Administration Guide for Cisco IP Communicator

Release 7.0
January 19, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-10898-01

Administration Guide for Cisco IP Communicator

CONTENTS

CHAPTER 1

Overview of Cisco IP Communicator

Revised: 1/19/11

Overview of Cisco IP Communicator Features

Cisco IP Communicator is a software-based application that allows users to place and receive phone calls by using their personal computers. Cisco IP Communicator depends upon the Cisco Unified Communications Manager call-processing system (formerly known as Cisco Unified CallManager) to provide telephony features and voice-over-IP capabilities through eight telephone lines (or a combination of lines, softkeys, and direct access to telephony features).

Note Depending on context, this guide refers to Cisco IP Communicator as a *phone*, *device*, *application*, or an *interface*.

When registered to Cisco Unified Communications Manager, Cisco IP Communicator has the capabilities of a full-featured Cisco Unified IP Phone, including the ability to transfer calls, forward calls, and conference additional participants to an existing call. This means that you can provision and upgrade Cisco IP Communicator as any other Cisco Unified IP Phone, greatly simplifying IP phone management. Through automatic software updates, Cisco IP Communicator keeps pace with new software features and changes.

Cisco IP Communicator enables you to deliver Extensible Markup Language (XML)-based applications to the display and provide quick access to diverse information such as weather, stocks, quote of the day, or any other web-based information.

Cisco IP Communicator offers high-quality audio features such as the Audio Tuning Wizard, an advanced (adaptive) jitter buffer and packet loss (error) concealment, acoustic echo cancellation, noise suppression, voice activity detection, and silence suppression.

Cisco IP Communicator offers other advanced features that accommodate ever-mobile users and changing network conditions. These features include auto-detection of Cisco VPN clients, automated support for most VPN clients (including Microsoft PPTP client), interoperability with Cisco Unified Video Advantage for desktop video calls, and non-MAC-based device name for easy PC refreshes (requires a Cisco Unified Communications Manager version 4.1.3 or later).

For details about configuring Cisco IP Communicator for different protocols, for security features, and for details about supported call features, see the Related Topics section.

For details about the all Cisco IP Communicator features, see the data sheet at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_data_sheet09186a00801f8e48.html

For details about using the application, see the user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

Related Topics

- How to Configure Cisco IP Communicator the SCCP or SIP Protocol, page 2-9
- How to Configure Security Features for Cisco IP Communicator, page 2-12
- Telephony Features Available for Cisco IP Communicator, page 5-2

Supported Networking Protocols

Table 1-1 lists the industry-standard and Cisco networking protocols required for voice communication Use this information to help you design your network.

Table 1-1 Supported Networking Protocols

Networking Protocol	Purpose	Usage Notes
BootP (Bootstrap Protocol)	Enables a network device such as Cisco IP Communicator to discover certain startup information, such as its IP address.	If you are using BootP to assign IP addresses to Cisco IP Communicator, the BOOTP Server option shows "Yes" in the network configuration settings on the phone.
CDP(Cisco Discovery Protocol)	Device-discovery protocol that runs on all Cisco-manufactured equipment. By using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	Cisco IP Communicator uses CDP to communicate information such as auxiliary VLAN ID, per-port power management details, and QoS (quality of service) configuration information with the Cisco Catalyst switch.
DHCP (Dynamic Host Configuration Protocol)	Dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect Cisco IP Communicator into the network and have it become operational without you manually assigning an IP address or configuring additional network parameters.	We recommend that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DCHP configurations, see the *Cisco Unified Communications Manager System Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
HTTP (HyperText Transfer Protocol)	Uses TCP to transfer web content over the Internet.	Cisco IP Communicator uses HTTP to obtain the configuration file, LDAP directories configuration, dialing rules, XML services, and locale strings.

Table 1-1 Supported Networking Protocols (continued)

Networking Protocol	Purpose	Usage Notes
IP (Internet Protocol)	Messaging protocol that addresses and sends packets across the network.	To communicate by using IP, network devices must have an assigned IP address, subnet, and gateway. Cisco IP Communicator obtains its IP information from the system network configuration.
LDAP (Lightweight Directory Access Protocol)	Protocol for accessing directories.	Cisco IP Communicator can use LDAP to search for names and phone numbers.
RTP (Real-Time Transport Protocol)	Standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco IP Communicator uses the RTP to receive from and send real-time voice traffic to other Cisco IP Communicators and gateways.
RTCP (Real-Time Control Protocol)	RTCP works with Real-Time Transport Protocol (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 using Cisco Unified Communications Manager.
SDP (Session Description Protocol)	Portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that are supported by all endpoints in the conference.	SDP capabilities (such as codec types, DTMF detection, and comfort noise) are normally configured on a global basis by Cisco Unified Communications Manager or the Media Gateway in operation. Some SIP endpoints might allow these parameters to be configured on the endpoint. This might vary from vendor to vendor.
SCCP (Skinny Client Control Protocol)	Includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.	Cisco IP Communicator to can use either SCCP or SIP.
SIP (Session Initiation Protocol)	Standard for setting up telephone calls, multimedia conferencing, and other types of communications on the Internet. SIP can be used to establish, maintain, and terminate calls between two or more endpoints. SIP provides signaling, which allows call information to be carried across network boundaries. SIP provides session management, which controls the attributes of an end-to-end call.	Cisco IP Communicator to can use either SCCP or SIP.
TCP (Transmission Control Protocol)	Connection-oriented transport protocol.	Cisco IP Communicator uses TCP to connect to Cisco Unified Communications Manager and to access XML services.

Table 1-1 Supported Networking Protocols (continued)

Networking Protocol	Purpose	Usage Notes
TFTP (Trivial File Transfer Protocol)	Allows you to transfer files over the network. On Cisco IP Communicator, 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 Cisco IP Communicator to use a TFTP server other than the one specified by the DHCP server, you must manually assign the TFTP server in Cisco IP Communicator.
TLS (Transport Layer Security)	Standard protocol for securing and authenticating communications.	When security is implemented, Cisco IP Communicator uses the TLS protocol when securely registering with Cisco Unified Communications Manager.
UDP (User Datagram Protocol)	Connectionless messaging protocol for delivery of data packets.	Cisco IP Communicator transmits and receives RTP streams, which uses UDP.

Related Topics

- How Cisco IP Communicator Interacts with Cisco Unified Communications Manager, page 1-4
- How Cisco IP Communicator Interacts With the Network at Startup, page 1-5

How Cisco IP Communicator Interacts with Cisco Unified Communications Manager

Cisco IP Communicator is a software application that enables you to communicate by using voice over a data network. To provide this capability, Cisco IP Communicator depends upon Cisco Unified Communications Manager to set up and tear down calls between phone devices, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages all components of the IP telephony system—the phone devices, access gateways, and the resources necessary for such features as conference calls and route plans. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Authentication (if configured for the telephony system)
- Device configuration file and certificate trust list (CTL) file through the TFTP service
- Cisco IP Communicator registration
- Call preservation so that a media session continues if signaling is lost between the primary Cisco Unified Communications Manager and Cisco IP Communicator

As you would do with other Cisco Unified IP Phones that rely on Cisco Unified Communications Manager, you must configure and manage Cisco IP Communicator as a network device through Cisco Unified Communications Manager Administration. For details, see *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

For details about supported Cisco Unified Communications Manager releases, see the Cisco IP Communicator release notes at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html

Related Topics

- How Cisco IP Communicator Interacts With the Network at Startup, page 1-5
- About Configuration Files, page 1-6
- QoS Modifications to Prioritize Voice Traffic, page 1-8
- Network, Server, and Client PC Requirements, page 2-1
- Telephony Features Available for Cisco IP Communicator, page 5-2

How Cisco IP Communicator Interacts With the Network at Startup

At startup, Cisco IP Communicator interacts with the network as follows:

1. Locates the configuration server.

   Upon startup, Cisco IP Communicator always attempts to use DHCP to locate its TFTP server. Cisco IP Communicator first tries to use HTTP (by default) to retrieve files from the server, and if it is not able, Cisco IP Communicator uses TFTP.

   If you used the Cisco IP Communicator Administration Tool, Cisco IP Communicator can also use HTTP to retrieve software updates, thereby accelerating file transfer for remote users. This tool is for Windows-based Cisco Unified Communications Managers only.

   If you do not use DHCP in your network to identify TFTP servers, or if you want the device to use an alternate TFTP server, you must manually configure your TFTP server from Cisco IP Communicator or instruct users to do this task.

2. Requests the CTL file (if security is configured).

   The TFTP server stores the CTL file, which contains a list of Cisco Unified Communications Managers and TFTP servers that Cisco IP Communicator is authorized to connect to. It also contains the certificates necessary for establishing a secure connection between Cisco IP Communicator and Cisco Unified Communications Manager.

   The security CTLFile.tlv file is downloaded to the [*ApplicationData*]\Cisco\Communicator\sec folder.

3. Requests configuration files.

   Configuration files (.cnf.xml) reside on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires a device to be reset, a change is made to the configuration file for that device.

   - If you have enabled auto-registration in Cisco Unified Communications Manager, Cisco IP Communicator accesses a default configuration file (xmldefault.cnf.xml) from the TFTP server.
   - Otherwise, Cisco IP Communicator accesses a .cnf.xml file corresponding to its device name.

4. Downloads locale strings.

   The.cnf.xml file configuration file tells Cisco IP Communicator which user locale strings to use. To make this request, Cisco IP Communicator first tries to use HTTP. If you have not enabled HTTP access, Cisco IP Communicator uses TFTP.

5. Contacts Cisco Unified Communications Manager.

   After obtaining the configuration file from the TFTP server, Cisco IP Communicator attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If security is implemented, Cisco IP Communicator makes a TLS connection; otherwise, it makes a nonsecure TCP connection.

   – If the device was added to the database individually (through Cisco Unified Communications Manager Administration or in bulk through the Bulk Administration Tool (BAT), Cisco Unified Communications Manager identifies the device. This is only true if you are not using BAT with the Tool for Auto-Registered Phones Support (TAPS).

   – Otherwise, the device attempts to register itself in the Cisco Unified Communications Manager database (when auto-registration is enabled in Cisco Unified Communications Manager).

Note Auto-registration is disabled when security is enabled on Cisco Unified Communications Manager. In this case, you must manually add Cisco IP Communicator to the Cisco Unified Communications Manager database.

Related Topics

- About Configuration Files, page 1-6
- About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6
- How to Configure Cisco IP Communicator the SCCP or SIP Protocol, page 2-9
- How to Configure Security Features for Cisco IP Communicator, page 2-12
- Specifying a TFTP Server, page 4-6
- About Updating the Application, page 3-6
- How to Resolve Startup Problems, page 8-5

About Configuration Files

Configuration files for Cisco IP Communicator are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires Cisco IP Communicator to be reset, a change is automatically made to the configuration file on Cisco IP Communicator.

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on Cisco IP Communicator has a valid certificate for Cisco Unified Communications Manager, Cisco IP Communicator establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, Cisco IP Communicator establishes a TCP connection. The transport protocol in the configuration file must also be set to TLS (corresponding to the transport type in the SIP Security Profile on Cisco Unified Communications Manager).

Note If the device security mode in the configuration file is set to Authenticated or Encrypted, but Cisco IP Communicator has not received a CTL file, Cisco IP Communicator continuously tries to obtain a CTL file so that it can register securely.

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, refer to the “Configuring Encrypted Phone Configuration Files” chapter in *Cisco Unified Communications Manager Security Guide*.

Related Topics

- Cisco IP Communicator Requests for Configuration Files, page 1-7
- Configuration Files Stored on the TFTP Server, page 1-7

Cisco IP Communicator Requests for Configuration Files

Cisco IP Communicator requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

If auto-registration is not enabled and Cisco IP Communicator has not been added to the Cisco Unified Communications Manager database, the registration request is rejected. In this case, Cisco IP Communicator resets and repeatedly attempts to register.

If this installation of Cisco IP Communicator has registered before, Cisco IP Communicator accesses the configuration file named *device_name*.cnf.xml, where *device_name* is the user-defined device name for this instance of Cisco IP Communicator.

Related Topics

- About Configuration Files, page 1-6
- Configuration Files Stored on the TFTP Server, page 1-7

Configuration Files Stored on the TFTP Server

The TFTP server provides these configuration files for SIP and SCCP devices:

- IP Phones:
  - For unsigned and unencrypted files—*device_name*.cnf.xml
  - For signed files—*device_name*.cnf.xml.sgn
  - For signed and encrypted files—*device_name*.cnf.xml.enc.sgn
- Dial Plan—*dialplan*.xml

  You must configure and associate dial plans with a phone device to enable dial plans to be sent to the configuration file. If you do not configure a phone dial plan, Cisco IP Communicator does not display any indication of a dial plan.

  If you are using a version of Cisco Unified Communications Manager other than 4.x, you can configure SIP dial rules. You configure these dial rules from the SIP Dial Rule Configuration window (**Call Routing > Dial Rules > SIP Dial Rules**) in Cisco Unified Communications Manager Administration.

You configure SCCP dial rules from the Application Dial Rules Configuration window (**Call Routing > Dial Rules > Application Dial Rules**) in Cisco Unified Communications Manager Administration.

For details about configuring dial rules, see the *Cisco Unified Communications Manager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- Softkey Template—*softkey_template*.xml

The filenames are derived from the devicename field in the Cisco Unified Communications Manager database. The devicename uniquely identifies a particular Cisco IP Communicator installation.

Related Topics

- How Cisco IP Communicator Interacts With the Network at Startup, page 1-5

QoS Modifications to Prioritize Voice Traffic

Voice quality can be compromised on an IP device by data traffic. Because Cisco IP Communicator is a software-based phone instead of a hardware phone, you cannot solve this problem by isolating voice-over-IP traffic to an auxiliary VLAN. We recommend that the prioritization of voice traffic is done on the network level rather than on an individual user system. This allows voice data traffic to be prioritized over generic data traffic.

For details about configuring QoS in your network, see:

Cisco Unified Communications SRND based on Cisco Unified Communications Manager

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html

Related Topics

- How Cisco IP Communicator Interacts with Cisco Unified Communications Manager, page 1-4
- Selections for Audio Port Range, page 4-11
- How to Resolve Voice-Quality Issues, page 8-9

CHAPTER 2

Preparing to Deploy Cisco IP Communicator

Revised: 1/19/11

This chapter describes the required and recommended tasks for deploying Cisco IP Communicator. It also provides instructions for adding Cisco IP Communicator devices to the Cisco Unified Communications Manager (formerly known as Cisco Unified CallManager) database.

Tip Cisco Unified Communications Manager documentation is available from the Help menu in the Cisco Unified Communications Manager Administration or from the web: http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Network, Server, and Client PC Requirements

Before deploying the Cisco IP Communicator application to users, make sure you comply with the network, server, and client PC requirements that are described in the release notes at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html

Related Topics

- How Cisco IP Communicator Interacts with Cisco Unified Communications Manager, page 1-4
- Configuration and Deployment Checklist, page 2-2

Configuration and Deployment Checklist

Table 2-1 provides an overview of the administrative tasks involved in preparing for, deploying, and configuring Cisco IP Communicator.

The table is divided into these sections:

- Gathering information and adding devices to Cisco Unified Communications Manager
- Configuring features and settings in Cisco Unified Communications Manager Administration
- Deploying and configuring the Cisco IP Communicator application

Some of the tasks in the table are not specific to Cisco IP Communicator but apply to any Cisco Unified Communications Manager-supported phone device.

Note In general, to ensure that features are properly set up for the user at first launch and remain consistent thereafter, we recommend that you configure the settings in Cisco Unified Communications Manager Administration before deploying Cisco IP Communicator.

Table 2-1 Configuration and Deployment Checklist

Task	Notes	For details, see...
Gathering information and adding devices to Cisco Unified Communications Manager		
1. For each device, gather this information: • Users in the Cisco Unified Communications Manager database to associate with it • Lines and directory numbers to assign to it • Features to be added to and configured for it • The device pool, calling search space, and other data for the Device Information field (if applicable)	Optional. Use this information to configure devices in Cisco Unified Communications Manager Administration. On the Phone Configuration window, the Device Information fields automatically populate if information is relevant and available. Edit fields only if you want to override system settings on a per-device basis.	• Configuring Features and Services for Cisco IP Communicator, page 5-1 • *Cisco Unified Communications Manager System Guide* • *Cisco Unified Communications Manager Administration Guide*
2. Decide on the method for adding devices to the Cisco Unified Communications Manager database (see the far right column for details): – Auto-registration – Cisco Unified Communications Manager Administration only – BAT[1] only – BAT and TAPS[2]	Required. The method that you use to add devices determines how the directory number is assigned and how the device name for each client PC is specified. If you do not use auto-registration or TAPS to add a devices, add the device to Cisco Unified Communications Manager before deploying the application.	• About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6 • *Cisco Unified Communications Manager Administration Guide* • *Bulk Administration Tool User Guide*

Table 2-1 Configuration and Deployment Checklist (continued)

Task	Notes	For details, see...
3. Choose a method to gather the device name (use the MAC address of the appropriate network interface on the client PC or specify a free-form device name).	Not necessary if you use auto-registration or TAPS.	• About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6 • Command-Line Options for the MSI Package, page 3-4
4. Configure adjunct licensing.	Optional. Associates a secondary softphone device with a primary device and consumes only one device license per device. Not available in Cisco Unified Communications Manager versions earlier than 6.0(1).	• Configuring Cisco IP Communicator for Adjunct Licensing, page 2-9
5. Configure Cisco IP Communicator with different protocols.	Optional unless you want to use SIP.	• How to Configure Cisco IP Communicator the SCCP or SIP Protocol, page 2-9
6. Configure Cisco IP Communicator with security features.	Recommended. Prevents identity theft of a Cisco Unified IP Phone and the Cisco Unified Communications Manager server. You can configure encryption to prevent call signaling tampering.	• How to Configure Security Features for Cisco IP Communicator, page 2-12
Configuring features and settings in Cisco Unified Communications Manager Administration		
1. Configure Cisco Unified Communications Manager telephony features (call waiting, call forward, call park, call pickup); establish a voice messaging system.	As needed. Provides enhanced telephony functionality.	• Configuring Features and Services for Cisco IP Communicator, page 5-1 • *Cisco Unified Communications Manager Administration Guide* • *Cisco Unified Communications Manager Features and Services Guide*
2. Make Cisco IP Communicator a available in languages other than English.	As needed. All languages might not be immediately available. Check the website for updates. If you are using Cisco IP Communicator in a locale other than English, you should install the Cisco IP Telephony Locale Installer on every Cisco Unified Communications Manager server in the cluster. Doing so ensures that you have the latest translated text, user and network locales, and country-specific phone tones available.	• *Using the Cisco IP Telephony Locale Installer* a this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html • Deployment Methods, page 3-3

Table 2-1 Configuration and Deployment Checklist (continued)

Task	Notes	For details, see...
3. Modify phone button and softkey templates.	As needed. Phone button templates assign features to line and speed-dial buttons. Softkey templates manage softkeys associated with application that are supported by Cisco IP Communicator.	- Phone Button Template Modification, page 5-12 - Softkey Template Configuration, page 5-12
4. Configure Cisco Unified IP Phone services.	Recommended. Gives users access stock quotes and weather reports, for example, which are displayed on the phone as interactive content with text and graphics.	- Setting Up Services, page 5-13 - *Cisco Unified Communications Manager Administration Guide* - *Cisco Unified Communications Manager Features and Services Guide*
5. Run the Cisco IP Communicator Administration Tool on the Cisco Unified Communications Manager publisher (the TFTP server where phone loads will be installed).	You must run the tool to install the Directory Wizard (used to configure the Quick Search and Dialing Rules features). Obtain the tool from the product software download web site: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661. It is located inside the zipped folder with your build. (For Windows-based Cisco Unified Communications Managers only) If any users in your network rely on unsupported VPN clients, you must enable HTTP access (the tool sets up an IP reflector web page to resolve audio IP auto-detection problems). Enabling HTTP access also improves performance for remote users.	- Resolving Audio IP Address Auto-Detection Problems, page 4-10 - Modifications for Remote Use, page 4-12 - About Configuring Corporate and Personal Directories, page 5-13
6. Set up directories, including configuration files for the Quick Search and Dialing Rules features.	Recommended. Quick Search can search both corporate and personal directories. Use Dialing Rules to apply a dialing plan. If you are integrated with the Cisco Unified Communications Manager directory, use the Directory Wizard to auto-detect configuration values and to configure Quick Search and Dialing Rules. First, run the Administration Tool (see the previous step).	- About Configuring Corporate and Personal Directories, page 5-13 - *Cisco Unified Communications Manager Administration Guide*

Table 2-1 Configuration and Deployment Checklist (continued)

Task	Notes	For details, see...
7. Add users to Cisco Unified Communications Manager.	Recommended. Associate users with device IDs to enable access to the User Options web pages. Include users and their phone numbers in relevant Quick Search results (when integrated with a Cisco Unified Communications Manager directory).	• Adding Users to Cisco Unified Communications Manager, page 5-1 • *Cisco Unified Communications Manager Administration Guide* • *Bulk Administration Tool User Guide*
Deploying and configuring Cisco IP Communicator		
1. Decide on the method for deploying Cisco IP Communicator: – Place an installer package on a shared location where you or a user can run it – Perform installation for an entire enterprise by using a software distribution tool – Deploy directly on a computer	With the first option, users must have administrative privileges on their PCs for you to deploy software. If you use a Microsoft Windows installer package, you can provide command-line options to specify values during deployment.	How to Deploy the Application, page 3-2
2. Set up a web site, or use another method to tell users how to: – Install and configure the application – Obtain user documentation – Access the User Options web pages	Recommended. By providing this information, you can improve the user experience of the product.	Providing Information to Users About Cisco IP Communicator, page A-1
3. Install audio devices on each client PC or provide installation information to users.	You or the user must install audio devices that rely on USB headset and handset drivers. Ideally, you should perform this task before the application is installed on the client PC.	• Installation and Configuration of Headsets and Other Audio Devices, page 3-1 • About Selecting and Tuning Audio Devices, page 4-5
4. Configure, or help users configure, the installed application as necessary.	Before the application will function at initial startup, some configuration tasks might be required.	Configuring Cisco IP Communicator, page 4-1

[1] BAT = Bulk Administration Tool

[2] TAPS = Tool for Auto-Registered Phones Support

Related Topics

- About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6
- How to Deploy the Application, page 3-2
- About Updating the Application, page 3-6
- Overview of Configuration Tasks, page 4-1

About Methods for Adding Devices to the Cisco Unified Communications Manager Database

Before installing the Cisco IP Communicator application, you must decide how to add devices to the Cisco Unified Communications Manager database.

Table 2-2 lists your options.

Table 2-2 Options for Adding Devices to Cisco Unified Communications Manager

Method for Adding Devices	Requires Device Name?	Notes	For details, see...
Auto-registration	No	Results in automatic assignment of directory numbers.	Auto-Registration Method for Adding Devices, page 2-6
Auto-registration with TAPS	No	Requires auto-registration and BAT. Updates information in Cisco IP Communicator and in Cisco Unified Communications Manager Administration.	Auto-Registration and TAPS Method for Adding Devices, page 2-7
Cisco Unified Communications Manager Administration	Yes	Requires devices to be added individually. You must add the device to Cisco Unified Communications Manager before installing the application on the client PC.	Cisco Unified Communications Manager Administration Method for Adding Devices, page 2-8
BAT	Yes	Allows for bulk registration of devices. You must add the device to Cisco Unified Communications Manager before installing the application on the client PC.	BAT Method for Adding Devices, page 2-8

Auto-Registration Method for Adding Devices

You can use this auto-registration method without first gathering device names from client PCs.

When auto-registration is enabled, Cisco Unified Communications Manager provides a directory number as soon as you run Cisco IP Communicator after installation. During auto-registration, Cisco Unified Communications Manager automatically assigns the next available sequential directory number to the device.

You can use auto-registration to quickly submit devices into the Cisco Unified Communications Manager database. You can then modify settings, such as the directory numbers, from Cisco Unified Communications Manager. Additionally, you can move auto-registered devices to new locations and assign them to different device pools without affecting their directory numbers.

Note When you configure the Cisco Unified Communications Manager cluster for mixed mode through the Cisco Certificate Trust List (CTL) client, auto-registration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, auto-registration is automatically enabled.

For details about enabling and configuring auto-registration, see the *Cisco Unified Communications Manager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Related Topics

- Configuration and Deployment Checklist, page 2-2
- Auto-Registration and TAPS Method for Adding Devices, page 2-7
- Cisco Unified Communications Manager Administration Method for Adding Devices, page 2-8
- BAT Method for Adding Devices, page 2-8
- Configuring Cisco IP Communicator for Adjunct Licensing, page 2-9

Auto-Registration and TAPS Method for Adding Devices

You can use the auto-registration with TAPS method without first gathering MAC addresses from client PCs.

The TAPS works with the BAT to update devices that were previously added with dummy device names to the Cisco Unified Communications Manager database. Use TAPS to update MAC addresses and to download predefined configurations for Cisco IP Communicator devices.

For TAPS to function, make sure that you enable auto-registration in Cisco Unified Communications Manager Administration (**System > Cisco Unified Communications Manager**).

Note When you configure the Cisco Unified Communications Manager cluster for mixed mode through the Cisco CTL client, auto-registration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, auto-registration is automatically enabled.

Then you or the user dial a TAPS directory number and follow voice prompts. When the process is complete, Cisco IP Communicator downloads its directory number and other settings.
Cisco IP Communicator is updated in Cisco Unified Communications Manager Administration with the correct device name.

For details, see the *Bulk Administration Tool User Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Related Topics

- Configuration and Deployment Checklist, page 2-2
- Auto-Registration Method for Adding Devices, page 2-6
- Cisco Unified Communications Manager Administration Method for Adding Devices, page 2-8
- BAT Method for Adding Devices, page 2-8
- Configuring Cisco IP Communicator for Adjunct Licensing, page 2-9

Cisco Unified Communications Manager Administration Method for Adding Devices

To add devices individually to the Cisco Unified Communications Manager database through Cisco Unified Communications Manager Administration, you must collect the appropriate device name (use a MAC address of the appropriate network interface on the client PC or specify a free-form device name with the MSI package) for each client on which you want Cisco IP Communicator installed.

After you collect the device names, choose **Device > Phone** in Cisco Unified Communications Manager Administration (or **Device > Add a New Device** in Cisco Unified Communications Manager Administration 4.x). For complete instructions, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Related Topics

- Configuration and Deployment Checklist, page 2-2
- Auto-Registration Method for Adding Devices, page 2-6
- Auto-Registration and TAPS Method for Adding Devices, page 2-7
- BAT Method for Adding Devices, page 2-8
- Command-Line Options for the MSI Package, page 3-4
- Configuring Cisco IP Communicator for Adjunct Licensing, page 2-9

BAT Method for Adding Devices

The Bulk Administration Tool (BAT) is a plug-in application for Cisco Unified Communications Manager that enables you to perform batch operations (including registration) on large numbers of devices, including Cisco Unified IP Phones and Cisco IP Communicator devices.

To add devices by using BAT only (meaning, not with TAPS), collect the appropriate device name (use a MAC address or specify a free-form device name with the MSI package) for each client on which you want Cisco IP Communicator installed.

For details about using BAT, see the *Cisco Unified Communications Manager Administration Guide* and the *Bulk Administration Tool User Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Related Topics

- Configuration and Deployment Checklist, page 2-2
- Auto-Registration Method for Adding Devices, page 2-6
- Auto-Registration and TAPS Method for Adding Devices, page 2-7
- Cisco Unified Communications Manager Administration Method for Adding Devices, page 2-8
- Configuring Cisco IP Communicator for Adjunct Licensing, page 2-9
- Command-Line Options for the MSI Package, page 3-4

Configuring Cisco IP Communicator for Adjunct Licensing

In Cisco Unified Communications Manager releases 6.0(1) and later, you can associate a secondary softphone device with a primary device and consume only one device license per device (also known as secondary licensing or adjunct licensing). For releases prior to Cisco Unified Communications Manager Release 6.0(1), three device licenses are consumed.

You can configure adjunct licensing manually through the Phone Configuration window, through Cisco AXL Web Service, or through BAT.

Restrictions

- Adjunct licensing has these restrictions:
  - You can associate up to two secondary softphone devices to a primary phone.
  - You cannot delete the primary phone unless you remove the associated secondary softphone devices.
  - The primary phone must be the device that consumes the most licenses You cannot make the softphone device the primary phone and associate a Cisco Unified IP Phone as the secondary device.
  - Secondary softphone devices are limited to Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device > Phone**.

Step 2 Add Cisco IP Communicator by clicking **Add New**, or if the device is already in the database, search for the softphone device name.

Step 3 On the Phone Configuration window, configure all required fields for your environment.

Step 4 Select the device name of the Cisco Unified IP Phone to associate with Cisco IP Communicator for Primary. Phone.

Step 5 Click **Save**.

How to Configure Cisco IP Communicator the SCCP or SIP Protocol

Cisco IP Communicator can operate with SCCP or SIP. You can convert Cisco IP Communicator from one protocol to the other.

- Converting a New Cisco IP Communicator from SCCP to SIP, page 2-10
- Converting an Existing Cisco IP Communicator from SCCP to SIP, page 2-11
- Converting an Existing Cisco IP Communicator from SIP to SCCP, page 2-11
- Deploying Cisco IP Communicator in an SCCP and SIP Environment, page 2-11
- Switching Cisco IP Communicator Between SCCP and SIP Configurations, page 2-12

Note If you configure Cisco IP Communicator as a SIP endpoint, it will no longer support Cisco Unified Video Advantage. Cisco Unified Video Advantage can be used only with Cisco IP Communicator as an SCCP endpoint.

Converting a New Cisco IP Communicator from SCCP to SIP

When you install Cisco IP Communicator for the first time, it is set for SCCP by default, but you can convert it to SIP.

Procedure

Step 1 Perform one of these actions:

- To auto-register Cisco IP Communicator, set the Auto Registration Phone Protocol parameter (**System > Enterprise Parameters**) to SIP.
- To provision Cisco IP Communicator by using the Bulk Administration Tool (BAT), choose the Cisco IP Communicator and then choose SIP from the BAT.
- To manually provision Cisco IP Communicator, select **SIP** as the protocol (**Device > Phone**), click **Next**, and then make the appropriate changes for SIP on the Phone Configuration window.

For details, see the *Cisco Unified Communications Manager Administration Guide* for your release and the *Bulk Administration Tool User Guide* for your release at these URLs:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_user_guide_list.html

Step 2 Ensure that the SIP flag is turned on for the client.

Step 3 If you are not using DHCP in your network, configure the network parameters appropriately.

If you do not use DHCP in your network to identify TFTP servers, or if you want the device to use an alternate TFTP server, you must configure your TFTP server with command-line options when you deploy Cisco IP Communicator.

Optionally, you can instruct users to manually configure the TFTP servers.

Related Topics

- Command-Line Options for the MSI Package, page 3-4
- Specifying a TFTP Server, page 4-6

Converting an Existing Cisco IP Communicator from SCCP to SIP

You can use the BAT to convert a phone in use in your network from SCCP to SIP.

Procedure

Step 1 To access the BAT, choose **Bulk Administration > Phones > Migrate Phones > SCCP to SIP**.

Step 2 Migrate phones by following the *Bulk Administration Tool User Guide* for your release at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_user_guide_list.html

Converting an Existing Cisco IP Communicator from SIP to SCCP

Procedure

Step 1 Delete the existing Cisco IP Communicator from the database.

Step 2 Create the instance of Cisco IP Communicator as an SCCP device (**Device > Phone**).

For details, see the *Cisco Unified Communications Manager Administration Guide* for your release at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Deploying Cisco IP Communicator in an SCCP and SIP Environment

To deploy Cisco IP Communicator in an environment that includes SCCP and SIP and in which the Cisco Unified Communications Manager Auto-Registration parameter is SCCP, perform these general steps:

Procedure

Step 1 Set the Cisco Unified Communications Manager auto_registration_protocol parameter to SCCP.

Step 2 From Cisco Unified Communications Manager Administration, choose System > Enterprise Parameters.

Step 3 Change the Auto Registration Protocol enterprise parameter to SIP

Step 4 Install Cisco IP Communicator.

Step 5 Auto-register the Cisco IP Communicator. This needs to be a SIP device.

Switching Cisco IP Communicator Between SCCP and SIP Configurations

After Cisco IP Communicator is registered, you can use the device name feature in Cisco IP Communicator to quickly change from an SCCP configuration to a SIP configuration.

Limitation

Cisco Unified Communications Manager release 4.x does not support the device name feature.

Procedure

Step 1 On the Phone Configuration page, add Cisco IP Communicator as an SCCP device, specify a device name (for example, *SCCPconfig)*, specify other settings as appropriate, and click **Save**.

Step 2 Repeat Step 1, but add Cisco IP Communicator as an SIP device, and specify a device name (for example *SIPconfig*), and click **Save**.

Step 3 Right-click Cisco IP Communicator, and choose **Preferences > Network** tab.

Step 4 Select the Use this Device Name option, and enter the name you specified as the SCCP configuration or as the SIP configuration.

Step 5 Click **OK**.

Cisco Unified Communications Manager uses the specified name to apply the correct configuration to Cisco IP Communicator.

How to Configure Security Features for Cisco IP Communicator

By configuring security features in Cisco Unified Communications Manager, you can prevent identity theft of the phone (prevent Cisco IP Communicator from impersonating another Cisco Unified IP Phone) and the Cisco Unified Communications Manager server. By configuring phones in encrypted mode, you can also prevent call signaling tampering. To alleviate these threats, the Cisco IP telephony network establishes and maintains authenticated communication streams between Cisco IP Communicator and the server by using Transport Layer Security (TLS)-based, mutual authentication using certificates when connected to Cisco Unified Communications Manager. Two-way authentication with the Certificate Authority Proxy Function (CAPF) and a Locally Significant Certificate (LSC) are used. The LSC is a digital X.509v3 certificate that is installed on Cisco IP Communicator and is issued by a third-party certificate authority or by the CAPF.

- Supported Security Features, page 2-13
- Identification of Encrypted and Authenticated Phone Calls, page 2-14
- Security Restrictions for Barging into an Authenticated Call, page 2-16
- Configuring Security with Cisco Unified Communications Manager, page 2-17
- Configuring Security with Cisco Unified Communications Manager Release 4.X, page 2-18
- Authentication Mode Settings, page 2-19
- Verifying the Security Configuration, page 2-20
- How to Unlock Options to Make Configuration Changes, page 2-20
- Where to Find Additional Security Information, page 2-21

Supported Security Features

Table 2-3 describes the security features that Cisco IP Communicator supports.

Note Most security features are available only if a CTL is installed on Cisco IP Communicator. For details about the CTL, see the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

This guide also provides a list of interactions, restrictions, and limitations for security.

Table 2-3 Security Features Supported on Cisco IP Communicator

Feature	Description
Customer-site certificate installation	Each installation of Cisco IP Communicator requires a unique certificate for device authentication. Cisco IP Communicator allows you to specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the CAPF. Alternatively, you can initiate the installation of an LSC from the Security Configuration menu.
Device authentication	Occurs between Cisco Unified Communications Manager and Cisco IP Communicator when each entity accepts the certificate of the other entity. Determines whether a secure connection between Cisco IP Communicator and Cisco Unified Communications Manager should occur, and, if necessary, creates a secure signaling path between the entities by using the TLS protocol. Cisco Unified Communications Manager does not register Cisco IP Communicator for a user unless it can authenticate the software. Signed binary files (with the *.sbn* extension) prevent tampering with the firmware image before it is loaded on Cisco IP Communicator. Device authentication relies on the creation of the Cisco CTL file (for authenticating the Cisco Unified Communications Manager server and applications) and the CAPF (for authenticating the phone device). The CTL file is created when you install and configure the Cisco CTL client on a Windows workstation or server that has a USB port. You install the Cisco CTL client plug-in from Cisco Unified Communications Manager Administration.
File authentication	Validates digitally signed files that the phone downloads. The 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 phone. The phone rejects such files without further processing.
Signaling authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission. Signaling authentication relies on the creation of the CTL file.
CAPF	Implements parts of the certificate generation procedure that are too processing-intensive for Cisco IP Communicator. It interacts with Cisco IP Communicator for key generation and certificate installation. You can configure the CAPF to request certificates from customer-specified certificate authorities on behalf of Cisco IP Communicator, or you can configure it to generate certificates locally. The CAPF is a process by which a supported device can request an LSC by using Cisco Unified Communications Manager Administration. This certificate type installs on Cisco IP Communicator after you perform the necessary tasks that are associated with the Cisco CAPF.

Table 2-3 Security Features Supported on Cisco IP Communicator (continued)

Feature	Description
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 creation of a media master key pair for the devices, delivery of the keys to the devices, and secures the delivery of the keys while the keys are in transport.
Signaling encryption (SCCP phones only)	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
Security profiles	Defines whether Cisco IP Communicator is nonsecure, authenticated, or encrypted. To view the security profile name, choose **Settings > Security Configuration** from the Cisco IP Communicator interface. See the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
Encrypted configuration files	Allows you to ensure the privacy of phone configuration files.
Disabling settings access	Disables local access to network and other settings for Cisco IP Communicator from the Cisco Unified Communications Manager Administration Phone Configuration window. See Disabling Local Settings Access, page 4-13.

Related Topics

- Identification of Encrypted and Authenticated Phone Calls, page 2-14
- Security Restrictions for Barging into an Authenticated Call, page 2-16
- How to Configure Security Features for Cisco IP Communicator, page 2-12

Identification of Encrypted and Authenticated Phone Calls

When you implement security for Cisco IP Communicator, you can identify encrypted and authenticated phone calls by the icon on the main screen. In an authenticated call, all devices participating in the establishment of the call are authenticated by the Cisco Unified Communications Manager. The system uses TLS to secure the tunnel through which the signaling and voice traffic passes.

When a call in progress is authenticated end-to-end, the call progress icon to the right of the call duration timer changes to this icon:

In an encrypted call, all devices participating in the establishment of the call are authenticated by the Cisco Unified Communications Manager. In addition, call signaling and media streams are encrypted. An encrypted call offers the highest level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to this icon:

Related Topic

- Security Restrictions for Barging into an Authenticated Call, page 2-16

Establishing and Identifying Secure Conference Calls

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

1. A user initiates the conference from a secure phone (encrypted or authenticated security mode).
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone (encrypted or authenticated) and maintains the secure level for the conference.
4. The phone displays the security level of the conference call. A secure conference displays 🔒 (encrypted) or 🛡 (authenticated) icon to the right of "Conference" on the phone screen. If ▶ icon displays, the conference is not secure.

Note There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participant's phones and the availability of secure conference bridges. See Table 2-4 and Table 2-5 for information about these interactions.

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 also security in the system. Table 2-4 provides information about changes to call security levels when using Barge.

Table 2-4 Call Security Interactions When Using Barge

Initiator's Phone Security Level	Feature Used	Call Security Level	Results of Action
Non-secure	Barge	Encrypted call	Call barged and identified as non-secure call
Secure (encrypted)	Barge	Authenticated call	Call barged and identified as authenticated call
Secure (authenticated)	Barge	Encrypted call	Call barged and identified as authenticated call
Non-secure	Barge	Authenticated call	Call barged and identified as non-secure call

Table 2-5 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 2-5 Security Restrictions with Conference Calls

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Non-secure	Conference	Encrypted or authenticated	Non-secure conference bridge Non-secure conference
Secure (encrypted or authenticated)	Conference	At least one member is non-secure	Secure conference bridge Non-secure conference

Table 2-5 Security Restrictions with Conference Calls (continued)

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Secure (encrypted)	Conference	All participants are encrypted	Secure conference bridge Secure encrypted level conference
Secure (authenticated)	Conference	All participants are encrypted or authenticated	Secure conference bridge Secure authenticated level conference
Non-secure	Conference	Encrypted or authenticated	Only secure conference bridge is available and used Non-secure conference
Secure (encrypted or authenticated)	Conference	Encrypted or authenticated	Only non-secure conference bridge is available and used Non-secure conference
Secure (encrypted or authenticated)	Conference	Encrypted or secure	Conference remains secure. When one participant tries to hold the call with MOH, the MOH does not play.
Secure (encrypted)	Join	Encrypted or authenticated	Secure conference bridge Conference remains secure (encrypted or authenticated)
Non-secure	cBarge	All participants are encrypted	Secure conference bridge Conference changes to non-secure
Non-secure	MeetMe	Minimum security level is encrypted	Initiator receives message "Does not meet Security Level", call rejected.
Secure (encrypted)	MeetMe	Minimum security level is authenticated	Secure conference bridge Conference accepts encrypted and authenticated calls
Secure (encrypted)	MeetMe	Minimum security level is non-secure	Only secure conference bridge available and used Conference accepts all calls

Security Restrictions for Barging into an Authenticated Call

A user can barge into an authenticated call even if the phone that is used to barge is nonsecure. The authentication icon continues to appear on the authenticated devices in the call even if the initiator phone does not support security.

Configuring Security with Cisco Unified Communications Manager

Before You Begin

1. Configure the Cisco CTL client.

   http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

2. Configure the CAPF, and install the LSC.

For details, follow the steps in the *Cisco Unified Communications Manager Security Guide* that apply to your release of Cisco Unified Communications Manager:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Procedure

Step 1 From Cisco Unified Communications Manager Administration, configure phone security profiles:

a. Choose **System > Security Profile > Phone Security Profile**.

b. For the Phone Security Profile Type, select **Cisco IP Communicator**.

c. For the phone security profile protocol, select either **SCCP** or **SIP**.

d. In the Phone Security Profile Information section, enter a name and a description (optional) for the profile.

e. (SIP only) For Nonce Validity Time, use the default setting.

f. For Device Security Mode, select **Encrypted** or **Authenticated**, as applicable.

   If SIP is the profile protocol, the Transport Type field automatically selects **TCP** for Non Secure and **TLS** for Authenticated or Encrypted.

g. In the Phone Security Profile CAPF Information section, for Authentication Mode, choose the method by which you want Cisco IP Communicator to authenticate with CAPF. For a description of the methods, see Table 2-6 on page 2-19.

h. For Key Size, choose the key size for the certificate. If you choose a higher key size than the default setting, Cisco IP Communicator takes longer to generate the entropy that is required to generate the keys.

i. Click **Save**.

Step 2 Apply a phone security profile to Cisco IP Communicator:

a. Choose **Device > Phone**, and find a Cisco IP Communicator device.

b. In the Protocol Specific Information section, for Device Security Profile, select the profile that you created in Step 1.

Step 3 Specify the settings for the CAPF section:

a. For Certificate Operation, select **Install/Upgrade** to install a new or upgrade an existing LSC.

b. For Authentication Mode, choose the method by which you want Cisco IP Communicator to authenticate with CAPF. For details about the modes, see Step 1g.

c. (If you chose **By Authentication String** in Step 1g) For Authentication String, manually enter a string or generate a string by clicking **Generate String**. The string must contain four to 10 digits.

   To install, upgrade, delete, or troubleshoot an LSC certificate, you or the Cisco IP Communicator must unlock the configuration and enter the authentication string in Cisco IP Communicator.

d. For Key Size, choose the key size for the certificate. If you choose a higher key size than the default setting, Cisco IP Communicator takes longer to generate the entropy that is required to generate the keys.

e. For Operation Completes By, specify the date and time by which Cisco IP Communicator must register with Cisco Unified Communications Manager.

f. Click **Save**.

Related Topics

- Verifying the Security Configuration, page 2-20
- How to Unlock Options to Make Configuration Changes, page 2-20
- How to Resolve Security Problems, page 8-7

Configuring Security with Cisco Unified Communications Manager Release 4.X

Before You Begin

1. Configure the Cisco CTL client.

   http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

2. Configure the Certificate Authority Proxy Function (CAPF), and install the LSC.

   For details, follow the steps in the *Cisco Unified Communications Manager Security Guide* that apply to your release of Cisco Unified Communications Manager:

   http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

3. Make sure you downloaded and installed the Cisco Unified Communications Manager device pack to add support for security features in Cisco IP Communicator. For details, see the Cisco IP Communicator release notes at this URL:

   http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html

Procedure

Step 1 From Cisco Unified Communications Manager Administration, perform *one* of these tasks:

a. Configure the security device system default (**System > Enterprise Parameters**) by following the steps in the Release 4.x security guide and by setting the Device Security Mode to **Encrypted** or **Authenticated**, as applicable.

b. Configure the device security mode for a single Cisco IP Communicator device in the Phone Configuration window (**Device > Phone**), and set Device Security Mode to **Encrypted** or **Authenticated,** or to **Use System Defaults** (if you performed Step 1a).

c. Configure the device security mode by using the Bulk Administration Tool. For details, see the user guide at this URL:

   http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_user_guide_list.html

Step 2 On the Phone Configuration page (**Device > Phone**), specify the settings for the CAPF section:

a. For Certificate Operation, select **Install/Upgrade** to install a new or upgrade an existing LSC.

b. For Authentication Mode, choose the method by which you want Cisco IP Communicator to authenticate with CAPF. For a description of the methods, see Table 2-6 on page 2-19.

c. (If you chose **By Authentication String** in Step 2b) For Authentication String, manually enter a string or generate a string by clicking **Generate String**. The string must contain four to 10 digits.

To install, upgrade, delete, or troubleshoot an LSC, you or the Cisco IP Communicator must unlock the configuration and enter the authentication string in Cisco IP Communicator.

d. For Key Size, choose the key size for the certificate. If you choose a higher key size than the default setting, Cisco IP Communicator takes longer to generate the entropy that is required to generate the keys.

e. For Operation Completes By, specify the date and time by which Cisco IP Communicator must register with Cisco Unified Communications Manager.

f. Click **Insert** (if adding a new device) or **Update** (if modifying an existing device).

Related Topics

- Verifying the Security Configuration, page 2-20
- How to Unlock Options to Make Configuration Changes, page 2-20
- How to Resolve Security Problems, page 8-7

Authentication Mode Settings

Table 2-6 Security Authentication Settings Supported on Cisco IP Communicator

Authentication Mode Field	Description
By Authentication String	Installs or upgrades, deletes, or troubleshoots an LSC only when you or the user enters the CAPF authentication string on Cisco IP Communicator.
By Null String	Installs or upgrades, deletes, or troubleshoots an LCS without user intervention **Note** This option provides no security; we strongly recommend that you choose this option only for closed, secure environments.
By Existing Certificate (Precedence to LSC)	Installs or upgrades, deletes, or troubleshoots an LSC if an LSC exists on Cisco IP Communicator. If an LSC exists on Cisco IP Communicator, authentication occurs through the LSC, whether or not another certificate exists on Cisco IP Communicator. If another certificate and an LSC exist on Cisco IP Communicator, authentication occurs through the LSC. Before you choose this option, verify that a certificate exists on Cisco IP Communicator. If you choose this option and no certificate exists on Cisco IP Communicator, the operation fails. At any time, Cisco IP Communicator uses only one certificate to authenticate to CAPF. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate through the other certificate, you must update the authentication mode.

Note The By Existing Certificate (Precedence to MIC) option is not supported by Cisco IP Communicator.

Verifying the Security Configuration

Procedure

Step 1 Verify that the CTL file is installed on the client PC that is running Cisco IP Communicator.

In Cisco IP Communicator, choose **Settings > Security Configuration > CTL File**. Verify that a 32-digit hexadecimal string displays instead of displaying *Not Installed*.

Step 2 Verify the security configuration on Cisco IP Communicator by choosing **Settings > Security Configuration**.

- For Authenticated - Ensure that the Security Mode displays *Authenticated* and that the LSC displays *Installed*.
- For Encrypted - Ensure that the Security Mode displays *Encrypted* and that the LSC displays *Installed*.

Step 3 Check **Settings** > **Status > Status Messages** for other messages that might display.

Related Topics

- Status Messages Displayed, page 7-9

How to Unlock Options to Make Configuration Changes

By default, configuration options that can be changed are locked to prevent users from making changes that could affect the operation of Cisco IP Communicator.

During the security configuration in Cisco Unified Communications Manager Administration, if you set the Authentication Mode to **By Authentication String**, you must unlock options to enter the authentication string. You might also need to unlock options to erase a CTL file.

Related Topics

- Unlocking Options to Enter the Authentication String, page 2-20
- Erasing the CTL File, page 2-21

Unlocking Options to Enter the Authentication String

When options are inaccessible for modification, locked padlock icon 🔒 appears on the configuration menu.

When options are unlocked and accessible for modification, unlocked padlock icon 🔓 appears.

Procedure

Step 1 From Cisco IP Communicator, click **Settings**.

Step 2 Type ****#** to unlock settings.

Step 3 Scroll to **Security Configuration > LSC**, and click **Update**.

Step 4 Enter the authentication string by using the computer keyboard or by using the Cisco IP Communicator dial pad, and click **Submit**.

Depending on how you configured the CAPF, Cisco IP Communicator begins to install the LSC. During the procedure, a series of messages appear in the LSC option in the Security Configuration menu so that you can monitor progress. When the procedure successfully completes, Cisco IP Communicator displays *Installed*.

Note When you are finished, make sure to lock settings by pressing **#. This action either locks or unlocks the options depending on the previous state.

Erasing the CTL File

If Cisco IP Communicator experiences an error with the CTL file, you can remove it.

Procedure

Step 1 From Cisco IP Communicator, click **Settings > Security Configuration > CTL File**.

Step 2 Click **# to unlock settings.

Step 3 Click **Erase** to delete the CTL file from Cisco IP Communicator and restart it.

Note When you are finished, make sure to lock settings by pressing **#. This action either locks or unlocks the options depending on the previous state.

Where to Find Additional Security Information

Table 2-7 shows where you can find additional information about security.

Table 2-7 Cisco IP Communicator and Cisco Unified Communications Manager Security Topics

Topic	See...
Detailed explanation of security, including set up, configuration, and troubleshooting information	*Cisco Unified Communications Manager Security Guide* http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
Security and the Cisco IP Communicator startup process	How Cisco IP Communicator Interacts With the Network at Startup, page 1-5
Security and Cisco IP Communicator configuration files	About Configuration Files, page 1-6
TLS connection	Supported Networking Protocols, page 1-2 About Configuration Files, page 1-6
Unified CM Configuration Menu security icons for the Unified CM 1 through Unified CM 5	Device Configuration Information, page 7-2

Table 2-7   Cisco IP Communicator and Cisco Unified Communications Manager Security Topics (continued)

Topic	See...
Security Configuration menu items	Security Configuration Information, page 7-7
Status messages	Status Messages Displayed, page 7-9
Troubleshooting	How to Resolve Security Problems, page 8-7 *Cisco Unified Communications Manager Security Guide* http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

CHAPTER 3

Deploying and Updating Cisco IP Communicator

Revised: 1/19/11

This chapter describes how to deploy and update Cisco IP Communicator. Before completing tasks covered in this chapter, be sure to read Chapter 2, "Preparing to Deploy Cisco IP Communicator," which provides an overview of tasks that you might need to perform before deployment.

Some tasks in this chapter required configuration in Cisco Unified Communications Manager, formerly known as Cisco Unified CallManager.

- Installation and Configuration of Headsets and Other Audio Devices, page 3-1
- Use of Third-Party Headsets and Handsets with Cisco IP Communicator, page 3-2
- How to Deploy the Application, page 3-2
- About Updating the Application, page 3-6

Installation and Configuration of Headsets and Other Audio Devices

Before the user installs Cisco IP Communicator on the client PC, you or the user should install and configure any audio devices that require drivers, such as sound cards, universal serial bus (USB) handsets, or USB headsets. For details about supported audio devices, see the release notes at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html

If users are installing audio devices and Cisco IP Communicator, recommend that they complete any guided installations (such as the Found New Hardware Wizard or manufacturer instructions) after plugging in audio devices and before installing Cisco IP Communicator.

At first launch after installation, users must *select* and *tune* audio devices before using those devices with Cisco IP Communicator. At initial start up, the Audio Tuning Wizard automatically launches, and users must complete the wizard before Cisco IP Communicator launches.

Related Topics

- Use of Third-Party Headsets and Handsets with Cisco IP Communicator, page 3-2
- About Selecting and Tuning Audio Devices, page 4-5

Use of Third-Party Headsets and Handsets with Cisco IP Communicator

While Cisco does perform basic testing of third-party headsets and handsets for use with Cisco IP Communicator, it is ultimately the customer's responsibility to test this equipment in their own environment to determine suitable performance. Due to the many inherent environmental and hardware inconsistencies in the locations where Cisco IP Communicator is deployed, there is not a single “best” solution that is optimal for all environments.

Before customers begin deploying any headsets or handsets (especially deployment in quantity) in their production network, Cisco recommends thorough testing at the customer site to check for voice quality issues, especially hum and echo.

The primary reason that support of a headset or handset would be inappropriate for an installation is the potential for an audible hum. This hum can either be heard by the remote party or by both the remote party and the Cisco IP Communicator user. Causes for this humming sound range from electrical lights near the PC to the PC power source itself. In some cases, a hum heard on a headset that is plugged directly into the PC USB port might be reduced or eliminated by using a powered USB hub.

In some instances, the mechanics or electronics of various headsets can cause remote parties to hear an echo of their own voice when they speak to Cisco IP Communicator users. The Cisco IP Communicator user are not aware of this echo.

Finally, some analog headsets do not match the electrical characteristics for which some soundcards are designed. The microphones on such headsets are frequently too sensitive, even when the input levels in Cisco IP Communicator are reduced to their lowest values; the users of such headsets sound distorted to remote parties.

It is important to ask Cisco IP Communicator users whether a particular headset sounds good to them. Remote parties should be queried as to the reception from Cisco IP Communicator when using a particular headset.

Related Topics

- About Selecting and Tuning Audio Devices, page 4-5

How to Deploy the Application

- Installer Package Names, page 3-2
- Deployment Methods, page 3-3
- Command-Line Options for the MSI Package, page 3-4

Installer Package Names

You can deploy Cisco IP Communicator by using either of the installer packages listed in Table 3-1.

Table 3-1 Installer Packages for Cisco IP Communicator

Filename	Description
CiscoIPCommunicatorSetup.exe	This executable contains the required Windows Installer engines and default verbose logging for typical deployments.
CiscoIPCommunicatorSetup.msi	This Microsoft Windows Installer package (MSI package) provides deployment customization through command-line options. Logging is not automatically set when you use the MSI package.

Note If users in your system have more than one network interface on their PCs or use laptops with docking stations, see About Selecting a Device Name, page 4-7.

Related Topics

- Deployment Methods, page 3-3
- Command-Line Options for the MSI Package, page 3-4

Deployment Methods

By using either the executable or MSI package, you have the options listed in Table 3-2 for performing the installation.

Note If users in your company do *not* have administrator rights on their computers, use a software deployment tool for initial deployment. Alternately, you can manually install Cisco IP Communicator on each client PC.

Table 3-2 Deployment Methods

Method	Description
Shared location	Place the installer (executable or MSI) on a shared location, such as a web server, where you or a user can run it. To use this method, users must have administrative privileges on their PCs. Alternately, you can use a command line with the MSI package to create a server image of Cisco IP Communicator at a specified network location.

Table 3-2 Deployment Methods (continued)

Method	Description
Software deployment tool	Perform the installation for an entire enterprise by using a software distribution technology. This method can temporarily elevate user privileges on the client PC for installation purposes. You can use a software deployment tool to distribute Cisco IP Communicator to client PCs. You must use this deployment method if users do not have administrative privileges on their computers (and if you want to avoid manually installing the application on each client PC). Software deployment tools include group policy-based tools such as Active Directory, or more advanced tools, such as the SMS[1] software. By using a software deployment tool that can pass a command line to a system, you can take advantage of the Windows Installer package and customize values, such as the device name and TFTP server addresses, during deployment. Specifying these values at deployment means that users do not have to configure these settings after installation and greatly simplifies the post-installation process for users. **Note** Cisco IP Communicator does not support the "advertising" or "publishing" deployment in which users install the application by opening an icon that the administrator places on the their desktop.
Installer on the client PC	You can deploy either the executable or the MSI package directly to the client PC and perform the installation by running the installer and following the installation wizard. If necessary, use an administrator account to do this task. If you use the MSI package, you can use a command line on the client PC to customize the installation.
Languages other than English (when localized versions are available)	If you are using the *.exe* file, the installation prompts you to choose the language (if a language other than English is available) for which you want to install Cisco IP Communicator. Alternatively, you can customize the deployment to specify a language locale by using a command line.

[1] SMS = Microsoft System Management Server

Related Topics

- Command-Line Options for the MSI Package, page 3-4
- About Updating the Application, page 3-6

Command-Line Options for the MSI Package

Table 3-3 provides examples of command-line options that are specific to the deployment of Cisco IP Communicator with the MSI package. (Values given for variables are examples only.)

For a complete list of command-line options that can be used and examples of their usage, see this URL:

http://msdn2.microsoft.com/en-us/library/aa367988.aspx

These command-line options customize the installation and management of the application. For example, by using command-line options to specify the device name, the TFTP server addresses, and other variables, you reduce the number of configuration tasks that users will otherwise need to perform during and after installation.

Table 3-3 Using Command-Line Options with the MSI Package

If you want to....	Use this command line
For SIP-only deployments, allow devices to auto-register.	`msiexec /i CiscoIPCommunicatorSetup.msi /qb SIP=1`
Install a language locale by associating the locale .mst file to the TRANSFORMS parameter.	For example, to install the French locale: `msiexec /i CiscoIPCommunicatorSetup.msi /qb+ TRANSFORMS="French.mst"`

Specify the device name by using the network interface of the target PC.	`msiexec /i CiscoIPCommunicatorSetup.msi /qb`
	`DEVICENAME=“Network Adapter Device Name”`
	If users have PCs with multiple network interfaces and/or a removable network interface (such as a laptop with a docking station), it is helpful if you specify the network interface.
	If users in your company use multiple computer models with a combination of network interfaces, configure a software distribution tool to detect the target computer model and then execute the corresponding command-line option with the appropriate device name variable specified.

Specify the device name by using a free-form device name.
Note Free-form device names are not supported with Cisco Unified Communications Manager 4.x.
	`msiexec /i CiscoIPCommunicatorSetup.msi /qb`
	`FREEFORMDEVICENAME="freeformdevice"`
	This option allows you to specify a unique device name that is not based on MAC addresses. This option is helpful in companies where PCs are refreshed often. When a PC is refreshed, you can install Cisco IP Communicator on the new PC by using the same device name that was used on the old PC, eliminating further administration. The free-form device name must be less than 15 characters, including alphanumeric characters, dot, dash, and underscores (but no spaces).

Specify one TFTP server address.	`msiexec /i CiscoIPCommunicatorSetup.msi /qb TFTP1=”IP Address 1”`

Specify multiple TFTP server addresses.	`msiexec /i CiscoIPCommunicatorSetup.msi /qb`
	`TFTP1=”IP Address 1” TFTP2=”IP Address 2”`

Combine the device name by using a network interface and TFTP server addresses in one command.	`msiexec /i CiscoIPCommunicatorSetup.msi /qb`
	`DEVICENAME="Network Adapter Device Name" TFTP1=”IP Address 1”`
	`TFTP2=”IP Address 2”`

Combine the device name by using a free-form device name and TFTP server addresses in one command.
Note Free-form device names are not supported with Cisco Unified Communications Manager 4.x.
	`msiexec /i CiscoIPCommunicatorSetup.msi /qb`
	`FREEFORMDEVICENAME="freeformdevice"`
	`TFTP1=”IP Address 1” TFTP2=”IP Address 2”`

Note

- If you want Cisco IP Communicator to display a dialog box that users must manually dismiss before the installer reboots the PC, add a “+” character after “qb” to the commands in Table 3-3.
- The options to specify the device name and TFTP addresses apply to new installations only, not upgrades.

- For the DEVICENAME option, the device name string that you enter must be the exact device name of one of the network adapters that appears in the Network Adapter drop-down list in Cisco IP Communicator (**right-click > Preferences > Network** tab).
- If you use the DEVICENAME option, it hides the free-form device name option from the user in Cisco IP Communicator (**right-click > Preferences > Network** tab).
- If you use the FREEFORMDEVICENAME option, it hides the network adapter selection in Cisco IP Communicator (**right-click > Preferences > Network** tab).
- If you do not use either the DEVICENAME option or the FREEFORMDEVICENAME option, the user can use either the network interface card or a free-form string to generate the device name in Cisco IP Communicator (**right-click > Preferences > Network** tab).

Related Topics

- About Updating the Application, page 3-6
- Specifying a TFTP Server, page 4-6
- About Selecting a Device Name, page 4-7

About Updating the Application

- Software Download Site, page 3-6
- Pushing Updates by Using a Software Deployment Tool, page 3-6

Software Download Site

You can download the latest available software from this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/ip-comm

Pushing Updates by Using a Software Deployment Tool

If users do *not* have administrative privileges on their client PCs or if you do not want to administer updates locally on each client PC, use a software deployment tool to handle updates. A software deployment tool can temporarily elevate privileges for installation purposes. (In this case, you probably used a software deployment tool to initially deploy the application.)

Related Topics

- Deployment Methods, page 3-3
- Command-Line Options for the MSI Package, page 3-4

CHAPTER 4

Configuring Cisco IP Communicator

Revised: 1/19/11

This chapter describes the configuration tasks that you or the user might need to perform after installation and before first use so that Cisco IP Communicator can function properly or so that users can access some features.

Some tasks in this chapter required configuration in Cisco Unified Communications Manager, formerly known as Cisco Unified CallManager.

- Overview of Configuration Tasks, page 4-1
- About Required Configuration Tasks, page 4-4
- About Recommended or Optional Configuration Tasks, page 4-11
- Local Configuration, page 4-13
- Disabling Local Settings Access, page 4-13
- User Help for Configuration Tasks, page 4-14

Overview of Configuration Tasks

Table 4-1 and Table 4-2 provide an overview of the required and recommended (optional) configuration tasks that you or the user might need to perform. The necessity of these tasks depends upon variables such as settings on the client PC and software VPN solution used by the user, among other factors.

Note

- If you expect users to perform configuration tasks, provide them with detailed instructions, including access to the *User Guide for Cisco IP Communicator*. For details, see User Help for Configuration Tasks, page 4-14.
- Some settings (such as configuring a custom audio port range) can be configured both locally (on the client PC) and remotely (in Cisco Unified Communications Manager Administration). Be aware that if a value is modified locally, the modified value becomes the active value, overwriting or preempting a value that is specified remotely. Therefore, once a setting is modified on the client PC, the only way to change it is on the client PC. For details, see Local Configuration, page 4-13.

Table 4-1 ***Required Configuration Tasks***

Task	Required?	Configuration Notes	For details, see...
Select and tune audio devices when prompted at startup	Required at initial startup. Allows the application to recognize installed audio devices.	Use the Audio Tuning Wizard, which automatically launches at initial start up. To manually launch: • Cisco IP Communicator right-click menu. • Choose the program group from the Windows Start menu. For device selection in Cisco IP Communicator: **right-click > Preferences > Audio** tab.	About Selecting and Tuning Audio Devices, page 4-5
Specify a TFTP server address immediately after initial startup	Required if you are not using DHCP with Option 150 enabled in your network or if you want to specify an alternate TFTP address (only if you have not already specified this variable through a command-line option during deployment).	Cisco IP Communicator **right-click > Preferences > Network** tab **> TFTP Servers** section. If users share a PC and do not have elevated privileges, you must perform this task by using an administrator account.	How to Deploy the Application, page 3-2 Specifying a TFTP Server, page 4-6 How to Resolve Startup Problems, page 8-5
Select a device name when prompted after initial startup	Required at first launch if the client PC has multiple network interfaces or if it is a laptop with a docking station (and if you have not already specified this variable through a command-line option during deployment).	Cisco IP Communicator **right-click > Preferences > Network** tab **> Device Name** section. If users share a PC and do not have elevated privileges, you must perform this task by using an administrator account.	How to Deploy the Application, page 3-2 About Selecting a Device Name, page 4-7 How to Resolve Startup Problems, page 8-5

Table 4-1 Required Configuration Tasks (continued)

Task	Required?	Configuration Notes	For details, see...
If you have not done so already, run the Cisco IP Communicator Administration Tool, and enable HTTP access. Specify the URL in Cisco Unified Communications Manager Administration	Required to resolve audio IP address detection problems caused by unsupported VPN clients. Recommended to improve performance for remote users and to install the Directory Wizard.	Obtain the tool from the product software download web site: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661. It is located inside the zipped folder with your build. Enter the getIP.asp URL in Cisco Unified Communications Manager Administration (**Device > Phone,** Phone Configuration window, IP Address Auto detection URL field).	Resolving Audio IP Address Auto-Detection Problems, page 4-10 How to Resolve Startup Problems, page 8-5
Provide users with username and password	Required for these features: • Quick Search Directory • User Options web pages	In Cisco Unified Communications Manager Administration: Releases other than 4.x: **User Management > End User** Release 4.x: **User > Add a New User**	Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18 Appendix A, "Providing Information to Users About Cisco IP Communicator"

Note If multiple users share a PC, the device name and TFTP server settings remain with the PC; all other settings in this environment follow the user.

Table 4-2 Recommended (Optional) Configuration Tasks

Task	Required?	Who configures where?	For details, see...
Modify advanced audio properties	Optional. Recommended for advanced users to improve sound quality.	Cisco IP Communicator **right-click** > **Preferences** > **Audio** tab > **Advanced** button.	Modifications for Remote Use, page 4-12
Specify low-bandwidth setting for remote use	Optional. Remote users with low-bandwidth connections might experience better audio quality by using a low-bandwidth codec.	Cisco IP Communicator **right-click** > **Preferences** > **Audio** tab.	Modifications for Remote Use, page 4-12
Configure a custom audio port range	Optional. You might use this option if you want to open up a single port to pass audio through a firewall or want to apply a QoS[1] policy by using a restricted range of RTP[2] ports.	Cisco IP Communicator **right-click** > **Preferences** > **Audio** tab > **Network** button. Or, from Cisco Unified Communications Manager Administration in the Phone Configuration window, Product Specific Configuration section. Local configuration takes precedence over Cisco Unified Communications Manager configuration.	Selections for Audio Port Range, page 4-11

[1] QoS = quality of service

[2] RTP = Real-Time Transport Protocol

Related Topics

- About Required Configuration Tasks, page 4-4
- About Recommended or Optional Configuration Tasks, page 4-11
- User Help for Configuration Tasks, page 4-14
- Customizing Cisco IP Communicator, page 6-1
- Troubleshooting Cisco IP Communicator, page 8-1

About Required Configuration Tasks

You might need to complete these tasks before Cisco IP Communicator can function properly or before a user can access important features. The necessity of these tasks depends upon variables such as settings on the client PC and the s software VPN solution used by the user, among other factors.

Related Topics

- About Selecting and Tuning Audio Devices, page 4-5
- Specifying a TFTP Server, page 4-6
- About Selecting a Device Name, page 4-7
- About Audio IP Address Auto-Detection Problems, page 4-9

About Selecting and Tuning Audio Devices

At first launch after installation, users must select and tune audio devices before using those devices with Cisco IP Communicator. At initial start up, the Audio Tuning Wizard automatically launches, and users must complete the wizard before Cisco IP Communicator launches.

Users are not prompted to use the Audio Tuning Wizard again unless the audio device that they try to select by other means cannot be found (because it has not yet been tuned), or in cases where users directly modify the volume on an audio device. Users can manually launch the Wizard from the Cisco IP Communicator right-click menu or from the Windows Start menu.

For details about installing devices while Cisco IP Communicator is running, see the information about removing and re-installing audio devices in the user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

Related Topics

- Device Selection for Use with Audio Modes and the Ringer, page 4-5
- Device Tuning, page 4-5
- Common Tuning Mistakes, page 4-6

Device Selection for Use with Audio Modes and the Ringer

Before users can use an audio device that requires a device driver, they must select at least one audio mode (headset, speakerphone, or handset) for the device. Users should also make sure that the device that they want to use to alert them to incoming calls is selected as the ringer. For details about audio mode selections, see the user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

Related Topics

- Device Tuning, page 4-5
- Common Tuning Mistakes, page 4-6

Device Tuning

After selecting a device for each audio mode and the ringer, users must tune the device before using it. Tuning a device means testing and, if necessary, adjusting the input/output levels of the device from the Audio Tuning Wizard.

The Audio Tuning Wizard runs at the first launch of Cisco IP Communicator after installation, pops up if the user tries to select an untuned device from the Preferences menu, and can be launched anytime from the Cisco IP Communicator right-click menu. If users have changed the volume levels for an audio device since last tuning it, Cisco IP Communicator prompts them to retune, revert to previous settings, or cancel.

Note Changing the volume level on a USB device directly (such as moving the volume slider on a USB headset) alters the volume level as perceived by the Audio Tuning Wizard. However, changing the volume level on the Cisco IP Communicator interface does not.

Ideally, users should use the Audio Tuning Wizard to establish acceptable volume levels for both listening and speaking for each audio device, and then rely on the volume controls on Cisco IP Communicator to adjust volume levels for listening on a per-call basis thereafter. This strategy allows users to maintain acceptable volume settings in the Audio Tuning Wizard without requiring constant adjustments. In this case, users can choose the revert option when prompted instead of relaunching the Audio Tuning Wizard.

Related Topics

- Device Selection for Use with Audio Modes and the Ringer, page 4-5
- Common Tuning Mistakes, page 4-6

Common Tuning Mistakes

Users often initially set the volume levels high from the master or wave sliders in the Audio Tuning Wizard and later reduce the levels by using Microsoft Windows volume controls or laptop sound keys because other applications sound too loud. When users subsequently discover that Cisco IP Communicator sounds too soft, users set the volume button on the main Cisco IP Communicator interface to sharply increase the call volume.

Note A high volume setting in the application can cause voices to sound distorted.

For details about adjusting the volume through the Audio Tuning Wizard, see the voice quality section in the troubleshooting chapter of the *User Guide for Cisco IP Communicator* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

Related Topics

- Device Selection for Use with Audio Modes and the Ringer, page 4-5
- Device Tuning, page 4-5

Specifying a TFTP Server

You must specify a TFTP server for each Cisco IP Communicator device if either of the these conditions apply:

- You are not using DHCP Option 150 in your network
- You want to specify an alternate TFTP server

Note If you specify a device name by using the command line-option when you deploy the application, you do not need to specify the TFTP server address after installation.

Unless local access is disabled, users can also specify this setting in Cisco IP Communicator (**right-click > Preferences > Network** tab **> TFTP Servers** section), but you must tell them which TFTP server addresses to enter.

If your company uses Cisco IP Communicator in an environment where users do not have administrative privileges, and if multiple users share a PC, this task cannot be completed by the user. You must use an administrator account to run Cisco IP Communicator one time after installation on each machine and select the network interface (if this selection is required). This instruction also applies to selecting network interface (device name) in this circumstance.

Related Topics

- How to Deploy the Application, page 3-2
- About Selecting a Device Name, page 4-7
- Local Configuration, page 4-13

About Selecting a Device Name

Cisco IP Communicator formulates its device name in these ways:

- By using the MAC address of the network interface that it associates with during the installation process. You can specify the network interface by using a command-line option while deploying the Cisco IP Communicator application. In this case, users do not need to choose a network interface.
- By using a free-form device name. You can specify a free-form device name by using a command-line option while deploying the Cisco IP Communicator application but only if you are integrating with a Cisco Unified Communications Manager version later than 5.0(1). In this case, the user does not need to enter the free-form device name.

If you do not use a command-line option to specify a device name, Cisco IP Communicator makes the association automatically during the installation or prompts the user to make a selection:

- If there is only one enabled network interface available on the client PC, Cisco IP Communicator automatically associates with that interface.
- If multiple network interfaces are available, Cisco IP Communicator prompts the user to choose one (first launch only).
- Alternatively, if connecting to a Cisco Unified Communications Manager version other than 4.x, the user can enter a free-form device name. The device name must be less than 15 characters, including alphanumeric characters, dot, dash, and underscores (but no spaces).

If you are using the network interface to create the device name, choosing the correct interface is critical because Cisco IP Communicator uses the MAC address of the associated network interface to identify its device name to Cisco Unified Communications Manager much like hardware-based Cisco Unified IP Phones. Therefore, every time Cisco IP Communicator starts, it verifies that the associated interface is still installed in the client PC. This prevents users from modifying the original device name for Cisco IP Communicator.

Related Topics

- How to Deploy the Application, page 3-2
- Device Name and Multiple Network Interfaces, page 4-8
- Device Name and Shared PCs, page 4-8
- Device Name After Disabling or Removing an Interface, page 4-8

Device Name and Multiple Network Interfaces

Tell users exactly which network interface to choose when multiple network interfaces exist (for example, a laptop that uses both a wireless (802.11) and wired (Ethernet) network interface, or a laptop with a docking station).

Choose the interface that is most likely to provide permanent connectivity or the one that is always enabled (even if it is inactive). In most cases, this means choosing an integrated Ethernet card over a wireless card, docking station, or PC card. Avoid choosing wireless cards because they can appear disabled if they are not associated with a base station.)

Note At first launch, Cisco IP Communicator automatically chooses an Ethernet interface, if one is present. Because some laptop docking stations contain additional Ethernet interfaces, advise laptop users to undock before launching the application for the first time. Doing so helps Cisco IP Communicator choose the appropriate network.

Related Topics

- Device Name and Shared PCs, page 4-8
- Device Name After Disabling or Removing an Interface, page 4-8

Device Name and Shared PCs

If your company uses Cisco IP Communicator in an environment where users do not have administrative privileges, and if multiple users share a PC, a user cannot select the device name. Instead, you must use an administrator account to run Cisco IP Communicator one time after installation on each client PC and select the device name (if this selection is required). This instruction also applies to specifying a TFTP server address in this circumstance, if one is required.

Related Topics

- Specifying a TFTP Server, page 4-6
- Device Name and Multiple Network Interfaces, page 4-8
- Device Name After Disabling or Removing an Interface, page 4-8

Device Name After Disabling or Removing an Interface

If you use a network interface to create the device name, and if the associated network interface is later disabled or removed, Cisco IP Communicator prompts the user to either re-install the interface or choose a new interface. If you or the user choose a new interface, you must create a new device record in Cisco Unified Communications Manager to preserve the original DN for the user, softkey template, settings, and so on. Delete the old device record.

Tell users to coordinate with you before choosing a new interface.

Related Topics

- Device Name and Multiple Network Interfaces, page 4-8
- Device Name and Shared PCs, page 4-8

About Audio IP Address Auto-Detection Problems

If the PC on which Cisco IP Communicator is running uses an unsupported software VPN client, audio IP address auto-detection may not work. The resulting symptom is one-way audio.

- Supported Software VPN Clients, page 4-9
- How Cisco IP Communicator Obtains an Audio IP Address with a VPN, page 4-9
- Resolving Audio IP Address Auto-Detection Problems, page 4-10

Supported Software VPN Clients

Supported software VPN clients include Cisco Systems VPN Client 5.x, and the Microsoft PPTP client. Other third-party VPN clients may not be supported. A VPN solution is typically unsupported if it is not a Cisco product or does not function like a network interface card. Refer to the release notes for the most current information about support.

Please note that Cisco IP Communicator requires the VPN client to assign an IP Address when connecting using VPN software.

Related Topics

- How Cisco IP Communicator Obtains an Audio IP Address with a VPN, page 4-9
- Resolving Audio IP Address Auto-Detection Problems, page 4-10

How Cisco IP Communicator Obtains an Audio IP Address with a VPN

Software VPN clients are overlaid on top of an existing IP network, meaning that there are essentially two IP addresses on the computer when a VPN is in use:

- The IP address from the underlying network
- The IP address provided by the VPN client that is used by parties on the remote side of the connection to communicate with applications on the computer

Some VPN client assign the VPN IP address at a very low level, which makes it difficult for Cisco IP Communicator to specify the correct address. To eliminate this problem, Cisco IP Communicator queries the Cisco VPN client directly.

Other VPN Clients (for example, Microsoft PPTP Client) appear as alternative network interfaces. In these cases, the IP address can be selected with the same auto-detection process that is used to resolve selection when there are multiple interfaces.

Other third-party VPN clients may not be supported and result in one-way audio. You can resolve this problem by running the Cisco IP Communicator Administration Tool to create a **getIP.asp** audio IP address reflector web page. Cisco IP Communicator attempts to fetch this reflector page rather than using other methods of auto-detection. The reflector page returns the IP address from which it sees the request originate, which is a relatively reliable way to identify VPN IP address of Cisco IP Communicator.

Related Topics

- Resolving Audio IP Address Auto-Detection Problems, page 4-10
- Supported Software VPN Clients, page 4-9
- Modifications for Remote Use, page 4-12

Resolving Audio IP Address Auto-Detection Problems

Before You Begin

Obtain the Administration Tool from the same software download web site as Cisco IP Communicator:

http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661.

It is located inside the zipped folder with your build.

Restriction

This procedure applies to Windows-based Cisco Unified Communications Managers only.

Procedure

Step 1 Run the Cisco IP Communicator Administration Tool, and select **Enable HTTP Access**. This creates a getIP.asp reflector web page.

Step 2 In Cisco Unified Communications Manager Administration, specify the location of the getIP.asp web page on the Phone Configuration window (Product Specific Configuration section, IP Address Auto detection URL field).

By default, getIP.asp is stored at this URL:

http://<server>/communicatorloads/communicator/getIP.asp

To change the location of the getIP.asp reflector web page, copy the getIP.asp from the default location, place it in a new location, and enter the new URL in the Cisco Unified Communications Manager Administration (see Step 2). Make sure you place getIP.asp on a Microsoft IIIS Web server so that auto-detection works properly.

Tip You can access the audio IP address settings from Cisco IP Communicator (**right-click > Preferences > Audio** tab **> Network** button **> Audio IP Address** section.

Related Topics

- Supported Software VPN Clients, page 4-9
- How Cisco IP Communicator Obtains an Audio IP Address with a VPN, page 4-9
- Modifications for Remote Use, page 4-12

About Recommended or Optional Configuration Tasks

You might need to complete these recommended configuration tasks because of certain network conditions (to improve audio quality, specify custom port range for RTP audio, or to modify settings for remote users on VPNs).

- Modification of Advanced Audio Settings, page 4-11
- Selections for Audio Port Range, page 4-11
- Modifications for Remote Use, page 4-12

Modification of Advanced Audio Settings

Modifying advanced audio properties are optional. Users might want to increase noise suppression levels to reduce or eliminate background noise. You access the advanced audio settings from Cisco IP Communicator (**right-click > Preferences > Audio** tab **> Advanced** button).

For details about the fields in this window and for troubleshooting voice quality issues, see the user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

Related Topics

- Selections for Audio Port Range, page 4-11
- Modifications for Remote Use, page 4-12

Selections for Audio Port Range

You might need to select an audio port range for Cisco IP Communicator to use if the network uses a custom port range for RTP audio. For example, if a single port is opened to allow audio to pass through a firewall or if a QoS policy has been applied to only those routers and switches with a restricted range of RTP ports.

You can do this from the Phone Configuration window (Product Specific Configuration section) in Cisco Unified Communications Manager Administration. Alternately, users can do this from Cisco IP Communicator (**right-click > Preferences > Audio** tab **> Network** button **> Audio Port Range** section).

Note The Audio Port Range controls in Cisco IP Communicator are not functional when the device is configured as SIP in Cisco Unified Communications Manager. Instead, the port setting is in the SIP device profile.

Note Unless local settings access is disabled, you can configure the audio port range locally (on the client PC) and remotely (in Cisco Unified Communications Manager Administration). Be aware that if the value is modified locally, the modified value becomes the active value, overwriting or preempting a value that is specified remotely. Therefore, once a setting is modified on the client PC, the only way to change it is on the client PC.

Related Topics

- QoS Modifications to Prioritize Voice Traffic, page 1-8
- Modifications for Remote Use, page 4-12
- Local Configuration, page 4-13

Modifications for Remote Use

Depending on the VPN client that is used to connect to the network, users who run Cisco IP Communicator remotely, or outside of the LAN, might need to modify certain settings in Cisco IP Communicator. Table 4-3 describes these settings.

Table 4-3 Modifications for Remote Use

Configuration Task	Purpose	Where to Do It
Optimize for low bandwidth.	Remote users with low-bandwidth connections might experience better audio quality by using a low-bandwidth codec. For details about supported audio formats, see the release notes at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html	Cisco IP Communicator **right-click > Preferences > Audio** tab **> Optimize for Low Bandwidth**.
Specify the TFTP address at first startup.	Remote users are probably not going to receive their TFTP address from DHCP. However, Cisco IP Communicator caches the last TFTP address that it received and tries to use it the next time it starts up. First-time remote users with a freshly installed application cannot use Cisco IP Communicator until they have specified a TFTP address.	Cisco IP Communicator **right-click > Preferences > Network** tab **> Use these TFTP Servers**. See Specifying a TFTP Server, page 4-6.
Run the Cisco IP Communicator Administration Tool.	Enabling HTTP access improves the performance for remote users. Obtain the tool from the product software download web site: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661. It is located inside the zipped folder with your build. It resolves audio IP address auto-detection problems caused by unsupported software VPN clients. You must enter the URL for getIP.asp (an IP address reflector page) in Cisco Unified Communications Manager Administration.	Cisco IP Communicator **right-click > Preferences > Audio** tab**> Network > Audio IP Address** section. See Resolving Audio IP Address Auto-Detection Problems, page 4-10.

Related Topics

- User Help for Configuration Tasks, page 4-14
- Troubleshooting Cisco IP Communicator, page 8-1

Local Configuration

Many required and recommended configuration tasks can be performed locally on the client PC by you or the user. However, the tasks that require access to Cisco Unified Communications Manager Administration must be performed by you.

Some settings (such as configuring a custom audio port range) can be configured both locally (on the client PC) and remotely (in Cisco Unified Communications Manager Administration). Be aware that if a value is modified locally, the modified value becomes the active value, overwriting or preempting a value that is specified remotely. Therefore, once a setting is modified on the client PC, the only way to change it is on the client PC.

To prevent this scenario, you can disable access to some network settings so that they appear grayed-out on the client PC.

Related Topics

- Disabling Local Settings Access, page 4-13

Disabling Local Settings Access

To prevent users from modifying settings that you have already specified and which are normally accessible from the client PC (such as the Alternate TFTP Server setting), you must disable settings access when you provision the Cisco IP Communicator device record prior to deployment. Otherwise, if a user modifies these settings, you are locked out of performing any changes remotely and must override local settings from the client desktop.

Note Keep in mind that local configuration (on the client PC) always takes precedence over remote configuration (from Cisco Unified Communications Manager Administration) for those settings that are accessible from both locations.

You disable settings access on the Phone Configuration window (Product Specific Configuration section, Settings Access field) in Cisco Unified Communications Manager Administration.

The affected settings appear grayed-out in Cisco IP Communicator:

- All settings accessed from the Settings button
- Settings in Cisco IP Communicator:
  - **right-click > Preferences > Network** tab: all settings in the TFTP Servers section and the Use This Device Name field
  - **right-click > Preferences > Audio** tab **> Network** button: all settings in the Audio Port Range section

Related Topics

- Specifying a TFTP Server, page 4-6
- Selections for Audio Port Range, page 4-11
- User Help for Configuration Tasks, page 4-14

User Help for Configuration Tasks

With a few exceptions, most of the configuration tasks that are recommended or required for Cisco IP Communicator to function properly must be performed on the client PC and are likely to be performed by users.

As the administrator, you should be prepared to perform configuration tasks at the client PC on behalf of users, or you should provide users with the specific information necessary to complete these tasks. The *User Guide for Cisco IP Communicator* provides general information to help users perform the configuration, but users are likely to need more specific direction from you—most tasks are recommended on the basis of certain technical conditions that users might not know how to recognize or interpret.

Related Topics

- Overview of Configuration Tasks, page 4-1
- Providing Information to Users About Cisco IP Communicator, page A-1

CHAPTER 5

Configuring Features and Services for Cisco IP Communicator

Revised: 1/19/11

After you add Cisco IP Communicator to Cisco Unified Communications Manager (formerly known as Cisco Unified CallManager), you can add users, configure telephony features, modify phone templates, and set up services for Cisco IP Communicator. You can also configure product-specific settings for Cisco IP Communicator.

Tip In general, it is preferable to configure the settings in Cisco Unified Communications Manager Administration before deploying Cisco IP Communicator to ensure that features are set up properly for the user at first launch and remain consistent thereafter.

Adding Users to Cisco Unified Communications Manager

When you add users through Cisco Unified Communications Manager Administration, you can display and maintain information about them. After they are added, users can perform these actions:

- Set up speed dial and call forwarding numbers
- Subscribe to services that are accessible from Cisco IP Communicator
- Access the corporate directory and other customized directories from Cisco IP Communicator
- Create a personal directory (Personal Address Book service)

You can add users to Cisco Unified Communications Manager by using either of these methods:

- To add users individually:
  - In releases other than 4.x: choose **User Management > End User**.

- In Release 4.x: choose **User > Add a New User**.

For details about adding users, see the *Cisco Unified Communications Manager Administration Guide*. For details about user information, see the *Cisco Unified Communications Manager System Guide*.

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- To add users in batches, use the Bulk Administration Tool (BAT). This method also enables you to set an identical default password for all users.

  For details, see the *Bulk Administration Tool User Guide* at this URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_user_guide_list.html

Related Topics

- Telephony Features Available for Cisco IP Communicator, page 5-2
- Phone Button Template Modification, page 5-12
- Softkey Template Configuration, page 5-12
- Setting Up Services, page 5-13
- About Configuring Corporate and Personal Directories, page 5-13

Telephony Features Available for Cisco IP Communicator

After you add Cisco IP Communicator devices to Cisco Unified Communications Manager, you can add functionality to those devices. Table 5-1 lists the supported telephony features, many of which you can configure through Cisco Unified Communications Manager Administration.

Note Cisco Unified Communications Manager documentation is available from the application Help menu and from this URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Client matter codes (CMC) (SCCP phones only)	Enables a user to specify that a call relates to a specific client matter.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Client Matter Codes" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Client Matter Codes and Forced Authorization Codes" chapter.
Direct transfer (SCCP phones only)	Allows users to connect two calls to each other (without remaining on the line).	For more information, refer to *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Forced authorization codes (FAC) (SCCP phones only)	Controls the types of calls that certain users can place.	For more information, refer to: • *Cisco Unified Communications Manager System Guide*, "Forced Authorization Codes (FAC)" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Client Matter Codes and Forced Authorization Codes" chapter.
Join (SCCP phones only)	Allows users to join two or more calls that are on one line to create a conference call and remain on the call.	For more information, refer to *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter.
Malicious call identification (MCID) (SCCP phones only)	Allows users to notify the system administrator about suspicious calls that are received.	For more information refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Malicious Call Identification" chapter.
Multilevel Precedence and Preemption (MLPP) (SCCP phones only)	Provides a method of prioritizing calls within your phone system. Use this feature when users work in an environment where they need to make and receive urgent or critical calls.	For more information refer to *Cisco Unified Communications Manager Features and Services Guide,* "Multilevel Precedence and Preemption" chapter.
Anonymous Call Block (SIP phones only)	Allows a user to reject calls from anonymous callers.	*Cisco Unified Communications Manager Administration Guide,* "SIP Profile Configuration" chapter.
Abbreviated dialing	Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad. Users assign index codes from the User Options web pages.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter.
Audible Message Waiting Indicator	A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line. **Note** The stutter tone is line-specific. You hear it only when using the line with the waiting messages.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Message Waiting Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset.	For more information, refer to *Cisco Unified Communications Manager Administration Guide, "*Configuring Directory Numbers" chapter.
Auto-pickup	Allows a user to use one-touch, pickup functionality for call pickup, group call pickup, and other group call pickup.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*, "Pickup Group Configuration" chapter. • *Cisco Unified Communications Manager System Guide, "*Call Pickup and Group Call Pickup" chapter.
Barge	Allows a user to join a non-private call on a shared phone line. Barge features include cBarge and Barge. **Note** Users (who share the line) can only see the Barge, cBarge softkeys if the Privacy option is set to "OFF" on both devices in Cisco Unified Communications Manager. • cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. • Barge adds a user to a call but does not convert the call into a conference. The phones support Barge in two conference modes: • Built-in conference bridge at the target device (the phone that is being barged). This mode uses the **Barge** softkey. • Shared conference bridge. This mode uses the **cBarge** softkey.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, "*Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide, "*Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide, "*Barge and Privacy" chapter.
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, refer to *Cisco Unified Communications Manager Features and Services Guide*, "External Call Transfer Restrictions" chapter.
Busy Lamp Field (BLF) speed dial	Allows a user to monitor the call state of a directory number (DN) associated with a speed-dial button.	For more information, refer to *Cisco Unified Communications Manager Features and Services Guide*, "Presence" chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Call display restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide, "*Understanding Route Plans" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Call Display Restrictions" chapter.
Call forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, "*Directory Number Configuration" chapter. • *Cisco Unified Communications Manager System Guide, "*Cisco Unified IP Phones" chapter.
Call forward configurable display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Call forward destination override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.	For more information, refer to *"Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter.
Call park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, "*Call Park*"* chapter. • *Cisco Unified Communications Manager System Guide, "*Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Call Park" chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Call pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and/or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, “Call Pickup Group” chapter.
Call recording	Allows a supervisor to record an active call. The user might hear an intermittent tone (beep tone) during a call when it is being recorded.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide,* “Monitoring and Recording” chapter.
Call waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	For more information, refer to the *Cisco Unified Communications System Guide*, “Understanding Directory Numbers” chapter.
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* “Cisco Unified IP Phones” chapter.” • *Cisco Unified Communications Manager System Guide,* “Understanding Route Plans” chapter. • *Cisco Unified Communications Manager Features and Services Guide*, “Call Display Restrictions” chapter.
Caller ID Blocking	Allows users to block their phone numbers or e-mail addresses from displaying on phones that have caller identification enabled.	For more information, refer to: • *Cisco Unified Communications Manager System Guide*, “Understanding Route Plans” chapter. • *Cisco Unified Communications Manager Administration Guide*, “Directory Number Configuration” chapter. • *Cisco Unified Communications Manager Administration Guide*, “SIP Profile Configuration” chapter.
Cisco Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* “Cisco Unified IP Phones” chapter. • *Cisco Unified Communications Manager Features and Services Guide*, “Cisco Call Back” chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Cisco Unified Communications Manager Assistant	Enables managers and their assistants to work together more effectively by providing a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified CM Assistant Configuration Wizard" chapter. • *Cisco Unified Communications Manager System Guide, "*Cisco Unified Communications Manager Assistant" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Communications Manager Assistant With Proxy Line Support" and "Cisco Unified Communications Manager Assistant With Shared Line Support" chapters.
Conference	• Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me. • Allows a non-initiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line.	• For more information, refer to *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter. • The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features. **Note** Be sure to inform your users whether these features are activated.
Configurable call forward display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, "*Directory Number Configuration" chapter. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number. **Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.	For more information refer to *Cisco Unified Communications Manager Features and Services Guide,* "Call Park and Directed Call Park" chapter.
Do Not Disturb (DND)	When DND is turned on, no audible rings occur during the ringing-in state of a call. You can configure the phone to have a softkey template with a DND softkey or a phone-button template with DND as one of the selected features. The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration: • Do Not Disturb—Choose **Device > Phone > Phone Configuration**. • DND Incoming Call Alert—Choose the type of alert to play on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration takes precedence). • Include DND In BLF Status—Enables DND status to override busy/idle state.	*Cisco Unified Communications Manager Features and Services Guide*, "Do Not Disturb" chapter.
Extension Mobility Service	Allows a user to temporarily apply a phone number and user profile settings to a shared Cisco Unified IP Phone by logging into the Extension Mobility service on that phone. Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.	For more information, refer to: • *Cisco Unified Communications Manager Features and Services Guide,* "Cisco Unified Communications Manager Extension Mobility" chapter. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified Communications Manager Extension Mobility and Phone Login Features" chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* “Cisco Unified IP Phone Services Configuration” chapter. • *Cisco Unified Communications Manager System Guide,* “Cisco Unified IP Phone Services” chapter.
Group call pickup	Allows a user to answer a call ringing on a phone in another group by using a group pickup code.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, “*Pickup Group Configuration” chapter. • *Cisco Unified Communications Manager System Guide, “*Call Pickup” chapter.
Hold	Allows the user to move a connected call from an active state to a held state.	• Requires no configuration, unless you want to use music on hold. See “Music on Hold” in this table for information. • See also: “Hold Reversion” in this table.
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble and a brief message on the status line. You can configure call focus priority to favor incoming or reverting calls.	For more information about configuring this feature, refer to *Cisco Unified Communications Manager Features and Services Guide, “*Hold Reversion” chapter.
Hunt Group	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, “*Hunt Group Configuration” chapter. • *Cisco Unified Communications Manager System Guide, “*Understanding Route Plans” chapter.
Immediate Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system.When a call is diverted, the line becomes available to make or receive new calls.	For more information, refer to: • *Cisco Unified Communications Manager System Guide, “*Cisco Unified IP Phones” chapter. • *Cisco Unified Communications Manager Features and Services Guide*, “Immediate Divert” chapter

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Immediate Divert—Enhanced	Allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line.	• *Cisco Unified Communications Feature and Services Guide*, Release 6.1, "Intercom chapter" • *Cisco Unified Communications Feature and Services Guide*, Release 6.1, "Cisco Extension Mobility" chapter"
Join Across Lines (SCCP phones only)	Allows users to apply the Join feature to calls that are on multiple phone lines.	For more information: • See Softkey Template Configuration, page 5-12. • Refer to *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Log out of hunt groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phone.	For more information • See Softkey Template Configuration, page 5-12. • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter.
Meet-Me conference	Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.	For more information refer to *Cisco Unified Communications Manager Administration Guide*, "Meet-Me Number/Pattern Configuration" chapter.

Table 5-1 Configuring Telephony Features Through Cisco Unified Communications Manager Administration

Feature	Description	Configuration Reference
Message waiting indicator	A light on the handset that indicates that a user has one or more new voice messages.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Message Waiting Configuration" chapter. • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and a remote device such as a cellular phone.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Mobile Connect and Mobile Voice Access" chapter.
Recording Tone	Indicates whether a recording tone (often referred to as a beep tone) is enabled or disabled for the phone. If the recording tone option is enabled, the phone plays the beep tone in both directions of every call, regardless of whether the call actually gets recorded. The beep tone first sounds when a call is answered. You should notify your users if you enable this option. Default: Disabled This option is globally enabled using the Service Parameter Configuration page in Cisco Unified Communications Manager.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide,* Monitoring and Recording" chapter.
Silent Monitoring	Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear an intermittent tone (beep tone) during a call when it is being monitored. **Note** The intercom feature is disabled when a call is being monitored or recorded.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide,* "Monitoring and Recording" chapter.

Related Topics

- Phone Button Template Modification, page 5-12
- Softkey Template Configuration, page 5-12
- Setting Up Services, page 5-13
- About Configuring Corporate and Personal Directories, page 5-13

Phone Button Template Modification

Phone button templates enable you to assign features to line and speed dial buttons. You should modify templates before registering devices on the network. In this way, you can access customized template options from Cisco Unified Communications Manager during registration.

You modify a template from **Device > Device Settings > Phone Button Template**. You assign a template to a device on the Phone Configuration window (Phone Button Template field). For details, see the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

The default Cisco IP Communicator template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 for speed dial numbers. You access other telephony features (such as call park, call forward, redial, hold, resume, voice messaging system, conferencing, and so on) by using Cisco IP Communicator softkeys.

Related Topics

- Telephony Features Available for Cisco IP Communicator, page 5-2
- Softkey Template Configuration, page 5-12
- Setting Up Services, page 5-13

Softkey Template Configuration

By using Cisco Unified Communications Manager, you can manage softkeys associated with applications that are supported by Cisco IP Communicator. Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. An application that supports softkeys can have one or more standard softkey templates associated with it. You cannot modify standard softkey templates; you can modify only nonstandard templates.

You configure softkey templates from **Device > Device Settings > Softkey Template**. You assign a softkey template to a device on the Phone Configuration window (Softkey Template field). For details, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Related Topics

- Telephony Features Available for Cisco IP Communicator, page 5-2
- Phone Button Template Modification, page 5-12
- Setting Up Services, page 5-13

Setting Up Services

Users can click the **Services** button on Cisco IP Communicator to access XML applications that enable the display of interactive content with text and graphics on the Cisco IP Communicator phone screen. Examples of services include local movie times, stock quotes, and weather reports. Before a user can access these services, you must perform this procedure.

Procedure

Step 1 Gather the URLs for the sites you want to set up, and verify that users can access those sites from your corporate IP telephony network.

Step 2 Configure available services:

- In releases other than 4.x: **Device > Device Settings > Phone Services**
- In release 4.x: **Features > Cisco Unified IP Phone Services**

For details, see *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Step 3 Verify that your users have access to the User Options web pages from which they can select and subscribe to configured services. For details that you must provide to users, see Appendix A, "Providing Information to Users About Cisco IP Communicator."

Step 4 Tell users to access the User Options web page through Cisco IP Communicator (**right-click > Cisco User Options**) and to subscribe to services.

Related Topics

- Telephony Features Available for Cisco IP Communicator, page 5-2
- Phone Button Template Modification, page 5-12
- Softkey Template Configuration, page 5-12

About Configuring Corporate and Personal Directories

Through Cisco IP Communicator, users can search corporate and personal directories if you integrate Cisco Unified Communications Manager with a directory server and configure the Quick Search feature.

- Directory Search Features, page 5-13
- Cisco Unified Communications Manager Integration with a Directory Server, page 5-14
- How to Configure Quick Search, page 5-15

Directory Search Features

Table 5-2 lists the directory search features that are supported by Cisco IP Communicator.

Table 5-2 Directory Search Features Supported by Cisco IP Communicator

Search Feature	To Invoke...	Configuration Tasks
Corporate directory searches through the Directories button	Click the Cisco IP Communicator **Directories** button, or enter a shortcut (Ctrl + D), and then choose the directory from the phone screen menu.	If necessary, integrate *Cisco Unified Communications Manager* with a directory server; no additional configuration is required.
Corporate and personal directory searches through the Quick Search feature	Cisco IP Communicator (**right-click > Quick Search**), or enter a shortcut (Alt + K). This feature is specific to Cisco IP Communicator.	Use the Cisco IP Communicator Directory Wizard to configure the Quick Search feature (and the Dialing Rules feature). Users can create personal directories by subscribing to the Personal Address Book service from the User Options web page.
Personal directory searches through the Services button	Click the Cisco IP Communicator **Services** button, or enter a shortcut (Ctrl + R)[1], and then choose the Personal Address Book service from the phone screen menu.	Users create personal directories by subscribing to the Personal Address Book service from the User Options web page.

[1] In all releases prior to Release 2.0, this keyboard shortcut is Ctrl + V

Related Topics

- Cisco Unified Communications Manager Integration with a Directory Server, page 5-14
- How to Configure Quick Search, page 5-15
- Configuring Quick Search to Access a Personal Address Book with Windows-Based Cisco Unified Communications Managers, page 5-20
- Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18
- Applying Dialing Rules to Quick Search Dialing, page 5-19

Cisco Unified Communications Manager Integration with a Directory Server

To allow searches against corporate and personal directories through the Cisco IP Communicator Directories button, integrate Cisco Unified Communications Manager with a directory server (if necessary). You might have already completed this task to support other phone devices in your network.

For details, see the *Installing the Cisco Unified Communications Manager Customer Directory Configuration Plugin* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

This document guides you through the process of integrating Cisco Unified Communications Manager with Microsoft Active Directory and Netscape Directory Server.

Related Topics

- Directory Search Features, page 5-13
- How to Configure Quick Search, page 5-15

How to Configure Quick Search

Quick Search allows users to search one or more directories (corporate and personal address books) with a single search command.

Note Cisco IP Communicator cannot read the user information if anonymous bind is disabled in the Active Directory. Anonymous bind is disabled by default. For Cisco IP Communicator to download the user information for quick search you must enable the anonymous bind in Active Directory

You can set up Quick Search to function in these ways:

- To apply to all devices in a Cisco Unified Communications Manager cluster or to access directories that exist on Cisco Unified Communications Manager

  Use the Cisco IP Communicator Directory Wizard to configure Quick Search. The Directory Wizard creates an XML configuration file (LdapDirectories.xml) that tells Cisco IP Communicator which Lightweight Directory Access Protocol (LDAP) directories to search.

- To apply to a specific Cisco IP Communicator device or to access directories that are external to Cisco Unified Communications Manager

  Manually create a custom Quick Search configuration file that tells Cisco IP Communicator which LDAP directories to search.

Cisco IP Communicator downloads the LdapDirectories.xml file at startup and saves the list of specified LDAP directories. When a user invokes the Quick Search feature, Cisco IP Communicator searches the specified LDAP directories, stopping at the first directory where one or more matches are found. Therefore, if you specify two directories, and the search string is matched in the first directory, the second directory is not searched regardless of whether or not it contains matching entries.

Tip On the Cisco Unified Communications Manager Administration User Configuration window, make sure that the Telephone Number field shows the phone number for the user. The Quick Search feature displays this phone number in search results.

- Configuring Quick Search by Using the Directory Wizard, page 5-15
- Configuring Quick Search Manually with Windows-Based Cisco Unified Communications Managers, page 5-17
- Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18
- Applying Dialing Rules to Quick Search Dialing, page 5-19
- Configuring Quick Search to Access a Personal Address Book with Windows-Based Cisco Unified Communications Managers, page 5-20

Configuring Quick Search by Using the Directory Wizard

Use this procedure only if you are setting up Quick Search to access a personal or a corporate directory for all Cisco IP Communicator devices that exists on the Cisco Unified Communications Manager server. Otherwise, follow the procedure to configure Quick Search manually on a Windows-based Cisco Unified Communications Manager.

Before You Begin

- Obtain the Cisco IP Communicator Administration Tool from this URL:

  http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661.

  It is located inside the zipped folder with your build.

  From the Zip file:

  - For Windows-based Cisco Unified Communications Managers, obtain the Cisco IP Communicator Administration tool, which includes the Directory Wizard.
  - For Linux-based Cisco Unified Communications Managers, obtain the Directory Wizard tool (directorywizard. cop.sgn).
- For Linux-based Cisco Unified Communications Managers, before running the Cisco Options Package (COP) installer, make sure to synchronize the LDAP directories so that the LDAPDirectories.xml and the LdapDialingRules.xml files are created correctly.
- Run the Cisco IP Communicator Administration Tool on the Cisco Unified Communications Manager publisher to install the Directory Wizard. For Windows-based Cisco Unified Communications Managers, the tool installs DirectoryWizard.exe and LdapDirectories.README.txt in this folder: *TFTPPath*\Communicator.

Restrictions

- Quick Search is supported when Cisco IP Communicator is integrated with Windows-based Cisco Unified Communications Manager Release 4.x.

Procedure for Linux-based Cisco Unified Communications Managers

Step 1 Install the COP file on the Linux-based Cisco Unified Communications Manager.

Step 2 In Cisco Unified Communications Manager Administration, navigate to **Cisco Unified OS Administration** and click **Go**.

Step 3 Enter your Administrator username and password.

Step 4 Choose **Software Upgrades > Install/Upgrade** to install the COP file.

Step 5 Follow the instructions from the online help.

Procedure for Windows-based Cisco Unified Communications Managers

Step 1 Launch the Cisco IP Communicator Directory Wizard (directorywizard.exe) from the program group or from the Cisco IP Communicator Administration Tool.

Step 2 Enter information as prompted. (See the Tips section that follows for help.)

Step 3 Restart the TFTP service by navigating to Cisco Unified Communications Manager Serviceability window and choosing **Tools > Control Center**).

Note You must restart the TFTP service after completing the Directory Wizard—both for new configurations and updates.

Based on the information that you entered, the Directory Wizard creates directory and/or Dialing Rules configuration files and stores these files in the appropriate location on the server so that Cisco Unified Communications Manager can access them.

Tips for Configuring Directory Wizard on Windows-based Cisco Unified Communications Manager

- Directory Wizard prompts you to make decisions about user authentication. To help you make these decisions, see Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18.
- You can use Directory Wizard to configure the Dialing Rules feature at the same time that you configure Quick Search, or you can do it at another time as a separate task. See Applying Dialing Rules to Quick Search Dialing, page 5-19.
- The auto-detection feature in the Directory Wizard works only if you have installed and run Directory Wizard on the Cisco Unified Communications Manager publisher.
- Typically, the Cisco Unified Communications Manager publisher is also the TFTP server where phone loads will be installed. If this is not the case, copy the LdapDirectories.xml and the LdapDialingRules.xml files to the TFTP server (after running the Directory Wizard on the Cisco Unified Communications Manager publisher.)
- In the Cisco Unified Communications Manager Administration Phone Configuration window, if you leave the LDAP Server Information File field blank, Cisco IP Communicator users automatically use the configuration generated by the Directory Wizard (assuming configuration files are placed in the correct location).
- Directory Wizard does not use any existing information that you entered but always creates new files. Therefore, make sure to back up your previous configuration if you want to access it again.
- Users must restart Cisco IP Communicator before accessing the Quick Search feature.

Related Topics

- Configuring Quick Search Manually with Windows-Based Cisco Unified Communications Managers, page 5-17
- Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18
- Applying Dialing Rules to Quick Search Dialing, page 5-19

Configuring Quick Search Manually with Windows-Based Cisco Unified Communications Managers

You must manually create the Quick Search configuration file if either of these situations apply:

- You want to apply special Quick Search configuration parameters to specific Cisco IP Communicator devices (not to all devices).
- You want Quick Search to access a personal or corporate directory that is external to the Cisco Unified Communications Manager server.

Before You Begin

- Obtain the Cisco IP Communicator Administration Tool from this URL:

  http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661.

  It is located inside the zipped folder with your build.

- Run the Cisco IP Communicator Administration Tool on the Cisco Unified Communications Manager publisher to install the Directory Wizard. The tool installs DirectoryWizard.exe and LdapDirectories.README.txt in this folder: *TFTPPath*\Communicator.

Restrictions

- Configuring Quick Search manually applies only to Windows-based Cisco Unified Communications Manager Release 4.x.

Procedure

Step 1 Open the LdapDirectories.README.TXT file from the Cisco IP Communicator program group.

Step 2 Follow the instructions in this example file to create a custom LdapDirectories.xml file.

Step 3 Store the file in a location relative to *TFTPpath*.

Step 4 Specify the filename and path in the Phone Configuration window (LDAP Server Information File field) of Cisco Unified Communications Manager Administration.

Step 5 Restart the TFTP service by navigating to the Cisco Unified Communications Manager Serviceability window, and by choosing **Tools > Control Center**.

Related Topics

- Configuring Quick Search by Using the Directory Wizard, page 5-15
- Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18
- Applying Dialing Rules to Quick Search Dialing, page 5-19

Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers

Cisco Unified Communications Manager uses an LDAP directory to store authentication and authorization information. Authentication establishes the right of the user to access the system and identifies the telephony resources that a user is permitted to use, such as a specific telephone extension.

To configure Quick Search, you must decide how user authentication is going to work. (This is true whether you configure Quick Search through the Directory Wizard or through manual methods.)

These are your options:

- Specify a global user ID and password (recommended).

  This approach allows Quick Search to search corporate and personal directories even when the user does not specify any credentials in Cisco IP Communicator.

- Do *not* specify a user ID or password.

  With this approach, you must provide users with their user ID and password and tell them to enter this information in Cisco IP Communicator (**right-click > Preferences > Directories** tab). If user authentication credentials are not specified either in the Quick Search configuration file or the Directories tab, the feature will not function properly.

Implementation Tips

- Do *not* use global credentials if any Cisco Unified Communications Manager user ID does not match the directory user ID. You specify the user ID in Cisco Unified Communications Manager Administration on the User Configuration window. This could be the case if you are using Microsoft Active Directory or Netscape with Cisco Unified Communications Manager.
- Users should enter the credentials for the directory account of the directory that will be searched. If more than one directory will be searched, the credential information must be the same for all of the them.

Related Topics

- Configuring Quick Search by Using the Directory Wizard, page 5-15
- Configuring Quick Search Manually with Windows-Based Cisco Unified Communications Managers, page 5-17
- Applying Dialing Rules to Quick Search Dialing, page 5-19

Applying Dialing Rules to Quick Search Dialing

The Cisco IP Communicator Dialing Rules feature applies pre-established dialing rules stored in Cisco Unified Communications Manager to Quick Search phone numbers. Before you can use the Cisco IP Communicator Dialing Rules feature, make sure that you set up dialing rules in your Cisco Unified Communications Manager cluster. You have these options:

- Set up route patterns to apply to all methods of making a call.

  A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a to gateway. Route patterns provide flexibility in network design. They work with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

  You configure route patterns as follows:

  - Releases other than 4.x: **Call Routing > Route/Hunt > Route Pattern**
  - Release 4.x: **Route Plan > Route/Hunt > Route Pattern**

- Set up application dialing rules to apply to calls made by using an application like Cisco IP Communicator.

  Application dialing rules automatically strip numbers from or add numbers to telephone numbers that the user dials. For example, the dial rules automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

  You configure application dialing rules as follows:

  - Releases other than 4.x: **Call Routing > Dial Rules > Application Dial Rules**
  - Release 4.x: **Route Plan > Application Dial Rules**

If you are using application dialing rules instead of a route pattern, you must set up a configuration file that tells Cisco IP Communicator where to find the dialing rules stored in Cisco Unified Communications Manager. To set up the Dialing Rules file, launch the Cisco IP Communicator Directory Wizard, and follow the relevant steps. The wizard can help you configure the Quick Search feature and Dialing Rules.

Tip Users must restart Cisco IP Communicator before dialing rules apply to Quick Search dialing.

For details about route plan options, see the *Cisco Unified Communications Manager System Guide* and the *Cisco Unified Communications Manager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Related Topics

- Configuring Quick Search by Using the Directory Wizard, page 5-15
- Configuring Quick Search Manually with Windows-Based Cisco Unified Communications Managers, page 5-17
- Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18

Configuring Quick Search to Access a Personal Address Book with Windows-Based Cisco Unified Communications Managers

Personal Directory provides a personal address book that is stored in the Cisco Unified Communications Manager LDAP directory. Personal directory also provides these features:

- Cisco Unified IP Phone Address Book Synchronizer—Allows users to synchronize Microsoft Outlook and Outlook Express address book entries with the directory in Cisco Unified Communications Manager.
- Two Cisco Unified IP Phone services—The Personal Address Book service and the Personal Fast Dial service. From Cisco IP Communicator, a user can search and dial from the Personal Address Book service.

If properly configured, Quick Search searches against the Personal Address Book for the user first and against a corporate directory second. Quick Search stops at the first directory where it finds a match.

Procedure

Step 1 Configure Quick Search to integrate with personal directories.

Step 2 Create the service on the IP Phone Services Configuration window.

For details, see the *Cisco Unified Communications Manager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Step 3 Tell users to subscribe to the Personal Address Book service in Cisco IP Communicator (**right-click > Cisco User Options**).

Step 4 Provide users with the directory username and password to enter in Cisco IP Communicator (**right-click > Preferences > Directories** tab). Users should enter the credentials for the directory account of the directory that will be searched. If more than one directory will be searched, the credential information must be the same for all of the them.

Step 5 For users who want to synchronize with Microsoft Outlook, provide the Cisco Unified IP Phone Address Book Synchronizer utility, and tell them to install it. You obtain the software as follows:

- For releases other than 4.x: **Application > Plugins > Cisco Unified IP Phone Address Book Synchronizer**
- For release 4.x: **Application > Install Plugins > Cisco Unified Communications Manager Address Book Synchronizer**

Step 6 Use the URL to download the software.

Related Topics

- Configuring Quick Search by Using the Directory Wizard, page 5-15
- Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18
- Appendix A, "Providing Information to Users About Cisco IP Communicator"

CHAPTER 6

Customizing Cisco IP Communicator

Revised: 1/19/11

This chapter describes how to customize phone ring sounds, background images, and the idle display at your site through Cisco Unified Communications Manager (formerly known as Cisco Unified CallManager). Ring sounds play when Cisco IP Communicator receives a call. Background images appear on the phone screen. The idle display appears on the phone screen when the application has not been used for a designated period.

- About Custom Phone Rings, page 6-1
- About Custom Background Images, page 6-3
- About Configuring the Idle Display, page 6-6

About Custom Phone Rings

Cisco IP Communicator software provides two default ring types: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with the RingList.xml file that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

You can customize the phone ring types that are available at your site by creating your own PCM files and editing the RingList.xml file.

- RingList.xml File Format Requirements, page 6-1
- PCM File Requirements for Custom Ring Types, page 6-2
- Configuring a Custom Phone Ring, page 6-3

RingList.xml File Format Requirements

The RingList.xml file defines an XML object that contains a list of phone ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that appears in Cisco IP Communicator (**Settings** button **> User Preferences > Rings**).

The CiscoIPPhoneRingList XML object uses this tag set to describe the information:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

You must include the required DisplayName and FileName for each phone ring type. These characteristics apply to the definition names:

- DisplayName defines the name of the custom ring for the associated PCM file that displays in Cisco IP Communicator (**Settings** button **> User Preferences > Rings**).
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Note The DisplayName and FileName fields must not exceed 25 characters.

This example shows a RingList.xml file that defines two phone ring types:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

Related Topics

- PCM File Requirements for Custom Ring Types, page 6-2
- Configuring a Custom Phone Ring, page 6-3

PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet these requirements for proper playback on Cisco IP Communicator:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- uLaw compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring is evenly divisible by 240.
- Ring starts and ends at the zero crossing.
- To create PCM files for custom phone rings, you can use any standard audio editing packages that support these file format requirements.

Related Topics

- RingList.xml File Format Requirements, page 6-1
- Configuring a Custom Phone Ring, page 6-3

Configuring a Custom Phone Ring

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines.

Step 2 Place the new PCM files that you created as specified:

- For Cisco Unified Communications Manager Releases other than 4.x: on the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For details, see the Software Upgrades chapter in *Cisco IP Telephony Platform Administration Guide* at this URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- For Cisco Unified Communications Manager Release 4.x: in the C:\Program Files\Cisco\TFTPPath directory on the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster.

Step 3 Use a text editor to edit the RingList.xml file. Ensure that the file complies with the format guidelines.

Step 4 Save your modifications, and close the RingList.xml file.

Step 5 To cache the new RingList.xml file, stop and start the TFTP service through Cisco Unified Communications Manager Serviceability, or disable and re-enable the *Enable Caching of Constant and Bin Files at Startup* TFTP service parameter (located in the Advanced Service Parameters).

Related Topics

- RingList.xml File Format Requirements, page 6-1
- PCM File Requirements for Custom Ring Types, page 6-2

About Custom Background Images

You can provide users with a choice of background images for their Cisco IP Communicator phone screens. Users select the background image that appears on the phone screen from the **Settings** button > **User Preferences > Background Images**.

The image choices come from PNG images and an XML file (called List.xml) that are stored on the TFTP server used by the phone. By storing your own PNG files and editing the XML file on the TFTP server, you can designate the background images from which users can choose. In this way, you can provide custom images, such as your company logo.

You can customize the background images that are available at your site by creating your own PNG files and editing the List.xml file.

- List.xml File Format Requirements, page 6-4
- PNG File Requirements for Custom Background Images, page 6-4
- Configuring a Background Image, page 6-5

List.xml File Format Requirements

The List.xml file defines an XML object that contains a list of background images.

Note If you are manually creating the directory structure and the List.xml file, make sure that the directories and files can be accessed by the user\CCMService, which is used by the TFTP service.

The List.xml file can include up to 50 background images. The images are presented in the order that they appear in the Background Images menu. For each background image, the List.xml file contains ImageItem element, which includes these attributes:

- Image—Uniform resource identifier (URI) that specifies where the phone obtains the thumbnail image that appears on the Background Images menu.
- URL—URI that specifies where the phone obtains the full size image.

List.xml Example

This example shows a List.xml file that defines two images. The required Image and URL attributes must be included for each image.The TFTP URI in the example is the only supported method for linking to full size and thumbnail images. HTTP URL support is not provided.

```
<CiscoIPPhoneImageList>
<ImageItem Image=”TFTP:Desktops/320x212x12/TN-Fountain.png”
URL=”TFTP:Desktops/320x212x12/Fountain.png”/>
<ImageItem Image=”TFTP:Desktops/320x212x12/TN-FullMoon.png”
URL=”TFTP:Desktops/320x212x12/FullMoon.png”/>
</CiscoIPPhoneImageList>
```

Cisco IP Communicator software includes a default background image. This image is not defined in the List.xml file. Cisco IP Communicator displays the default image if you do not create custom images or if there is an error retrieving a custom image. The default image is always the first image that appears in the Background Images menu.

Related Topics.

- PNG File Requirements for Custom Background Images, page 6-4.
- Configuring a Background Image, page 6-5

PNG File Requirements for Custom Background Images

Each background image requires two PNG files:

- Full size image—Version that appears on the phone screen.
- Thumbnail image—Version that appears on the Background Images screen from which users can select an image. The thumbnail image must be 25 percent of the size of the full size image.

Tip Many graphics programs provide a feature to resize a graphic. An easy way to create a thumbnail image is to first create and save the full size image, and then use the sizing feature in the graphics program to create a version of that image that is 25 percent of the original size. Save the thumbnail version by using a different name.

For proper display on Cisco IP Communicator, the PNG files for background images must meet these requirements:

- Full size image—320 pixels (width) X 212 pixels (height).
- Thumbnail image—80 pixels (width) X 53 pixels (height).
- Color palette—Includes up to 12-bit color (4096 colors). You can use more than 12-bit color, but Cisco IP Communicator reduces the color palette to12-bit before displaying the image. For best results, reduce the color palette of an image to 12-bit when you create a PNG file.

Tip If you are using a graphics program that supports a posterize feature for specifying the number of tonal levels per color channel, set the number of tonal levels per channel to 16 (16 red X 16 green X 16 blue = 4096 colors).

Related Topics.

- List.xml File Format Requirements, page 6-4.
- Configuring a Background Image, page 6-5

Configuring a Background Image

Procedure

Step 1 Create two PNG files for each image (a full size version and a thumbnail version). Ensure the PNG files comply with the format guideline.

Step 2 Place the new PNG files that you created as specified:

- For Cisco Unified Communications Manager Releases other than 4.x: on the TFTP server for each Cisco Unified Communications Manager in the cluster. For details, see the Software Upgrades chapter in *Cisco IP Telephony Platform Administration Guide* at this URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- For Cisco Unified Communications Manager Release 4.x: in the C:\Program Files\Cisco\TFTPPath\Desktops\320x212x12 folder on the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster.

Tip We recommend that you also store backup copies of custom image files in another location. You can use these backup copies if the files in the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 3 Use a text editor to edit the List.xml file. Ensure that the file complies with the format guidelines.

Step 4 Save your modifications, and close the List.xml file.

Note When you upgrade Cisco Unified Communications Manager, a default List.xml file replaces the List.xml file that you customized. After you customize the List.xml file, make a copy of the file, and store it in another location. After upgrading Cisco Unified Communications Manager, replace the default List.xml file with your stored copy.

Step 5 To cache the new List.xml file, stop and start the TFTP service by using Cisco Unified Communications Manager Serviceability, or disable and re-enable the *Enable Caching of Constant and Bin Files at Startup* TFTP service parameter (located in the Advanced Service Parameters).

Related Topics.

- List.xml File Format Requirements, page 6-4
- PNG File Requirements for Custom Background Images, page 6-4

About Configuring the Idle Display

You can specify an idle display that appears on the phone screen. The idle display is an XML service that Cisco IP Communicator invokes when it is idle (not in use) for a designated period, and no feature menu is open. XML services that can be used as idle displays include company logos, product pictures, and stock quotes.

Configuring the idle display consists of these general steps:

1. Formatting an image.
2. Configuring Cisco Unified Communications Manager to display the image.

For details about creating and displaying the idle display, see the *Creating Idle URL Graphics on Cisco Unified IP Phone* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

In addition, see the *Cisco Unified Communications Manager Administration Guide* or the *Bulk Administration Tool User Guide* at these URLs:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_user_guide_list.html

- Specifying the URL of the idle display XML service:
  - For a single phone device—Idle field on the Phone Configuration window (**Device > Phone)**
  - For multiple devices simultaneously—URL Idle field on the Enterprise Parameters Configuration window (**System > Enterprise Parameters**), or the Idle field in the Bulk Administration Tool (BAT)
- Specifying the length of time that Cisco IP Communicator is not used before the idle display XML service is invoked:
  - For a single device—Idle Timer field on the Phone Configuration window (**Device > Phone**)
  - For multiple devices simultaneously—URL Idle Time field on the Enterprise Parameters Configuration window (**System > Enterprise Parameters**), or the Idle Timer field in the BAT

From Cisco IP Communicator, you can see settings for the idle display XML service URL and the length of time the application must be inactive before this service is invoked. To see these settings, click the **Settings** button and choose **Device Configuration**, and scroll to Idle URL and Idle URL Time.

Related Topics.

- About Custom Phone Rings, page 6-1
- About Custom Background Images, page 6-3

CHAPTER 7

Viewing Operational Information for Cisco IP Communicator

Revised: 1/19/11

Some tasks in this chapter required configuration in Cisco Unified Communications Manager, formerly known as Cisco Unified CallManager.

Operational Information Overview

Table 7-1 describes how to access different types of operational information (status messages, network statistics, and other types of operational information). You can access this information through these methods:

- Locally (on the Cisco IP Communicator interface)
- Remotely (from a web site)

Table 7-1 Overview of Operational Information

If you want to view...	Look here...	For details, see...
Model Information	• Cisco IP Communicator: **Settings** button > **Model Information**	Model Information, page 7-7
Device Information	• Cisco IP Communicator: **Settings** button > **Device Configuration** • Service web page: **Device Information**	• Device Configuration Information, page 7-2 • Device Information, page 7-16
Security Configuration	Cisco IP Communicator: **Settings** button > **Security Configuration**	Security Configuration Information, page 7-7
Software Version	Cisco IP Communicator: **right-click > About Cisco IP Communicator**	Build Versions in the About Window Vary, page 8-15

Table 7-1 Overview of Operational Information (continued)

If you want to view...	Look here...	For details, see...
Status Messages	• Cisco IP Communicator: **Settings** button > **Status > Status Messages** • Device web page: **Device Logs > Status Messages**	• Status Messages Displayed, page 7-9 • Status Messages, Device Logs, and Alarm Information, page 7-18
Statistics	• Cisco IP Communicator: click the **?** button twice quickly during a call • Device web page: **Streaming Statistics > Stream 1**, **Stream 2**, or **Stream 3**	• Call Statistic Information, page 7-13 • Streaming Statistic Information, page 7-19
Alarm Messages	Device web page: **Device Logs > Debug Display**	Status Messages, Device Logs, and Alarm Information, page 7-18

Related Topics

- Accessing the Web Page for a Device, page 7-15

About Operational Information Displayed Locally on Cisco IP Communicator

- Device Configuration Information, page 7-2
- Model Information, page 7-7
- Security Configuration Information, page 7-7
- Status Messages Displayed, page 7-9
- Call Statistic Information, page 7-13

Device Configuration Information

To view the Device Configuration screen, click **Settings** > **Device Configuration**. Table 7-2 describes the non-networking settings in the display.

To modify configurable items that appear in this menu, use Cisco Unified Communications Manager Administration.

Table 7-2 Device Configuration Information Displayed in Cisco IP Communicator

Option	Description
Unified Communications Manager Configuration	List of servers in prioritized order (Unified CM 1 through Unified CM 5) that are available for processing calls from this application. For an available server, an option shows server IP address and one of these states: • Active—Server from which the application is currently receiving call-processing services. • Standby—Server to which the application switches if the current server becomes unavailable. • Blank—No current connection to this server. An option might also include the Survivable Remote Site Telephony (SRST) designation, which indicates an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in Cisco Unified Communications Manager Administration (**System > Device Pool**).
HTTP Configuration	This menu has these options: • Directories URL—URL of the server from which the application obtains directory information. • Services URL—URL of the server from which the application obtains Cisco Unified IP Phone services. • Messages URL—URL of the server from which the application obtains message services. • Information URL—URL of the help text that appears in the application. • Authentication URL—URL that the application uses to validate requests made to the application web server. • Proxy Server URL—URL used to proxy HTTP requests for access to non-local host addresses from the application HTTP client. • Idle URL—URL that the application displays when the application has not been used for the time specified in the Idle URL Time option. For example, you can use the Idle URL option and the Idle URL Timer option to display a log on the phone screen when the application is not used for five minutes. • Idle URL Time—Amount of time in seconds that elapses before the URL specified in the Idle URL option appears.
Locale Configuration	This menu has these options: • User Locale—User locale associated with the application user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information. • Network Locale—Network locale associated with the application user. The network locale identifies a set of detailed information to support the application in a specific location, including definitions of the tones and cadences used by the application. • User Locale Version—Version of the user locale loaded on the application. • Network Locale Version—Version of the network locale loaded on the application. • User Locale Char Set—Character set that the application uses for the user locale.

Table 7-2 Device Configuration Information Displayed in Cisco IP Communicator (continued)

Option	Description
UI Configuration	• Auto Line Select Enabled—When enabled, the phone shifts the call focus to incoming calls on all lines. When disabled, the phone shifts the focus to incoming calls only on the currently used line. • BLF for Call Lists—When enabled, the phone displays phone status (presence information such as off-hook and on-hook) in the call lists. • Reverting Focus Priority— Indicates whether the phone shifts the call focus on the phone screen to an incoming call or a reverting hold call. • Auto Call Select—Indicates whether the phone automatically shifts the call focus to an incoming call on the same line when the user is already on a call. • "more" Softkey Timer—Indicates the number of seconds that additional softkeys are displayed after the user presses **more**. If this timer expires before the user presses another softkey, the display reverts to the initial softkeys.
SIP Configuration	Provides access to the SIP General Configuration menu and the Line Settings menu. See the "Related Topics."

Related Topics

- SIP General Configuration Information, page 7-4
- Line Settings Information, page 7-5
- Call Preferences Information, page 7-6

SIP General Configuration Information

To view the SIP General Configuration screen, click **Settings** > **Device Configuration > SIP Configuration > SIP General Configuration**. Table 7-3 describes the SIP parameters on Cisco IP Communicator.

You can modify configurable items that appear in this screen through Cisco Unified Communications Manager Administration Releases (other than 4.x) by choosing **Device > Device Settings > SIP Profile**.

Table 7-3 SIP General Configuration Information Displayed in Cisco IP Communicator

Option	Description
Preferred CODEC	Displays the CODEC to use when a call is initiated. This value is always set to none and is not configurable.
Out of Band DTMF	Displays the configuration of the out-of-band signaling (for tone detection on the IP side of a gateway). The SIP Phone supports out-of-band signaling through the AVT tone method. This value is always set to avt and is not configurable.
Register with Proxy	Displays if the phone must register with a proxy server during initialization. This value is always set to true and is not configurable.
Register Expires	Displays the amount of time, in seconds, after which a registration request expires.
Phone Label	Displays the text that is on the top right status line of the Cisco IP Communicator phone screen. This text is for end-user display only and has no effect on caller identification or messaging. This value is always set to null and is not configurable.
Enable VAD	Displays if VAD[1] is enabled.

Table 7-3 SIP General Configuration Information Displayed in Cisco IP Communicator (continued)

Option	Description
Start Media Port	Displays the start RTP[2] range for media.
End Media Port	Displays the end RTP range for media.
Backup Proxy	Displays the IP address of the backup proxy server or gateway. This value is always set to USECALLMANAGER and is not configurable.
Backup Proxy Port	Displays the port number of the backup proxy server or gateway. This value is always be set to 5060 and is not configurable.
Emergency Proxy	Displays the IP address of the emergency proxy server or gateway. This value is always set to USECALLMANAGER and is not configurable.
Emergency Proxy Port	Displays the port number of the emergency proxy server or gateway. This value is always set to 5060.
Outbound Proxy	Displays the IP address of the outbound proxy server. This value is always set to USECALLMANAGER and is not configurable.
Outbound Proxy Port	Displays the port number of the outbound proxy server. This value is always set to 5060 and is not configurable.
NAT Enabled	Displays if NAT is enabled. This value is always set to false and is not configurable.
NAT Address	Displays the WAN IP address of the NAT[3] or firewall server. This value is always set to null and is not configurable.
Call Statistics	Displays if call statistics are enabled on the phone.

[1] VAD = voice activation detection

[2] RTP = Real-Time Transport Protocol

[3] NAT = Network Address Translation

Related Topics

- Line Settings Information, page 7-5
- Call Preferences Information, page 7-6

Line Settings Information

To view the Line Settings screen, click **Settings** > **Device Configuration** > **SIP Configuration** > **Line Settings**. The Line Settings screen displays information about the configurable parameters for each of the lines on your SIP phone. Table 7-4 describes the options in the display. These options are SIP specific.

To modify configurable items that appear in this screen, use Cisco Unified Communications Manager Administration.

Table 7-4 Line Settings Information Displayed in Cisco IP Communicator

Option	Description
Name	Displays the number the line uses when registering.
Short Name	Displays the short name configured for the line.
Authentication Name	Displays the name used by the phone for authentication if a registration is challenged by the call control server during initialization.

Table 7-4 Line Settings Information Displayed in Cisco IP Communicator (continued)

Option	Description
Display Name	Displays the identification the phone uses for display for caller identification purposes.
Proxy Address	Displays the IP address of the proxy server that will be used by the phone. This value is always set to USECALLMANAGER and is not configurable.
Proxy Port	Displays the port number of the proxy server that will be used by the phone. This value is always set to 5060 and is not configurable.
Shared Line	Displays if the line is part of a shared line (Yes) or not (No) and is not configurable.

Related Topics

- SIP General Configuration Information, page 7-4
- Call Preferences Information, page 7-6

Call Preferences Information

To view the Call Preferences screen, click **Settings** > **Device Configuration > Call Preferences**. Table 7-5 describes the options in the display. These options are SIP specific.

Table 7-5 Call Preferences Information Displayed in Cisco IP Communicator

Option	Description
Do Not Disturb	Indicates whether do not disturb is enabled (Yes) or disabled (No) for the phone. To change this setting, choose **Device > Device Settings > SIP Profile** in Cisco Unified Communications Manager Administration. You can also modify this setting from the phone if enabled in Cisco Unified Communications Manager. **Note** This feature is not supported in Cisco Unified Communications Manager release 4.x.
Caller ID Blocking	Indicates whether caller ID blocking is enabled (Yes) or disabled (No) for the phone. To change this setting, choose **Device > Device Settings > SIP Profile** in Cisco Unified Communications Manager Administration. **Note** This feature is not supported in Cisco Unified Communications Manager release 4.x.
Anonymous Call Block	Indicates whether anonymous call block is enabled (Yes) or disabled (No) for the phone. To change this setting, choose **Device > Device Settings > SIP Profile** in Cisco Unified Communications Manager Administration. **Note** This feature is not supported in Cisco Unified Communications Manager release 4.x.
Call Waiting Preferences	Displays a sub-menu that indicates whether call waiting is enabled (Yes) or disabled (No) for each line. To change this setting, use Cisco Unified Communications Manager Administration.
Call Hold Ringback	Indicates whether the call hold ringback feature is enabled (Yes) or disabled (No) for the phone. To change this setting, choose **Device > Device Settings > SIP Profile** in Cisco Unified Communications Manager Administration. **Note** This feature is not supported in Cisco Unified Communications Manager release 4.x.

Table 7-5 Call Preferences Information Displayed in Cisco IP Communicator (continued)

Option	Description
Stutter Msg Waiting	Indicates whether stutter message waiting is enabled (Yes) or disabled (No) for the phone. To change this setting, choose **Device > Device Settings > SIP Profile** in Cisco Unified Communications Manager Administration. **Note** This feature is not supported in Cisco Unified Communications Manager release 4.x.
Call Logs BLF Enabled	Indicates whether BLF for call logs is enabled (Yes) or disabled (No) for the phone. To change this setting, use Cisco Unified Communications Manager Administration.
Auto Answer Preferences	Displays a sub-menu that indicates whether auto answer is enabled (Yes) or disabled (No) for the each line. To change this setting, choose **Call Routing > Directory Number** in Cisco Unified Communications Manager Administration. **Note** This feature is not supported in Cisco Unified Communications Manager release 4.x.
Speed Dials	Displays a sub-menu that displays the lines available on the phone. Select a line to see the speed dial label and number assigned to that line. To change this setting, go to the Phone Configuration page > **Add/Update Speed Dials** in Cisco Unified Communications Manager Administration.

Related Topics

- SIP General Configuration Information, page 7-4
- Line Settings Information, page 7-5

Model Information

To view the Model Information screen, click **Settings** > **Model Information**. This screen provides the phone model number of the phone, the factory-installed load running on the phone, and shows whether the phone is running SCCP or SIP.

Security Configuration Information

To view the Security Configuration screen, click **Settings** > **Security Configuration**. Table 7-6 describes the options in the display.

Table 7-6 Security Configuration Information Displayed in Cisco IP Communicator

Option	Description
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for Cisco IP Communicator.
Security Mode	Displays the security mode that is set for Cisco IP Communicator. You configure the device security mode in Cisco Unified Communications Manager Administration. For details, see How to Configure Security Features for Cisco IP Communicator, page 2-12. For details, see the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Table 7-6 Security Configuration Information Displayed in Cisco IP Communicator (continued)

Option	Description
LSC[1]	Indicates whether an LSC, which is used for the security features, is installed on the phone (Yes) or is not installed (No) on Cisco IP Communicator. For details about managing the LSC for your phone, see the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
CTL[2] File	Displays the MD5 hash of the CTL file that is installed for Cisco IP Communicator. If no CTL file is installed, this field displays *No*. If security is configured for Cisco IP Communicator, the CTL file automatically installs when Cisco IP Communicator reboots or resets. For details, see the "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html If a CTL file is installed, this option also provides access to the CTL File screen.
Trust List	Displays information about all of the servers that the phone trusts. If a CTL file is installed, this option provides access to the Trust List menu.
CAPF[3] Server	Displays the IP address and the port of the CAPF that Cisco IP Communicator uses.

[1] LSC = Locally Significant Certificate

[2] CTL = certificate trust list

[3] CAPF = Certificate Authority Proxy Function

Related Topics

- CTL File Information, page 7-8
- Trust List Information, page 7-9

CTL File Information

If a CTL file is installed on Cisco IP Communicator, you can access the CTL File screen by clicking **Settings** > **Security Configuration** > **CTL File**.

Table 7-7 describes the options in the display.

Table 7-7 CTL File Information Displayed in Cisco IP Communicator

Option	Description
CTL File	Displays the MD5 hash of the CTL file that is installed for Cisco IP Communicator. If no CTL file is installed, this field displays *No*. If security is configured for Cisco IP Communicator, the CTL file automatically installs when Cisco IP Communicator reboots or resets. For details, see the "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html A locked padlock icon 🔒 means that the CTL file is locked. An unlocked padlock icon 🔓 means that the CTL file is unlocked.

Table 7-7 CTL File Information Displayed in Cisco IP Communicator (continued)

Option	Description
CAPF Server	Displays the IP address of the CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server.
CallManager/TFTP Server	Displays the IP address of the Cisco Unified Communications Manager and the TFTP server used by the phone. Also displays a certificate icon 📜 if a certificate is installed for this server.

Related Topics

- Security Configuration Information, page 7-7
- Trust List Information, page 7-9

Trust List Information

The Trust List screen displays information about all of the servers on the trusted list.

If a CTL file is installed on Cisco IP Communicator, you can access the Trust List screen by choosing **Settings** > **Security Configuration > Trust List**.

Table 7-8 describes the options in the display.

Table 7-8 Trust List Information Displayed in Cisco IP Communicator

Option	Description
CAPF Server	Displays the IP address of the CAPF that is used by Cisco IP Communicator. Also displays a certificate icon 📜 if a certificate is installed for this server.
CallManager/TFTP Server	Displays the IP address of a Cisco Unified Communications Manager server and a TFTP server that is used by Cisco IP Communicator. Also displays a certificate icon 📜 if a certificate is installed for this server.
SRST Router	Displays the IP address of the trusted SRST router that is available to Cisco IP Communicator, if such a device has been configured in Cisco Unified Communications Manager Administration. Also displays a certificate icon 📜 if a certificate is installed for this server.

Related Topics

- Security Configuration Information, page 7-7
- CTL File Information, page 7-8

Status Messages Displayed

The Status menu displays the Status Messages screen, which shows a log of important system messages. To display the Status menu, click **Settings** > **Status > Status Messages**. Table 7-9 describes the possible messages.

Table 7-9 Status Messages Displayed in Cisco IP Communicator

Message	Description	Possible Explanation and Action
BootP server used	Cisco IP Communicator obtained its IP address from a BootP server rather than from a DHCP server.	None. This message is informational only.
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	The configuration file is created when Cisco IP Communicator is added to the Cisco Unified Communications Manager database. If it has not been added to the database, the TFTP server generates a `CFG File Not Found` response. • Cisco IP Communicator is not registered with Cisco Unified Communications Manager. You must manually add Cisco IP Communicator to the database if you are not allowing these devices to auto-register. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check the TFTP server configuration.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down; otherwise, the files might be corrupted.
CTL Installed	A CTL file is installed on Cisco IP Communicator.	None. This message is informational only. See the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
CTL update failed	Cisco IP Communicator could not update its CTL file.	A problem occurred with the CTL file on the TFTP server. See the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
DHCP timeout	DHCP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DHCP server and Cisco IP Communicator —Verify the network connections. • DHCP server is down—Check the DHCP server configuration. • Errors persist—Consider assigning a static IP address.

Table 7-9 Status Messages Displayed in Cisco IP Communicator (continued)

Message	Description	Possible Explanation and Action
DNS timeout	DNS server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DNS server and Cisco IP Communicator—Verify the network connections. • DNS server is down—Check the DNS server configuration.
DNS unknown host	DNS could not resolve the TFTP server name or Cisco Unified Communications Manager.	• Verify that the TFTP server host names of Cisco Unified Communications Manager are properly configured in DNS. • Consider using IP addresses rather than host names.
Duplicate IP	Another device is using the IP address assigned to Cisco IP Communicator.	• If Cisco IP Communicator has a static IP address, verify that you have not assigned a duplicate IP address. If you are using DHCP, check the DHCP server configuration.
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	Check that these files are located within subdirectories in the TFTPPath directory: • Located in subdirectory with same name as network locale: – g3-tones.xml • Located in subdirectory with same name as user locale: – ipc-sccp.jar – ipc-sip.jar
File auth error	An error occurred when Cisco IP Communicator tried to validate the signature of a signed file. This message includes the name of the file that failed.	• The file is corrupted. If the file is a phone configuration file, delete Cisco IP Communicator from the database. Then add it to the database by using Cisco Unified Communications Manager Administration. • There is a problem with the CTL file, and the key for the server from which files are obtained is bad. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.
File not found	Cisco IP Communicator cannot locate the phone load file that is specified in the phone configuration file on the TFTP server.	Make sure that the phone load file is on the TFTP server and that the entry in the configuration file is correct.
IP address released	Cisco IP Communicator has been configured to release its IP address.	Cisco IP Communicator remains idle until you reset the DHCP address.

Table 7-9 Status Messages Displayed in Cisco IP Communicator (continued)

Message	Description	Possible Explanation and Action
Load Auth Failed	Cisco IP Communicator could not load a configuration file.	The configuration file that Cisco IP Communicator received from the server identified in this message is corrupt. Make sure that a good version of the configuration file exists on that server.
Load Auth Failed	A signed phone load file has been modified or renamed.	Make sure that the phone load file that Cisco IP Communicator is downloading has not been altered or renamed.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to Cisco IP Communicator in Cisco Unified Communications Manager Administration (**Device > Phone**). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you were attempting to install a version of software on this Cisco IP Communicator that did not support hardware changes on this newer phone. Check the load ID assigned to the phone in Cisco Unified Communications Manager Administration (**Device > Phone**). Re-enter the load displayed on the phone.
No CTL installed	A CTL file is not installed in Cisco IP Communicator.	Occurs if security is not configured or, if security is configured, because the CTL file does not exist on the TFTP server. See the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
No default router	DHCP or static configuration did not specify a default router.	• If Cisco IP Communicator has a static IP address, verify that the default router has been configured. • If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	If Cisco IP Communicator has a static IP address, verify that the DNS server has been configured. If you are using a DHCP server, it did not provide a DNS server address. Check the DHCP server configuration.
Programming Error	Cisco IP Communicator failed during programming.	Attempt to resolve this error by exiting (or closing) the application and then relaunching it. If the problem persists, contact Cisco technical support for assistance.
TFTP access error	TFTP server is pointing to a directory that does not exist.	• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check the TFTP server configuration.
TFTP Error	Cisco IP Communicator does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.

Table 7-9 Status Messages Displayed in Cisco IP Communicator (continued)

Message	Description	Possible Explanation and Action
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to Cisco IP Communicator in Cisco Unified Communications Manager Administration (**Device > Phone**). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
TFTP server not authorized	The specified TFTP server could not be found in CTL for Cisco IP Communicator.	• The DHCP server is not configured properly, and the TFTP server address is not correct. In this case, update the TFTP server configuration to specify the correct TFTP server. • If Cisco IP Communicator is using a static IP address, the phone might be configured with the wrong TFTP server address. In this case, enter the correct TFTP server address in the Network Configuration menu on the phone. • If the TFTP server address is correct, there might be a problem with the CTL file. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.
TFTP timeout	TFTP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the TFTP server and Cisco IP Communicator—Verify the network connections. • TFTP server is down—Check TFTP server configuration.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault.cnf.xml, or .cnf.xml corresponding to Cisco IP Communicator device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

Related Topics

- Device Configuration Information, page 7-2
- Security Configuration Information, page 7-7
- Call Statistic Information, page 7-13

Call Statistic Information

The Call Statistics screen shows counters and statistics for the current call. To display the Call Statistics screen, click the **?** button twice rapidly during a call. Table 7-10 describes the options in the display.

Table 7-10 Call Statistics Displayed in Cisco IP Communicator

Item	Description
Rcvr Codec	Type of voice stream received (RTP[1] streaming audio). For a list of supported codecs, see the data sheet at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_data_sheet09186a00801f8e48.html
Sender Codec	Type of voice stream transmitted (RTP streaming audio). For a list of supported codecs, see the data sheet at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_data_sheet09186a00801f8e48.html
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets 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.
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.
Avg Jitter	The estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Max Jitter	Maximum jitter observed since the receiving voice stream was opened.
RxDisc	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The application discards payload type 19 comfort noise packets that are generated by Cisco Gateways, which increments this counter.
Recvr Lost Packets	Missing RTP packets (lost in transit).

[1] RTP = Real-Time Transport Protocol

About Operational Information Displayed Remotely from a Web Page

Each Cisco IP Communicator device has a web page from which you can view operational information. You can use this information to remotely monitor the device and to assist with troubleshooting.

Note Remote access is not possible if you disabled the internal web server.

You can also obtain much of this information directly from Cisco IP Communicator. For details, see About Operational Information Displayed Locally on Cisco IP Communicator, page 7-2. For troubleshooting information, see Chapter 8, "Troubleshooting Cisco IP Communicator."

- Accessing the Web Page for a Device, page 7-15
- Device Information, page 7-16
- Network Configuration Information, page 7-16
- Status Messages, Device Logs, and Alarm Information, page 7-18
- Streaming Statistic Information, page 7-19

Accessing the Web Page for a Device

Procedure

Step 1 Search for the device in Cisco Unified Communications Manager Administration (**Device > Phone**). Devices registered with Cisco Unified Communications Manager display the IP address at the top of the Phone Configuration web page.

Step 2 Click the IP address or open a separate web browser, and enter the following URL, where *IP_address* is the IP address of Cisco IP Communicator:

http://*IP_address*

Tip If you are performing this on the PC on which Cisco IP Communicator is installed, you can use *localhost* for the IP address if Cisco IP Communicator is running.

Related Topics

- Device Information, page 7-16
- Network Configuration Information, page 7-16
- Status Messages, Device Logs, and Alarm Information, page 7-18
- Streaming Statistic Information, page 7-19

Device Information

To display device information, access the applicable web page, and click **Device Information**. The web page displays device settings and related information. Table 7-11 describes the information.

Table 7-11 Device Information Items Displayed on the Web Page

Item	Description
Host Name	Host name that the DHCP server assigned to the device.
Phone DN	Directory number assigned to the device.
Version	Version of the boot load running on the device.
Model Number	Model number of the device.
Message Waiting	Indicates if there is a voice message waiting on any line for the device.

Related Topics

- Accessing the Web Page for a Device, page 7-15
- Network Configuration Information, page 7-16
- Status Messages, Device Logs, and Alarm Information, page 7-18
- Streaming Statistic Information, page 7-19

Network Configuration Information

To display network configuration information, access the applicable web page, and click **Network Configuration**.

The web page displays network configuration information and information about other settings. You can view some of these items in Cisco IP Communicator (**Settings** > **Device Configuration**).

Table 7-12 describes the information.

Table 7-12 Network Configuration Items Displayed on the Web Page

Item	Description
DHCP Server	IP address of the DHCP server from which the device obtains its TFTP server address.
Host Name	Host name that the DHCP server assigned to the device.
IP Address	IP address of the device.
Default Router 1–5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5.
TFTP Server 1	Primary TFTP server used by the device.

Table 7-12 Network Configuration Items Displayed on the Web Page (continued)

Item	Description
Unified CM1–5	Servers, in prioritized order, that are available for processing calls from the device. For an available server, an option shows the server IP address and one of these states: • Active—Server from which the device is currently receiving call-processing services. • Standby—Server to which the device switches if the current server becomes unavailable. • Blank—No current connection to this server. An option might also include the SRST designation, which indicates an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers even if it is active. You configure the SRST router address in Cisco Unified Communications Manager Administration (**System > Device Pool**).
Information URL	URL of the help text that appears on the device.
Directories URL	URL of the server from which the device obtains directory information.
Messages URL	URL of the server from which the device obtains message services.
Services URL	URL of the server from which the device obtains Cisco Unified IP Phone services.
Alternate TFTP	Indicates whether the device is using an alternative TFTP server.
Idle URL	URL that the phone displays when the device has not been used for the time specified by Idle URL Time.
Idle URL Time	Time in seconds that elapses before the URL shown in Idle URL appears.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the device HTTP client and provides responses from the non-local host to the device HTTP client.
Authentication URL	URL that the device uses to validate requests made to the web server.
TFTP Server 2	Backup TFTP server that the device uses if the primary TFTP server is unavailable.
User Locale	User locale associated with the Cisco IP Communicator user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the Cisco IP Communicator user. Identifies a set of detailed information to support the device in a specific location, including definitions of tones and cadences.
Headset Enabled	Current state of the Cisco IP Communicator headset (enabled or disabled).
User Locale Version	Version of the user locale loaded on the device.
Network Locale Version	Version of the network locale loaded on the phone.
Auto Line Select Enabled	When enabled, the phone shifts the call focus to incoming calls on all lines. When disabled, the phone shifts the focus to incoming calls only on the currently used line.

Related Topics

- Accessing the Web Page for a Device, page 7-15
- Device Configuration Information, page 7-2
- Device Information, page 7-16

- Status Messages, Device Logs, and Alarm Information, page 7-18
- Streaming Statistic Information, page 7-19

Status Messages, Device Logs, and Alarm Information

To display status messages or debug display information, access the applicable web page, and click **Status Messages** or **Debug Display**. The web page displays device logs, which provides information you can use to help monitor and troubleshoot the application.

The Status Messages area displays up to the 10 most recent status messages that Cisco IP Communicator generated since it was last powered up. These are the same status messages that you can see on the interface (**Settings** > **Status > Status Message**). Table 7-9 on page 7-10 describes the status messages that can appear.

The Debug Display area displays a log of up to the 50 most recent alarms for the phone. Alarms indicate a variety of errors or conditions. Table 7-13 describes the alarm messages.

Table 7-13 Alarms Displayed on the Web Page

Alarm Number	Explanation
1	Configuration file that the device tried to obtain from the TFTP server was too large (greater than 2 MB)
3	Firmware image that the device tried to obtain has an incorrect name
4	The PC on which Cisco IP Communicator is installed has run out of disk space
6	Configuration file that the device requested does not exist on the TFTP server
7	A request to the TFTP server timed out
8	The device could not log in to the TFTP server
9	General TFTP error
14	Cisco Unified Communications Manager closed socket
15	The device lost its connection to the remote host
16	Cisco Unified Communications Manager indicates that the device could not unregister for some reason
17	Cisco Unified Communications Manager stopped responding to KeepAlive requests
18	The device failed back to a higher priority Cisco Unified Communications Manager
20	User clicked **#** on the phone
21	The device obtained a new IP address
22	Cisco Unified Communications Manager sent a reset instruction to the device
23	Cisco Unified Communications Manager sent a restart instruction to the device
24	Cisco Unified Communications Manager rejected a registration attempt from the device
25	No prior reset cause (default condition)
32	General alarm
33	Could not write to the hard drive

Related Topics

- Accessing the Web Page for a Device, page 7-15
- Device Information, page 7-16
- Network Configuration Information, page 7-16
- Streaming Statistic Information, page 7-19

Streaming Statistic Information

To display streaming statistics, access the applicable web page, and click **Stream 1**, **Stream 2**, or **Stream 3**. The web pages provides streaming statistics information.

Cisco IP Communicator can simultaneously stream information to and from up to three devices. It streams information when it is on a a call or running a service that sends or receives audio or data. Most calls use only one stream (Stream 1), but some calls use two or three streams. For example, a barged call uses Stream 1 and Stream 2. Table 7-14 describes the streaming statistics information.

Table 7-14 Streaming Statistics Displayed on the Web Page

Item	Description
Domain	Domain of the device
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.
Sender Joins	Number of times the device has started transmitting a stream
Receiver Joins	Number of times the device has started receiving a stream
Byes	Number of times the device has stopped transmitting a stream
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the device start transmitting packets
Row Status	Whether the device is streaming
Host Name	Host name of the device
Sender Packets	Total number of RTP data packets transmitted by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Octets	Total number of payload octets transmitted in RTP data packets by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Tool	Type of audio encoding used for the stream
Sender Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the device resets)
Sender Report Time	Internal time stamp indicating when this streaming statistics report was generated
Sender Start Time	Time that the stream started
Rcvr Lost Packets	Total number of RTP data packets that have been lost since starting receiving data on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or duplicate. The value displays as 0 if the connection was set to send-only mode.
Rcvr Jitter	Maximum jitter of stream
Receiver Tool	Type of audio encoding used for the stream

Table 7-14 Streaming Statistics Displayed on the Web Page (continued)

Item	Description
Rcvr Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the device resets)
Rcvr Report Time	Internal time stamp indicating when this streaming statistics report was generated
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the device start receiving packets

Related Topics

- Accessing the Web Page for a Device, page 7-15
- Device Information, page 7-16
- Network Configuration Information, page 7-16
- Status Messages, Device Logs, and Alarm Information, page 7-18

How to Set Up and Run the Windows Performance Tool

- Setting Up and Running the Windows XP Performance Tool, page 7-20
- Setting Up and Running the Windows Vista Performance Tool, page 7-21

Setting Up and Running the Windows XP Performance Tool

You can monitor application performance by using the Windows Performance tool to gauge the impact that other applications might have on Cisco IP Communicator (for example, in preparation for an internal pilot). You might also want to monitor performance if users complain of degraded Cisco IP Communicator performance when other applications are running.

Before You Begin

Before starting this test, ensure that only the operating system and applications that run all the time (anti-virus, security, instant message applications, and so forth) are running along with Cisco IP Communicator.

Procedure

Step 1 Start the Windows Performance Tool by choosing **Start > Control Panel > Administrative Tools > Performance**.

Step 2 Click **Performance Logs and Alerts** to expand it in the left pane of the Performance window.

Step 3 Name the log file:

a. In the left pane, select **Counter Logs**, right-click, and choose **New Log Settings**.

b. In the New Log Settings pop-up, enter the log file name, and click **OK**.

Step 4 Choose Cisco IP Communicator-specific performance counters when the next pop-up window appears:

a. Make sure the General Tab is selected, and click **Add Counters** to add counters to monitor.

b. In the next window, perform these steps:

- Choose **Select Counters From Computer** (the name of the computer should appear in the list).
- Set Performance Object to **Process**.
- In Select Counters From List, choose process-related counters (**% Processor Time**, **IO Other Bytes**, I**O Read Bytes/sec**, **IO Write Bytes/sec**, **Private Bytes, Working Set**) recommended) from the list. While selecting these counters, press the **Ctrl** key to add more than one at a time.
- In Select Instances From List, choose **communicatork9** from the list, and click **Add**.

c. When you are finished adding counters, click **Close**.

d. In the window that appears, review the list of counters that you added. Make adjustments, if necessary.

Step 5 Define the time interval for monitoring. Enter values for Interval and Units (for example Interval = 1 and Units = seconds). This setting applies to all counters in the list.

Step 6 Select the Log Files Tab, and define the format in which performance data is saved:

a. For Log File Type, select **Text File (Comma Delimited)** to create a comma-delimited file.

b. Note the location where the file is saved.

c. Click **Apply**.

Step 7 Select the Schedule Tab, and enter information to start and stop the log. Click **Apply** and **OK**.

You can also manually start and stop the log by clicking the buttons on the toolbar.

Run the test for the duration that seems appropriate for the type of problem that you are trying to resolve. For example, if Cisco IP Communicator fails right after it is launched, you might want to run the performance test for only 5 to 10 minutes. However, if there are problems that occur after a long period of usage, you might need to run the test for 8 hours.

Step 8 Run the test again when other CPU intensive applications (Microsoft Excel, Outlook, Word) are running in the background.

Compare the results from the tests. Cisco IP Communicator CPU usage should stay near the baseline while other applications are running in the background.

Step 9 Import the file from its saved location into a spreadsheet.

Setting Up and Running the Windows Vista Performance Tool

You can monitor application performance by using the Windows Performance tool to gauge the impact that other applications might have on Cisco IP Communicator (for example, in preparation for an internal pilot). You might also want to monitor performance if users complain of degraded Cisco IP Communicator performance when other applications are running.

Before You Begin

Before starting this test, ensure that only the operating system and applications that run all the time (anti-virus, security, instant message applications, and so forth) are running along with Cisco IP Communicator.

Procedure

Step 1 From the Control Panel, choose **Performance Information and Tools**.

Step 2 From the Tasks pane on the left, choose **Advanced Tools**.

Step 3 From the list of tools, click **Open Reliability and Performance Monitor**.

Step 4 In the Reliability and Performance Monitor window, in the left pane, click **Data Collector Sets** to expand it.

Step 5 Right-click **User Defined**, and choose **New > Data Collector Set**.

Step 6 In the Create New Data Collector Set window:

a. Enter a name for the collector set, click **Create Manually (Advanced)**, and click **Next**.

b. For what type of data do you want to include, click **Performance Counter**, and click **Next**.

c. Define the sample interval for the performance counters you want to log, and click **Add**.

d. Under the Available Counters section in the left panel, click **Process** to expand it:

- Select **% Processor Time**, **IO Other Bytes**, I**O Read Bytes/sec**, **IO Write Bytes/sec**, **Private Bytes, Working Set** (recommended) from the list. While selecting these counters, press the **Ctrl** key to add more than one at a time.
- From the Instance of Selected Object list, select **communicatork9**, click **Add**, and then **OK**.

e. Verify the list of performance counters, and click **Next**.

f. Define the folder for the log file by clicking **Browse**.

g. Click **Finish**.

Step 7 In the Reliability and Performance Monitor window, in the left pane, select the name of the collector set that you specified in Step 6a under **Data Collector Sets > User Defined**, and double-click the corresponding **DataCollector01** in the right pane.

Step 8 In the DataCollector01 Properties window, Performance Counters tab, select the log format as **Comma Separated**, click **Apply**, and **OK** to dismiss the window.

Step 9 In the Reliability and Performance Monitor window, in the left pane, right-click the name of the collector set, and select **Start**.

Run the test for the duration that seems appropriate for the type of problem that you are trying to resolve. For example, if Cisco IP Communicator fails right after it is launched, you might want to run the performance test for only 5 to 10 minutes. However, if there are problems that occur after a long period of usage, you might need to run the test for 8 hours.

Step 10 Run the test again when other CPU intensive applications (Microsoft Excel, Outlook, Word) are running in the background.

Compare the results from the tests. Cisco IP Communicator CPU usage should stay near the baseline while other applications are running in the background.

Step 11 Import the file from its saved location into a spreadsheet.

CHAPTER 8

Troubleshooting Cisco IP Communicator

Revised: 1/19/11

This chapter provides troubleshooting information for common Cisco IP Communicator issues. Some tasks in this chapter require configuration in Cisco Unified Communications Manager, formerly known as Cisco Unified CallManager.

- How to Use Diagnostic Tools, page 8-1
- How to Resolve Installation Problems, page 8-4
- How to Resolve Startup Problems, page 8-5
- How to Resolve Security Problems, page 8-7
- How to Resolve Voice-Quality Issues, page 8-9
- How to Resolve General Application Problems, page 8-14

For additional troubleshooting information, see these documents:

- *User Guide for Cisco IP Communicator*—Contains detailed information about installation and voice-quality issues in the troubleshooting section. It is available at this URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

- *Using the 79xx Status Information For Troubleshooting*—This technical note is geared toward hardware Cisco Unified IP Phones but contains information that you might find useful for Cisco IP Communicator. It is available at this URL:

  http://www.cisco.com/en/US/products/hw/phones/ps379/products_tech_note09186a00800945bd.shtml

How to Use Diagnostic Tools

- Diagnosing Problems by Using the TAC Case Collection Tool, page 8-2
- Reporting Voice-Quality and Other Issues, page 8-2
- Capturing Logs Automatically When the Application Crashes, page 8-3
- Capturing Detailed Logs for Other Application Problems, page 8-4

Diagnosing Problems by Using the TAC Case Collection Tool

By using the Cisco Technical Assistance Center (TAC) Case Collection tool, you can interactively diagnose common problems involving hardware, configuration, and performance issues with solutions provided by Cisco TAC engineers.

Restrictions

This tool is available only to registered Cisco.com users with a Cisco service contract.

Procedure

Step 1 Log in to Cisco.com.

Step 2 Choose **Support > Tools and Resources**, and select **TAC Case Collection**.

Step 3 Select a technology or product area to begin troubleshooting.

For example, if you select **Voice**, you access a knowledge base for voice-over-data networks and IP telephony:

- Voice applications, Cisco Unified Communications Manager, Cisco Unity Connection, and so forth
- Voice quality (with diagnostic sound samples)
- Voice gateways
- Other voice-related issues

For more information, click the **TAC Case Collection** link at this URL:

http://www.cisco.com/public/support/tac/tools.shtml

Related Topics

- Reporting Voice-Quality and Other Issues, page 8-2
- Capturing Logs Automatically When the Application Crashes, page 8-3

Reporting Voice-Quality and Other Issues

The Quality Report Tool (QRT) is a voice-quality and general problem-reporting tool for Cisco IP Communicator and other Cisco Unified IP Phone devices. The QRT is installed as part of the Cisco Unified Communications Manager installation.

Restrictions

The QRT softkey is available only when Cisco IP Communicator is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

Procedure

Step 1 Configure Cisco IP Communicator to use with QRT so users can report problems with phone calls.

For details about QRT, see the *Cisco Unified Communications Manager Serviceability Administration Guide* and the *Cisco Unified Communications Manager Serviceability System Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Step 2 Tell users to report issues by clicking the QRT softkey and by choosing the appropriate problem category.

Feedback is logged in an XML file. Actual information logged depends on the user selection and whether the destination device is Cisco IP Communicator.

Related Topics

- Capturing Logs Automatically When the Application Crashes, page 8-3

Capturing Logs Automatically When the Application Crashes

If Cisco IP Communicator unexpectedly crashes, the Cisco Unified Problem Reporting Tool automatically collects installation, application, and client PC system information to automate the trace and crash-dump collection process on the client PC. It also creates a dump file.

Before You Begin

For users who roam from one computer to another, they must generate the problem report on the PC from which the problem occurred so that the correct logs are attached. By design, log files do not roam with a user from computer to computer.

Procedure

Step 1 Tell users to follow the troubleshooting instructions in the online help and in the user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

- Locate the automatically generated Zip file on their desktop.
- Send the Zip file from their desktop to you through e-mail.

Step 2 Provide the Zip file to the Cisco Technical Assistance Center (TAC) representative, if requested.

Troubleshooting Tips

If a blue screen failure occurs, the Cisco Unified Problem Reporting Tool might not generate an application crash dump even if the cause of the blue screen might be attributed to an interoperability issue between Cisco IP Communicator and the Windows OS.

Related Topics

- Capturing Detailed Logs for Other Application Problems, page 8-4

Capturing Detailed Logs for Other Application Problems

Sometimes, you need detailed log files to help troubleshoot problems with Cisco IP Communicator. Detailed logs have these characteristics:

- By default, detailed logging is enabled, and logs are collected at the verbose level.
- When enabled, detailed logging applies only to the client PC on which Cisco IP Communicator is running when users enabled it.

Procedure

Step 1 Verify detailed logging is enabled. Right click **Preferences > User** tab **> Enable Logging**) before launching the Problem Reporting Tool.

Step 2 If possible, restart Cisco IP Communicator to put the application in a known state and to provide accurate logs. If the problem is intermittent or unexpected, capture the logs without restarting the application.

Step 3 Recreate the problem, if possible.

Step 4 Manually launch the Problem Reporting Tool (**Start > All Programs > Cisco IP Communicator > Create CIPC Problem Report**) and send the report to you.

Step 5 Provide the Zip file to the Cisco Technical Assistance Center (TAC) representative, if requested.

Related Topics

- Reporting Voice-Quality and Other Issues, page 8-2

How to Resolve Installation Problems

- Not Enough Disk Space on Drive C, page 8-4
- Uninstall Does Not Remove All Files, page 8-5

Not Enough Disk Space on Drive C

Problem The user reports that there is not enough space on the C drive.

Solution Even if the TEMP variable is set to D:\temp, the installation program copies files by default in the C:\Program Files\InstallShield folder for repairing existing installations. Approximately 100 MB of additional space is required for the installation. To fix the problem, ask the user to free up additional space on the C drive.

Related Topics

- How to Resolve Startup Problems, page 8-5

Uninstall Does Not Remove All Files

Problem The user reports that the uninstall does not remove all files.

Solution The uninstall program does not remove files that are added or modified during runtime; you need to manually delete these files:

C:\Documents and Settings*username*\Application Data\Cisco\Communicator

Note that the Application Data folder is hidden.

Related Topics

- How to Resolve Startup Problems, page 8-5

How to Resolve Startup Problems

- Application Does Not Start Up Properly, page 8-5
- Application Startup is Unresponsive or Slow, page 8-6
- Error Messages “Registering” or “Defaulting to TFTP Server” Repeat, page 8-6
- Application Fails to Register and Shows the “Error DBConfig” Message, page 8-6
- Application Cannot Find the Network Interface Device or Shows the Wrong Extension Number, page 8-7

Application Does Not Start Up Properly

Problem The user reports that the application does not start up properly.

Solution After installing Cisco IP Communicator and adding it to Cisco Unified Communications Manager, Cisco IP Communicator should start up. If the application does not start up properly, try these solutions:

- Check network connectivity. If the network is down between Cisco IP Communicator and the TFTP server or Cisco Unified Communications Manager, Cisco IP Communicator cannot start up properly.
- Verify TFTP settings. Make sure that the correct TFTP settings are selected in Cisco IP Communicator (**right-click > Preferences > Network** tab). First-time remote users with a freshly installed application might not be able to use Cisco IP Communicator until specifying a TFTP address.
- Verify that the device name in Cisco IP Communicator (**right-click > Preferences > Network** tab) is correct and matches the device name specified in Cisco Unified Communications Manager.
- Verify that Cisco IP Communicator has been added to Cisco Unified Communications Manager.
- If Cisco IP Communicator is in the Cisco Unified Communications Manager database, and the criteria in the previous bullet points have been met, the device might experience startup problems if its configuration file is damaged. In this case, delete the device from the Cisco Unified Communications Manager database, make a copy of a configuration file for a functional device of the same type as the problematic device, and rename the file. Use the convention SEP*MAC_address*.cnf.xml, where *MAC_address* is the MAC address (or device name) of the deleted device. Replace the old configuration file with the new one, and add the device to the Cisco Unified Communications Manager database.

Related Topics

- How Cisco IP Communicator Interacts With the Network at Startup, page 1-5
- About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6

Application Startup is Unresponsive or Slow

Problem The user reports the Cisco IP Communicator startup seems unresponsive or slow.

Enable HTTP access to the Communicator folder on the TFTP server. To do this, run the Cisco IP Communicator Administration Tool, and select the option to enable HTTP access. Obtain the tool from the product software download web site: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661.

It is located inside the zipped folder with your build.

Related Topics

- Table 4-3 on page 4-12
- Resolving Audio IP Address Auto-Detection Problems, page 4-10

Error Messages "Registering" or "Defaulting to TFTP Server" Repeat

Problem The user reports that error messages *Registering* or *Defaulting to TFTP server* repeat, and lines never appear.

Solution Cisco IP Communicator is unable to contact the TFTP server. Try these solutions:

- Check network connectivity to the TFTP server. If you can ping the server, ensure that DHCP option 150 is correctly set.
- If you are not using DHCP in your network, make sure that the TFTP server address is specified in Cisco IP Communicator (**right-click > Preferences > Network** tab).
- Make sure remote users can establish network connectivity before launching Cisco IP Communicator.

Related Topics

- Status Messages Displayed, page 7-9

Application Fails to Register and Shows the "Error DBConfig" Message

Problem The user reports that Cisco IP Communicator fails to register and shows the error *Error DBConfig*.

Solution There is no device record for this Cisco IP Communicator device in Cisco Unified Communications Manager, or auto-registration is disabled. Try these solutions:

- Ensure that device record that you have created matches the device name chosen with Cisco IP Communicator (**right-click > Preferences > Network** tab).
- Ensure that the selected network adapter still exists in the computer (for example, ensure that a selected wireless card has not been removed).

- Ensure that Cisco IP Communicator is configured to use the correct TFTP server setting (**right-click > Preferences > Network** tab).

Related Topics

- Specifying a TFTP Server, page 4-6
- About Selecting a Device Name, page 4-7
- Status Messages Displayed, page 7-9

Application Cannot Find the Network Interface Device or Shows the Wrong Extension Number

Problem The user reports that Cisco IP Communicator cannot find the network interface device and prompts the user to re-insert it or choose a new one, or Cisco IP Communicator shows the wrong extension number at startup.

Solution Try these solutions:

- Ensure that the network interface chosen for Cisco IP Communicator (**right-click > Preferences > Network** tab **> Network Adapter**) is installed on the system.

  The network adapter setting allows Cisco IP Communicator to identify itself to the network; it is not used for audio transmission. For this reason, you do not need to change this setting once it is established unless you are permanently removing or disabling the selected network interface. In this case, select the new interface, re-administer the device in Cisco Unified Communications Manager administration, and delete the old device record.

- As a rule, users with laptops that use docking stations should undock before launching Cisco IP Communicator for the first time after installation.

Related Topics

- About Selecting a Device Name, page 4-7
- Status Messages Displayed, page 7-9
- How to Resolve Installation Problems, page 8-4

How to Resolve Security Problems

- LSC Does Not Install on the Client PC, page 8-7
- Message "Registration Rejected: Security Error" Appears on the Cisco IP Communicator Phone Screen, page 8-8
- Message "Configuring IP" Appears on the Cisco IP Communicator Phone Screen, page 8-9

LSC Does Not Install on the Client PC

Problem The LSC does not install on the client PC.

Solution The LSC should install on the client PC before Cisco IP Communicator registers with Cisco Unified Communications Manager. If this is not the case, perform these steps in Cisco Unified Communications Manager:

Procedure

Step 1 If Cisco IP Communicator does not register, verify the CAPF settings on the Phone Configuration page. Make sure that Certificate Operation is set to **Install/Upgrade** (not **No Pending**).

Step 2 For Cisco Unified Communications Manager Releases other than 4.x, click **Save**, and then click **Reset** to reset Cisco IP Communicator.

For Cisco Unified Communications Manager Release 4.x, click **Update**, and then click **Reset Phone** to reset Cisco IP Communicator.

Related Topics

- Status Messages Displayed, page 7-9

Message "Registration Rejected: Security Error" Appears on the Cisco IP Communicator Phone Screen

Problem The user reports that the message *Registration rejected: security error* appears on the Cisco IP Communicator phone screen.

Solution Complete this procedure:

Procedure

Step 1 Make sure the LSC is installed under the personal certificate store. From **Start > Run**, enter **certmgr.msc**.

Step 2 Select **Personal > Certificates**, and make sure the device name on the certificate matches the Cisco IP Communicator device name (**right-click > Preferences > Network** tab **> Device Name** section).

Step 3 For Cisco Unified Communications Manager Releases other than 4.x, on the Phone Configuration page, click **Reset** to clear the configuration cache on the TFTP server.

For Cisco Unified Communications Manager Release 4.x, on the Phone Configuration page, click **Reset Phone** to clear the configuration cache on the TFTP server.

Related Topics

- Status Messages Displayed, page 7-9

Message "Configuring IP" Appears on the Cisco IP Communicator Phone Screen

Problem The user reports that the message *Configuring IP* message appears on the Cisco IP Communicator phone screen.

Solution Complete this procedure:

Procedure

Step 1 In Cisco IP Communicator, verify that the CTL file downloaded. Choose **Settings > Security Configuration > CTL File**. The display should show a string of 32 hexadecimal digits (instead of showing *Not Installed*).

Step 2 In Cisco IP Communicator, make sure that the correct Cisco Unified Communications Manager is listed under the CTL File menu. Choose **Settings > Security Configuration > CTL File**, and click **Select**.

Related Topics

- Status Messages Displayed, page 7-9

How to Resolve Voice-Quality Issues

- Poor Audio Quality When Calling Digital Cell Phones Using a Low-Bandwidth Codec, page 8-10
- Codec Mismatch Between Cisco IP Communicator and Another Device, page 8-10
- Sound Sample Mismatch Between Cisco IP Communicator and Another Device, page 8-10
- Gaps in Voice Calls, page 8-10
- User Cannot Hear Audio or Dial Tone, page 8-10
- One-Way Audio Problems, page 8-11
- Echo Problems, page 8-11
- Voice of Remote Party Is Disrupted, page 8-12
- Remote Party Hears Distorted Or Robotic Audio or Background Noise, page 8-12
- Voice Quality is Degraded, page 8-13

Poor Audio Quality When Calling Digital Cell Phones Using a Low-Bandwidth Codec

Problem The user reports poor quality when calling digital cell phones using a low-bandwidth codec.

Solution When the user chooses to use low bandwidth, calls between Cisco IP Communicator and a digital cellular phone might have poor voice quality. Use the low-bandwidth setting only when absolutely necessary.

Codec Mismatch Between Cisco IP Communicator and Another Device

Problem A codec mismatch occurred between Cisco IP Communicator and another device.

Solution The RxType and the TxType statistics show the codec that is being used for a codec conversation between this IP device and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation or that a transcoder is in place to handle the service.

Related Topics

- Call Statistic Information, page 7-13

Sound Sample Mismatch Between Cisco IP Communicator and Another Device

Problem A sound sample mismatch occurred between Cisco IP Communicator and another device.

Solution The RxSize and the TxSize statistics show the size of the voice packets that is being used in a conversation between this IP device and the other device. The values of these statistics should match.

Related Topics

- Call Statistic Information, page 7-13

Gaps in Voice Calls

Problem The user reports that there are gaps in voice calls.

Solution Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity.

Related Topics

- Call Statistic Information, page 7-13

User Cannot Hear Audio or Dial Tone

Problem The user reports that there is no audio, not even a dial tone.

Solution See the troubleshooting section of the Cisco IP Communicator user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

One-Way Audio Problems

Problem The user reports one-way audio problems.

Solution If the remote party cannot hear the person who placed the call on a Cisco IP Communicator, it might be for one of these reasons:

- The Cisco IP Communicator party has muted the recording device.
- The Cisco IP Communicator party has plugged the headset and speaker plugs into the wrong ports on the PC.
- The Cisco IP Communicator party is running another application that is using the microphone, such as a sound recorder or another software-based phone.
- The Cisco IP Communicator audio settings are incorrect. See the *User Guide for Cisco IP Communicator* for more information.

If the Cisco IP Communicator party cannot hear the remote party, it might be for these reasons:

- The Cisco IP Communicator user is relying on a unsupported VPN. To resolve the issue, you must set up a web reflector page or manually specify the IP address in the Network Audio Settings window (**right-click > Audio** tab **> Network** button).
- The Cisco IP Communicator user is relying on a unsupported VPN, and Cisco IP Communicator is integrated with a Linux-based Cisco Unified Communications Manager (Releases other than 4.x). To resolve this issue, run the Cisco IP Communicator Administration Tool on a Windows server to resolve the audio IP address auto-detection problem.
- If Cisco IP Communicator is behind a firewall, make sure that the firewall is configured to pass TFTP and RTP traffic by using the appropriate port range.

Tip In cases of occasional one-way audio, try holding and resuming the call while the symptom is occurring. This can resolve the problem.

Related Topics

- Supported Software VPN Clients, page 4-9
- About Audio IP Address Auto-Detection Problems, page 4-9
- Resolving Audio IP Address Auto-Detection Problems, page 4-10
- Selections for Audio Port Range, page 4-11

Echo Problems

Problem The user reports hearing echoes during calls with Cisco IP Communicator.

Solution If the local or remote user hears echo, see the troubleshooting section of the Cisco IP Communicator user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

Voice of Remote Party Is Disrupted

Problem The user reports that the voice of the remote party is disrupted by unintended silences or sounds jittery.

Solution Try these solutions:

- Close any unnecessary applications. Be aware that launching applications and performing network-intensive tasks, such as sending e-mail, might affect audio quality.
- Occasional pops, clicks, or broken audio might occur if the network is experiencing congestion or data traffic problems.
- If the user is using Cisco IP Communicator over a remote connection (for example, on a VPN connection from home or a hotel), voice quality is probably suffering from insufficient bandwidth. Enable the Optimize for Low Bandwidth feature (**right-click > Preferences > Audio** tab). If the problem persists, verify that sound cards and audio drivers are correctly installed on client PCs.

Remote Party Hears Distorted Or Robotic Audio or Background Noise

Problem The remote party hears distorted or robotic audio, background noise, or inconsistent volume levels.

Solution The volume slider in Cisco IP Communicator might be set too high. This can cause various kinds of problems, including robotic transmitted audio, background noise, and sometimes changing volume levels in received audio.

Procedure

Step 1 Test the volume level of Cisco IP Communicator for each audio mode (handset mode, speakerphone mode, or headset mode) by going off-hook with each mode. (To test handset mode, lift the handset. To test speakerphone or headset mode, make sure that only the speakerphone or headset button is lit.)

Step 2 Once you hear a dial tone, click the volume button in the main interface. A volume slider appears above the volume button. If the position of the slider is not in the middle of the range, press the volume button to reposition the slider so that the volume level is near the middle of the range.

Step 3 Repeat steps 1 and 2 for each audio mode.

Step 4 Run the Audio Tuning Wizard (**right-click > Audio Tuning Wizard**) to verify that the sound levels are satisfactory.

Step 5 If the problem is not volume related, suppress background noise. Enable noise suppression or increase the noise suppression aggressiveness level (**right-click > Preferences > Audio** tab **> Advanced** button). Noise suppression is applied to the microphone (input device) to prevent the transmission of noise to the remote end.

Voice Quality is Degraded

Problem The user reports voice quality is degraded when Cisco IP Communicator is used while Windows is starting up.

Solution Verify that Windows has completed its startup process and that no other applications are still loading before using Cisco IP Communicator.

Problem The user reports voice quality is degraded when workstation physical memory becomes low.

Solution Cisco IP Communicator is recommended to operate with approximately 60MB of available physical memory - this is different from minimum required workstation memory as other applications will be consuming workstation memory. By ensuring other applications - including the operating system - have left enough available memory for Cisco IP Communicator will reduce sound distortions based on low-available RAM conditions. If users experience this condition, you may want to have them close some applications when running Cisco IP Communicator or increase the RAM in their system.

Problem The user reports voice quality is degraded when using Cisco IP Communicator with other applications that consume available bandwidth.

Solution Minimize the use of applications that consume large amounts of bandwidth (examples: applications that transfer large files, send or receive video, perform “screen sharing” operations, etc.) while on an active call.

Problem The user reports voice quality is degraded when the laptop is physically moved.

Solution Some computer manufacturers have introduced a feature called “HDD Protection” which prevents damage to the computer's hard drive when the laptop experiences movement. This feature may also temporarily affect applications which are currently running on the workstation. The recommendation is to not physically move a computer enabled with this feature while on an active call.

How to Resolve General Application Problems

Application Resets Unexpectedly

Problem The user reports that the application resets unexpectedly.

Solution Cisco IP Communicator resets when it loses contact with the Cisco Unified Communications Manager server. This lost connection can be caused by these conditions:

- Any network connectivity disruption such as cable breaks, switch outages, and switch reboots.
- Roaming out of range while using a wireless network connection.
- Another system administrator with access to Cisco Unified Communications Manager might have intentionally reset the devices.

Application is Slow to Load

Problem The user reports the Cisco IP Communicator is slow to load.

Solution Verify that the desktop system where Cisco IP Communicator is installed is in same domain as Cisco Unified Communications Manager. You can also verify that the desktop system where Cisco IP Communicator is installed can resolve Cisco Unified Communications Manager by both FQDN and by name.

If the desktop where Cisco IP Communicator is installed cannot resolve Cisco Unified Communications Manager by name, go to Control Panel > Network Connections> choose your network connection -> Properties -> Internet Protocol (TCP/IP) -> Properties -> Advanced -> DNS -> Append These DNS Suffixes. Add a suffix that corresponds to the Cisco Unified Communications Manager suffix in the DNS entry.

Digits Are Not Recognized By the Application

Problem The user reports that when trying to make a call, digits are not recognized by the application.

Solution The user is experiencing DTMF delay and should enter the digits more slowly.

Degraded Application Performance

Problem Users complain of degraded application performance when Cisco IP Communicator and other applications are running.

Solution Assess the CPU usage under these conditions by using the Windows Performance Tool.

Related Topics

- Setting Up and Running the Windows XP Performance Tool, page 7-20
- Setting Up and Running the Windows Vista Performance Tool, page 7-21

Quick Search Does Not Work

Problem The user reports that Quick Search does not work.

Solution If you want to configure Quick Search to work with an external directory, you cannot use the Directory Wizard. Instead you must create a custom configuration file. The user might need to enter credential information.

Quick Search of the Personal Address Book is not supported with all Cisco Unified Communications Manager releases.

Solution Cisco IP Communicator cannot read the user information if anonymous bind is disabled in the Active Directory. Anonymous bind is disabled by default. For Cisco IP Communicator to download the user information for quick search you must enable the anonymous bind in Active Directory.

Related Topics

- How to Configure Quick Search, page 5-15
- Configuring Quick Search Manually with Windows-Based Cisco Unified Communications Managers, page 5-17

Build Versions in the About Window Vary

Problem Build version numbers that are listed in the Cisco IP Communicator About window vary by software component.

Solution This is a normal outcome of installing or upgrading the application and does not indicate a problem with the installation or upgrade process.

To view build versions for software components, **right-click > About Cisco IP Communicator**. Build versions are listed in the right column.

APPENDIX A

Providing Information to Users About Cisco IP Communicator

Revised: 1/19/11

As the system administrator, you are likely the primary source of information for Cisco IP Communicator users in your network or company. It is important to provide current and thorough information to users. We recommend that you create a web page on your internal support site that provides users with important information about Cisco IP Communicator. Table A-1 lists the information.

Table A-1 Information Needed By Users

Provide This Information	Explanation
Location of the Microsoft hotfix for USB audio devices.	Leverage information from the release notes at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html
List of supported audio devices (USB headsets and handsets).	Leverage information from the release notes at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html
Installation link (or executable file) for Cisco IP Communicator.	Depends on the deployment method. For details, see Deployment Methods, page 3-3.
Information needed to complete application configuration tasks.	Provide this information: • Which network adapter the user should select or which device name to enter (**right-click > Preferences > Network** tab). For details, see About Selecting a Device Name, page 4-7. • Which TFTP servers to use (supply IP addresses for **right-click > Preferences > Network** tab). For details, see Specifying a TFTP Server, page 4-6. • If you added devices to Cisco Unified Communications Manager with auto-registration through TAPS[1], provide the TAPS directory number to the user to dial. For details, see About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6.

Table A-1 Information Needed By Users (continued)

Provide This Information	Explanation
Cisco Unified Communications Manager username and password.	Tell users to enter this information when they access their User Options web pages from Cisco IP Communicator (**right-click > Cisco User Options**) unless you disabled access to the options through the Settings button in Cisco Unified Communications Manager Administration. For details, see Specifying a TFTP Server, page 4-6. Access to the User Options web pages enables users to subscribe to phone services and set up speed dialing, for example. You created the user accounts when you associated users with device IDs in Cisco Unified Communications Manager. For details, see Configuration and Deployment Checklist, page 2-2.
Directory username and password (if required; depends on how you responded to user authentication prompts in the Directory Wizard). For users who want to synchronize with Microsoft Outlook, provide the Cisco Unified IP Phone Address Book Synchronizer utility, and tell them to install it.	Tell users to enter their username and password information in Cisco IP Communicator (**right-click > Preferences > Directories** tab). For details, see this information: • Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers, page 5-18 • Configuring Quick Search to Access a Personal Address Book with Windows-Based Cisco Unified Communications Managers, page 5-20 For details about configuring and using a personal directory, provide to users the *Customizing Your Cisco Unified IP Phone on the Web* at this URL: http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html

Table A-1 Information Needed By Users (continued)

Provide This Information	Explanation
List of supported features that you configured in Cisco Unified Communications Manager Administration.	For details, see Telephony Features Available for Cisco IP Communicator, page 5-2. For example, provide information if these features are configured: • Auto answer—Causes the speakerphone or headset to automatically go off-hook when an incoming call is received. Inform users who receive a high volume of incoming calls or handle calls on behalf of others that this feature is enabled for them. • Call forwarding restrictions (if any)—you might restrict the call forwarding feature to numbers within your company. • Call park—Allows a user to place a call on hold so it can be retrieved from another phone in the system. Provide users with the call park extension so that the call can be retrieved. Tell users the amount of time to retrieve the parked call. • Call pickup group—Allows users to pick up incoming calls outside of their own group. Provide users with the call group pickup number. • CMC[2] or FAC[3]—CMC enables a user to specify that a call relates to a specific client matter, and FAC controls the types of calls that certain users can place. Provide users with the codes when placing a call using a billing or tracking code. • Meet-me conference—Enables other callers to join in a conference. Provide users with the Meet-me phone number. • MLPP[4]—Allows properly validated users to place priority calls. Provide users with the MLPP access number. Also provide a list of corresponding precedence numbers so that users can select the priority (precedence) level for an outgoing call.
Whether video calls are supported.	• Provide supported camera and installation information. For details about supported cameras, supported Cisco Unified Communications Manager releases, and supported Cisco Unified Video Advantage releases, see the release notes at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html • Provide the quick start and user guide at these URLs: – http://www.cisco.com/en/US/products/sw/voicesw/ps5662/prod_installation_guides_list.html – http://www.cisco.com/en/US/products/sw/voicesw/ps5662/products_user_guide_list.html

Table A-1 Information Needed By Users (continued)

Provide This Information	Explanation
Instructions for accessing a voice messaging system.	Provide this information to users: • How to access the voice messaging system account. Make sure you have configured the Cisco IP Communicator Messages button. • Initial password for accessing the voice messaging system. Make sure you have configured a default voice messaging system password for all users. • How Cisco IP Communicator shows that voice messages are waiting. Make sure that you used Cisco Unified Communications Manager Administration to set up a message waiting indicator method. For details, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
Instructions for installing, setting up, and using the application.	Provide the user guide for Cisco IP Communicator. http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html Direct users to read the introduction chapter for the installation and set-up information. Remind users to use the online help that is embedded in the application Access it through the ? button on the Cisco IP Communicator interface, through the menu button, or by accessing the right-click menu.
Internal company support for the application.	Provide users with the names of people to contact for assistance and the instructions for contacting those people.
Information about how to report problems with Cisco IP Communicator.	Tell users about these embedded tools: • QRT—how and when to use it. For details, see Reporting Voice-Quality and Other Issues, page 8-2. • Problem Reporting Tool and enable logging—how and when to use them. For details, see Capturing Logs Automatically When the Application Crashes, page 8-3.

[1] TAPS = Tool for Auto-Registered Phones Support

[2] CMC = client matter code

[3] FAC = forced authorization code

[4] MLPP = Multilevel Precedence and Preemption