# Cisco Unified IP Phone Setup

This chapter provides information about working with and configuring Cisco Unified IP Phones in Cisco Unified Communications Manager Administration.



# About Cisco Unified IP Phones and Device Setup

Cisco Unified IP Phones are full-featured telephones that you can connect directly to your IP network. Use the Cisco Unified Communications Manager Administration Phone Configuration window to configure the following Cisco Unified IP Phones and devices:

- Cisco Unified IP Phone 7900 family for both SCCP and SIP
- Cisco Unified IP Phone 9951 or 9971

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 6900 family.
- Cisco IP Video Phone 7985
- Cisco Unified IP SIP Phone 3911
- Cisco IP Phone 30 VIP and Cisco IP Phone 30 SP+
- Cisco IP Phone 12 S, Cisco IP Phone 12 SP, Cisco IP Phone 12 SP+
- H.323 clients
- Computer Telephony Integration (CTI) ports

  Be aware that CTI ports may not be associated with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, that DN cannot get associated with a CTI port that you configure with the Phone Configuration window.
- Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator
- Cisco ATA 186 Analog Telephone Adaptor
- Third-party SIP Device (Basic) and (Advanced)
- IP-STE
- Cisco VG248 and VG224 ports (analog phones)

  You configure the Cisco VG248 and VG224 analog phone gateways from the Gateway Configuration window of Cisco Unified Communications Manager Administration. From this window, you configure the gateway analog phone ports (doing this takes you to the Phone Configuration window). When you want to update the VG248 and VG224 ports, use the Phone Configuration window.

See topics related to the Cisco Unified IP Phones in the *Cisco Unified Communications Manager System Guide* lists the configuration steps for Cisco Unified IP Phones that support SIP.

# Phone Setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Phone** menu path to configure phones.

### Finding Phones Tips

The Cisco VG248 and VG224 Analog Phone Gateways will not display when you search for phones. You can search for the Cisco VG248 and VG224 Analog Phone ports from the Find and List Phones window of Cisco Unified Communications Manager Administration.

**Tip** For methods to limit your search, see the related topics section and the *Cisco Unified Communications Manager System Guide*.

**Tip** After you configure the phone in Cisco Unified Communications Manager Administration, you can view the IP address for the phone in the Find and List Phones window. For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the window. For phones with an IPv6 address only, the IP Address displays as 0.0.0.0 in the IP Address column in the Find and List Phones window. To identify the IPv6 address for the phone, click the Device Name link in the Find and List Phones window, which causes the Phone Configuration window to display. For the IPv6 Only device, the Phone Configuration window displays an IPv4 address of 0.0.0.0, listed as IP Address, above the IPv6 address.

### Phone Configuration Tips

When you add a new phone, you can choose a phone template that was created by the Bulk Administration Tool to configure automatically some of the phone configuration settings, based on the template.

For each phone device type, the Phone Configuration window displays either Device is trusted or Device is not trusted, along with a corresponding icon. The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

**Note** The Product-Specific Configuration section contains model-specific fields that the phone manufacturer defines. Cisco Unified Communications Manager dynamically populates the fields with default values.

To view field descriptions and help for product-specific configuration items, click the "?" question icon in the Product Specific Configuration area to display help in a popup window.

If you need more information, see the documentation for the specific phone that you are configuring or contact the manufacturer.

Select the "Override Common Settings" box for any corresponding setting in the Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.

### Phone Reset Tips

For instructions on how to reset a phone, see the descriptions of the Reset Selected and Reset buttons.

You do not have to reset a Cisco Unified IP Phone after you add a directory number or update its settings for your changes to take effect. Cisco Unified Communications Manager automatically performs the reset. Phones that have a shared line may reset when the shared directory number is added to another phone, or when those directory number settings are updated. You can reset a Cisco Unified IP Phone at any time by using the following procedure.

**Note** If a call is in progress, the phone does not reset until the call completes.

For all SIP endpoints, **Apply Config** is triggered automatically just after updating or saving Phone Product Specific Configuration.

You can also updating the phone with the latest configuration changes by using the least-intrusive method.

# Phone Deletion Preparation

Before you delete the phone, determine whether the directory number that is associated with the phone needs to be removed or deleted. To remove the directory number before deleting the phone; otherwise, the directory number remains in the Cisco Unified Communications Manager database when the phone gets deleted.

You can view the directory numbers that are assigned to the phone from the Association Information area of the Phone Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the Phone Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records.

# Phone Settings

| Field | Description |
|---|---|
| Device Information | |
| Active Load ID | This field displays the name of the active firmware load if the Cisco Unified IP Phone has registered with Cisco Unified Communications Manager.<br><br>In some cases, the Active Load ID field displays “Unknown.” For example, Cisco Unified Communications Manager Administration might display “Unknown” in the Active Load ID field for any of the following circumstances:<br><br>• For SCCP phones, when the phone is a Cisco Unified IP Phone 7940 (SCCP), 7960 (SCCP), or 7985 (SCCP), because these phone models do not support the necessary version of SCCP.<br>• For SCCP and SIP phones, when the phone is any third-party phone.<br>• When Cisco Unified Communications Manager cannot determine the status of the phone. |
| Device is Active | The Device Is Active message in the Phone Configuration window in Cisco Unified Communications Manager Administration displays when a phone consumes device license units and when a phone can register with Cisco Unified CM.<br><br>For a phone that uses a real MAC address, not the dummy MAC address that is created via BAT, the Device Is Active message displays, which indicates that the phone uses device license units and can register with Cisco Unified Communications Manager.<br><br>For a phone that uses the dummy MAC address that is created via BAT, the Device Is Active message does not display. If you manually convert the dummy MAC address to a real MAC address in the Phone Configuration window, the Device Is Active message displays after you save the configuration; this ensures that the phone can register with Cisco Unified Communications Manager and that licensing consumes device license units for the phone. |

| Field | Description |
|---|---|
| Device Trust Mode | Select whether the device is trusted or not trusted. You can configure this setting for analog phones using SCCP, and for some third-party endpoints. |
| MAC Address | Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones (hardware phones only). Make sure that the value comprises 12 hexadecimal characters.<br><br>For information on how to access the MAC address for your phone, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model.<br><br>Cisco VG248 Analog Phone Gateway:<br><br>The MAC address for the Cisco VG248 gateway specifies the endpoint from the Gateway Configuration window of Cisco Unified Communications Manager Administration.<br><br>Only one MAC address exists for the Cisco VG248 Analog Phone Gateway. All 48 ports share the same MAC address. Cisco Unified CM requires unique MAC addresses for all devices.<br><br>Cisco Unified Communications Manager converts the MAC address for each device by<br><br>• Dropping the first two digits of the MAC address<br>• Shifting the MAC address two places to the left<br>• Adding the two-digit port number to the end of the MAC address (to the right of the number)<br><br>`EXAMPLEMAC Address for the Cisco VG248 is 000039A44218 the MAC address for registered port 12 in the Cisco Unified Communications Manager is0039A4421812`<br><br>Cisco VG224 Analog Phone Gateway:<br><br>You can configure a Cisco VG224 gateway as an MGCP gateway or an SCCP gateway. When it is configured as an SCCP gateway, it can have 24 analog phone endpoints. When it is configured this way, it functions similarly to an IOS SCCP gateway. The MAC address for each individual phone gets calculated by using a formula that considers the slot position, subunit, port, and the last 10 characters of the original MAC address. |

| Field | Description |
|---|---|
| Device Name | Enter a name to identify software-based telephones, H.323 clients, and CTI ports.<br><br>For device names that are not based on a MAC address, as a general rule, you can enter 1 to 15 characters comprised of alphanumeric characters (a-z, A-D, 0-9). In most cases you can also use dot (.), dash (-), and underscore (_).<br><br>**Tip** Because the rules for the device name field depend on the device type, Cisco recommends that you see the product documentation to determine which character set is valid for your device, as well as the number of characters allowed. For example, when you configure the device name for the Cisco Unified Personal Communicator, make sure that the name starts with UPC.<br><br>**Note** For Cisco Spark Remote Devices (Cisco Spark-RDs), you can enter 1 to 32 characters comprising of alphanumeric characters like a-z, A-D, 0-9 and the following special characters: dot (.), dash (-), and underscore (_).<br><br>**Note** Ensure that the device name of a Cisco Unified Mobile Communicator does not exceed 15 characters. If the device name of a Cisco Unified Mobile Communicator exceeds 15 characters, migration of this device will fail upon upgrade to a different release of Cisco Unified Communications Manager. If an existing Cisco Unified Mobile Communicator device name specifies a longer name, shorten the device name to 15 or fewer characters.<br><br>Cisco Unified Mobile Communicator supports dual mode phones. The preceding limit of 15 characters also applies to Cisco Unified Mobile Communicator dual mode. When the MI for a dual mode phone is longer than 15 characters, the cellular network rejects the phone registration. |
| Description | Identify the purpose of the device. You can enter the user name (such as John Smith) or the phone location (such as Lobby) in this field.<br><br>For Cisco VG248 gateways, begin the description with **VGC<mac address>**.<br><br>The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). |
| Device Pool | Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template. |
| Common Device Configuration | Choose the common device configuration to which you want this phone assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure the common device in the Common Device Configuration window.<br><br>To see the common device configuration settings, click the View Details link. |

| Field | Description |
|---|---|
| Phone Button Template | Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.<br>Cisco Unified CM does not make this field available for H.323 clients or CTI ports. |
| Saving or Applying a configuration change | The following icons and buttons are found in the Configuration windows of the Cisco Unified Communications Manager Administration GUI to Save or Apply configuration changes:<br>• Save—Saves the current record.<br>• Reset—Opens a popup window that offers the following choices:<br>  • Reset—Shuts down the device and then restarts it.<br>  • Restart—Restarts the device without shutting it down.<br>  • Close—Closes the popup window without taking any action.<br>• Apply Config—When you change the configuration settings of a record, you may receive a message that directs you to click the **Apply Config** button to have the changes take effect. When you click the **Apply Config** button, a popup window advises of the possible actions that will take place when you click **OK**. |
| Softkey Template | Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template. |
| Common Phone Profile | From the drop-down list box, choose a common phone profile from the list of available common phone profiles. |
| Calling Search Space | From the drop-down list box, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS.<br>**Note** When set to <none>, Unified CM uses the device mobility calling search space, which is configured on the device pool. |
| AAR Calling Search Space | Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. |

| Field | Description |
|---|---|
| Media Resource Group List | Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List.<br><br>If you choose <None>, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool. |
| User Hold MOH Audio Source | To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays.<br><br>If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.<br><br>**Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**. |
| Network Hold MOH Audio Source | To specify the audio source that is played when the network initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays.<br><br>If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.<br><br>**Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**. |
| Location | Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location.<br><br>From the drop-down list box, choose the appropriate location for this Cisco Unified IP Phone.<br><br>A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this Cisco Unified IP Phone consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.<br><br>To configure a new location, use the **System** > **Location** menu option. |
| AAR Group | Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line. |

| Field | Description |
|---|---|
| User Locale | From the drop-down list box, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information to support users, including language and font.<br><br>Cisco Unified CM makes this field available only for phone models that support localization.<br><br>**Note** If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the common device configurations.<br><br>If the users require that information be displayed (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the Cisco Unified Communications Manager Locale Installer documentation. |
| Network Locale | From the drop-down list box, choose the locale that is associated with the phone. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses.<br><br>Cisco Unified CM makes this field available only for phone models that support localization.<br><br>**Note** If no network locale is specified, Cisco Unified CM uses the network locale that is associated with the device pool.<br><br>If users require that country-specific tones be played (on the phone), verify that the locale is installed before configuring the network locale. See the *Cisco Unified Communications Manager* Locale Installer documentation. |
| Built In Bridge | Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list box (choose On, Off, or Default).<br><br>**Note** Cisco Unified IP Phones 7940 and 7960 cannot support two media stream encryptions or SRTP streams simultaneously. To prevent instability due to this condition, the system automatically disables the built-in bridge for 7940 and 7960 phones when the device security mode is set to encrypted. |
| Privacy | For each phone that wants Privacy, choose On in the Privacy drop-down list box. |

| Field | Description |
|---|---|
| Device Mobility Mode | From the drop-down list box, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device.<br>Click View Current Device Mobility Settings to display the current values of these device mobility parameters:<br>• Cisco Unified Communications Manager Group<br>• Roaming Device Pool<br>• Location<br>• Region<br>• Network Locale<br>• AAR Group<br>• AAR Calling Search Space<br>• Device Calling Search Space<br>• Media Resource Group List<br>• SRST |
| Wireless LAN Profile Group | Select a wireless LAN profile group from the drop-down list box. You may also click **View Details** to display the settings for this wireless LAN profile group.<br>**Note** You can specify the Wireless LAN Profile Group at the Device Pool level or the individual phone level.<br>**Note** This field does not apply to all phone models. |
| Wi-Fi Hotspot Profile | Select a Wi-Fi Hotspot Profile from the drop-down list box. You may also click **View Details** to display the settings for this Wi-Fi Hotspot Profile.<br>**Note** This field does not apply to all phone models. |
| Signaling Port | This field applies only to H.323 devices. The value designates the H.225 signaling port that this device uses.<br>Default value specifies 1720. Valid values range from 1 to 65535. |
| Video Capabilities Enabled/disabled | This check box turns video capabilities on and off.<br>**Note** This field does not apply to all phone models. |
| Owner User ID | From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from “Unassigned Devices” to “Users” in the License Usage Report. |

| Field | Description |
|---|---|
| Mobility User ID<br>(Dual-mode phones only) | From the drop-down list box, choose the user ID of the person to whom this dual-mode phone is assigned.<br>**Note** The Mobility User ID configuration gets used for the Cisco Unified Mobility and Mobile Voice Access features for dual-mode phones.<br>The Mobility User Id is taken from the admin page and is the same as Owner User Id. |
| Phone Personalization | The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. From the Phone Personalization drop-down list box, choose one of the following options:<br>• Disabled-The user cannot customize the Cisco Unified IP Phone by using Phone Designer.<br>• Enabled-The user can use Phone Designer to customize the phone.<br>• Default-The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window.<br>You must install and configure Phone Designer, so the phone user can customize the phone. Before you install and configure Phone Designer, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer documentation. For more information on Phone Designer, see the Phone Designer documentation. |

| Field | Description |
|---|---|
| Services Provisioning | From the drop-down list box, choose how the phone will support the services:<br>• Internal—The phone uses the phone configuration file to support the service.<br>Choose this option or Both for Cisco-provided default services where the Service URL has not been updated; that is, the service URL indicates `Application:Cisco/<name of service>`; for example, `Application:Cisco/CorporateDirectory`.<br>Choose Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file.<br>• External URL—Choosing External URL indicates that the phone ignores the services in the phone configuration file and retrieves the services from a Service URL.<br>If you configured a custom Service URL for a service, including a Cisco-provided default service, you must choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the phone.<br>• Both—Choosing Both indicates that the phone support both the services that are defined in the configuration file and external applications that are retrieved from service URLs. |
| Primary Phone | Choose the physical phone that will be associated with the application, such as IP communicator or Cisco Unified Personal Communicator. When you choose a primary phone, the application consumes fewer device license units and is considered an “adjunct” license (to the primary phone). |
| Wait for Far End H.245 Terminal Capability Set | This field applies only to H.323 devices.<br>This check box specifies that Cisco Unified CM waits to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. By default, the system checks this check box. To specify that Cisco Unified CM should initiate capabilities exchange, uncheck this check box. |
| Phone Load Name | Enter the custom software for the Cisco Unified IP Phone.<br>The value that you enter overrides the default value for the current model.<br>For more information about Cisco Unified IP Phone software and configuration, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager, which is specific to the phone model and Unified CM release. |
| Single Button Barge | From the drop-down list box, enable or disable the Single Button Barge/cBarge feature for this device or choose Default to use the service parameter setting.<br>• Off—This setting disables the Single Button Barge/cBarge feature; however, the regular Barge or cBarge features will still work.<br>• Barge—This setting enables the Single Button Barge feature.<br>• CBarge—This setting enables the Single Button cBarge feature.<br>• Default—Uses the Single Button Barge/cBarge setting that is in the service parameter. |

| Field | Description |
|---|---|
| Join Across Lines | From the drop-down list box, enable or disable the Join Across Lines feature for this device or choose Default to use the service parameter setting.<br>• Off—This setting disables the Join Across Lines feature.<br>• On—This setting enables the Join Across Lines feature.<br>• Default—This setting uses the Join Across Lines setting that is in the service parameter. |
| Use Trusted Relay Point | From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:<br>• Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.<br>• Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.<br>• On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.<br>A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.<br>Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent).<br>If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP.<br>If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP.<br>If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. |
| BLF Audible Alert Setting (Phone Idle) | This setting determines the busy lamp field (BLF) audible alert setting when no current call exists on the BLF DN:<br>• On—An audible alert sounds.<br>• Off—No audible alert sounds.<br>• Default—The configuration in the Service Parameters Configuration window determines the alert option. |
| BLF Audible Alert Setting (Phone Busy) | This setting determines the BLF audible alert setting when at least one active call exists on the BLF DN, but no call pickup alerts exist:<br>• On—An audible alert sounds.<br>• Off—No audible alert sounds.<br>• Default—The configuration in the Service Parameters Configuration window determines the alert option. |

| Field | Description |
|---|---|
| Always Use Prime Line | From the drop-down list box, choose one of the following options:<br>• Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received.<br>• On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls.<br>• Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service. |
| Always Use Prime Line for Voice Message | From the drop-down list box, choose one of the following options:<br>• On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.<br>• Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified CM always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.<br>• Default—Cisco Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service. |
| Geolocation | From the drop-down list box, choose a geolocation.<br>You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.<br>You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. |
| Feature Control Policy | From the drop-down list box, you can choose a feature control policy that has already been configured in the Feature Control Policy configuration window (**Device** > **Device Settings** > **Feature Control Policy**). |
| Retry Video Call as Audio | This check box applies only to video endpoints that receive a call. If this phone receives a call that does not connect as video, the call tries to connect as an audio call.<br>By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting.<br>If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via automatic alternate routing (AAR) and/or route/hunt list. |

| Field | Description |
|---|---|
| Ignore Presentation Indicators (internal calls only) | Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.<br><br>Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call.<br><br>See the translation configuration settings for more information about the calling line ID presentation and the connected line ID presentation parameters. |
| Allow Control of Device from CTI | Check this check box to allow CTI to control and monitor this device.<br><br>If the associated directory number specifies a shared line, the check box should be enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports. |
| Logged into Hunt Group | This check box, which gets checked by default for all phones, indicates that the phone is currently logged in to a hunt list (group). When the phone gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box.<br><br>Users use the softkey on the phone to log their phone in or out of the hunt list. |
| Remote Device | If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box in the Phone Configuration window. Checking this check box tells Cisco Unified CM to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone.<br><br>**Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option.<br><br>Cisco Unified CM sends the bundled messages to the phone when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires.<br><br>To specify a setting other than the default setting (100 msec) for the Bundle Outbound SCCP Messages timer, configure a new value in the Service Parameters Configuration window for the Cisco CallManager service. Although 100 msec specifies the recommended setting, you may enter 15 msec to 500 msec.<br><br>The phone must support SCCP version 9 to use this option. The following phones do not support SCCP message optimization: Cisco Unified IP Phone 7935/7936. This feature may require a phone reset after update. |

| Field | Description |
|---|---|
| Protected Device | Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media.<br><br>Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide* .<br><br>If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected. |
| Hotline Device | Check this check box to make this device a Hotline device. Hotline devices can only connect to other Hotline devices. This feature is an extension of PLAR, which configures a phone to automatically dial one directory number when it goes off-hook. Hotline provides additional restrictions that you can apply to devices that use PLAR.<br><br>To implement Hotline, you must also create a softkey template without supplementary service softkeys, and apply it to the Hotline device. |
| Require off-premise location | Check this check box if the device inserted requires off-premise location update upon registration. Off-premise location update is required when the device location cannot be detected automatically by Cisco Emergency Responder.<br><br>Check this check box only for remote or mobile devices that change locations frequently. |
| Caller ID For Calls From This Phone | |
| Calling Party Transformation CSS<br><br>for Calls from this Phone | From the drop-down list box, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the calling number when this phone initiates a call.<br><br>Cisco Unified CM transforms the calling party using the digit transformations configured on the matching calling party transformation pattern when this phone initiates a call. This setting allows you to transform the calling party number before Cisco Unified CM routes the call. For example, a transformation pattern can change a phone extension to an E.164 number. This setting is generally configured when a user dials using a URI instead of digits. Cisco Unified CM allows calling party transformations on various patterns when dialing using digits, this setting provides similar transformation provision even when dialing using a URI. |

| Field | Description |
|---|---|
| Use Device Pool Calling Party Transformation CSS<br><br>(Caller ID for Calls from this Phone) | Check this check box to use the Calling Party Transformation CSS configured at the device pool to which this phone belongs to transform the calling party for calls initiated from this phone. At the device pool, Calling Party Transformation CSS present under Phone Settings is used to transform the calling party for calls initiated from this phone.<br><br>Leave this check box unchecked to apply the Calling Party Transformation CSS setting that appears in this configuration window. |
| Remote Number Transformation | |
| Calling Party Transformation CSS<br><br>for Remote Number | From the drop-down list box, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this phone. Cisco Unified CM transforms the remote calling number using the digit transformations configured on the matching calling party transformation pattern before presenting it to this device. For example, a transformation pattern can change remote number in E.164 format to a localized version.<br><br>This setting can be used to transform the remote connected number for direct calls initiated from this phone. This setting can also be used to transform remote connected number post feature invocation irrespective of the direction of the call. The transformation of a remote connected number is controlled using the service parameter "Apply Transformations On Remote Number" (present under advanced section of Cisco Call Manager service). Refer to this parameter description for more details. |
| Use Device Pool Calling Party Transformation CSS<br><br>for Remote Number (Device Mobility Related Information) | Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this phone belongs to transform the remote calling and remote connected number. At the device pool, Calling Party Transformation CSS present under Device Mobility Related Information section is used to transform remote calling and remote connected number.<br><br>Leave this check box unchecked to apply the Calling Party Transformation CSS setting that appears in this configuration window for transforming the remote number. |
| Protocol Specific Information | |

| Field | Description |
|---|---|
| Packet Capture Mode | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box:<br>• None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting.<br>• Batch Processing Mode—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.<br>For more information on packet capturing, see the *Troubleshooting Guide for Cisco Unified Communications Manager* . |
| Packet Capture Duration | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.<br>This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes.<br>To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.<br>For more information on packet capturing, see the *Cisco Unified Communications Manager Troubleshooting Guide* . |
| SRTP Allowed | As this check box explains, if this flag is checked, IPSec needs to be configured in the network to provide end-to-end security. Failure to do so will expose keys and other information.<br>For more information on SRTP encryption, see the *Cisco Unified Communications Manager Security Guide* . |
| Presence Group | Configure this field with the Presence feature.<br>From the drop-down list box, choose a Presence group for the end user. The selected group specifies the devices, end users, and application users that can monitor this directory number.<br>The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box.<br>Presence authorization works with presence groups to allow or block presence requests between groups. |

| Field | Description |
|---|---|
| Device Security Profile | Choose the security profile to apply to the device.<br><br>You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. *Installing Cisco Unified Communications Manager* provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a nonsecure profile.<br><br>To identify the settings that the profile contains, choose **System** > **Security Profile** > **Phone Security Profile**.<br><br>**Note** The CAPF settings that are configured in the profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacturer-installed certificates (MICs) or locally significant certificates (LSC). See the Cisco Unified Communications Manager Security Guide for more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings. |
| SIP Dial Rules | If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed.<br><br>Leave the SIP Dial Rules field set to <None> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed. |
| MTP Preferred Originating Codec | From the drop-down list box, choose the codec to use if a media termination point is required for SIP calls. |
| Rerouting Calling Search Space | From the drop-down list box, choose a calling search space to use for rerouting.<br><br>The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message.<br><br>The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target. |
| Out-of-Dialog Refer Calling Search Space | From the drop-down list box, choose an out-of-dialog refer calling search space.<br><br>Cisco Unified CM uses the out-of-dialog (OOD) Refer Authorization calling search space (CSS) to authorize the SIP out-of-dialog Refer. The administrator can restrict the use of out-of-dialog Refer by configuring the OOD CSS of the Referrer. Refer Primitive rejects the OOD Refer request with a “403 Forbidden” message. |

| Field | Description |
|---|---|
| SUBSCRIBE Calling Search Space | Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified CM routes presence requests that come from the phone. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the phone.<br><br>From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the phone. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box.<br><br>If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.<br><br>To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces. |
| Outbound Call Rollover | Use this setting for the Cisco Unified IP Phone 7931.<br><br>• No Rollover—Conference and transfer will not work in this mode. If a user attempts to use either of these features, the phone status displays as "Error Pass Limit." Choose this setting only if you need to support CTI applications.<br>• Rollover Within Same DN—Conferences and call transfers complete by using the same directory number (on different lines). For example, consider a phone that has directory number 1506 that is assigned to both Line 6 and 7. The user has an active call on Line 6 and decides to transfer the call. When the user presses the Transfer button, the call on Line 6 gets placed on hold, and a new call initiates on Line 7 to complete the transfer.<br>• Rollover to any line—Conferences and call transfers complete by using a different directory number and line than the original call. For example, consider a phone that has directory number 1507 assigned to Line 8 and directory number 1508 assigned to Line 9. The user has an active call on Line 8 and decides to transfer the call. When the user presses the Transfer button, the call on Line 8 gets placed on hold, and a new call initiates on Line 9 to complete the transfer. |
| SIP Profile | Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control. |
| Digest User | Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security).<br><br>Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window.<br><br>After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file.<br><br>For more information on digest authentication, see the *Cisco Unified Communications Manager Security Guide* . |

| Field | Description |
|---|---|
| Media Termination Point Required | Use this field to indicate whether a media termination point is used to implement features that H.323 does not support (such as hold and transfer).<br><br>Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features.<br><br>Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source.<br><br>If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only. |
| Unattended Port | Check this check box to indicate an unattended port on this device. |
| Require DTMF Reception | For phones that are running SIP and SCCP, check this check box to require DTMF reception for this phone.<br><br>**Note** In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features. |
| RFC2833 Disabled | For phones that are running SCCP, check this check box to disable RFC2833 support. |
| Certification Authority Proxy Function (CAPF) Information | |
| Certificate Operation | From the drop-down list box, choose one of the following options:<br><br>• No Pending Operation—Displays when no certificate operation is occurring (default setting).<br>• Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone.<br>• Delete—Deletes the locally significant certificate that exists in the phone.<br>• Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type.<br><br>By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.<br><br>For more information on CAPF operations, see the *Cisco Unified Communications Manager Security Guide* . |

| Field | Description |
|---|---|
| Authentication Mode | This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation.<br><br>From the drop-down list box, choose one of the following options:<br><br>• By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone.<br>• By Null String— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention.<br><br>This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.<br><br>• By Existing Certificate (Precedence to LSC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC.<br><br>Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.<br><br>At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode.<br><br>• By Existing Certificate (Precedence to MIC)—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC.<br><br>Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.<br><br>**Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window. |
| Authentication String | If you chose the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits.<br><br>To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone. |

| Field | Description |
|---|---|
| Key Size (Bits) | For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048.<br>If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete.<br>**Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window. |
| Operation Completes by | This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation.<br>The values that display apply for the publisher database server. |
| Certificate Operation Status | This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field. |
| Expansion Module Information<br>(The following fields only display when the expansion modules are supported by the phone.) | |
| Module 1 | Choose the appropriate expansion module or none. |
| Module 1 Load Name | Enter the custom software for the appropriate expansion module, if applicable.<br>The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load. |
| Module 2 | Choose the appropriate expansion module or none. |
| Module 2 Load Name | Enter the custom software for the second expansion module, if applicable.<br>The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load. |
| Module 3 | Choose the appropriate expansion module or none. |
| Module 3 Load Name | Enter the custom software for the appropriate expansion module, if applicable.<br>The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load. |
| External Data Locations Information (Leave blank to use default) | |
| Information | Enter the location (URL) of the help text for the information (i) button. Leave this field blank to accept the default setting. |

| Field | Description |
|---|---|
| Directory | Enter the server from which the phone obtains directory information. Leave this field blank to accept the default setting.<br>**Note** If you set a Secured Directory URL enterprise parameter in the Enterprise Parameters Configuration window, that value overwrites the value of this field. |
| Messages | Leave this field blank (not used by Cisco Unified Communications Manager). |
| Services | Enter the location (URL) for IP phone services. |
| Authentication Server | Enter the URL that the phone uses to validate requests that are made to the phone web server. If you do not provide an authentication URL, the advanced features on the Cisco Unified IP Phone that require authentication will not function.<br>By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation.<br>Leave this field blank to accept the default setting. |
| Proxy Server | Enter the host and port (for example, proxy.cisco.com:80) that are used to proxy HTTP requests for access to non-local host addresses from the phone HTTP client.<br>The rule contains two parts for when to use the proxy server parameter:<br>**1.** The hostname contains a "."<br>**2.** The hostname specifies an IP address in any form.<br>If you do not configure this URL, the phone attempts to connect directly to the URL.<br>To accept the default setting, leave this field blank. |
| Idle | Enter the URL that displays on the Cisco Unified IP Phone display when the phone has not been used for the time that is specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes.<br>To accept the default setting, leave this field blank. |
| Idle Timer (seconds) | Enter the time (in seconds) that you want to elapse before the URL that is specified in the Idle field displays.<br>To accept the value of the Idle URL Timer enterprise parameter, leave this field blank. |

| Field | Description |
|---|---|
| Secure Authentication URL | Enter the secure URL that the phone uses to validate requests that are made to the phone web server.<br>**Note** If you do not provide a Secure Authentication URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.<br>By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation.<br>Leave this field blank to accept the default setting.<br>Maximum length: 255 |
| Secure Directory URL | Enter the secure URL for the server from which the phone obtains directory information. This parameter specifies the URL that secured Cisco Unified IP Phones use when you press the Directory button.<br>**Note** If you do not provide a Secure Directory URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.<br>Leave this field blank to accept the default setting.<br>Maximum length: 255 |
| Secure Idle URL | Enter the secure URL for the information that displays on the Cisco Unified IP Phone display when the phone is idle, as specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes.<br>**Note** If you do not provide a Secure Idle URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.<br>To accept the default setting, leave this field blank.<br>Maximum length: 255 |
| Secure Information URL | Enter the secure URL for the server location where the Cisco Unified IP Phone can find help text information. This information displays when the user presses the information (i) button or the question mark (?) button.<br>**Note** If you do not provide a Secure Information URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.<br>To accept the default setting, leave this field blank.<br>Maximum length: 255 |

| Field | Description |
|---|---|
| Secure Messages URL | Enter the secure URL for the messages server. The Cisco Unified IP Phone contacts this URL when the user presses the Messages button.<br>**Note** If you do not provide a Secure Messages URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.<br>To accept the default setting, leave this field blank.<br>Maximum length: 255 |
| Secure Services URL | Enter the secure URL for Cisco Unified IP Phone services. The is the location that the secure Cisco Unified IP Phone contacts when the user presses the Services button.<br>**Note** If you do not provide a Secure Services URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.<br>To accept the default setting, leave this field blank.<br>Maximum length: 255 |
| Extension Information | |
| Enable Extension Mobility | Check this check box if this phone supports extension mobility. |
| Log Out Profile | This drop-down list box specifies the device profile that the device uses when no one is logged in to the device by using Cisco Extension Mobility. You can choose either Use Current Device Settings or one of the specific configured profiles that are listed.<br>If you select a specific configured profile, the system retains a mapping between the device and the login profile after the user logs out. If you select Use Current Device Settings, no mapping gets retained. |
| Log In Time | This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the user logged in displays in this field. |
| Log Out Time | This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the system will log out the user displays in this field. |
| Configuration File Encryption Symmetric Key Information | |

| Field | Description |
|---|---|
| Symmetric Key | Enter a string of hexadecimal characters that you want to use for the symmetric key. Valid characters include numerals, 0-9, and upper/lower case characters, A-F (or a-f).<br><br>Make sure that you enter the correct bits for the key size; otherwise, Cisco Unified CM rejects the value. Cisco Unified CM supports the following key sizes:<br><br>• Cisco Unified IP Phones 7905 and 7912 (SIP only)—256 bits<br>• Cisco Unified IP Phones 7940 and 7960 (SIP only)—128 bits<br><br>Use this string for one-time use only. Every time that you update the configuration settings, you must generate a new key before you apply the configuration changes to the phone.<br><br>For more information on symmetric key operations for encrypted configuration file downloads, see the *Cisco Unified Communications Manager Security Guide* . |
| Generate String | If you want Cisco Unified Communications Manager Administration to generate a hexadecimal string for you, click the Generate String button. |
| Revert to Database Value | If you want to restore the value that exists in the database, click this button. This button proves useful if you enter an error in the Symmetric Key field before you save the configuration. |
| H.323 Information | |
| Outgoing Caller ID Pattern | For outgoing calls to the H.323 Client, enter the pattern, from 0 to 24 digits, that you want to use for caller ID. |
| Calling Party Selection | Choose the directory number that is sent on an outbound call to the H.323 Client.<br><br>The following options specify which directory number is sent:<br><br>• Originator—Send the directory number of the calling device.<br>• First Redirect Number—Send the directory number of the redirecting device.<br>• Last Redirect Number—Send the directory number of the last device to redirect the call.<br>• First Redirect Number (External)—Send the external directory number of the redirecting device.<br>• Last Redirect Number (External)—Send the external directory number of the last device to redirect the call. |
| Calling Party Presentation | Choose whether the Cisco Unified CM transmits or blocks caller ID.<br><br>If you want Cisco Unified CM to send caller ID, choose Allowed.<br><br>If you do not want Cisco Unified CM to send caller ID, choose Restricted.<br><br>Default specifies that caller ID does not get sent. |
| Display IE Delivery | This check box enables delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service.<br><br>The default setting checks this check box. |

| Field | Description |
|---|---|
| Redirecting Number IE Delivery Outbound | Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified CM includes the Redirecting Number IE.)<br>Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message.<br>You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.<br>**Note** The default setting leaves this check box unchecked. |
| Redirecting Number IE Delivery Inbound | Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CM. (The UUIE part of the SETUP message includes the Redirecting Number IE.)<br>Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CM.<br>You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.<br>**Note** Default leaves the check box unchecked. |
| Gatekeeper Information | |
| Gatekeeper Name | This field specifies the name of the gatekeeper that controls the H.323 client. Ensure the gatekeeper is configured in Cisco Unified CM before an H.323 client is allowed to specify the gatekeeper in its configuration. Default specifies empty. |
| E.164 | Always use a unique E.164 number. Do not use null value. |
| Technology Prefix | This field specifies a number ending with the # sign that describes the capability of an endpoint in a zone. This field has no impact if via Zone configuration can be used. Default specifies 1#*. Do not use null value. |
| Zone | This field specifies the zone name of the zone that the gatekeeper manages. Do not use the following values: same zone name for the H.323 client and trunk; null. |
| Associated Mobility Identity | |
| (mobility identity) | If a mobility identity has already been configured for this device, this area displays the Name and Destination Number of the mobility identity. You can click either value to display the Mobility Identity Information in the Remote Destination Configuration window.<br>**Note** This field displays only after a Cisco Unified Mobile Communicator device has been added. The Cisco Unified Mobile Communicator must be enabled for a mobile phone. |

| Field | Description |
|---|---|
| Add New Mobility Identity | If no mobility identity has been defined for this device, click this link to add a mobility identity. The Remote Destination Configuration window displays, which allows you to add a new mobility identity to associate with this device.<br>**Note** This field displays only after a Cisco Unified Mobile Communicator device has been added. |
| Associated Remote Destinations | |
| (remote destination) | If a remote destination has already been configured for this device, this area displays the Name and Destination Number of the remote destination(s). You can click the values to display the Remote Destination Information in the Remote Destination Configuration window. |
| Add a New Remote Destination | Click this link to add a remote destination to associate with this device. The Remote Destination Configuration window displays, which allows you to add a new remote destination to associate with this device. |
| Route calls to all remote destinations when client is not connected | Determines whether calls should be routed to all remote destinations when the active remote destination is not set. Check this check box to receive calls during network connection outage or to use a third-party voicemail system.<br>**Note** This field appears only on a CTI remote device type. |
| MLPP Information | |
| MLPP Domain | Choose an MLPP domain from the drop-down list box for the MLPP domain that is associated with this device. If you leave the None value, this device inherits its MLPP domain from the value that was set in the common device configuration. If the common device configuration does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter. |
| MLPP Indication | If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call.<br>From the drop-down list box, choose a setting to assign to this device from the following options:<br>• Default—This device inherits its MLPP indication setting from the common device configuration.<br>• Off—This device does not handle nor process indication of an MLPP precedence call.<br>• On—This device does handle and process indication of an MLPP precedence call.<br>**Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.<br>Turning on MLPP Indication (at the enterprise parameter or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device. |

| Field | Description |
|---|---|
| MLPP Preemption | Be aware that this setting is not available on all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call.<br>From the drop-down list box, choose a setting to assign to this device from the following options:<br>• Default—This device inherits its MLPP preemption setting from the common device configuration.<br>• Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.<br>• Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.<br>**Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. |
| Confidential Access Level | Select the appropriate CAL value from the drop-down list box. |
| Confidential Access Mode | From the drop-down list box, select one of the following options to set the CAL mode:<br>• Fixed—CAL value has higher precedence over call completion.<br>• Variable—Call completion has higher precedence over CAL level. |
| Do Not Disturb (DND) | |
| Do Not Disturb | Check this check box to enable Do Not Disturb on the phone. |
| DND Option | When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls:<br>• Call Reject—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.<br>• Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call.<br>• Use Common Phone Profile Setting—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device.<br>**Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device. |

| Field | Description |
|---|---|
| DND Incoming Call Alert | When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone.<br><br>From the drop-down list, choose one of the following options:<br><br>• None—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window gets used for this device.<br>• Disable—This option disables both beep and flash notification of a call, but, for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display, and no information gets sent to the device.<br>• Beep Only—For an incoming call, this option causes the phone to play a beep tone only.<br>• Flash Only—For an incoming call, this option causes the phone to display a flash alert. |
| Secure Shell Information | |
| Secure Shell User | Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include", %, &, <, >, and \. This field displays when the phone device that you are configuring supports SSH access.<br><br>Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.<br><br>See the *Cisco Unified Communications Manager Security Guide* for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear. |
| Secure Shell Password | Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 200 characters. Invalid characters include", %, &, <, >, and \. Contact TAC for further assistance.<br><br>See the *Cisco Unified Communications Manager Security Guide* for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH passwords to the phone in the clear. |
| Association Information | |
| Modify Button Items | After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.<br><br>Click this button to manage button associations for this phone. A dialog box warns that any unsaved changes to the phone may be lost. If you have saved any changes that you made to the phone, click OK to continue. The Reorder Phone Button Configuration window displays for this phone. |

| Field | Description |
|---|---|
| Line [1] - Add a new DN<br>Line [2] - Add a new DN | After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.<br>Click these links to add a directory number(s) that associates with this phone. When you click one of the links, the Directory Number Configuration window displays. |
| Add a new SD | After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.<br>Click this link to add speed-dial settings for this phone. When you click the link, the Speed Dial and Abbreviated Dial Configuration window displays for this phone. |
| Add a new SURL | After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.<br>Click this link to configure service URL buttons for this phone. When you click the link, the Configure Service URL Buttons window displays for this phone. |
| Add a new BLF SD | After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.<br>Click this link to configure busy lamp field/speed dial settings for this phone. When you click the link, the Busy Lamp Field Directed Call Park Configuration window displays for this phone. |
| Add a new BLF Directed Call Park | After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.<br>Click this link to configure busy lamp field/directed call park settings for this phone. When you click the link, the Busy Lamp Field Directed Call Park Configuration window displays for this phone. |
| Product-Specific Configuration Layout | |
| Model-specific configuration fields that the device manufacturer defines | To view field descriptions and help for product-specific configuration items, click the “?” information icon in the Product Specific Configuration area to display help in a popup dialog box.<br>If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.<br>Select the “Override Common Settings” box for any corresponding setting in the Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings. |

# Phone Settings Migration

You can migrate existing phone settings to a different phone.

# Speed-Dial and Abbreviated-Dial Setup

The following table describes the speed-dial button configuration settings. The Speed Dial and Abbreviated Dial Configuration window contains the following sections: speed-dial settings on the phone and abbreviated-dial settings that are not associated with a button. The descriptions in the table apply to both sections.

The system provides a total of 199 speed-dial and abbreviated-dial settings.

### Speed Dial Settings

Configure these settings for the physical buttons on the phone.

### Abbreviated Dial Settings

Configure these settings for the speed-dial numbers that you access with abbreviated dialing. When the user configures up to199 speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays on the phone, and the user can access any speed-dial entry by entering the appropriate index (code) for abbreviated dialing.

### Pause in Speed Dial Feature Specific Settings

In Cisco Unified Communication Manager, the user can configure Forced Authorization Code (FAC), Client Matter Code (CMC), and post-connect Dual Tone Multifrequency (DTMF) digits as a part of a speed dial number. The Unified CM recognizes the destination address digits, FAC, CMC, and post-connect DTMF digits that are configured as a part of a speed dial number.

The Unified CM uses the following:

1. Destination address digits to route the call
2. FAC digits to authorize the user before routing the call to a particular gateway or a trunk
3. CMC digits for billing before routing the call to a particular gateway or a trunk

The Unified CM sends out post-connect DTMF digits with appropriate pause duration after the call is connected and a media connection is established.

**Note** Even if the media connection is established before a call is connected, the DTMF digits are sent only after the call is connected.

There are two methods to configure this feature:

- Method I : Using a comma as a pause and also as a delimiter
- Method II : Entering destination address digits, FAC, CMC, and DTMF digits as a continuous string without using any delimiter

**Method I: Using comma as a pause and also as a delimiter**

1. Using comma as a pause

   The users can configure the special character comma (,) within speed dial, which acts as a pause duration of 2 seconds for sending post-connect DTMF digits. The Unified CM pauses for the appropriate duration corresponding to the number of commas entered before sending out DTMF digits to the remote side of the call.

   **Example 1: Reading a Voicemail message**

   Without the Pause in Speed dial feature, the user must perform the following to read a voicemail message:

   1. Click message button on the phone or 8000 [Voicemail pilot number] to reach the Cisco Unity Server.
   2. Enter 91941420# [PIN] after announcement of 2 seconds after the call is connected.
   3. Enter option 3 to read the latest message after a pause of around 6 seconds (while the operator reads the options) after the PIN is verified.

   With Pause in Speed dial feature, the user can configure speed dial as

   8000,91941420#,,,3 and press the speed dial key and read the latest message received. Here, the Unified CM waits for 2 seconds after the call is connected, then sends out the PIN [91941420#] to the Cisco Unity Server and again waits for 6 seconds before sending out the option [3] to the Cisco Unity Server.

2. Using comma as a delimiter

   A comma can be used as a delimiter in the following cases:

   - To separate the FAC from the destination address digits
   - To separate destination address digits and CMC (if FAC is not enabled)
   - To separate the FAC and CMC

   This enables Unified CM to recognize the destination address digits, FAC, CMC, and DTMF digits when user has configured the following:

   1. Overlapping dial patterns [Example: 9.XXXX and 9.XXXXX are overlapping Route patterns]
   2. Variable length dial patterns [Example: 8.!]
   3. Overlapping FAC and CMC [Example of overlapping FAC: 8787, 87879]

**Example 2: Connecting to IVR application over a gateway**

If the user wants to reach out to an IVR application over a gateway, to the user must enter FAC and CMC digits to reach the gateway and then send out IVR responses after the call is connected. The manual dialing works as follows:

1. Enter called number: 91886543
2. Enter Forced Authorization Code: 8787
3. Enter Client Matter Code: 5656
4. IVR response 4 seconds after the call is connected: 987989#

Using the Pause in Speed Dial feature, a user can configure speed dial as follows to achieve the same result:

**91886543,8787,5656,,987989#**

In this example, the Unified CM uses 8787 as FAC, 5656 as CMC before the call is routed to a gateway and sends out IVR response [987989#] 4 seconds after the call is connected.

**Note** Ensure the FAC always precedes the CMC when you configure a speed dial that includes FAC and CMC.

**Note** Ensure to use only a single comma as a delimiter. If more than one comma is configured, the digits after multiple commas are considered as DTMF digits and users are prompted to enter the FAC or CMC manually.

**Handling incorrect FAC or CMC when comma is used as a delimiter**

Whenever comma is used as a delimiter and FAC or CMC is configured as a part of speed dial is incorrect or unauthorized to make a particular call then the Unified CM disconnects the call with the following error message on the phone where speed dial is invoked:

*Error: Invalid Code in SpeedDial*

**Method II: Entering main address, FAC, CMC, and DTMF digits as a continuous string without using any delimiter**

With this method, speed dial is configured as a continuous string of digits and Unified CM identifies following components from the digit string:

1. Destination address digits
2. FAC
3. CMC
4. DTMF digits [DTMF digits are sent immediately after the call is connected]

This method allows the user to configure the Pause in Speed Dial feature on Cisco Unified Personal Communicator endpoints which do not have the speed dial option.

**Example 3: Connecting to IVR application, which prompts users to enter responses immediately after call is connected**

If the user wants to reach an IVR application and is required to enter FAC and CMC digits to reach to a gateway and then send out IVR response after call is connected, the manual dialing works as follows:

1. Enter called number: 91886543 [ Using Route Pattern 9.XXXXXXX ]
2. Enter Forced Authorization Code: 8787
3. Enter Client Matter Code: 5656
4. IVR response immediately after the call is connected: 987989#

Using the Pause in Speed Dial feature, a user can configure speed dial as follows to achieve the same result:

**9188654387875656987989#**

**Handling incorrect FAC or CMC when comma is not used as a delimiter**

Whenever a comma is not used as a delimiter and FAC or CMC is configured as a part of speed dial is incorrect or unauthorized to make a particular call then the Unified CM switches to manual dialing mode from the point of failure.

**Example:** If FAC entered is incorrect (even if CMC entered is correct), Unified CM switches to manual dialing mode and displays the following error message at the phone:

*Auth code failed: Enter manually*

After receiving this error message, the user must dial out FAC, CMC, and DTMF digits manually.

If FAC entered is correct and validated but CMC entered is incorrect, Unified CM switches to manual dialing mode and displays the following error message at the phone:

*CM code failed: Enter manually*

After receiving this error message, the user must dial CMC and DTMF digits manually.

The following table describes the comparison between using a comma and not using a comma as a delimiter.

***Table 1: Comparison Between Two Methods***

| Method I : Using comma as a delimiter and also as a pause | Method II : Not using comma as a delimiter |
|---|---|
| Can be configured when the customer has<br>• Overlapping route patterns<br>• Variable length dial patterns<br>• Overlapping FAC and CMC | Only preferred for calls made using fixed length route patterns. This method may not work when overlapping route patterns and overlapping FAC and CMC are configured. |
| DTMF digits can be sent after appropriate pause duration. | DTMF digits are always sent immediately after the call is connected. |
| Call is disconnected when invalid FAC or CMC is entered. | For FAC, CMC failure cases, Unified CM switches to manual dialing mode and user gets one more chance to enter correct code. |
| Can be used even when FAC and CMC are not required to make calls; that is, can be used for sending only DTMF digits. | Can be used only for the calls made over route patterns where at least one out of FAC and CMC is enabled. This method cannot be used for sending only DTMF digits. |

**Note** Unified CM ensures FAC, CMC, and DTMF digits are not displayed in the phone placed calls history for the calls made using speed dial with the codes configured.

After a call is successful, when the user presses the Redial softkey or dials out from the placed calls history, to the user must dial out FAC, CMC, and DTMF digits manually.

When the Unified CM sends a group of DTMF digits (configured as a part of speed dial) after a pause or after the call is connected, there is a possibility that the Unified CM may out-pulse these DTMF digits quickly for remote application or remote gateway to process.

To prevent this, Unified CM pauses for the duration specified in service parameter "Pause In Speed Dial InterDigit Interval." In the previous example DTMF digits are: **987989#**

Unified CM sends out the first DTMF digit, that is, 9, and waits for the duration specified in this service parameter before sending out the next digit, that is, 8. Similarly, it follows the same pattern before sending out each digit.

The following table describes the Speed-dial and abbreviated-dial configuration settings.

*Table 2: Speed-Dial and Abbreviated-Dial Configuration Settings*

| Field | Description |
|---|---|
| (number from 1 to 199 in the left column) | This column identifies the speed-dial button on the phone or on the Cisco Unified IP Phone Expansion Module (for example, 1, 2, 3, or 4) or the abbreviated-dial index for abbreviated dial. |
| Number | Enter the number that you want the system to dial when the user presses the speed-dial button. You can enter digits 0 through 9, *, #, and +, which is the international escape character. For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits. |
| Label | Enter the text that you want to display for the speed-dial button or abbreviated-dial number.<br>**Note** If you are configuring a Pause in Speed Dial, you must add a label so that FAC, CMC, and DTMF digits are not displayed on the phone screen.<br>Cisco Unified Communications Manager does not make this field available for the Cisco Unified IP Phone 7910. |

The following table describes the SIP Phone models and support information.

### Phone Model Support

*Table 3: SIP Phone Models and Support Information*

| Phone Model | Support | Description |
|---|---|---|
| Cisco Unified IP Phones 8961, 9951, 9971 using SIP | Fully Supported | • Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for the calls that are placed using the speed dial.<br>• DTMF digits are sent by both out of band and RFC2833 method. In both the cases, users can hear the tone that indicates the DTMF digit is sent. |
| Cisco Unified Personal Communicator Clients | Supported using only method II<br>[See Method II section] | • DTMF digits can be sent by both out of band and RFC2833 method. |

The following table describes the SCCP Phone models and support information.

*Table 4: SCCP Phone Models and Support Information*

| Phone Model | Support | Description |
|---|---|---|
| Cisco Unified IP Phones<br>7906, 7911, 7931, 7941, 7961, 7942, 7962, 7945,7965, 7970, 7971, 7975 using SCCP | Fully Supported | • Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for the calls placed using the speed dial.<br>• DTMF digits can be sent by both out of band and RFC2833 method. In both the cases, users can hear the tone that indicates the DTMF digit is sent. |
| Other SCCP Phone Models | Partially Supported | • Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for calls that are placed using speed dial.<br>• DTMF digit can be sent only by out of band method and no tone is played to indicate the digit is sent. |

**CME and SRST Limitations**

When a phone is in the CME (configured as SRST) or SRST mode, for the speed dial calls where a comma is used as a pause duration or as a delimiter, the phone sends only the digits before the first comma as the destination address digits to the CME or SRST router. Hence, the call proceeds in the manual dialing mode, provided the appropriate dial peer is configured on the router, and users are required to dial out FAC and DTMF digits manually.

For the speed dials where FAC , CMC, and DTMF digits are entered as a continuous string , the phone sends the entire set of digits to CME or SRST router and calls may fail because the CME and SRST router does not have capability to recognize the destination address digits , FAC, and DTMF digits from the digit string received.

# BLF Speed Dial Setup

When you configure Presence in Cisco Unified Communications Manager Administration, an interested party, known as a watcher, can monitor the real-time status of a directory number or SIP URI with a BLF/SpeedDial button on the device of the watcher.

For Presence-supported phones that are running SIP, you can configure directory numbers or SIP URIs as BLF/SpeedDial buttons. For Presence-supported phones that are running SCCP, you can configure only directory numbers as BLF/SpeedDial buttons.

For information on configuring BLF/SpeedDial buttons, see the *Cisco Unified Communications Manager Features and Services Guide*.

# BLF Directed Call Park Setup

Directed Call Park allows a user to transfer a parked call to an available user-selected directed call park number. Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number.

For information on configuring BLF/Directed Call Park buttons, see the *Cisco Unified Communications Manager Features and Services Guide*.

# Set Up Cisco Unified IP Phone

You can automatically add phones to the Cisco Unified Communications Manager database by using auto-registration or manually add phones by using the Phone Configuration windows.

By enabling auto-registration, you can automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you connect the phone to your IP telephony network. During auto-registration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone. In many cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to a phone.

**Note** Cisco recommends using auto-registration in small configurations or testing labs only.

If you configure the clusterwide security mode to mixed mode, Cisco Unified Communications Manager disables auto-registration.

If you do not use auto-registration, you must manually add phones to the Cisco Unified Communications Manager database.

After you add a Cisco Unified IP Phone to Cisco Unified Communications Manager Administration, the RIS Data Collector service displays the device name, registration status, and the IP address of the Cisco Unified Communications Manager to which the phone is registered in the Phone Configuration window.

Before a Cisco Unified IP Phone can be used, you must use this procedure to add the phone to Cisco Unified Communications Manager. You can also use this procedure to configure third-party phones that are running SIP, H.323 clients, CTI ports, the Cisco ATA 186 Telephone Adaptor, or the Cisco IP Communicator. H.323 clients can comprise Microsoft NetMeeting clients. CTI ports designate virtual devices that Cisco Unified Communications Manager applications such as Cisco SoftPhone and Cisco Unified Communications Manager Auto-Attendant use.

When you add a new phone, you can choose a phone template that was created by the Bulk Administration Tool to configure automatically some of the phone configuration settings, based on the template.

Phone templates must exist on the server before you can select a phone template. For more information about Bulk Administration Tool phone templates, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

**Note** Add the Cisco VG248 and VG224 Phone Ports from the Gateway Configuration window of Cisco Unified Communications Manager Administration.

**Tip** In the Phone Configuration window for a specific phone, you can view the IPv4 address and the IPv6 address, if applicable, that the phone uses. For phones in dual-stack mode that have both an IPv4 and IPv6 address, you can click the IPv4 or IPv6 address in the Phone Configuration window, which points to an IPv4 URL for the web server on the phone. For phones that use an IPv6 address only, you cannot click the IPv6 address because the web server on the phone only supports IPv4.

**Timesaver** If you plan on using nonstandard phone button and softkey templates, configure the templates before you add the phones.

### Procedure

**Step 1** Choose**Device** > **Phone**.

The Find and List Phones window displays.

**Step 2** Perform one of the followings tasks:

**Note** You can display the MAC address of a phone.

a) To copy an existing phone, locate the appropriate phone in the Find and List Phones window, click the Copy button next to the phone that you want to copy, and continue with Step 5, on page 41.
b) To copy an existing phone and copy the directory numbers, speed dials, busy lamp field/speed dials, and service URLs that are associated with the phone, locate the appropriate phone in the Find and List Phones window, click the Super Copy button next to the phone that you want to copy, and continue with Step 5, on page 41.

**Note** The lines that get copied become shared lines between the original phone and the new phone.

c) To add a new phone, click the Add New button and continue with Step 3, on page 40.
d) To update an existing phone, locate the appropriate phone and continue with Step 5, on page 41.

**Step 3** Perform one of the following tasks when you choose the phone model:

a) From the Phone Type drop-down list box, select the appropriate phone type or device and click Next. After you choose a phone type, you cannot modify it.
b) Select the Phone Template radio button, select the appropriate phone template from the drop-down list box, and click Next. (Only phone templates that were created in the Bulk Administration Tool display in the drop-down list box.)

**Step 4** If the Select the device protocol drop-down list box displays, choose the appropriate protocol of the device and click Next. Otherwise, continue with Step 5, on page 41.

The Phone Configuration window displays.

**Step 5** Enter the appropriate settings as described in Phone Settings, on page 4.

Only the settings that are appropriate to the chosen phone type display in the window.

**Step 6** Click Save.

If you are adding a phone, a message displays that states that the phone has been added to the database. To add a directory number to this phone, click one of the line links, such as Line [1] - Add a new DN, in the Association Information pane that displays on the left side of the window. Continue to configure the directory number settings.

If you are updating a phone, a message displays that states that you must click the Apply Config button for your changes to take effect and synchronize the phone.

### What to do next

You can continue to configure the following on the phone:

- speed-dial buttons
- services
- service URL buttons
- busy lamp field/speed-dial settings

# Migrate Existing Phone Settings to Another Phone

The Phone Migration window in Cisco Unified Communications Manager Administration allows you to migrate feature, user, and line configuration for a phone to a different phone. You can migrate data to a different phone model or to the same phone model that runs a different protocol. For example, you can migrate data from a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, or you can migrate data from a phone model that runs SCCP, for example, the Cisco Unified IP Phone 7965 (SCCP) and move it to the same phone model that runs SIP, for example, the Cisco Unified IP Phone 7965 (SIP).

**Tip** Phone migration allows you to port existing phone configuration to a new phone without the need to add a phone, lines, speed dials, and so on.

Before you migrate existing phone configuration to a different phone, see the topics related to phone migration for information to review before you migrate the settings and migration procedures.

### Before you begin

Before you can migrate phone configuration to a new phone, consider the following information:

- If the phone models do not support the same functionality, be aware that you may lose functionality on the new phone after the migration occurs. Before you save the migration configuration in the Phone Migration window, Cisco Unified Communications Manager Administration displays a warning that you may lose feature functionality.

- Some phone models do not support phone migration; for example, CTI port, H.323 client, Cisco Unified Mobile Communicator, Cisco IP Softphone, and so on.
- Before you can migrate the phone configuration, you must create a phone template in BAT for the phone model and protocol to which you want to migrate. For example, if you want to migrate the configuration for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.

  If the Phone Configuration window does not display a field for the original phone, but the field is required for the new phone, the new phone uses the value from the phone template for the required field.

- The new phone uses the same existing database record as the original phone, so migrating the phone configuration to the new phone removes the configuration for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database; that is, you cannot view or access the configuration for the original phone after the migration.

  Migrating to a phone that uses fewer speed dials or lines does not remove the speed dials or lines for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database, although some speed dials/lines do not display on the new phone. After you migrate the configuration, you can see all speed dials and lines for the original phone in the Phone Configuration window for the new phone.

- Before you migrate the phone configuration to a new phone, ensure that the phones are unplugged from the network. After you perform the migration tasks, you can plug the new phone into the network and register the device.
- Before you migrate the phone configuration to a new phone, ensure that you have enough device license units for the new phone.

**Tip** If you want to migrate the configuration for multiple phones, use the Bulk Administration Tool; for information on how to perform this task, see the Cisco Unified Communications Manager Bulk Administration Guide.

### Procedure

**Step 1** Make sure that you created a phone template in BAT for the phone model and protocol to which you want to migrate the data. In Cisco Unified Communications Manager Administration, choose **Bulk Administration** > **Phones** > **Phone Template**.

**Step 2** In the Find and List Phones window (**Device** > **Phone**), find the phone configuration that you want to migrate.

**Step 3** After you display the Phone Configuration window for the phone configuration that you want to migrate, choose Migrate Phone from the Related Links drop-down list box.

**Step 4** Enter the migration configuration settings, as described in Phone Migration Settings , on page 43.

**Step 5** Click Save.

**Step 6** If a warning displays that the new phone may lose feature functionality, click OK.

# Phone Migration Settings

| Field | Description |
|---|---|
| Phone Template | From the drop-down list box, choose the phone template for the phone model to which you want to migrate the phone configuration.<br>Only the phone templates that you configured in the Phone Template window in Bulk Administration display (**Bulk Administration** > **Phones** > **Phone Template**). |
| MAC Address | This field support hardware phones only. Enter the Media Access Control (MAC) address for the new Cisco Unified IP Phone to which you are migrating the configuration. Make sure that the value comprises 12 hexadecimal characters.<br>For information on how to access the MAC address for your phone, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model. |
| Description | If you want to do so, enter a description for the new phone. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). |

# Synchronize Phone

To synchronize a phone with the most recent configuration changes, perform the following procedure, which applies any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

### Procedure

**Step 1** Choose **Device** > **Phone**.

The Find and List Phones window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click **Find**.

The window displays a list of phones that match the search criteria.

**Step 4** Check the check boxes next to the phones that you want to synchronize. To choose all phones in the window, check the check box in the matching records title bar.

**Step 5** Click **Apply Config to Selected**.

The Apply Configuration Information dialog displays.

**Step 6** Click **OK**.

# Set Up Speed-dial Buttons or Abbreviated Dialing

You use Cisco Unified Communications Manager Administration to configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users use Cisco Unified Communications Self Care Portal to change the speed-dial buttons on their phones.

Table 2: Speed-Dial and Abbreviated-Dial Configuration Settings , on page 37 describes the speed-dial button and abbreviated dialing configuration settings. The Speed Dial and Abbreviated Dial Configuration window contains the following sections: speed-dial settings on the phone and abbreviated-dial settings that are not associated with a button. The descriptions in Table 2: Speed-Dial and Abbreviated-Dial Configuration Settings , on page 37 apply to both sections.

The system provides a total of 199 speed-dial and abbreviated-dial settings.

- Speed Dial Settings

  Configure these settings for the physical buttons on the phone.

- Abbreviated Dial Settings

  Configure these settings for the speed-dial numbers that you access with abbreviated dialing. When the user configures up to 199 speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays on the phone, and the user can access any speed-dial entry by entering the appropriate index (code) for abbreviated dialing.

**Note** Not all Cisco Unified IP Phones support abbreviated dialing. See the phone user guide for information.

### Procedure

**Step 1** From the Phone Configuration window, choose Add/Update Speed Dials from the Related Links drop-down list box at the top of the window and click Go.

The Speed Dial and Abbreviated Dial Configuration window displays for this phone.

**Note** To display the Phone Configuration window, choose **Device** > **Phone**. Enter your search criteria and click Find. Choose the phone for which you want to configure speed-dial buttons.

**Step 2** Enter the appropriate settings as described in Table 2: Speed-Dial and Abbreviated-Dial Configuration Settings , on page 37.

**Note** For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits.

**Step 3** To apply the changes, click Save.

**Step 4** To close the window, click Close.

# Set Up IP Phone Services

From certain phones, such as Cisco Unified IP Phone 7970, 7960, and 7940, users can access services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified Communications Manager Administration, you can set up the available services for phones. For some services, users can use the Cisco Unified Communications Self Care Portal menu to modify the services. For information about the Cisco Unified Communications Self Care Portal, see the Cisco Unified IP Phone User Guide that is specific to your phone model.

## Subscribe to Service

You (or an end user) cannot subscribe to services that are marked as enterprise subscriptions. (The enterprise subscription column displays in the Find and List IP Phone Services window. If true displays in the column, you (or an end user) cannot subscribe to the service. In a service is marked as an enterprise subscription, the service automatically displays on the phone, unless you disable the service in the Phone Services Configuration window.

To subscribe to new services for a phone, perform the following steps.

### Before you begin

If you need to do so, add the phone services to Cisco Unified Communications Manager.

### Procedure

**Step 1** Choose **Device** > **Phone**.

The Find and List Phones window displays.

**Step 2** To locate a specific phone, enter search criteria and click Find.

A list of phones that match the search criteria displays.

**Step 3** Choose the phone to which you want to add a service.

The Phone Configuration window displays.

**Step 4** On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.

The Subscribed IP phone services window displays for this phone.

**Step 5** From the Select a Service drop-down list box, choose the service that you want to add to the phone.

**Step 6** Click Next.

The window displays with the service that you chose. If you want to choose a different service, click Back and repeat Step 5, on page 45.

**Step 7** If the service has required parameters, enter that information into the field that is provided.

**Step 8** Click Subscribe.

The service displays in the Subscribed Services list.

**Step 9** If you want to subscribe to additional services, click the Subscribe a New Service link in the Subscribed Services area. Repeat Step 5, on page 45 through Step 8, on page 45.

# Update Service

Perform the following steps to update a service. You can update the service name and service parameter values, if necessary.

### Procedure

**Step 1** Choose **Device** > **Phone**.

The Find and List Phones window displays.

**Step 2** To locate a specific phone, enter search criteria and click Find.

A list of phones that match the search criteria displays.

**Step 3** Choose the phone for which you want to update a service.

The Phone Configuration window displays.

**Step 4** On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.

**Step 5** From the Subscribed Services list, choose a service.

**Step 6** Update the appropriate parameter and click Save.

# Unsubscribe From Service

To unsubscribe from a service, perform the following steps.

### Procedure

**Step 1** Choose **Device** > **Phone**.

The Find and List Phones window displays.

**Step 2** Enter search criteria to locate a specific phone and click Find.

A list of phones that match the search criteria displays.

**Step 3** Choose the phone from which you want to delete a service.

The Phone Configuration window displays.

**Step 4** On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.

**Step 5** From the Subscribed Services list, choose a service.

**Step 6** Click Unsubscribe.

A warning message verifies that you want to unsubscribe from the service.

**Step 7** To unsubscribe, click OK or click Cancel to restore your previous settings.

# Service URL Button Setup

From some Cisco Unified IP Phone models, users can access information services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified Communications Manager Administration, you can configure services to be available on a phone button (speed dial button) and then configure that button for the phone. See the Cisco Unified IP Phone User Guide that is specific for your phone model.

**Tip** When you configure a service, you specify whether you want the service to display under the Messages, Directory, or Services button. If your phone model has a Messages, Directory, or Services button/option, the service can display under any of these buttons in addition to the phone button for speed dials (service URL button). If a service is marked as an enterprise subscription, you cannot add the service to a service URL button.

## Add Service URL Button

To configure the service URL buttons for a phone, perform the following steps.

### Before you begin

Before you begin, perform the following configurations:

- Add the services to Cisco Unified Communications Manager.
- Configure the service URL button on the phone button template.
- Subscribe to the service.

### Procedure

**Step 1** Choose **Device** > **Phone**.

The Find and List Phones window displays.

**Step 2** To locate a specific phone, enter search criteria and click Find.

A list of phones that match the search criteria displays.

**Step 3** Choose the phone to which you want to add a service URL button.

The Phone Configuration window displays.

**Step 4** In the Association Information area on the left side of the Phone Configuration window, click the Add a new SURL link.

The Configure Service URL Buttons window displays for this phone.

**Step 5** From the Button Service drop-down list box, choose the service that you want to add to or update for the phone.

**Step 6** You can change the value in the Label field.

**Step 7** To add the service to or update for the phone button, click Save.

**Step 8** If more buttons and services are available, you can assign additional services to additional buttons by repeating **Add Service URL Button** through **Add Service URL Button**.

**Step 9** To close this window and return to the Phone Configuration window, click Close.

# Copy Phone Record to Remote Destination Profile

You can copy information from a phone record to a new remote destination profile, which is used for Cisco Unified Mobility and Mobile Voice Access. See the *Cisco Unified Communications Manager Features and Services Guide* for instructions on configuring remote destination profiles.

### Procedure

**Step 1** From the Phone Configuration window, choose Copy to Remote Destination Profile from the Related Links drop-down list box at the top of the window and click Go.

The Remote Destination Profile Configuration window displays for this phone.

**Step 2** Enter the appropriate settings as described in the topics related to Cisco Unified Mobility in the *Cisco Unified Communications Manager Features and Services Guide*.

**Step 3** To apply the changes, click Save.

**Step 4** To close the window, click Close.

# Modify Custom Phone Button Template Button Items

When you configure a phone and associate it with a custom, nonstandard phone button template, you can modify the phone button items in the associated phone button template. When you do so, you create a new phone button template that is customized for this particular phone. The new phone button template displays in the list of phone button templates with a name of the format “SEP999999999999-Individual Template”, where 999999999999 specifies the MAC address of the phone.

**Note** You cannot perform this procedure if the phone is associated with a standard phone button template. You must first associate this phone with a custom, nonstandard phone template.

To modify the button items of a custom, nonstandard phone button template, perform the following steps.

### Procedure

**Step 1** Choose **Device** > **Phone**.

The **Find and List Phones** window displays.

**Step 2** Enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

**Step 3** Choose the phone for which you want to modify the phone button items.

The **Phone Configuration** window displays.

**Step 4** Click **Modify Button Items** in the **Association Information** area on the left side of the window.

A popup window warns you that unsaved changes (to the phone) may be lost. If you have made changes to the phone configuration, click **Cancel** and save those changes before proceeding.

**Step 5** Click **OK** to continue.

The **Reorder Phone Button Configuration** window displays. This window comprises the following panes:

**Associated Items**
This pane displays a list of the items that are assigned to the phone buttons in this phone button template. The system assigns the first item in the list to button 1, the second item to button 2, and so forth.
**Unassigned Associated Items**
This pane displays a list of the items that are not assigned to phone buttons in this phone button template.
**Dissociate These Items**
This pane displays a list of the items that cannot presently be assigned to a phone button.

**Step 6** Select an item in the **Associated Items** pane and click the up or down arrows to change the order of the associated items.

**Step 7** Select an item in either the **Associated Items** or **Unassigned Associated Items** panes and click the left or right arrows to move the item to the other pane.

**Step 8** Select an item in the **Associated Items** or **Unassigned Associated Items** panes and click the up or down arrows to move that item to the **Dissociate These Items** pane or vice versa.

**Step 9** Click **Save** after you have finished moving items among the panes and all items are in the desired order.

**Step 10** Click **Close** to close the **Reorder Phone Button Configuration** window.

# Find an Actively Logged-In Device

The Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster features keep a record of the devices to which users are actively logged in. For the Cisco Extension Mobility feature, the actively logged-in device report tracks the local phones that are actively logged in by local users; for the Cisco Extension Mobility Cross Cluster feature, the actively logged-in device report tracks the local phones that are actively logged in by remote users.

Cisco Unified Communications Manager provides a specific search window for searching for devices to which users are logged in. Follow these steps to search for a specific device or to list all devices for which users are actively logged in.

### Procedure

**Step 1** Choose **Device** > **Phone**.

**Step 2** Select the **Actively Logged In Device Report** from the **Related Links** drop-down list in the upper right corner and click **Go**.

**Step 3** To find all actively logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

**Note** To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

**Step 4** Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Step 5** From the list of records that display, click the link for the record that you want to view.

**Note** To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

# Find a Remotely Logged-In Device

The Cisco Extension Mobility Cross Cluster feature keeps a record of the devices to which users are logged in remotely. The Remotely Logged In Device report tracks the phones that other clusters own but that are actively logged in by local users who are using the EMCC feature.

Cisco Unified Communications Manager provides a specific search window for searching for devices to which users are logged in remotely. Follow these steps to search for a specific device or to list all devices for which users are logged in remotely.

### Procedure

**Step 1** Choose **Device** > **Phone**.

**Step 2** Select **Remotely Logged In Device** from the **Related Links** drop-down list in the upper right corner and click **Go**.

**Step 3** To find all remotely logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

**Note** To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

**Step 4** Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Step 5** From the list of records that display, click the link for the record that you want to view.

**Note** To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

# Remotely Lock a Phone

Some phones can be locked remotely. When you remotely lock a phone, the phone cannot be used until you unlock it.

If a phone supports the Remote Lock feature, a **Lock** button appears in the top right hand corner.

### Procedure

**Step 1** Choose **Device** > **Phone**.

**Step 2** From the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

**Step 3** Choose the phone for which you want to perform a remote lock.

**Step 4** On the **Phone Configuration** window, click **Lock**.

If the phone is not registered, a popup window displays to inform you that the phone will be locked the next time it is registered. Click **Lock**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgement.

# Reset a Phone to Factory Defaults

Some phones support a remote wipe feature. When you remotely wipe a phone, the operation resets the phone to its factory settings. Everything previously stored on the phone is wiped out.

If a phone supports the remote wipe feature, a **Wipe** button appears in the top right hand corner.

**Caution** This operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

### Procedure

**Step 1** Choose **Device** > **Phone**.

**Step 2** In the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

**Step 3** Choose the phone for which you want to perform a remote wipe.

**Step 4** In the **Phone Configuration** window, click **Wipe**.

If the phone is not registered, a popup window displays to inform you that the phone will be wiped the next time it is registered. Click **Wipe**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgment.

# Search for Locked or Reset Devices

You can search for devices that have been remotely locked and/or remotely reset to factory default settings. Follow these steps to search for a specific device or to list all devices which have been remotely locked and/or remotely wiped.

### Procedure

**Step 1** Choose **Device** > **Phone**.

The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

**Step 2** Select the **Phone Lock/Wipe Report** from the **Related Links** drop-down list in the upper right corner of the window and click **Go**.

**Step 3** To find all remotely locked or remotely wiped device records in the database, ensure that the text box is empty; go to Step 4.

To filter or search records for a specific device:

a) From the first drop-down list box, select the device operation type(s) to search.
b) From the second drop-down list box, select a search parameter.
c) From the third drop-down list box, select a search pattern.
d) Specify the appropriate search text, if applicable.

**Note** To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

**Step 4** Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Step 5** From the list of records that display, click the link for the record that you want to view.

**Note** To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

# Display Phone MAC Address

The Media Access Control (MAC) address comprises a unique, 12-character, hexadecimal number that identifies a Cisco Unified IP Phone or other hardware device. Locate the number on a label on the bottom of the phone (for example, 000B6A409C405 for Cisco Unified IP Phone 7900 family of phones or SS-00-0B-64-09-C4-05 for Cisco IP Phone SP 12+ and 30 VIP). Cisco Unified Communications Manager makes the MAC address a required field for Cisco Unified IP Phone device configuration. When you enter the MAC address in Cisco Unified Communications Manager fields, do not use spaces or dashes and do not include the “SS” that may precede the MAC address on the label.

For more information on displaying the MAC Address or additional configuration settings on Cisco Unified IP Phones, see the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* that supports the phone model. To display the MAC address for the Cisco IP Phone 12 Series and Cisco IP Phone 30 Series phones or the Cisco VG248 Gateway, perform the following tasks:

- Cisco IP Phone 12 (SP +) Series and 30 Series (VIP)—Press ** to display the MAC address on the second line of the LCD display.
- Cisco VG248 phone ports—The MAC address specifies the endpoint from the Gateway Configuration window of Cisco Unified Communications Manager Administration.
- Cisco VG224 phone ports—You can configure a Cisco VG224 gateway as an MGCP gateway or an SCCP gateway. When it is configured as an SCCP gateway, it can have 24 analog phone endpoints. When it is configured this way, it functions similarly to an IOS SCCP gateway. The MAC address for each individual phone gets calculated by using a formula that considers the slot position, subunit, port, and the last 10 characters of the original MAC address.
- Cisco IP Communicator—Get the MAC address from the network interface of the client PC on which you want to install the Cisco IP Communicator application.