



Client services framework setup

In Cisco Unified Communications Manager Administration, use the **Device > Phone** menu path to configure the Cisco Unified Client Services Framework device. This section describes how to configure a Cisco Unified Client Services Framework device through the Phone Configuration Settings window.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Additional information

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see topics related to Cisco Unified Communications Manager Administration application in the *Cisco Unified Communications Manager Administration Guide*, which explain how to use the GUI and detail the functions of the buttons and icons.

Client Services Framework configuration settings

The following table describes the available settings to configure a CTI remote device through the Phone Configuration Settings window.

Table 1: Client Services Framework Configuration Settings

Field	Description
Cisco Unified Client Services Framework Information	
Device Protocol	Specifies the protocol used to the Cisco Unified Client Services Framework.
Active Remote Destination	Specifies the Remote Destination which is active. The CSF client can specific one remote destination as 'active' at any one given time. Incoming calls and Dial via Office (DVO) calls are routed to the active remote destination.
Device Information	
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies if the device is trusted or not.
Device Name	Enter a text name for the Client Services Framework. This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the Client Services Framework. This field can comprise up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Select the device pool which defines the common characteristics for Client Services Framework. For more information on how to configure the device pool, see Device Pool Configuration Settings.
Common Device Configuration	Using the drop-down list box, choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.

Field	Description
Phone Button Template	Using the drop-down list box, 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.
Common Phone Profile	Using the drop-down list box, choose the common phone profile to specify the data that is required by the Cisco TFTP.
Calling Search Space	Choose the calling search space to be used for routing Mobile Voice Access or Enterprise Feature Access calls. Note This calling search space setting applies only when you are routing calls from the remote destination, which specifies the outbound call leg to the dialed number for Mobile Voice Access and Enterprise Feature Access calls.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. 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.
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. If you choose <none>, Cisco Unified Communications Manager uses the Media Resource Group that is defined in the device pool.
User Hold MOH Audio Source	Using the drop-down list box, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Network Hold MOH Audio Source	Using the drop-down list box, choose the audio source to use for MOH when the network initiates a hold action.
Location	Using the drop-down list box, choose the location that is associated with the phones and gateways in the device pool.
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. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

Field	Description
User Locale	<p>From the drop-down list box, choose the locale that is associated with the CTI route point. The user locale identifies a set of detailed information to support users, including language and font.</p> <p>Cisco Unified Communications Manager makes this field available only for CTI route points that support localization.</p> <p>Note If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool.</p> <p>Note 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 that is in the Cisco Unified Communications Operating System Administration Guide.</p>
Network Locale	<p>From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area.</p> <p>Note Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.</p>

Field	Description
Device Mobility Mode	<p>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.</p> <p>Click View Current Device Mobility Settings to display the current values of these device mobility parameters:</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager Group • Roaming Device Pool • Location • Region • Network Locale • AAR Group • AAR Calling Search Space • Device Calling Search Space • Media Resource Group List • SRST <p>For more configuration information, see “Device Mobility” in the <i>Cisco Unified Communications Manager Features and Services Guide</i>.</p>
Owner User ID	<p>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.</p> <p>Note Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.</p>
Mobility User ID	<p>From the drop-down list box, choose the user ID of the person to whom this dual-mode phone is assigned.</p> <p>Note The Mobility User ID configuration gets used for the Mobile Connect and Mobile Voice Access features for dual-mode phones.</p> <p>Note The Owner User ID and Mobility User ID can differ.</p>
Primary Phone	<p>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). See “Licensing” in the <i>Cisco Unified Communications Manager Features and Services Guide</i>.</p>

Field	Description
Use Trusted Relay Point	<p>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:</p> <ul style="list-style-type: none"> • 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. • 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. • 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. <p>A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.</p> <p>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).</p> <p>If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the “TRP Insertion in <i>Cisco Unified Communications Manager</i>” in the <i>Cisco Unified Communications Manager System Guide</i> for details of call behavior.</p> <p>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.</p> <p>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.</p> <p>See the “Trusted Relay Point” section and its subtopics in the “Media Resource Management” chapter of the <i>Cisco Unified Communications Manager System Guide</i> for a complete discussion of network virtualization and trusted relay points.</p>

Field	Description
Always Use Prime Line	<p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • 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. • 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. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco Call Manager service.
Always Use Prime Line for Voice Message	<p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • 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. • 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. • Default—Cisco Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco Call Manager service.
Calling Party Transformation CSS	<p>This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</p> <p>Tip Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.</p>
Geolocation	<p>From the drop-down list box, choose a geolocation.</p> <p>You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.</p> <p>You can also choose a geolocation that has been configured with the System > Geolocation Configuration menu option.</p>

Field	Description
Ignore Presentation Indicators (internal calls only)	<p>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.</p> <p>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.</p>
Allow Control of Device from CTI Allow Control of Device from CTI	<p>Check this check box to allow CTI to control and monitor this device.</p> <p>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.</p>
Logged Into Hunt Group	<p>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.</p> <p>Users use the softkey on the phone to log their phone in or out of the hunt list.</p>

Field	Description
Remote Device	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Require off-premise location	
Call Routing Information	
Inbound/Outbound Calls Information	
Calling Party Transformation CSS	<p>This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</p>
Use Device Pool Calling Party Transformation CSS	<p>To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.</p>
Protocol Specific Information	

Field	Description
Packet Capture Mode	<p>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:</p> <ul style="list-style-type: none"> • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • 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. <p>For more information on packet capturing, see the <i>Troubleshooting Guide for Cisco Unified Communications Manager</i>.</p>
Packet Capture Duration	<p>This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.</p> <p>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.</p> <p>To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.</p> <p>For more information on packet capturing, see the <i>Cisco Unified Communications Manager Troubleshooting Guide</i>.</p>
Presence Group	<p>Configure this field with the Presence feature.</p> <p>Note If you are not using this application user with presence, leave the default (None) setting for presence group.</p> <p>From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor.</p>

Field	Description
SIP Dial Rules	<p>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.</p> <p>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.</p>
MTP Preferred Originating Codec	<p>From the drop-down list box, choose the codec to use if a media termination point is required for SIP calls.</p>
Device Security Profile	<p>Choose the security profile to apply to the device.</p> <p>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.</p> <p>To identify the settings that the profile contains, choose System > Security Profile > Phone Security Profile.</p> <p>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.</p>
Rerouting Calling Search Space	<p>From the drop-down list box, choose a calling search space to use for rerouting.</p> <p>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.</p> <p>The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.</p>

Field	Description
SUBSCRIBE Calling Search Space	<p>Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user.</p> <p>From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box.</p> <p>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.</p> <p>To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.</p>
SIP Profile	<p>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.</p>
Digest User	<p>Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security).</p> <p>Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window.</p> <p>For more information on digest authentication, see the <i>Cisco Unified Communications Manager Security Guide</i>.</p>
Media Termination Point Required	<p>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).</p> <p>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.</p> <p>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.</p> <p>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.</p>
Unattended Port	<p>Check this check box to indicate an unattended port on this device.</p>

Field	Description
Require DTMF Reception	<p>For phones that are running SIP and SCCP, check this check box to require DTMF reception for this phone.</p> <p>Note In configuring Cisco Unified Mobility features, when using intercluster DNSs 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.</p>
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation	<p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • 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. <p>By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.</p> <p>For more information on CAPF operations, see the <i>Cisco Unified Communications Manager Security Guide</i>.</p>

Field	Description
Authentication Mode	<p>This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation.</p> <p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. <p>This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.</p> • 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. <p>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.</p> <p>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.</p> • 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. <p>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.</p> <p>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.</p>

Field	Description
Authentication String	<p>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.</p> <p>To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.</p>
Key Size (Bits)	<p>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.</p> <p>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.</p> <p>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.</p>
Operation Completes By	<p>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.</p> <p>The values that display apply for the publisher database server.</p>
Certificate Operation Status	<p>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.</p>
Enable Extension Mobility	
Enable Extension Mobility	<p>Check this check box if this phone supports extension mobility.</p>
Log Out Profile	<p>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.</p> <p>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.</p>

Field	Description
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.
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 for the device pool of the device. If the device pool 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.
Do Not Disturb	
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device.
DND Option	When you enable DND on the phone, Ringer Off parameter turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call.
Product Specific Configuration Layout Information	
Video Capabilities	When enabled, indicates that the device will participate in video calls. Default: Enabled