



CHAPTER 2

Preparing to Deploy Cisco IP Communicator

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.

- [Network, Server, and Client PC Requirements, page 2-1](#)
- [Configuration and Deployment Checklist, page 2-2](#)
- [About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6](#)
- [Configuring Cisco IP Communicator for Adjunct Licensing, page 2-9](#)
- [How to Configure Cisco IP Communicator with Different Protocols, page 2-9](#)
- [How to Configure Security Features for Cisco IP Communicator, page 2-12](#)



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		
<ol style="list-style-type: none"> For each device, gather this information: <ul style="list-style-type: none"> • 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) 	<p>Optional. Use this information to configure devices in Cisco Unified Communications Manager Administration.</p> <p>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.</p>	<ul style="list-style-type: none"> • Configuring Features and Services for Cisco IP Communicator, page 5-1 • <i>Cisco Unified Communications Manager System Guide</i> • <i>Cisco Unified Communications Manager Administration Guide</i>
<ol style="list-style-type: none"> Decide on the method for adding devices to the Cisco Unified Communications Manager database (see the far right column for details): <ul style="list-style-type: none"> • Auto-registration • Cisco Unified Communications Manager Administration only • BAT¹ only • BAT and TAPS² 	<p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> • About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6 • <i>Cisco Unified Communications Manager Administration Guide</i> • <i>Bulk Administration Tool User Guide</i>

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.	<ul style="list-style-type: none"> • 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 soft-phone device with a primary device and consumes only one device license per device in Cisco Unified Communications Manager Release 6.0(1) and later.	<ul style="list-style-type: none"> • 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. When you install Cisco IP Communicator for the first time, it is set for SCCP by default.	<ul style="list-style-type: none"> • How to Configure Cisco IP Communicator with Different Protocols, 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. Also prevents call signaling tampering	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Configuring Features and Services for Cisco IP Communicator, page 5-1 • <i>Cisco Unified Communications Manager Administration Guide</i> • <i>Cisco Unified Communications Manager Features and Services Guide</i>
2. Make Cisco IP Communicator available in languages other than English.	<p>As needed. All languages might not be immediately available. Check the website for updates.</p> <p>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.</p>	<ul style="list-style-type: none"> • <i>Using the Cisco IP Telephony Locale Installer</i> at this URL: http://www.cisco.com/en/US/products/sw/voicew/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.	<ul style="list-style-type: none"> • About Modifying Phone Button Templates, page 5-6 • About Configuring Softkey Templates, page 5-7
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.	<ul style="list-style-type: none"> • Setting Up Services, page 5-7 • <i>Cisco Unified Communications Manager Administration Guide</i> • <i>Cisco Unified Communications Manager Features and Services Guide</i>
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.	<ul style="list-style-type: none"> • Resolving Audio IP Address Auto-Detection Problems, page 4-10 • Modifications for Remote Use, page 4-12 • About Configuring Corporate and Personal Directories, page 5-8
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).	<ul style="list-style-type: none"> • About Configuring Corporate and Personal Directories, page 5-8 • <i>Cisco Unified Communications Manager Administration Guide</i>

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).	<ul style="list-style-type: none"> • About Adding Users to Cisco Unified Communications Manager, page 5-1 • <i>Cisco Unified Communications Manager Administration Guide</i> • <i>Bulk Administration Tool User Guide</i>
Deploying and configuring Cisco IP Communicator		
1. Decide on the method for deploying Cisco IP Communicator: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 Release 5.x and later (or **Device > Add a New Device** in Cisco Unified Communications Manager Administration Release 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 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 Release 6.0(1), you can associate a secondary soft-phone 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 soft-phone devices to a primary phone.
 - You cannot delete the primary phone unless you remove the associated secondary soft-phone devices.
 - The primary phone must be the device that consumes the most licenses. You cannot make the soft-phone device the primary phone and associate a Cisco Unified IP Phone as the secondary device.
 - Secondary soft-phone 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 soft-phone device name.
 - Step 3** On the Phone Configuration window, configure all required fields for your environment.
 - Step 4** For Primary. Phone, select the device name of the Cisco Unified IP Phone to associate with Cisco IP Communicator.
 - Step 5** Click **Save**.
-

How to Configure Cisco IP Communicator with Different Protocols

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 Take 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* (Release 5.x and later) and 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

Step 2 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](#)
- [About 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 that is in use in your network from SCCP to SIP.

Procedure

-
- Step 1** To access BAT, choose **Bulk Administration > Phones > Migrate Phones > SCCP to SIP**.
- Step 2** Migrating phones by following the *Bulk Administration Tool User Guide* (Release 5.x and later) 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* (Release 5.x and later) 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 Auto Registration parameter is SCCP, perform this procedure:

Procedure

-
- Step 1** Choose **System > Enterprise Parameters**, and set the Auto Registration Phone Protocol parameter to **SCCP**.
- Step 2** Install the Cisco IP Communicators.
- Step 3** Change the Auto Registration Phone Protocol parameter to **SIP**.
- Step 4** Auto-register the Cisco IP Communicators.
-

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.

Restriction

The device name feature is supported in Cisco Unified Communications Manager Release 5.x and later.

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. 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 Authenticated Phone Calls, page 2-14](#)
- [Security Restrictions for Barging into an Authenticated Call, page 2-14](#)
- [Configuring Security by Using Cisco Unified Communications Manager Release 4.X, page 2-15](#)
- [Configuring Security by Using Cisco Unified Communications Manager Release 5.X and Later, page 2-16](#)
- [Authentication Mode Settings, page 2-17](#)
- [Verifying the Security Configuration, page 2-18](#)

- [How to Unlock Options to Make Configuration Changes](#), page 2-18
- [Where to Find Additional Security Information](#), page 2-19

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 <i>.sbn</i> 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 plugin from Cisco Unified Communications Manager Administration.
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
Security profiles	<p>Defines whether Cisco IP Communicator is nonsecure or authenticated. To view the security profile name, choose Settings > Security Configuration from the Cisco IP Communicator interface.</p> <p>See the <i>Cisco Unified Communications Manager Security Guide</i> at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html</p>
Disabling settings access	<p>Disables local access to network and other settings for Cisco IP Communicator from the Cisco Unified Communications Manager Administration Phone Configuration window.</p> <p>See the “About Disabling Local Settings Access” section on page 4-13.</p>

**Note**

In Cisco IP Communicator Release 2.1(1), encryption is not supported.

Related Topics

- [Identification of Authenticated Phone Calls, page 2-14](#)
- [Security Restrictions for Barging into an Authenticated Call, page 2-14](#)
- [How to Configure Security Features for Cisco IP Communicator, page 2-12](#)

Identification of Authenticated Phone Calls

When you implement security for Cisco IP Communicator, you can identify 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:

**Related Topic**

- [Security Restrictions for Barging into an Authenticated Call, page 2-14](#)

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 by Using 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 **Authenticated**.
 - 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 **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 2-4 on page 2-17](#).
 - 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 2-18](#)
- [How to Unlock Options to Make Configuration Changes, page 2-18](#)
- [How to Resolve Security Problems, page 8-8](#)

Configuring Security by Using Cisco Unified Communications Manager Release 5.X and Later

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 **Authenticated**.
If SIP is the profile protocol, the Transport Type field automatically selects **TCP** for Non Secure and **TLS** for Authenticated.
 - 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 2-4 on page 2-17](#).
 - 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 2-18](#)
- [How to Unlock Options to Make Configuration Changes, page 2-18](#)
- [How to Resolve Security Problems, page 8-8](#)

Authentication Mode Settings

Table 2-4 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**. Make sure that the Security Mode displays *Authenticate* 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 2-18](#)
- [Erasing the CTL File, page 2-19](#)

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 2-5 shows where you can find additional information about security.

Table 2-5 Cisco IP Communicator and Cisco Unified Communications Manager Security Topics

Topic	See...
Detailed explanation of security, including set up, configuration, and troubleshooting information	<i>Cisco Unified Communications Manager Security Guide</i> 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 1-7
TLS connection	Supported Networking Protocols, page 1-2 About Configuration Files, page 1-7
CallManager Configuration Menu security icons for the CallManager 1 through CallManager 5	Device Configuration Information, page 7-2

Table 2-5 *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 8-8 <i>Cisco Unified Communications Manager Security Guide</i> http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html