Cisco Unified IP Conference Phone 8831 and 8831NR

Cisco Unified IP Conference Phone 8831 and 8831NR Overview

The Cisco Unified IP Conference Phones 8831 and 8831NR are full-featured single line conference phones that provides voice communication over an IP network. They function much like a digital business phone, allowing you to place and receive calls and to access features such as mute, hold, transfer, call forward, and more. In addition, because conference phones connect to your data network, they offer enhanced IP telephony features, including access to network information and services, and customizable features and services. The conference phones also support certain security features.

The conference phone provides a backlit LCD screen and a variety of other sophisticated functions. Optional microphone extension kits provide enhanced room coverage that can be further expanded by linking two units together.

The Cisco Unified IP Conference Phone 8831 supports wired and wireless microphones. The Cisco Unified IP Conference Phone 8831NR supports only wired microphones.

The conference phone, like other network devices, must be configured and managed. The conference phones encode G.711a, G.711u, G.729a, G.722, G.729ab, iLBC, and decode all variants of G.711 and G.729. The conference phones also support 16-bit/16-kHz wideband audio.

Caution Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco Unified IP Conference Phone might cause interference. For more information, see the manufacturer's documentation of the interfering device.

Buttons and Hardware

The Conference Phone has two primary components:

- Display Control Unit (DCU)
- Sound Base

In addition, the following optional extension kits can be added to or used with the conference phone:

- Wired Microphone Extension Kit
- Wireless Microphone Extension Kit and Charger

For your conference phone to work, it must be connected to the corporate IP telephony network.

Display Control Unit

The Display Control Unit (DCU) is tethered to the Sound Base via a micro USB connector.

You can use the graphic and table below to identify buttons and hardware on the DCU.

Table 1: Display Control Unit Buttons and Softkeys

	Item	Description
1	Phone screen	LCD screen that displays conference phone menus and features.
2	Softkeys	Four programmable keys.
3	Navigation bar with Select key	2-way Navigation bar and Select key that allows you to scroll menus and select items on the display.

	Item	Description
4	Call button	LED backlit call button. Press this key to: • Go Off Hook • Answer an incoming call • Obtain a dial tone to initiate a call • Resume a call • Release a call
5	Keypad	Allows you to dial phone numbers and enter letters.
6	Mute button	Toggles the Mute feature. A red backlight indicates a call is on mute.
7	Volume rocker	2-way rocker switch that raises the volume of the speaker.

Note For details on DCU LED behavior, see LED State Definitions, on page 4.

Sound Base

The Sound Base provides 360 degree audio coverage via four built-in microphones and supports a full duplex speaker phone.

To provide enhanced room coverage, two sound base units can be linked together.

You can use the graphic and table below to identify buttons and connections on the Sound Base.

Table 2: Sound Base Buttons

	Item	Description
1, 2, 3	LED indicators	Three LED indicators provide call status information. For details on LED behaviour, see LED State Definitions, on page 4.
4	Mute button	Backlit mute button.

LED State Definitions

LEDs on the Sound Base and DCU provide information about the state of the conference phone.

For example, green flashing lights on the Sound Base and on the DCU Call button indicate that there is an incoming call. If the conference phone is on mute, then an incoming call will still flash green on the Call button, but the LED for the DCU mute button is solid red, the sound base LEDs are solid red, and the mute button on the Sound Base is also solid red.

The following table is a guide to the behaviour of the LEDs on the sound base and the DCU.

Table 3: Conference Phone LED State Table

Media Path Status	Call on Focus	Sound Base				Display Control Unit (DCU)			
		Base LEDs (3)		Mute Button		DCU Call Button		DCU Mute Button	
Off	No call								
Off	No call, with VM					red	solid		
Off	DND flash	green	flash			green	flash		
Off	Incoming call	green	flash			green	flash		
Off	Hold Revert Call	green	flash			green	flash		
Off	Hold Call	green	pulse			green	pulse		
Off	Hold Remote Call					red	pulse		
Off	Remote in use Call					red	solid		
Unmuted	Ringout/Connected Call	green	solid			green	solid		
Unmuted	DNDFlash	green	solid			green	flash		
Unmuted	Incoming Call	green	solid			green	flash		
Unmuted	Hold Revert Call	green	solid			green	flash		
Muted	Ringout/Connected	red	solid	red	solid	green	solid	red	solid

Media Path Status	Call on Focus	Sound Base				Display Control Unit (DCU)			
		Base LEDs (3)		Mute Button		DCU Call Button		DCU Mute Button	
Muted	DND Flash	red	solid	red	solid	green	flash	red	solid
Muted	Incoming Call	red	solid	red	solid	green	flash	red	solid
Muted	Hold Revert Call	red	solid	red	solid	green	flash	red	solid
Deep Sleep Mode	Deep Sleep Mode			gray	solid				

Phone Screen

The DCU contains the LCD phone screen. The idle or home screen displays information about the status of calls and features.

If the conference phone is in an offline state, the idle screen displays the message `Phone is not registered` and the **Apps** softkey remains available.

You can use the graphic and table below to identify the features and functions available on the screen.

Table 4: Phone Screen Layout.

	Item	Description
1	Header	Displays date, time, and current directory number. Displays menu name when applicable.
2	Line details and other phone information	Displays line label, call details, and status messages such as missed calls, message waiting, and line forwarding information.
3	Call State icon	Indicates the status of a call, such as ringing, hold, encrypted or connected call.
4	Softkey labels	Displays softkeys for currently available features or actions.

	Item	Description
5, 6	Feature icons	These icons are displayed when an associated feature, such as extension microphones (5) or Link mode (6) is connected.

Phone Screen Icons

Table 5: Phone Screen Icons

Icon	Description
	On hook
	Off hook
	Ringing in
	Connected
	Hold
	Shared line
	Microphone connected
	Linked mode
	Encrypted

Network Protocols

Cisco Unified IP Conference Phones support several industry-standard and Cisco networking protocols required for voice communication. The following table provides an overview of the networking protocols that the Cisco Unified IP Conference Phone supports.

Table 6: Supported Networking Protocols on the Cisco Unified IP Conference Phone

Networking Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco Unified IP Conference Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, go to the "Dynamic Host Configuration Protocol" chapter and the "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*. **Note** If you cannot use option 150, you may try using DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for: • Configuration file downloads • XML services • Firmware upgrades • Troubleshooting purposes

Networking Protocol	Purpose	Usage Notes
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	Cisco Unified IP Conference Phone implements the IEEE 802.1X standard by providing support for EAP-FAST and EAP-TLS authentication.
Internet Protocol (IP)	IP is a message protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Conference Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	The Cisco Unified IP Conference Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper at [illegible]

Networking Protocol	Purpose	Usage Notes
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can enable it on a per phone basis by using Cisco Unified Communications Manager.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Secure Real-Time Transfer Protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints.	Cisco Unified IP Phones use SRTP for media encryption.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Conference Phone use the TLS protocol when securely registering with Cisco Unified Communications Manager. For more information, see *Cisco Unified Communications Manager Security Guide*.

Networking Protocol	Purpose	Usage Notes
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP Conference Phone , TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Setup menu on the phone. For more information, see "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

Related Topics

Cisco Unified IP Communications Product Interactions
Phone Startup Process
Network Setup Menu

Supported Features

The Cisco Unified IP Conference Phones 8831 and 8831NR function much like digital business or conference phones, and allow you to place and receive teleconference phone calls. In addition to traditional telephony features, the conference phone includes features that enable you to administer and monitor the conference phone as a network device.

The Cisco Unified IP Conference Phone 8831 supports wired and wireless microphones. The Cisco Unified IP Conference Phone 8831NR supports only wired microphones.

Feature Overview

The Cisco Unified IP Conference Phone not only provides traditional telephony functionality, such as call forward and transfer, redial, and voice message system access, but it supports a full range of conference features. The conference phone also offers support for a variety of other features, such as WebDialer.

As with other network devices, the conference phone must be configured in order to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP for this process, you have fewer settings to configure on a device, but if your network requires it, an IP address, the TFTP server, and subnet information can be configured manually.

Conference phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate Cisco Unified Communications Manager with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for coworker

contact information directly from their IP devices. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information.

Finally, because the conference phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their conference phone.

Related Topics

Cisco Unified IP Conference Phone Settings
Features, Templates, Services, and User Setup
Troubleshooting and Maintenance

Telephony Feature Administration

You can modify additional settings for the Cisco Unified IP Conference Phone from Cisco Unified Communications Manager Administration. Use Cisco Unified Communications Manager Administration to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks.

For more information about Cisco Unified Communications Manager Administration, see Cisco Unified Communications Manager documentation, including *Cisco Unified Communications Manager System Guide*. You can also use the context-sensitive help available within the web-application for guidance.

You can access Cisco Unified Communications Manager documentation at this location:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.html

You can access Cisco Unified Communications Manager Business Edition documentation at this location:

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

Related Topics

Available Telephony Features

Network Parameters

If you are not using DHCP in your network, you must configure the following network settings on the Cisco Unified IP Conference Phone after installing the phone on the network:

- IP address
- IP subnet information
- TFTP server IP address
- You also may configure the domain name and the DNS server settings, if necessary.

Collect this information and see the instructions in Cisco Unified IP Conference Phone Settings.

Related Topics

Model Information, Status, and Statistics

Information for End Users

If you are a system administrator, you are likely the primary source of information for conference phone users within your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with conference phone documentation. Make sure to visit the Cisco Unified IP Phone 8800 web site:

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

From this site, you can access various user guides and documentation.

In addition to providing users with documentation, it is important to inform them about available conference phone features, including features specific to your company or network, as well as how to access and customize those features, if appropriate.

Related Topics

Internal Support Website

Cisco Unified IP Conference Phone Security Features

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the conference phone and Cisco Unified Communications Manager server and prevents data tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains secure communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco Unified IP Phones.

The Cisco Unified IP Conference Phone uses the Phone Security profile, which defines whether the device is nonsecure or encrypted. For information on applying the security profile to the conference phone, see *Cisco Unified Communications Manager Security Guide*.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, see "Configuring Encrypted Phone Configuration Files" chapter in *Cisco Unified Communications Manager Security Guide*.

The following table shows where you can find additional information about security.

Table 7: Phone and Cisco Unified Communications Manager Security Topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	See *Cisco Unified Communications Manager Security Guide*.
Security features supported on the Cisco Unified IP Conference Phone	See Supported Security Features, on page 14.
Restrictions regarding security features	See Security Restrictions, on page 19.
Viewing a security profile name	See Security Profiles, on page 16.
Identifying calls for which security is implemented	Encrypted Phone Call Identification.

Topic	Reference
TLS connection	See: • Network Protocols, on page 6 • Cisco Unified Communications Manager IP Phone Addition Methods
Security and the conference phone startup process	See Phone Startup Process.
Security and phone configuration files	See Cisco Unified Communications Manager IP Phone Addition Methods.
Changing the TFTP Server 1 or TFTP Server 2 option on the conference phone when security is implemented	See IPv4 Setup Menu Options.
Items on the Security Configuration menu that you access from the Device Configuration menu on the conference phone	See Security Setup Menu.
Items on the Security Configuration menu that you access from the Settings menu on the conference phone	See Security Setup Menu.
Applying a password to the phone so that no changes can be made to the administrative options	See Password Protection.
Disabling access to conference phone web pages	See Control Web Page Access.
Troubleshooting	See *Cisco Unified Communications Manager Security Guide*, "Troubleshooting" chapter.
Deleting the CTL file from the conference phone	See Cisco Unified IP Conference Phone Reset or Restore.
Reset or restore the conference phone	See Cisco Unified IP Conference Phone Reset or Restore.
802.1X Authentication	See: • 802.1X Authentication, on page 19 • Security Setup Menu • Status Menu

Note All Cisco Unified IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure or secure.

For information about configuring the security profile and applying the profile to the phone, see *Cisco Unified Communications Manager Security Guide*.

Supported Security Features

The following table provides an overview of the security features that the conference phone supports. For more information about these features and about Cisco Unified Communications Manager and conference phone security, see *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a conference phone, choose **Apps** > **Admin Settings** > **Security Setup**.

Note Most security features are available only if a certificate trust list (CTL) is installed on the conference phone. For more information about the CTL, see "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide*.

Table 8: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension `.sebn`) prevent tampering with the firmware image before it is loaded on a conference phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each conference phone requires a unique certificate for device authentication. Conference phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the conference phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the conference phone and a Cisco Unified Communications Manager should occur; and, if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager will not register conference phone unless they can be authenticated by the Cisco Unified Communications Manager.

Feature	Description
File authentication	Validates digitally signed files that the conference phone downloads. The conference phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the conference phone. The conference phone rejects such files without further processing.
Signalling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signalling packets during transmission.
Manufacturing installed certificate	Each conference phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the conference phone, and allows Cisco Unified Communications Manager to authenticate the phone.
Secure SRST reference	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the `cnf.xml` file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media primary key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the conference phone, and interacts with the conference phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the conference phone, or it can be configured to generate certificates locally.
Security profiles	Defines whether the conference phone is nonsecure or encrypted.
Encrypted configuration files	Allows you to ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a conference phone	You can prevent access to a conference phone web page, which displays a variety of operational statistics for the conference phone.

Feature	Description
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disabling access to web pages for a phone
802.1X Authentication	The Cisco Unified IP Conference Phone 8831 can use 802.1X authentication to request and gain access to the network.

Related Topics

Security Profiles, on page 16
802.1X Authentication and Status Menus
Cisco Unified IP Conference Phone Settings

Security Profiles

All Cisco Unified IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the conference phone is nonsecure or encrypted. For information about configuring the security profile and applying the profile to the conference phone, see the *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the conference phone, look at the Security Mode setting in the Security Configuration menu.

Related Topics

Security Setup Menu

Encrypted Phone Call Identification

When security is enabled for a phone, a lock icon is displayed on the phone screen during an encrypted call. In a secure call, a security tone plays at the beginning of a call to indicate that the other connected phone is also receiving and transmitting encrypted audio. If your call is connected to a non-protected phone, the security tone does not play.

In a secure call, all call signalling and media streams are encrypted. An encrypted call offers a high level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call icon on the phone screen changes to the lock icon: 🔒.

If the call is routed through non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

Note Secured calling is supported for connections between two phones only. Some features, such as conference calling, and Cisco Extension Mobility are not available when secured calling is configured.

Initiate Secure Conference Call

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established using this process:

Procedure

Step 1 A user initiates the conference from a secure conference phone.

Step 2 Cisco Unified Communications Manager assigns a secure conference bridge to the call.

Step 3 As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone and maintains the security level for the conference.

There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participant phones and the availability of secure conference bridges. For more information about the interactions, see Call Security Interactions and Restrictions, on page 17

Step 4 If the conference call is secure the 🔒 icon is displayed on the screen.

Initiate Secure Phone Call

A protected call is established when your phone and the phone on the other end are configured for protected calling. The other phone can be on the same Cisco IP network or on a network outside of the IP network. Protected calls can only be made between two phones. Conference calls cannot be protected.

A protected call is established using this process:

Procedure

Step 1 A user initiates the call from a protected phone (protected security mode).

Step 2 The phone displays the 🔒 icon (encrypted) on the phone screen. This icon indicates that the phone is configured for secure (encrypted) calls, but this does not mean that the other connected phone is also protected.

Step 3 A security tone plays if the call is connected to another protected phone, indicating that both ends of the conversation are encrypted and protected. If the call is connected to a unprotected phone, then the secure tone does not play.

Note Protected calling is supported for conversations between two phones. Some features, such as conference calling and Cisco Extension Mobility are not available when protected calling is configured.

Call Security Interactions and Restrictions

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and security in the system. The following table provides information about changes to call security levels when using Barge.

Table 9: Call Security Interactions When Using Barge

Initiator's Phone Security Level	Feature Used	Call Security Level	Results of Action
Nonsecure	cBarge	Encrypted call	Call barged and identified as nonsecure call
Secure	cBarge	Secure call	Call barged and identified as Secure call

The following table provides information about changes to conference security levels depending on the initiator's phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 10: Security Restrictions with Conference Calls

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Nonsecure	Conference	Encrypted	Nonsecure conference bridge Nonsecure conference
Secure	Conference	At least one member is nonsecure.	Secure conference bridge Nonsecure conference
Secure	Conference	All participants are encrypted.	Secure conference bridge Secure encrypted level conference
Secure	Join	Encrypted	Secure conference bridge Conference remains secure
Nonsecure	cBarge	All participants are encrypted.	Secure conference bridge Conference changes to nonsecure
Nonsecure	Meet Me	Minimum security level is encrypted.	Only nonsecure conference bridge is available and used Nonsecure conference
Secure	Meet Me	Minimum security level is nonsecure	Only secure conference bridge available and used Conference accepts all calls

802.1X Authentication

Cisco Unified IP Conference Phone supports 802.1X Authentication.

Overview

Cisco Unified IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements.

Cisco Unified IP Phones also contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses EAP-FAST and EAP-TLS options for network authentication.

Required Network Components

Support for 802.1X authentication on Cisco Unified IP Phones requires several components, including:

Cisco Unified IP Phone

The phone acts as the 802.1X *supplicant*, which initiates the request to access the network.

Cisco Secure Access Control Server (ACS) or another other third-party authentication server

The authentication server and the phone must both be configured with a shared secret that authenticates the phone.

Cisco Catalyst Switch or other third-party switch

The switch must support 802.1X, so it can act as the *authenticator* and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

Best Practices

The following list describes best practices for 802.1X configuration.

- Enable 802.1X Authentication: If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, be sure that you properly configure the other components before enabling it on the phone.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled: If you are using a switch that supports multi-domain authentication, you can continue to use the voice VLAN.
  - Disabled: If the switch does not support multi-domain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.
- Enter MD5 Shared Secret: If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted.

Security Restrictions

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. In this case, a reorder (fast busy) tone plays on the phone from which the barge was initiated.

If the initiator phone is configured for encryption, the barge initiator can barge into a nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call is encrypted.

Cisco Unified IP Conference Phone Deployment

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a complete Cisco IP telephony network, see the "System Configuration Overview" chapter in the *Cisco Unified Communications Manager System Guide*.

After the IP telephony system is setup and you have configured system-wide features in Cisco Unified Communications Manager, phones can be added to the system.

For an overview of procedures used to add phones to your network, see the "Installation" and "Setup in Cisco Unified Communications Manager" sections of this guide.

Cisco IP Phone Setup in Cisco Unified Communications Manager

To add conference phones to the Cisco Unified Communications Manager database, you can use:

- Autoregistration
- Cisco Unified Communications Manager Administration
- Bulk Administration Tool (BAT)
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

For more information about these choices, see Cisco Unified Communications Manager IP Phone Addition Methods.

For general information about configuring conference phones in Cisco Unified Communications Manager, see

- "Cisco Unified IP Phones", *Cisco Unified Communications Manager System Guide*
- "Cisco Unified IP Phone Configuration", *Cisco Unified Communications Manager Administration Guide*
- "Autoregistration Configuration",*Cisco Unified Communications ManagerAdministration Guide*

Set Up the Cisco Unified IP Conference Phone in Cisco Unified Communications Manager Administration

The following steps provide an overview and checklist of configuration tasks for the conference station in Cisco Unified Communications Manager Administration. The steps present a suggested order to guide you through the conference phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed information, see the sources listed.

Procedure

Step 1 Gather the following information about the conference station:

- Conference phone model
- MAC address
- Physical location of the conference station
- Name or user ID of conference station user
- Device pool
- Partition, calling search space, and location information
- Directory number assigned to the conference phone
- Cisco Unified Communications Manager user to associate with conference phone
- Conference phone usage information that affects conference station templates (button and softkey), features, services, or conference phone applications

Provides a list of configuration requirements for setting up conference phones and identifies preliminary configuration that you need to perform before configuring individual conference phones, such as conference phone key button templates or softkey templates. For more information, see the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter and also refer to Available Telephony Features.

Step 2 Customize button templates (if required). Allows you to create a custom button template with the Privacy feature. You can assign this template to shared conference phones so users have access to the Privacy feature. For more information, see *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter and Button Templates.

Step 3 Add and configure the conference phone. Adds the conference phone with its default settings to the Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. For more information about Product Specific Configuration fields, refer to the Help in the Phone Configuration window.

Step 4 Add and configure directory number on the conference phone. Adds the directory number and features associated with the directory number to the conference phone. For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Directory Number Configuration" and "Creating a Cisco Unity Voice Mailbox" sections, and Available Telephony Features.

Step 5 Customize softkey templates to add, delete, or change the order of softkey features that display on the conference phone to meet feature needs. For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter, and Softkey Templates.

Step 6 (Optional) Configure conference phone services and assign services.

Note Users can add or change services on their phones using Cisco Unified Communications Self Care Portal.

For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Services Configuration" chapter, and Services Setup.

Step 7 Add user information to the global directory for Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Add a New User" chapter, and Cisco Unified Communications Manager User Addition.

Note If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, see Corporate Directory Setup.

Step 8 Associate a user to a user group with a conference phone. Provides users with control over their conference phone such as forwarding calls or adding services.

Note Some conference phones, such as those in conference rooms, do not have an associated user.

For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Adding a New User" chapter, "Associate Devices with a User" section.

Cisco Unified IP Conference Phone 8831 Installation

After you have added the phone to the Cisco Unified Communications Manager database, you can complete the installation. The conference phone can be installed at the user's location either by you, or by the user.

After the conference phone connects to the network, the conference phone startup process begins and the conference phone registers with Cisco Unified Communications Manager. To finish installing the conference phone, configure the network settings on the conference phone depending on whether you want to enable or disable DHCP service.

If you used autoregistration, you need to update the specific configuration information for the conference phone such as associating the conference phone with a user, changing the button table, or directory number.

Note Upgrade the conference phone with the current firmware image before you install the phone. For information about upgrading, see the Readme file for the conference phone.

The conference phone supports seamless firmware upgrades. For instructions on upgrading the firmware, see the Release Notes.

These and other related documents can be located from http://www.cisco.com/en/US/products/ps12965/tsd_products_support_series_home.html.

Install the Cisco Unified IP Conference Phone

The following steps provide an overview and checklist of installation tasks for the conference phone. The steps present a suggested order to guide you through the conference phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the steps.

Procedure

Step 1 Choose the power source for the conference phone:

- Power over Ethernet (PoE)
- External power supply

Determines how the conference phone receives power. For more information, see Conference Phone Power.

Step 2 Assemble the conference phone, adjust placement, and connect the network cable. Locates and installs the phone in the network. For more information, see Phone Connections.

Step 3 Monitor the conference phone startup process. Verifies that the conference phone is configured properly. For more information, see IP Phone Startup Verification.

Step 4 Configure these network settings on the conference phone by choosing **Apps** > **Settings** > **Network Configuration**.

Step 5 To enable DHCP:

a) Set DHCP Enabled to **Yes**.
b) To use an alternate TFTP server, set Alternate TFTP to **Yes**.
c) Enter an IP address for TFTP Server 1.

With DHCP enabled, the IP address is automatically assigned and the conference phone is directed to a TFTP Server. Consult with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP.

For more information, see Network Settings and Network Setup Menu.

Step 6 To disable DHCP:

a) Set DHCP Enabled to **No**.
b) Enter a static IP address for the conference phone.
c) Enter the Subnet Mask.
d) Enter the IP address for Default Router 1.
e) Enter the Domain Name where the conference phone resides.
f) Set Alternate TFTP to **Yes**.
g) Enter an IP address for TFTP Server 1.

Without DHCP, you must configure the IP address, TFTP server, subnet mask, domain name, and default router locally on the conference phone.

For more information, see Network Settings and Network Setup Menu.

Step 7 Set up security on the conference phone. Provides protection against data tampering threats and identity theft of conference phones. For more information, see Security Setup Menu.

Step 8 Place calls with the conference phone. Verifies that the conference phone and features work correctly. For more information, see the phone user guide.

Step 9 Provide information to end users about how to use their conference phones and how to configure their conference phone options. Ensures that users have adequate information to successfully use their conference phones. For more information, see Internal Support Website.

Terminology Differences

The following table highlights some of the important differences in terminology that is used in these documents:

- *Cisco Unified IP Conference Phone 8831 and 8831NR Administration Guide*

- *Cisco Unified IP Conference Phone 8831 and 8831NR User Guide*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*

Table 11: Terminology Reference

User Guide	Administration and System Guides
Conference across Lines	Join Across Lines
Conference	Join or Conference
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Programmable Feature Button	Programmable Line Button or Programmable Line Key (PLK)
Voicemail System	Voice Messaging System