones when they seek to establish an HTTPS connection with the provisioning server.

The phone implements up to 256-bit symmetric encryption, using the American Encryption Standard (AES), in addition to 128-bit RC4. The phone supports the Rivest, Shamir, and Adelman (RSA) algorithm for public/private key cryptography.

Server Certificates

Each secure provisioning server is issued an secure sockets layer (SSL) server certificate, directly signed by Cisco. The firmware running on the Cisco IP phone clients recognizes only these certificates as valid. The clients try to authenticate the server certificate when connecting via HTTPS, and reject any server certificate not signed by Cisco.

This mechanism protects the service provider from unauthorized access to the Cisco IP phone endpoint, or any attempt to spoof the provisioning server. This might allow the attacker to reprovision the Cisco IP phone to gain configuration information, or to use a different VoIP service. Without the private key corresponding to a valid server certificate, the attacker is unable to establish communication with a Cisco IP phone.

Client Certificates

In addition to a direct attack on the phone, an attacker might attempt to contact a provisioning server using a standard web browser, or other HTTPS client, to obtain the phone configuration profile from the provisioning server. To prevent this kind of attack, each phone carries a unique client certificate, also signed by Cisco, including identifying information about each individual endpoint. A certificate authority root certificate capable of authenticating the device client certificate is given to each service provider. This authentication path allows the provisioning server to reject unauthorized requests for configuration profiles.

Obtain a Server Certificate

To obtain a server certificate:

Step 1 Contact a Cisco support person who will work with you on the certificate process. If you are not working with a specific support person, you can email your request to ciscosb-certadmin@cisco.com.)

Step 2 Generate a private key that will be used in a CSR (Certificate Signing Request). This key is private and you do not need to provide this key to Cisco support. Use open source “openssl” to generate the key. For example:

```
openssl genrsa -out <file.key> 1024
```

Step 3 Generate CSR a that contains fields that identify your organization, and location. For example:

```
openssl req -new -key <file.key> -out <file.csr>
```

You must have the following information:

- Subject field—Enter the Common Name (CN) that must be a FQDN (Fully Qualified Domain Name) syntax. During SSL authentication handshake, the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control verifies that the certificate it receives is from the machine that presented it.
- Server's hostname—For example, provserv.domain.com.
- Email address—Enter an email address so that customer support can contact you if needed. This email address is visible in the CSR.

Step 4 Email the CSR (in zip file format) to the Cisco support person or to ciscosb-certadmin@cisco.com. The certificate is signed by Cisco and given to you.

Manually Provision a Phone from the Keypad

Typically the conference phone is configured to be provisioned when first connected to the network and at configured intervals that are set when the phone is preprovisioned (configured) by the service provider or the VAR. Service providers can authorize VARs or advanced users to manually provision the phone by using the phone keypad.

The status of the provisioning process is indicated by the phone mute button blinking in the following patterns:

- Red/orange slow blink (1.0 seconds on, 1.0 seconds off): Contacting server, server not resolvable, not reachable, or down.
- Red/orange fast blink (0.2 seconds on, 0.2 seconds off, 0.2 seconds on, 1.4 seconds off): Server responded with file not found or corrupt file.

To manually provision the phone by using the keypad:

Step 1 Press **Setup**, then scroll to **Profile Rule**.

Step 2 Enter the profile rule by using the following format:

protocol://server[:port]/profile_pathname

For example:

```
tftp://192.168.1.5/CP_8831_3PCC.cfg
```

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).

Step 3 Press the **Resync** softkey.

Sample Configuration File

Refer to the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.

Update Profiles and Firmware

Cisco conference phones support secure remote provisioning (configuration) and firmware upgrades. An unprovisioned phone can receive an encrypted profile specifically targeted for that device without requiring an explicit key by using a secure first-time provisioning mechanism using SSL functionality.

User intervention is not required to initiate or complete a profile update or firmware upgrade. If intermediate upgrades are required to reach a future upgrade state from an older release, the Cisco IP phone upgrade logic is capable of automating multi-stage upgrades. A profile resync is only attempted when the Cisco IP phone is idle, because this might trigger a software reboot and disconnect a call.

General purpose parameters manage the provisioning process. Each Cisco IP phone can be configured to periodically contact a normal provisioning server (NPS). Communication with the NPS does not require the use of a secure protocol because the updated profile is encrypted by a shared secret key. The NPS can be a standard TFTP, HTTP or HTTPS server with client certificates.

The administrator can upgrade, reboot, restart, or resync Cisco IP phones by using the phone web user interface. The administrator can also perform these tasks by using a SIP notify message.

Configuration profiles are generated by using common, open-source tools that integrate with service provider provisioning systems. (Provisioning is described in detail in the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.)

Allow and Configure Profile Updates

The profile updates can be allowed at specified intervals. Updated profiles are sent from a server to the phone by using TFTP, HTTP, or HTTPS.

To configure a profile update:

Step 1 Click **Admin Login > advanced > Voice > Provisioning**.

Step 2 Under **Configuration Profile** in the Provision Enable field, choose **Yes**.

Step 3 Enter the parameters defined in the table:

Parameter	Description
Provision Enable	Allows or denies resync actions. Defaults to **Yes**.
Resync On Reset	The device performs a resync operation after power-up and after each upgrade attempt when set to **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 powered 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 failures.
Resync At (HHmm)	Time in 24-hour format (hhmm) to resync the device. When this parameter is provisioned, the Resync Periodic parameter is ignored. Default is empty.

Parameter	Description
Resync At Random Delay	To avoid flooding the server with simultaneously resync requests from multiple phones set to resync at the same time, the phone triggers the resync up to ten minutes after the specified time. The input value (in seconds) is converted to minutes. The default value is 600 seconds (10 minutes). If the parameter value is set to less than 600, the default value is used.
Resync Periodic	Time in seconds between periodic resyncs. If this value is empty or zero, the device does not resync periodically.
Resync Error Retry Delay	If a resync operation fails because the IP Telephony device was unable to retrieve a profile from the server, if the downloaded file is corrupt, or an internal error occurs, the device tries to resync again after a time specified in seconds. If the delay is set to 0, the device does not try to resync again following a failed resync attempt.
Forced Resync Delay	The resync typically takes place when the voice lines are idle. When a voice line is active and a resync is due, the IP Telephony device delays the resync procedure until the line becomes idle. However, it waits no longer than the Forced Resync Delay (seconds). A resync might cause configuration parameter values to change. This causes a firmware reboot and terminates any voice connection active at the time of the resync.
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.
Profile Rule Profile Rule B Profile Rule C Profile Rule D	Remote configuration profile rules evaluated in sequence. Each resync operation can retrieve multiple files, potentially managed by different servers.
Resync DHCP Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles.
Transport Protocol	The transport protocol used to retrieve firmware and profiles. If none is selected, TFTP is assumed and the IP address of the TFTP server is obtained from the DHCP server.
Log Request Msg	The message sent to the syslog server at the start of a resync attempt. The default value is: `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`
Log Success Msg	The syslog message issued upon successful completion of a resync attempt. The default value is: `$PN $MAC –Successful % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
User Configurable Resync	Allows a user to resync the phone from the phone screen.

Allow and Configure Firmware Updates

The firmware updates can be allowed at specified intervals. Updated firmware is sent from a server to the phone by using a TFTP or HTTP. Security is less of an issue with a firmware upgrade, because firmware does not contain personal information.

To configure a firmware update:

Step 1 Click **Admin Login > advanced > Voice > Provisioning**.

Step 2 Under **Firmware Upgrade** in the Upgrade Enable field, choose **Yes**.

Step 3 Enter the parameters defined in the table:

Parameter	Description
Upgrade Enable	Allows firmware update operations independent of resync actions. Defaults to Yes.
Upgrade Error Retry Delay	The interval applied in the event of an upgrade failure. The firmware upgrade error timer activates after a failed firmware upgrade attempt and is initialized with this value. The next firmware upgrade attempt occurs when this timer counts down to zero. The default is 3600 seconds.
Upgrade Rule	A firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule. (See "Manually Provision a Phone from the Keypad" section on page 5-4 for the Upgrade Rule syntax.) The default is (empty).

Firmware Upgrade

The 3PCC supports single one image upgrade by tftp/http/https.

Step 1 Put the 3PCC image cp-8831-sip.9-3-3-5-3PCC.bin.sgn on the tftp/http/https download directory.

Step 2 Configure Upgrade Rule on the 'Provisioning' tab in the web page, with the valid URL format:

```
<schema>:// <server[:port]> /filepath
```

Note A device (with new base and DCU) may not be downgraded to an earlier firmware release, such as 9.3(3). For details, refer to the hardware information and the firmware/hardware compatibility information in the current *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Release Notes*.

Firmware Upgrade With a Browser Command

An upgrade command entered into the browser address bar can be used to upgrade firmware on a phone. The phone updates only when it is idle. The update is attempted automatically after the call is complete.

To upgrade the conference phone CP-8831-3PCC via URL on web browser enter this command:

```
http://<phone_ip>/admin/upgrade?<schema>://<serv_ip[:port]>/filepath
```

Configure a Custom Certificate Authority

Digital certificates can be used to authenticate network devices and users on the network. They can be used to negotiate IPSec sessions between network nodes.

A third party uses a Certificate Authority certificate to validate and authenticate two or more nodes that are attempting to communicate. Each node has a public and private key. The public key encrypts data. The private key decrypts data. Because the nodes have obtained their certificates from the same source, they are assured of their respective identities.

The device can use digital certificates provided by a third-party Certificate Authority (CA) to authenticate IPSec connections. See the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide* for more information.

The phones support a set of preloaded Root Certificate Authority embedded in the firmware:

- Cisco Small Business CA Certificate
- CyberTrust CA Certificate
- Verisign CA certificate
- Sipura Root CA Certificate
- Linksys Root CA Certificate

On the phone web user interface:

Step 1 Click **Admin Login > advanced > Voice > Info**.

Step 2 Select **Download Status** and scroll to **Custom CA Status** and see the following fields:

- Custom CA Provisioning Status—Indicates the provisioning status.
  - Last provisioning succeeded on mm/dd/yyyy HH:MM:SS; or
  - 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.

General Purpose Parameters

The general purpose parameters GPP_* are used as free string registers when configuring the conference phone to interact with a particular provisioning server solution. The GPP_* parameters are empty by default. 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.

The GPP_* parameters are available for macro expansion within other provisioning parameters. For this purpose, single-letter upper-case macro names (A through P) are sufficient to identify the contents of GPP_A through GPP_P. Also, the two-letter upper-case macro names SA through SD identify GPP_SA through GPP_SD as a special case when used as arguments of the **key** URL option.

These parameters can be used as variables in provisioning and upgrade rules. They are referenced by prepending the variable name with a '$' character, such as $GPP_A.

To configure general purpose parameters, navigate to **Admin Login > advanced > Voice > Provisioning**.

Configure Dial Plan

Dial plans determine how the 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.

The dial plans can be configured on the IP phone by using the phone web user interface.

This section includes information that you need to understand dial plans, as well as procedures for configuring your own dial plans:

- About Dial Plan, page 6-1
- Edit Dial Plan on the IP Phone, page 6-7
- Reset the Control Timers, page 6-7

About Dial Plan

The conference 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 collecting the dialed digits. The inter-digit timers starts tracking the time that elapses between digits.
2. If the inter-digit 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 the **Voice** tab > **Extension** 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.

Digit Sequence	Function
[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.
<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, 1xxxxxxxxx An outside line dial tone is sounded after the user presses `9`. The tone continues until the user presses `1`.
! (exclamation point)	Prohibits a dial sequence pattern. For example: 1900xxxxxx! 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 inter-digit timer to 0 seconds, or enter `L0` to reduce the long inter-digit 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 hot line and warm line, with a 0 delay for the hot line and a non-zero delay for a warm line. For example: **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 dial any three-digit number that starts with the digits 1 through 8. If your system uses four-digit extensions, you would instead 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 transmitting the number to the carrier.

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

```
EXAMPLE: ( [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 is example is useful where a local area code is required by the carrier but the majority of 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 transmitting the number to the carrier.

U.S. long distance dialing:

```
EXAMPLE: ( [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:

```
EXAMPLE: ( [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 press 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:

```
EXAMPLE: ( [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:

```
EXAMPLE: ( [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 more digits are entered by the user, the set of candidates diminishes until only one or none are 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 do not match any sequence in the dial plan.	The number is rejected.
Dialed digits exactly match one sequence in the dial plan.	If the sequence is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. If the sequence is blocked by the dial plan, 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 specified by the applicable interdigit timer. The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan. The default value is 10 seconds. The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. The default value is 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 value is 5.

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 is transmitted 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 will be transmitted as shown. If you omit the number substitution, <:n>, then 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:

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

P9 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 the digits.

Create a hotline for all sequences on the System Dial Plan:

EXAMPLE: (**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> 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.

Create a hotline on a line button for an extension:

EXAMPLE: (**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. See the "Reset the Control Timers" section on page 6-7.

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

EXAMPLE: **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, 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. It 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 it is valid, the call proceeds. If it is invalid, the call is rejected. The default value is 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

Set the timer for the entire dial plan:

EXAMPLE: **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, While entering a number with the phone off hook, a 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:

EXAMPLE: `(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 With the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

Edit Dial Plan on the IP Phone

You can edit the dial plan and modify the control timers. To edit the dial plan on the IP conference phone:

Step 1 Navigate to **Admin Login > advanced > Voice**.

Step 2 Click the **Extension** tab and scroll to Dial Plan.

Step 3 In the Dial Plan section, enter the digit sequences in the Dial Plan field. For more information and examples, see the "Digit Sequences" section on page 6-1.

The default (US-based) system-wide dial plan appears automatically in the field. You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan. For more information and examples, see the "Digit Sequences" section on page 6-1.

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

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

Step 4 Click **Submit All Changes**. The phone reboots.

Step 5 Verify that you can successfully complete a call using each digit sequence that you entered in the dial plan.

Note If you hear a reorder (fast busy) tone, you need to review your entries and modify the dial plan appropriately. See the "Digit Sequences" section on page 6-1.

Reset the Control Timers

You can use the following procedure to reset the default timer settings for all calls.

If you need to edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan. See the "About Dial Plan" section on page 6-1.

Step 1 Log in to the phone web user interface.

Step 2 Click **Admin Login** and **advanced**.

Step 3 Click **Voice > Regional**.

Step 4 Scroll down to the *Control Timer Values (sec)* section.

Step 5 Enter the desired values in the *Interdigit Long Timer* field and the *Interdigit Short Timer* field. Refer to the definitions at the beginning of this section.

Configure Regional Parameters and Supplementary Services

Use the **Regional** tab to configure regional and local settings, such as control timer parameters, dictionary server script, language Selection, and locale to change localization:

- Control Timer Values (sec), page 7-1
- Localize Your Conference Phone, page 7-2

Control Timer Values (sec)

The table describes Control Timer parameters.

Field	Description
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. Ranges from 0 to 64 seconds. Setting this value high can result in a longer post dialing delay (PDD), which is the time between the start of a call and the time the phone starts ringing. A value that is too low can result in dialed digits not being correctly recognized. Defaults to 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. Ranges from 0 to 64 seconds. Defaults to 3.

Localize Your Conference Phone

The following table describes the localization parameters in the **Voice > Regional** tab under **Time** section.

Field	Description
Set Local Date (mm/dd)	Enter the local date (*mm* represents the month and *dd* represents the day). The year is optional and uses two or four digits. For example, May 1, 2014, can be entered as: **05/01** or **05/01/14** or **05/01/2014**.
Set Local Time (HH/mm)	Enter the local time (*HH* represents hours and *MM* represents minutes). Seconds are optional.
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-1:00, GMT-0:00, GMT+01:00, GMT+02:00, …, GMT+13:00. Defaults to GMT-08:00.
Time Offset (HH/mm)	Enter the offset from GMT to use for the local system time.
Ignore DHCP Time Offset	When used with some routers that have DHCP with time offset values configured, the conference phone uses the router settings and ignores the 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. The default value is Yes.
Daylight Saving Time Rule	Enter the rule for calculating daylight saving time. See the "Configure Daylight Saving Time" section on page 7-3.
Daylight Saving Enable	Select **Yes** to enable or **No** to disable DST on the phone. This setting affects all lines (extensions) on the phone.
Dictionary Server Script	Defines the location of the dictionary server, the languages available, and the associated dictionary. See the "Create a Dictionary Server Script" section on page 7-5.

Language Selection	Specifies the default language. The value must match one of the languages supported by the dictionary server. The script (dx value) is:
	`<Language_Selection ua="na">`
	`</Language_Selection>`
	Defaults to blank; the maximum number of characters is 512. For example:
	`<Language_Selection ua="na"> Spanish`
	`</Language_Selection>`

Locale	Choose the locale that should be set in the HTTP Accept-Language header.

Manage the Time and Date

The Cisco conference 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.
- SIP Messages—Each SIP message (request or response) sent to the phone could contain a Date header with the current time information. If the header is present, the phone uses it to set its clock.
- Manual Setup—The time and date can be entered manually by using the phone web user interface. However, this value is overwritten by the NTP time or SIP Message Date whenever they are available to the phone. Manual setup requires that you enter the time in 24-hour format only.

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

The *Time Zone* parameter can be configured by using 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.

Configure Daylight Saving Time

The phone supports auto adjustment for daylight saving time. You must set *Daylight Saving Time Enable* to **Yes** and enter the DST rule. This option affects the time stamp on the *CallerID*.

To enter the rule for calculating DST, include the start, end, and save values separated by semi-colons (;) as follows:

```
Start = start-time; end=end-time; save = save-time
```

For example, the default DST rule is:

```
start=3/-1/7/2;end=10/-1/7;save=1.
```

The *start-time* and *end-time* values specify the start and end dates and times of daylight saving time. The format is:

```
month/day/weekday[/HH:mm:ss]
```

The *month* value equals any value in the range 1-12 (January-December).

The *day* value equals any + or - value in the range 1-31. If the day value is -1, the time changes on the last occurrence of a weekday in that month. If the day value is -2 to -31 (max day value for that month) then the time changes on the weekday in that month (or previous month) on or before that day of the month.

The *weekday* value equals any value in the range 1-7 (Monday-Sunday). It can also be 0. If the weekday value is 0, it means that the date to start or end daylight saving is the given date. In that case, the day value must not be negative. If the weekday value is positive (but not 0) then the daylight saving starts or ends on the weekday value on or after the given date. If the weekday value is negative (not -1), then the daylight saving starts or ends on the weekday value on or before the given date.

Optional time values: *HH* represents hours (0-23), *mm* represents minutes (0-59). and *ss* represents seconds (0-59). Optional values inside brackets [ ] are assumed to be 0 if not specified. Midnight is represented by 0:0:0.

The *save-time* value is the number of hours, minutes, and/or seconds to add to the current time during DST.

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
```

Select a Display Language

This section describes how to localize the display language on the conference phone. You can define up to twelve languages, in addition to English, to be available and host the dictionaries for each of the languages on the HTTP or TFTP provisioning server. Language support follows Cisco dictionary principles.

Use the Language Selection parameter to select the phone default display language. The value must match one of the languages supported by the dictionary server. The script (dx value) is as follows:

- <Language_Selection ua="na">
- </Language_Selection>

Defaults to blank; the maximum number of characters is 512. For example:

```
<Language_Selection ua="na"> Spanish
</Language_Selection>
```

During startup, the phone checks the selected language and downloads the dictionary from the TFTP/HTTP provisioning server indicated in the phone configuration. The dictionaries are available at the support website. See Appendix B, “Related Documentation,” for the website location.

The end user can change the language of the phone on the phone by following these steps:

Step 1 Press the **Setup** button.

Step 2 Select **Language**, then press the **Select** soft button.

Step 3 Select **Option** to change the language.

Step 4 With the desired language highlighted, press **Save**.

Create a Dictionary Server Script

The Dictionary Server Script defines the location of the dictionary server, the languages available and the associated dictionary. Up to five language entries are recognized in the script. The syntax is:

```
Dictionary_Server_Script
serv=http://locale_server/locale_path/;d1=French;l1=fr-FR;x1=French/fr-FR.tar;d2=Danis
h;l2=da-DK;x2=Danish_Denmark/da-DK.tar;d3=German;l3=de-DE;x3=German_Germany/de-DE.tar;
d4=Russian;l4=ru-RU;x4=Russian/ru-RU.tar;d5=Hebrew;l5=he-IL;x5=Hebrew/he-IL.tar.
```

Note TFTP, HTTP, and HTTPS are supported for the dictionary download.

Defaults to blank; the maximum number of characters is 512. The detailed format is as follows:

```
serv={server ip port and root path};
d0=language0;l0=locale0;x0=dictionary0 filename;
d1=language1;l1=locale1;x1=dictionary1 filename;
d2=language2;l2=locale2;x2=dictionary2 filename;
d3=language3;l3=locale3;x3=dictionary3 filename;
d4=language4;l4=locale4;x4=dictionary4 filename;
d5=language5;l5=locale5;x5=dictionary5 filename;
d6=language6;l6=locale6;x6=dictionary6 filename;
d7=language3;l7=locale7;x7=dictionary7 filename;
d8=language8;l8=locale8;x8=dictionary8 filename;
d9=language5;l9=locale9;x9=dictionary9 filename;
```

The following languages are supported on the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control:

- da-DK : Danish_Denmark
- nl-NL : Dutch_Netherlands
- fr-FR : French_France
- de-DE : German_Germany
- he-IL : Hebrew_Israel
- it-IT : Italian_Italy
- no-NO : Norwegian_Norway
- pt-PT : Portuguese_Portugal
- ru-RU : Russian_Russian_Federation
- es-MX : Spanish_Mexico
- es-ES : Spanish_Spain
- sv-SE : Swedish_Sweden

Localization Configuration Example

Language Selection: French

(Entry dx must match one of the languages supported by the dictionary server.)

Locale: fr-FR

(Entry lx must be within the Locale option list.)

Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Field Reference

This appendix describes the fields in the following sections (tabs) of the phone web user interface:

- Info, page A-1
- Voice, page A-8
- Call History, page A-24

Info

The fields on this tab are read-only and cannot be edited.

System Status

System Information

Parameter	Description
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.
Host Name	Displays the current host name assigned to the phone.
Domain	Displays the network domain name of the phone. Defaults to cisco.com.
Current Netmask	Displays the network mask assigned to the phone.
DNS from DHCP	Displays the IP address assigned by DHCP server.
Primary DNS	Displays the primary DNS server assigned to the phone.
Current Gateway	Displays the default router assigned to the phone.
Secondary DNS	Displays the secondary DNS server assigned to the phone.

Reboot History

The conference phone stores the reasons for the last five reboots or refreshes. When the phone is reset to factory defaults, this information is deleted.

The reboot history is displayed in reverse chronological order, with the reasons for the latest reboot displayed in the **Reboot Reason 1** field.

Each Reboot Reason field displays the reason for the reboot and a time stamp indicating when the reboot took place as in the following examples:

```
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 following is a list of the supported reboot/refresh reasons:

Reason	Description
Upgrade	An upgrade operation caused a reboot (regardless whether the upgrade completed or failed).
Provisioning	Changes made to parameter values by using the phone LCD or Web GUI, or a resync caused a reboot.
SIP Triggered	A SIP request caused a reboot.
RC	A remote customization caused a reboot.
User Triggered	The user manually triggered a cold reboot.
IP Changed	The phone IP address was changed triggering a warm reboot.

You can view the reboot history from the phone Web GUI, and the phone Status Dump file (http://*phoneIP*/status.xml or http://*phoneIP*/admin/status.xml).

Viewing the 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/>
```

The Web GUI and the LCD screen get the reboot history from these tags.

Product Information

Parameter	Description
Product Name	Model number of the conference phone.
Software Version	Version number of the conference phone software.
MAC Address	Hardware address of the conference 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 conference phone.
Hardware Version	Version number of the conference phone hardware.
Client Certificate	Status of the client certificate, which authenticates the conference phone for use in the ITSP network. This field indicates if the client certificate is properly installed in the phone.
Wireless Microphone Region	Wireless microphone region of the conference phone.

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.
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.

Call Status

Ext Status

The following parameters show for each extension on the phone.

Parameter	Description
Registration State	Shows “Registered” if the phone is registered, “Not Registered” if the phone is not registered to the ITSP.
Last Registration At	Last date and time the line was registered.

Parameter	Description
Next Registration In	Number of seconds before the next registration renewal.
Mapped SIP Port	Port number of the SIP port mapped by NAT.

Call 1 Status/Call 2 Status

The following parameters show for each line and call on the phone.

Parameter	Description
Call State	Status of the call.
Duration	Duration of the call.
Remote Address	Address of the remote device.
Local Address	Address of the local device.
Start Time	Starting time of the call
Type	Direction of the call.
Peer Name	Name of the internal phone.
Peer Phone	Phone number of the internal phone.
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.
Sender Octets	Total number of octets sent by the phone.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, iLBC, G.711 u-law, or G.711 A-law.
Rcvr Lost Packets	Missing RTP packets (lost in transit.)
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, iLBC, G.711 u-law, or G.711 A-law.
Rcvr Packets	Number of RTP voice packets received since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold
Rcvr Octets	Total number of octets received by the phone.

Parameter	Description
MOS-LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control uses.
AVG MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.722 gives 4.5 • G.729 A /AB gives 3.7 • iLBC gives 3.9
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames 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 Secs:	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Number of milliseconds for latency.
Max Jitter	Number of milliseconds for receiver jitter.
Rcvr Discarded	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.

Download Status

Downloaded Ring Tone

Parameter	Description
Ring Tone Download Status	Indicates whether the phone is downloading a ring tone (and from where) or if it is idle.
Ring Tone 1	Information about the user downloaded ring tone 1: name, size, and time-stamp of the tone.
Ring Tone 2	Information about the user downloaded ring tone 2: name, size, and time-stamp of the tone.

Downloaded Locale Package

Parameter	Description
Locale Download Status	Displays the downloaded locale package status.
Downloaded Dictionary Info	Dictionary downloaded from the TFTP/HTTP provisioning server indicated in the phone.
Downloaded Font Info	Displays the downloaded font name.

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	

Note The Upgrade and Provisioning Status are displayed in reverse chronological order (like reboot history) displaying status with time and reason.

Custom CA Status

These fields display the status of provisioning using a custom Certificate Authority (CA).

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; or • 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.

Custom CA certificates are configured in the Provisioning tab. For more information about custom CA certificates, see the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.

Debug Info

Console Logs

Displays the syslog output of the phone in the reverse order, where messages is the latest one. Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.

1

Parameter	Description
Debug Message 0	messages
Debug Message 1	messages.0
Debug Message 2	messages.1
Debug Message 3	messages.2
Debug Message 4	messages.3
Debug Message 5	messages.4
Debug Message 6	messages.5
Debug Message 7	messages.6
Debug Message 8	messages.7

Browser Info

Parameter	Description
Loading Time	The amount of elapsed time when the page is loaded on the browser. **Note** Safari and IE version before 9 does not support this parameter.
Browser Version	Version of the browser. For example, Firefox 31
OS Version	Version of the Windows operating system.
Platform	The platform to which the browser is compiled.
Width	Current width of the browser.
Height	Current height of the browser.

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. Defaults to Yes.
Web Server Port	Port number of the phone web user interface. Defaults to 80.
Enable Web Admin Access	Lets you enable or disable local access to the phone web user interface. Select Yes or No from the drop-down menu. Defaults to Yes.
Admin Password	Password for the administrator. Defaults to no password.

Parameter	Description
User Password	Password for the user. Defaults to blank.
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. The default is no. Specific parameters are then designated as “na” or “ro” using provisioning files. Parameters designated as “na” will not appear on the phone interface. Parameters designated as “ro” will not be editable by the user.

Internet Connection Type

Parameter	Description
Connection Type	Choose the type of internet connection: • DHCP • Static IP

Static IP Settings

Parameter	Description
Static IP	If static IP was chosen as the type of internet connection, displays the static IP address assigned to the phone.
Netmask	If static IP was chosen as the type.
Gateway	Default router IP address. Blank if DHCP assigned.

Optional Network Configuration

Parameter	Description
Host Name	The host name of the conference phone.
Domain	The network domain of the conference phone.
Primary DNS	DNS server used by the conference phone in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the primary DNS server. Defaults to 0.0.0.0.
Secondary DNS	DNS server used by the conference phone in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the secondary DNS server. Defaults to 0.0.0.0.

Parameter	Description
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.
Debug Level	The debug level from 0-3. The higher the level, the more debug information is generated. Zero (0) means no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Defaults to 0.
Layer 2 Logging	Used for IP phone network layer debugging purposes. Do not use except when advised to do so by Cisco technical support, as this may impact system performance. Set to No by default.
Primary NTP Server	IP address or name of primary NTP server.
Secondary NTP Server	IP address or name of secondary NTP server.
SSH Access	If enabled, the phone supports console access for debugging and testing.
DNS Cache TTL Ignore	If enabled, the phone continues to use the previous cached DNS result if the DNS server does not respond when the phone tries to renew its DNS query. When disabled, the phone uses the previous TTL value and clears the DNS query result cache.
SSH User ID	User ID for SSH login.
SSH Password	Password for the SSH login.

VLAN Settings

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.

Parameter	Description
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.

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. Defaults to 70.
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. Defaults to 5.
SIP User Agent Name	Used in outbound REGISTER requests. Defaults to $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. Defaults to $VERSION.

Parameter	Description
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. Defaults to 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.
RFC 2543 Call Hold	If set to yes, unit will include 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. Defaults to Yes.
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. Defaults to 5060.
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. Defaults to 5080.
Caller ID Header	Provides the option to take the caller ID from PAID-RPID-FROM, P-ASSERTEDIDENTITY, REMOTE-PARTY-ID, or FROM header.
Max INVITE Retry Attempts	Maximum number of INVITE retry attempts by the phone. Defaults to 6.
Max NON-INVITE Retry Attempts	Maximum number of NON-INVITE retry attempts by the phone. Defaults to 6.

SIP Timer Values

Parameter	Description
SIP T1	RFC 3261 T1 value (RTT estimate) that can range from 0 to 64 seconds. Defaults to 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. Defaults to 4 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. Defaults to 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. Defaults to 30.
Reg Retry Intv	Interval to wait before the conference phone retries registration after failing during the last registration. Defaults to 30.
Reg Retry Long Intvl	When registration fails with a SIP response code that does not match<Retry Reg RSC>, the conference 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. Defaults to 1200.
Reg Retry Random Delay	Random delay range (in seconds) to add to <Register Retry Intvl> when retrying REGISTER after a failure. Defaults to 0.
Reg Retry Long Random Delay	Random delay range (in seconds) to add to <Register Retry Long Intvl> when retrying REGISTER after a failure. Defaults to 0.
Reg Retry Intvl Cap	The maximum value to cap the exponential back-off retry delay (which starts at <Register Retry Intvl> and doubles on every REGISTER retry after a failure). In other words, the retry interval is always at <Register Retry Intvl> seconds after a failure. If this feature is enabled, <Reg Retry Random Delay> is added on top of the exponential back-off adjusted delay value. Defaults to 0.

Response Status Code Handling

Parameter	Description
Try Backup RSC	This parameter may be set to invoke failover upon receiving specified response codes. Defaults to blank
Retry Reg RSC	Interval to wait before the CP-8831-3PCC retries registration after failing during the last registration. Defaults to blank.

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. Defaults to 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. Defaults to 16538.
RTP Packet Size	Packet size in seconds, which can range from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. Defaults to 0.02.
RTCP Tx Enable	Enables RTCP for an active connection. Defaults to No.

SDP Payload Types

Parameter	Description
AVT Dynamic Payload	AVT dynamic payload type. Ranges from 96-127. Defaults to 101.

NAT Support Parameters

Parameter	Description
NAT Keep Alive Intvl	Interval between NAT-mapping keep alive messages. Defaults to 15.

Provisioning

For information about the Provisioning page, see the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.

Regional

Control Timer Values (sec)

Parameter	Description
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. Defaults to 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. Defaults to 3.

Time

Parameter	Description
Set Local Date (mm/dd)	Sets the local date (mm represents the month and dd represents the day). The year is optional and uses two or four digits.
Set Local Time (HH/mm)	Sets the local time (hh represents hours and mm represents minutes). Seconds are optional.
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. Defaults to GMT-08:00.
Time Offset (HH/mm)	This specifies the offset from GMT to use for the local system time.
Ignore DHCP Time Offset	When used with some routers that have DHCP with time offset values configured, the 3PCC phone uses the router settings and ignores the 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. The default value is Yes.

Parameter	Description
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).
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). The default Daylight Saving Time Rule is start=3/-1/7/2;end=10/-1/7/2;save=1.
Daylight Saving Time Enable	Select **Yes** to enable Daylight Saving Time.

Localization

Parameter	Description
Dictionary Server Script	Defines the location of the dictionary server, the languages available, and the associated dictionary. See the "Create a Dictionary Server Script" section on page 7-5.

Language Selection	Specifies the default language. The value must match one of the languages supported by the dictionary server. The script (dx value) is:
	`<Language_Selection ua="na">`
	`</Language_Selection>`
	Defaults to blank; the maximum number of characters is 512. For example:
	`<Language_Selection ua="na"> Spanish`
	`</Language_Selection>`

Locale	Choose the locale that should be set in the HTTP Accept-Language header

Phone

QoS Settings

Parameter	Description
SIP TOS Value	TOS field value in UDP IP packets carrying a SIP message. Defaults to 0x60.
RTP TOS Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. Defaults to 0xb8.

General

Parameter	Description
Station Display Name	Name to identify the conference phone; appears on the phone screen. You can use spaces in this field and the name does not have to be unique.
Text Logo	Text logo 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.
PNG Picture Download URL	URL locating the (.png) file to display on the phone screen background. For more information, see the "Configure Phone Information and Display Settings" section on page 2-1.
Select Logo	Select from None, PNG Picture, or Text Logo. Defaults to None.
Select Background Picture	Select from PNG Picture, or None. Defaults to Default.
Screen Saver Enable	Enables a screen saver on the phone. When the phone is idle for a specified time, it enters screen saver mode.
Screen Saver Wait	Amount of idle time before screen saver displays. Defaults to 300.
Screen Saver Icon	In screen saver mode, the display unit can display: • A background picture. • Station time in the middle of the screen. • A moving Cisco icon. When the phone is locked, the status line displays a scrolling message "Press any key to unlock your phone." • Cisco Logo • The station date and time in the middle of the screen.
Co-branding Banner Picture Download URL	URL to download a .gif (.png or .jpeg) image on the web GUI for co-branding.

Miscellaneous Line Key Settings

Parameter	Description
Call Appearances Per Line	This parameter allows you to choose the number of calls per line button. You can choose a value from 2 (the default) to 10.

Supplementary Services

Parameter	Description
Conference Serv	Enable/disable Three way conference service. Defaults to Yes.
Attn Transfer Serv	Enable/disable attended-call-transfer service. Defaults to Yes.
Blind Transfer Serv	Enable/disable blind-call-transfer service. Defaults to Yes.
Cfwd All Serv	Enable/disable call-forward-all service. Defaults to Yes.
Cfwd Busy Serv	Enable/disable call-forward-on-busy service. Defaults to Yes.
Cfwd No Ans Serv	Enable/disable call-forward-no-answer service. Defaults to Yes.

BroadSoft Settings

Parameter	Description
Directory Enable	Set to Yes to enable BroadSoft directory for the phone user. Defaults to Yes.
XSI Host Server	Enter the name of the server; for example, xsi.iop1.broadworks.net.
Directory Name	Name of the directory. Displays on the phone as a directory choice.
Directory Type	Select the type of BroadSoft directory: Enterprise (default): 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.

Parameter	Description
Directory User ID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.
Directory Password	Alphanumeric password associated with the User ID.

LDAP Corporate Directory Search

Parameter	Description
LDAP Dir Enable	Choose Yes to enable LDAP.
LDAP Corp Dir Name	Enter a free-form text name, such as "Corporate Directory."
LDAP Server	Enter a fully qualified domain name or IP address of LDAP server, in the following format: nnn.nnn.nnn.nnn
LDAP 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.

LDAP Client DN	Enter the distinguished name domain components [dc]; for example:
	`dc=cv2bu,dc=com`
	If 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`

LDAP Username	Enter the username for a credentialed user on the LDAP server.
LDAP Password	Enter the password for the LDAP username.
LDAP 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`
LDAP Last Name Filter	This defines the search for surnames [sn], known as last name in some parts of the world. For example, sn:(sn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end.

Parameter	Description
LDAP First Name Filter	This defines the search for the common name [cn]. For example, cn:(cn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end.
LDAP Search Item 3	Additional customized search item. Can be blank if not needed.
LDAP Item 3 Filter	Customized filter for the searched item. Can be blank if not needed.
LDAP Search Item 4	Additional customized search item. Can be blank if not needed.
LDAP Item 4 Filter	Customized filter for the searched item. Can be blank if not needed.
LDAP Display Attrs	Format of LDAP results display 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, then 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 will be ignored. • p—phone number When p is assigned to a type attribute, example t=p, then the retrieved number is dialable by the phone.
LDAP 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.

XML Service

Parameter	Description
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.
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
XML Password	XML service password for authentication purposes

User

Call Forward

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. Defaults to voicemail.
Cfwd No Ans Dest	Enter the extension to forward calls to when the call is not answered. Defaults to voice mail.
Cfwd No Ans Delay	Enter the delay in time (in seconds) to wait before forwarding a call that is unanswered. Defaults to 20 seconds.

Speed Dial

You can configure speed dials on the conference phone from the LCD GUI or the web GUI.

Speed Dial 2 through 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.

Defaults to blank.

Supplementary Services

Parameter	Description
Time Format:	Choose the time format for the phone (12 or 24 hour).
Date Format	Choose the date format for the phone (month/day or day/month).

Audio

Parameter	Description
Ringer Volume	Sets the default volume for the ringer.
Speaker Volume	Sets the default volume for the speakerphone.

LCD

Parameter	Description
LCD Contrast	Enter a number value from 1 to 30. The higher the number, the greater the contrast on the IP phone screen.
Back Light Timer (seconds)	Select the number of seconds before the back light should turn off (10s, 20s, or 30s) or Off or Always On.

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

Line Enable: To enable this line for service, select yes. Otherwise, select no. Defaults to yes.

NAT Settings

Parameter	Description
NAT Keep Alive Enable	To send the configured NAT keep alive message periodically, select yes. Otherwise, select no. Defaults to 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. Defaults to $NOTIFY.

Call Feature Settings

Parameter	Description
Default Ring	Type of ring heard. Choose from No Ring or 1 through 10.

Call History

Displays the call history for the phone. To change the information displayed, select the type of call history from the drop-down list:

- All Calls
- Received Calls
- Placed Calls
- Missed Calls

Related Documentation

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control.

Use the following sections to obtain related information:

- Cisco IP Phone 8800 Series Documentation, page B-1
- Cisco IP Phone Firmware Support Policy, page B-1
- Documentation, Service Requests, and Additional Information, page B-1

Cisco IP Phone 8800 Series Documentation

Refer to publications that are specific to your language and phone model, and phone firmware release. Navigate from the following documentation URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-series-home.html

Cisco IP Phone Firmware Support Policy

For information on the support policy for Cisco IP Phones, see http://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-ip-phone-7900-series/116684-technote-ipphone-00.html.

Documentation, Service Requests, and Additional Information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.