Trunk Setup

This chapter provides information about Cisco Unified Communications Manager trunk configuration.

About Trunk Setup

Use a trunk device to configure a logical route to a gatekeeper (that is, the wholesale network or an intercluster trunk with gatekeeper control), to an intercluster trunk without a gatekeeper, or to a SIP network. Choose from the following available trunk types:

- H.225 trunk (gatekeeper controlled)
- Intercluster trunk (gatekeeper controlled)
- Intercluster trunk (non-gatekeeper controlled)
- SIP trunk

Tip Configure SIP Trunk Security Profiles and SIP Profiles before you configure a SIP Trunk. For more information, see the *Cisco Unified Communications Manager Security Guide*.

Tip Resetting a trunk drops any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting/restarting an H.323 or SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed. Trunks do not have to undergo a Restart or Reset when Packet Capture is enabled or disabled.

H.225 and Intercluster Trunks Settings

The following table describes the trunk settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks.

Table 1: H.225 and Intercluster Trunks Settings

Field	Description
Device Information	
Device Name	Enter a unique identifier for the trunk.
Description	Enter a descriptive name for the trunk. 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 appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically. **Note** Calls that are initiated from a phone that is registered to a Cisco Unified Communications Manager that does not belong to the device pool of the trunk use different Cisco Unified Communications Managers of this device pool for different outgoing calls. Selection of nodes occurs in a random order.A call that is initiated from a phone that is registered to a Cisco Unified Communications Manager that does belong to the device pool of the trunk uses the same Cisco Unified Communications Manager node for outgoing calls if the Cisco Unified Communications Manager is up and running.
Common Device Configuration	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
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. The alerting tones are provided by Cisco Unified Communications Manager Annunciators. Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.

Field	Description
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. From the drop-down list box, choose the appropriate location for this trunk. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this trunk consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location Info** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*. The location also associates with the RSVP policy with regard to other locations. The configuration allows RSVP to be enabled and disabled based upon location pairs.
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.
Tunneled Protocol	This drop-down list box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. Choose the QSIG option if you want to use trunks to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified Communications Manager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, and Message Waiting Indication.

Field	Description
QSIG Variant	To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, choose one of the following options: • No Changes— Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • ECMA—Choose for ECMA PBXs that use Protocol Profile 0x91. • ISO—Choose for PBXs that use Protocol Profile 0x9F. For more information, see the following information: • Be aware that the QSIG Variant can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, choose one of the following options: • No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • Use Global Value ECMA—If you chose the ECMA option from the QSIG Variant drop-down list box, choose this option. • Use Global Value ISO—If you chose the ISO option from the QSIG Variant drop-down list box, choose this option. • Use Local Value For more information, see the following information: • Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

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: • 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 Communications Manager 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 Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager 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 IREC 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. **Tip** You do not have to reset the trunk after enabling/disabling Packet Capturing. For more information on capturing packets, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Field	Description
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. 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. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. For more information on capturing packets, see the *Cisco Unified Communications Manager Troubleshooting Guide*.
Media Termination Point Required	This check box is used to indicate whether a media termination point (MTP) is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use a media termination point to implement features. Uncheck the Media Termination Point Required check box if you do not want to use a media termination point to implement features. 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. If you check this check box to require an MTP and one or both parties are a video endpoint, the call operates as audio only.
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. For trunks, this check box pertains to calls that are received from Cisco Unified Communications Manager but not to calls that are received from the wide-area network (WAN). 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. 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
Wait for Far-End H.245 Terminal Capability Set	This field applies only to H.323 devices. This check box specifies that Cisco Unified Communications Manager 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 Communications Manager should initiate capabilities exchange, uncheck this check box.
Path Replacement Support	If you choose the QSIG option from the Tunneled Protocol drop-down list box, this check box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. This setting works with QSIG tunneling (Annex M.1) to ensure that non-H.323 information gets sent on the leg of the call that uses path replacement. **Note** The default setting leaves the check box unchecked. When you choose the QSIG Tunneled Protocol option, the system automatically checks the check box.
Transmit UTF-8 for Calling Party Name	If the Transmit UTF-8 for Calling Party Name is checked to obtain the locale, the SIP trunk attempts to obtain the locale from the device. If that fails, the SIP trunk attempts to obtain the user locale from the Common Device Configuration and if that fails the SIP trunk obtains the user locale used for the Enterprise Parameters.
Unattended Port	Check this check box if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port. The default value for this check box leaves it unchecked.

Field	Description
SRTP Allowed	Check the SRTP Allowed check box if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the trunk. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP. **Caution** If you check this check box, Cisco strongly recommends that you configure IPSec, so you do not expose keys and other security-related information during call negotiations. If you do not configure IPSec correctly, consider signaling between Cisco Unified Communications Manager and the gateway as nonsecure. For more information on encryption for trunks, see the *Cisco Unified Communications Manager Security Guide*.
H.235 Pass Through Allowed	This feature allows Cisco Unified Communications Manager to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel. To allow H.235 pass through, check the check box.
Enable SAF	Check this check box if you want to enable this intercluster (non-gatekeeper controlled) trunk for SAF. When a trunk is enabled for SAF, the trunk can support the call control discovery feature. SAF-enabled trunks that are assigned to the CCD advertising service in the Advertising Service window handle inbound calls from remote call-control entities that use the SAF network. (**Call Routing** > **Call Control Discovery** > **Advertising Service**) SAF-enabled trunks that are assigned to the CCD requesting service handle outgoing calls to learned patterns. (**Call Routing** > **Call Control Discovery** > **Requesting Service**) For more information on the call control discovery feature, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • 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. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager 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). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Field	Description
PSTN Access	If you use the Cisco Intercompany Media Engine feature, check this check box to indicate that calls made through this trunk might reach the PSTN. Check this check box even if all calls through this trunk device do not reach the PSTN. For example, check this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN. When checked, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. By default, this check box remains checked. For more information on Cisco Intercompany Media Engine, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.
Intercompany Media Engine (IME)	
E.164 Transformation Profile	Check this check box if you want to use the Cisco Intercompany Media Engine and calls might reach the PSTN. For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*. From the drop-down list box, choose the appropriate E.164 transformation that you created on the Intercompany Media Services E.164 Transformation Configuration window (**Advanced Features** > **Intercompany Media Services** > **E.164 Transformation**). For more information on Cisco Intercompany Media Engine, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.
Incoming Calling Party Settings	
Clear Prefix Setting	To delete all prefixes for all calling party number types, click Clear Prefix Settings.
Default Prefix Setting	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	

Field	Description
	Configure the following settings to globalize calling party numbers that use National for the Calling Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use National for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the calling search space that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the 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. **Tip** For more information on configuring these settings, see the *Cisco Unified*

Field	Description
	Communications Manager Features and Services Guide.

Field	Description
International Number	

Field	Description
	Configure the following settings to globalize calling party numbers that use International for the Calling Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use International for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes. • Use Device Pool CSS— Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to globalize the calling party number of International calling party number type 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. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the 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. **Tip** For more information on configuring

Field	Description
	these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
Subscriber Number	

Field	Description
	Configure the following settings to globalize calling party numbers that use Subscriber for the Calling Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Subscriber for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to globalize the calling party number of Subscriber calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the 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. **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features*

Field	Description
	and Services Guide.

Field	Description
Unknown Number	

Field	Description
	Configure the following settings to globalize calling party numbers that use Unknown for the Calling Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to globalize the calling party number of Unknown calling party number type 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. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the 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. **Tip** For more information on configuring these settings, see the *Cisco Unified*

Field	Description
	Communications Manager Features and Services Guide.
Incoming Called Party Settings The H.323 protocol does not support the international escape character +. To ensure the correct prefixes, including the +, get applied to inbound calls over H.323 trunks, configure the incoming called party settings; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk.	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	

Field	Description
	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of National type before it applies the prefixes. • Use Device Pool CSS— Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you

Field	Description
	want to assign to this device.

Field	Description
International Number	

Field	Description
	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation

Field	Description
	pattern that you want to assign to this device.

Field	Description
Unknown Number	

Field	Description
	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains

Field	Description
	the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	

Field	Description
	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation

Field	Description
	pattern that you want to assign to this device.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that was set for the device pool. 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.
MLPP Indication	If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. **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.
Call Routing Information	
Inbound Calls	
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the H.323 device. Choose the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called.

Field	Description
Calling Search Space	From the drop-down list box, select the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Calling Search Spaces window. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing 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.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.

Field	Description
Redirecting Number IE Delivery - Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE. 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. **Note** Default leaves the check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.
Enable Inbound FastStart	Check this check box to enable the H.323 FastStart call connections on incoming calls. By default, the check box remains unchecked for the H.323 gateway. For intercluster calls, you must check the Enable Inbound FastStart check box on Cisco Unified Communications Manager servers in other clusters for the outbound FastStart feature to work.
Connected Party Settings	

Field	Description
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number that Cisco Unified Communications Manager sends in another format, such as a DID or E.164 number. This setting is applicable while sending connected number for basic call as well as sending connected number after inbound call is redirected. Cisco Unified Communications Manager includes the transformed number in the Connected Number Information Element (IE) of CONNECT and NOTIFY messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Connected Party Transformation CSS	To use the Connected 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 Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.

Field	Description
Use Device Pool Called Party Transformation CSS	To use the Called 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 Called Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. 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. **Tip** 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.
Use Device Pool Calling Party Transformation CSS	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.
Calling Party Selection	Choose the directory number that is sent on an outbound call on a gateway. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call.

Field	Description
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP) as a supplementary service to control the display of the calling party number on the called party phone display screen. Choose Default if you do not want to change the presentation setting. Choose Allowed if you want calling number information to display. Choose Restricted if you do not want the calling number information to display.
Called Party IE Number Type Unknown	Choose the format for the type of number in called party directory numbers. Cisco Unified Communications Manager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • Cisco Unified Communications Manager—Cisco Unified Communications Manager sets the directory number type. • Unknown—This option indicates that the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Field	Description
Calling Party IE Number Type Unknown	Choose the format for the type of number in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • Cisco Unified Communications Manager—Cisco Unified Communications Manager sets the directory number type. • Unknown—This option indicates that the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number. **Tip** In the Gateway and Trunk Configuration window, you can configure the Calling Party IE Number Type Unknown setting. If you can configure this setting and choose any other option except Cisco Unified Communications Manager, which is the default, your configuration for this field overwrites the Calling Party Number Type setting for the outgoing call through a particular gateway.

Field	Description
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called numbering plan to be encoded to a non-national numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option indicates that the dialing plan is unknown.

Field	Description
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling numbering plan to be encoded to a non-national numbering plan. Choose one of the following options: • Cisco Unified Communications Manager—Cisco Unified Communications Manager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option indicates that the dialing plan is unknown.
Caller ID DN	Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk. For example, in North America • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can enter the international escape character +.

Field	Description
Display IE Delivery	Check this check box to enable delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service. **Note** The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.
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 Communications Manager includes the Redirecting Number IE.) Uncheck the check box to exclude the first Redirecting Number and the redirecting reason. 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. **Note** The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.
Enable Outbound FastStart	Check this check box to enable the H.323 FastStart feature on outgoing calls. By default, the check box remains unchecked for the H.323 gateway or trunk. When you check the Enable Outbound FastStart check box, you must set the Media Termination Point Required, Media Resource Group Lists, and Codec for Outbound FastStart.

Field	Description
Codec For Outbound FastStart	Choose the codec for use with the H.323 device for an outbound FastStart call: • G711 mu-law 64K (default) • G711 a-law 64K • G723 • G729 • G729AnnexA • G729AnnexB • G729AnnexA-AnnexB When you check the Enable Outbound FastStart check box, you must choose the codec for supporting outbound FastStart calls.
Gatekeeper Information (for gatekeeper-controlled H.225 trunks and intercluster trunks)	
Gatekeeper Name	Choose the gatekeeper that controls this trunk. **Note** For a gatekeeper-controlled trunk to register correctly with a gatekeeper through use of H.323 dynamic addressing, you must set the Send Product ID and Version ID service parameter to True. (The default value specifies False.) To do so, choose System > Service Parameters and find the Send Product ID and Version ID service parameter for the Cisco CallManager service in the Clusterwide Parameters (Device - H323) portion of the Service Parameter Configuration window.
Terminal Type	Use the Terminal Type field to designate the type for all devices that this trunk controls. Always set this field to Gateway for normal trunk call admission control.

Field	Description
Technology Prefix	Use this optional field to eliminate the need for entering the IP address of every Cisco Unified Communications Manager when configuring the gw-type-prefix on the gatekeeper: • If you leave this field blank (the default setting), you must specify the IP address of each Cisco Unified Communications Manager that can register with the gatekeeper when you enter the gw-type-prefix command on the gatekeeper. • When you use this field, make sure that the value that you enter exactly matches the type-prefix value that is specified with the gw-type-prefix command on the gatekeeper. For example, if you leave this field blank and you have two Cisco Unified Communications Managers with IP addresses of 10.1.1.2 and 11.1.1.3, enter the following gw-type-prefix command on the gatekeeper: gw-type-prefix 1#* default-technology gw ip 10.1.1.2 gw ip 11.1.1.3 If you enter 1#* in this field, enter the following gw-type-prefix command on the gatekeeper: gw-type-prefix 1#* default-technology
Zone	Use this optional field to request a specific zone on the gatekeeper with which Cisco Unified Communications Manager will register. The zone specifies the total bandwidth that is available for calls between this zone and another zone: • If you do not enter a value in this field, the zone subnet command on the gatekeeper determines the zone with which Cisco Unified Communications Manager registers. Cisco recommends the default setting for most configurations. • If you want Cisco Unified Communications Manager to register with a specific zone on the gatekeeper, enter the value in this field that exactly matches the zone name that is configured on the gatekeeper with the zone command. Specifying a zone name in this field eliminates the need for a zone subnet command for each Cisco Unified Communications Manager that is registered with the gatekeeper. See the command reference documentation for your gatekeeper for more information.

Field	Description
Remote Cisco Unified Communications Manager Information (for non-gatekeeper-controlled intercluster trunks)	
Server 1 IP Address/Host Name	Enter the IP address or host name of the first remote Cisco Unified Communications Manager that this trunk accesses.
Server 2 IP Address/Host Name	Enter the IP address or host name of the second remote Cisco Unified Communications Manager that this trunk accesses. **Note** If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a second Cisco Unified Communications Manager node, you must enter the second remote Cisco Unified Communications Manager IP address/host name in this field.
Server 3 IP Address/Host Name	Enter the IP address or host name of the third remote Cisco Unified Communications Manager that this trunk accesses. **Note** If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a third Cisco Unified Communications Manager node, you must enter the third remote Cisco Unified Communications Manager IP address/host name in this field.
UUIE Configuration	
Passing Precedence Level Through UUIE	Check this check box to enable passing MLPP information through the PRI 4ESS UUIE field. The system uses this box for interworking with DRSN switch. The system makes this check box available only if the PRI Protocol Type value of PRI 4ESS is specified for this trunk. The default value specifies unchecked.
Security Access Level	Enter the value for the security access level. Valid values include 00 through 99. The system makes this field available only if the Passing Precedence Level Through UUIE check box is checked. The default value specifies 2.

Field	Description
Geolocation Configuration	
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter** menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.
Send Geolocation Information	Check this box to send geolocation information for this device. For an overview and details of how logical partitioning uses geolocation information, see the Cisco Unified Communications Manager Features and Services Guide.

SIP Trunk Settings

The following table describes the settings for SIP trunks.

Table 2: SIP Trunk Settings

Field	Description
Trunk Service Type	Choose one of the following options from the Trunk Service Type drop-down list box: • None—Choose this option if the trunk will not be used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine. • Call Control Discovery—Choosing this option enables the trunk to support call control discovery. If you assign this trunk to the CCD advertising service in the Advertising Service window, the trunk handles inbound calls from remote call-control entities that use the SAF network. If you assign this trunk to the CCD requesting service in the Requesting Service window, the trunk handles outgoing calls to learned patterns. For more information on the call control discovery feature, see the *Cisco Unified Communications Manager Features and Services Guide*. • Extension Mobility Cross Cluster—Choose this option to enable the trunk to support the Extension Mobility Cross Cluster (EMCC) feature. Choosing this option causes the following settings to remain blank or unchecked and become unavailable for configuration, thus retaining their default values: Media Termination Point Required, Unattended Port, Destination Address, Destination Address IPv6, and Destination Address is an SRV. For more information about the EMCC feature, see the *Cisco Unified Communications Manager Features and Services Guide*. • Cisco Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field. **Tip** After you choose Call Control Discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine for the trunk service type and click Next, you cannot change the trunk to a different type.

Field	Description
Device Information	
Device Name	Enter a unique identifier for the trunk. Enter a unique identifier for the trunk. The device name can include up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only.
Description	Enter a descriptive name for the trunk. The description can include up to 114 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically. **Note** Calls that are initiated from a phone that is registered to a Cisco Unified Communications Manager that does not belong to the device pool of the trunk use different Cisco Unified Communications Managers of this device pool for different outgoing calls. Selection of Cisco Unified Communications Manager nodes occurs in a random order. A call that is initiated from a phone that is registered to a Cisco Unified Communications Manager that does belong to the device pool of the trunk uses the same Cisco Unified Communications Manager node for outgoing calls if the Cisco Unified Communications Manager is up and running. The default value for Device Pool specifies Not Selected.
Common Device Configuration	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
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). The default value for Call Classification is Use System Default. When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. The default value for Media Resource Group List specifies None.

Field	Description
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. From the drop-down list box, choose the appropriate location for this trunk. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this trunk consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*. The location also associates with the RSVP policy with regard to other locations. The configuration allows RSVP to be enabled and disabled based upon location pairs.
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. The default value for AAR Group specifies None.

Field	Description

Tunneled Protocol	Select the QSIG option if you want to use SIP trunks or SIP gateways to transport (tunnel) QSIG messages from Cisco Unified Communications Manager to other PINXs. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Path Replacement, and Message Waiting Indication (MWI).
	Note Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway.
	To turn off RPID headers on the SIP gateway, apply a SIP profile to the voIP dial peer on the gateway, as shown in the following example:
	`voice class sip-profiles 1000request ANY`
	`sip-header Remote-Party_ID remove`
	`response ANY sip-header Remote-Party-ID remove`
	`dial-peer voice 124 voip`
	`destination-pattern 3...`
	`signaling forward unconditional`
	`session protocol sipv2`
	`session target ipv4:<ip address>`
	`voice-class sip profiles 1000`

Field	Description
QSIG Variant	To display the options in the QSIG Variant drop-down list box, select QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, select one of the following options: • No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • ECMA—Select for ECMA PBX systems that use Protocol Profile 0x91. • ISO—Select for PBX systems that use Protocol Profile 0x9F. For more information, see the following information: • Be aware that the QSIG Variant can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
ASN.1 ROSE OID Encoding	To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, select one of the following options: • No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • Not Selected • Use Global Value ECMA—If you selected the ECMA option from the QSIG Variant drop-down list box, select this option. • Use Global Value ISO—If you selected the ISO option from the QSIG Variant drop-down list box, select this option. • Use Local Value For more information, see the following information: • Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the Cisco Unified Communications Manager System Guide.

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: • 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 Communications Manager 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 Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager 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. Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices. For more information on capturing packets, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Field	Description
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. 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. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. For more information on capturing packets, see the *Cisco Unified Communications Manager Troubleshooting Guide*.
Media Termination Point Required	You can configure Cisco Unified Communications Manager SIP trunks to always use an MTP. Check this check box to provide media channel information in the outgoing INVITE request. When this check box is checked, all media channels must terminate and reoriginate on the MTP device. If you uncheck the check box, the Cisco Unified Communications Manager can decide whether calls are to go through the MTP device or be connected directly between the endpoints. **Note** If check box remains unchecked (default case), Cisco Unified Communications Manager will attempt to dynamically allocate an MTP if the DTMF methods for the call legs are not compatible. For example, existing phones that run SCCP support only out-of-band DTMF, and existing phones that run SIP support RFC2833. Because the DTMF methods are not identical, the Cisco Unified Communications Manager dynamically allocates an MTP. If, however, a new phone that runs SCCP, which supports RFC2833 and out-of-band, calls an existing phone that runs SIP, Cisco Unified Communications Manager does not allocate an MTP because both phones support RFC2833. So, by having the same type of DTMF method supported on each phone, no need exists for MTP.

Field	Description
Retry Video Call as Audio	This check box pertains to outgoing SIP trunk calls and does not impact incoming calls. 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. 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.
Path Replacement Support	This check box displays when you select QSIG from the Tunneled Protocol drop-down list box. This setting works with QSIG tunneling to ensure that non-SIP information gets sent on the leg of the call that uses path replacement. **Note** The default setting leaves the check box unchecked. When you select the QSIG Tunneled Protocol option, the system automatically checks the check box. Alternatively, if the Tunneled Protocol option is set to None, the Path Replacement Support check box displays as grayed out and is not available.

Field	Description
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool. If the user locale setting matches the terminating phone user locale, the phone displays the characters. **Note** The phone may display malformed characters if the two ends of the trunk configure user locales that do not belong to the same language group. The default value for Transmit UTF-8 for Calling Party Name leaves the check box unchecked.
Transmit UTF-8 Names in QSIG APDU	This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode and encodes in UTF-8 format. If the user locale settings do not match, the device sends ASCII and encodes in UTF-8 format. If the configuration parameter is not set and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode (if the name uses 8-bit format) and encodes in ISO8859-1 format. The default value for Transmit UTF-8 Names in QSIG APDU leaves the check box unchecked.
Unattended Port	Check this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port. The default value for this check box leaves it unchecked.

Field	Description
SRTP Allowed	Check this check box if you want Cisco Unified Communications Manager to allow secure and nonsecure media calls over the trunk. Checking this check box enables Secure Real-Time Protocol (SRTP) SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP negotiation instead. The default value for this check box leaves it unchecked. **Caution** If you check this check box, Cisco strongly recommends that you use an encrypted TLS profile, so that keys and other security-related information do not get exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will get exposed in signaling and traces. In that case, you must ensure the security of the network between Cisco Unified Communications Manager and the destination side of the trunk. For more information on encryption for trunks, see the *Cisco Unified Communications Manager Security Guide*.
Consider Traffic on This Trunk Secure	This field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport. Choose one of the following values: • When using both sRTP and TLS—Default • When using sRTP Only—Displays when you check the SRTP Allowed check box For more information on security and trunks, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Route Class Signaling Enabled	From the drop-down list, enable or disable route class signaling for the port. Choose one of the following values: • Default—If you choose this value, the device uses the setting from the Route Class Signaling service parameter. • Off—Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter. • On—Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the Hotline feature.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • 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. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager 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). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Field	Description
PSTN Access	If you use the Cisco Intercompany Media Engine feature, check this check box to indicate that calls made through this trunk might reach the PSTN. Check this check box even if all calls through this trunk device do not reach the PSTN. For example, check this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN. When checked, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. By default, this check box remains checked. For more information on Cisco Intercompany Media Engine, see the Cisco Intercompany Media Engine Installation and Configuration Guide.
Run On All Active Unified CM Nodes	To enable the trunk to run on every node, check this check box.
Intercompany Media Engine (IME)	
E.164 Transformation Profile	Check this check box if you want to use the Cisco Intercompany Media Engine and calls might reach the PSTN. For more information, see the Cisco Intercompany Media Engine Installation and Configuration Guide. From the drop-down list box, choose the appropriate E.164 transformation that you created on the Intercompany Media Services E.164 Transformation Configuration window (**Advanced Features** > **Intercompany Media Services** > **E.164 Transformation**). For more information on Cisco Intercompany Media Engine, see the Cisco Intercompany Media Engine Installation and Configuration Guide.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that is set for the device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter. The default value for MLPP Domain specifies None.

Field	Description
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: • Fixed—CAL value has higher precedence over call completion. • Variable—Call completion has higher precedence over CAL level.
Call Routing Information	

Field	Description
Remote-Party-ID	

Field	Description
	Use this check box to allow or disallow the SIP trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Cisco Unified Communications Manager to the remote destination. If you check this box, the SIP trunk always sends the RPID header. If you do not check this box, the SIP trunk does not send the RPID header. **Note** Be aware that Calling Name Presentation, Connected Line ID, and Connected Name Presentation are not available when QSIG tunneling is enabled. Outgoing SIP Trunk Calls The configured values of the Calling Line ID Presentation and Calling Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. If either option is set to Default, the corresponding information (Calling Line ID Presentation and/or Calling Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Cisco Unified Communications Manager. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window. Incoming SIP Trunk Calls The configured values of the Connected Line ID Presentation and Connected Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. Be aware that the Connected Line ID Presentation and Connected Name Presentation options are relevant for 180/200 messages that the SIP trunk sends in response to INVITE messages that Cisco Unified Communications Manager receives. If either option is set to Default, the corresponding information (Connected Line ID Presentation and/or Connected Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Cisco Unified Communications Manager. If either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk

Field	Description
	configuration window. **Note** The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.

Field	Description
Asserted Identity	

Field	Description
	Use this check box to allow or disallow the SIP trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you check this check box, the SIP trunk always sends the Asserted-Type header; whether the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration. If the check box is not selected, the SIP trunk does not include any Asserted-Type or SIP Privacy headers in its SIP messages. For more information, see the descriptions of Asserted-Type and SIP Privacy in this table. Outgoing SIP Trunk Calls—P Headers The decision of which Asserted Identity (either P-Asserted-Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Cisco Unified Communications Manager Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Cisco Unified Communications Manager Call Control dictates the type of Asserted-Identity. Outgoing SIP Trunk Calls—SIP Privacy Header The SIP Privacy header gets used only when you check the Asserted Identity check box and when the SIP trunk sends either a PAI or PPI header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages). The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Cisco Unified Communications Manager Call Control. If the SIP Privacy option is set to Default, the Calling Line ID Presentation and Calling Name Presentation that the SIP trunk receives from Cisco Unified Communications Manager Call Control determines the SIP Privacy header. Incoming SIP Trunk Calls—P Headers The decision of which Asserted Identity (either P-Asserted-Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Cisco

Field	Description
	Unified Communications Manager Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Cisco Unified Communications Manager Call Control dictates the type of Asserted-Identity. Incoming SIP Trunk Calls—SIP Privacy Header The SIP Privacy header gets used only when you check the Asserted Identity check box and when the SIP trunk sends either a PAI or PPI header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages.) The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Cisco Unified Communications Manager Call Control. If the SIP Privacy option is set to Default, the Connected Line ID Presentation and Connected Name Presentation that the SIP trunk receives from Cisco Unified Communications Manager Call Control determine the SIP Privacy header. **Note** The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.

Field	Description
Asserted-Type	From the drop-down list, choose one of the following values to specify the type of Asserted Identity header that SIP trunk messages should include: • Default—This option represents the default value; Screening indication information that the SIP trunk receives from Cisco Unified Communications Manager Call Control determines the type of header that the SIP trunk sends. • PAI—The Privacy-Asserted Identity (PAI) header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Cisco Unified Communications Manager. • PPI—The Privacy Preferred Identity (PPI) header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Cisco Unified Communications Manager. **Note** These headers get sent only if the Asserted Identity check box is checked.

Field	Description
SIP Privacy	From the drop-down list, choose one of the following values to specify the type of SIP privacy header for SIP trunk messages to include: • Default—This option represents the default value; Name/Number Presentation values that the SIP trunk receives from the Cisco Unified Communications Manager Call Control compose the SIP Privacy header. For example, if Name/Number presentation specifies Restricted, the SIP trunk sends the SIP Privacy header; however, if Name/Number presentation specifies Allowed, the SIP trunk does not send the Privacy header. • None—The SIP trunk includes the Privacy:none header and implies Presentation allowed; this value overrides the Presentation information that comes from Cisco Unified Communications Manager. • ID—The SIP trunk includes the Privacy:id header and implies Presentation restricted for both name and number; this value overrides the Presentation information that comes from Cisco Unified Communications Manager. • ID Critical—The SIP trunk includes the Privacy:id;critical header and implies Presentation restricted for both name and number. The label critical implies that privacy services that are requested for this message are critical, and, if the network cannot provide these privacy services, this request should get rejected. This value overrides the Presentation information that comes from Cisco Unified Communications Manager. **Note** These headers get sent only if the Asserted Identity check box is checked.
Inbound Calls	

Field	Description
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the SIP device. Choose the number of significant digits to collect, from 0 to 32, or choose All. **Note** Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. The default value for Significant Digits specifies All.
Connected Line ID Presentation	Cisco Unified Communications Manager uses connected line ID presentation (COLP) as a supplementary service to provide the calling party with the connected party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Connected Line ID Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send connected line information. Choose Restricted if you do not want Cisco Unified Communications Manager to send connected line information. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. **Note** Be aware that this service is not available when QSIG tunneling is enabled. For more information about this field, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Connected Name Presentations	Cisco Unified Communications Manager uses connected name ID presentation (CONP) as a supplementary service to provide the calling party with the connected party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Connected Name Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send connected name information. Choose Restricted if you do not want Cisco Unified Communications Manager to send connected name information. **Note** Be aware that this service is not available when QSIG tunneling is enabled.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Calling Search Spaces window. Find and choose a calling search space name. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose CCMAdmin Parameters. The default value for Calling Search Space specifies None.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing 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. The default value for AAR Calling Search Space specifies None.

Field	Description
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.
Redirecting Diversion Header Delivery - Inbound	Check this check box to accept the Redirecting Number in the incoming INVITE message to the Cisco Unified Communications Manager. Uncheck the check box to exclude the Redirecting Number in the incoming INVITE message to the Cisco Unified Communications Manager. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Deliver - Inbound specifies not checked.
Incoming Calling Party Settings	
Clear Prefix Setting	To delete all prefixes for all calling party number types, click Clear Prefix Settings.
Default Prefix Setting	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
Incoming Number	

Field	Description
	Configure the following settings to globalize calling party numbers that use Unknown for the Calling Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality. • Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to globalize the calling party number of Unknown calling party number type 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. Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the 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. **Tip** For more information on configuring

Field	Description
	these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.
Incoming Called Party Settings	
Clear Prefix Settings	To delete the prefix for unknown number type for the called party, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for the Prefix field for unknown number type, click Default Prefix Settings.

Field	Description
Unknown Number	

Field	Description
	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown

Field	Description
	Number field that is configured in the device pool that is applied to the device.
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Cisco Unified Communications Manager includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing.
Use Device Pool Connected Party Transformation CSS	To use the Connected 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 Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Outbound Calls	
Called Party Transformation CSS	This settings allows you to send the transformed called party number in INVITE message for outgoing calls made over SIP Trunk. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Use Device Pool Called Party Transformation CSS	To use the Called 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 Called Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Calling Party Transformation CSS	This settings allows you to send the transformed calling party number in INVITE message for outgoing calls made over SIP Trunk. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number that is sent from Cisco Unified Communications Manager side in outgoing reINVITE / UPDATE messages. 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. **Tip** 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.
Use Device Pool Calling Party Transformation CSS	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.

Field	Description
Calling Party Selection	Choose the directory number that is sent on an outbound call. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call. The default value for Calling Party Selection specifies Originator.
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP) as a supplementary service to provide the calling party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Calling Line ID Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send calling number information. Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling number information.

Field	Description
Calling Name Presentation	Cisco Unified Communications Manager uses calling name ID presentation (CNIP) as a supplementary service to provide the calling party name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Choose Allowed, which is the default, if you want Cisco Unified Communications Manager to send calling name information. Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling name information. The default value for Calling Name Presentation specifies Default. **Note** Be aware that this service is not available when QSIG tunneling is enabled.
Caller ID DN	Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk. For example, in North America • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can enter the international escape character +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.

Field	Description
Calling and Connected Party Info Format	This option allows you to configure whether Cisco Unified Communications Manager inserts a directory number, a directory URI, or a blended address that includes both the directory number and directory URI in the SIP identity headers for outgoing SIP messages. From the drop-down list box, choose one of the following options: • Deliver DN only in connected party—In outgoing SIP messages, Cisco Unified Communications Manager inserts the calling party’s directory number in the SIP contact header information. This is the default setting. • Deliver URI only in connected party, if available—In outgoing SIP messages, Cisco Unified Communications Manager inserts the sending party’s directory URI in the SIP contact header. If a directory URI is not available, Cisco Unified Communications Manager inserts the directory number instead. • Deliver URI and DN in connected party, if available—In outgoing SIP messages, Cisco Unified Communications Manager inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Cisco Unified Communications Manager includes the directory number only. **Note** You should set this field to Deliver URI only in connected party or Deliver URI and DN in connected party only if you are setting up URI dialing between Cisco Unified CM systems of release 9.0 or greater, or between a Cisco Unified CM system of release 9. 0 or greater and a third party solution that supports URI dialing. Otherwise, you must set this field to Deliver DN only in connected party. For more information on URI dialing, see the URI dialing chapter in the *Cisco Unified Communications Manager System Guide*.

Field	Description
Redirecting Diversion Header Delivery - Outbound	Check this check box to include the Redirecting Number in the outgoing INVITE message from the Cisco Unified Communications Manager to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing INVITE message. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Delivery - Outbound specifies check box does not get checked.
SIP Information	
Destination Address	The Destination Address represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked. **Tip** For SIP trunks that can support IPv6 or IPv6 and IPv4s, configure the Destination Address IPv6 field in addition to the Destination Address field. **Note** SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. **Note** For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and check the Destination Address is an SRV Destination Port check box. If the remote end is a Cisco Unified Communications Manager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster.

Field	Description
Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field: • A fully qualified domain name (FQDN) • A DNS SRV record, but only if the Destination Address is an SRV field is checked. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Cisco Unified Communications Manager cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster. **Tip** For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field.
Destination Address is an SRV	This field specifies that the configured Destination Address is an SRV record. The default value specifies unchecked.
Destination Port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 - 65535, or 0. **Note** You can now have the same port number that is specified for multiple trunks. You need not enter a value if the destination address is an DNS SRV port. The default 5060 indicates the SIP port. The default value for Destination Port specifies 5060.

Field	Description
MTP Preferred Originating Codec	Indicate the preferred outgoing codec: • 711ulaw • 711alaw • G729/G729a • G729b/G729ab **Note** To configure G.729 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.729 codec. For more information, see the *Cisco Unified Communications Manager System Guide*. This field gets used only when the MTP Termination Point Required check box is checked.
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the SIP trunk. The selected group specifies the destinations that the device/application/server that is connected to the SIP trunk can monitor. The default value for Presence Group specifies Standard Presence group, which gets configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. See the *Cisco Unified Communications Manager Features and Services Guide* for information about configuring permissions between groups. **Tip** You can apply a presence group to the SIP trunk or to the application that is connected to the SIP trunk. If a presence group is configured for both a SIP trunk and SIP trunk application, the presence group that is applied to the application overrides the presence group that is applied to the trunk.

Field	Description
SIP Trunk Security Profile	Choose the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks that are configured in Cisco Unified Communications Manager Administration. Installing Cisco Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. To identify the settings that the profile contains, choose **System** > **Security Profile** > **SIP Trunk Security Profile**. For information on how to configure security profiles, see the *Cisco Unified Communications Manager Security Guide*. The default value for SIP Trunk Security Profile specifies Not Selected.
Rerouting Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The rerouting calling search space gets used to determine where a SIP user (A) can refer another user (B) to a third party (C). After the refer is completed, B and C connect. In this case, the rerouting calling search space that is used is that of the initial SIP user (A). **Note** Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. The default value for Rerouting Calling Search Space specifies None.
Out-of-Dialog Refer Calling Search Space	Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The out-of-dialog calling search space gets used when a Cisco Unified Communications Manager refers a call (B) that is coming into SIP user (A) to a third party (C) when no involvement of SIP user (A) exists. In this case, the system uses the out-of-dialog calling search space of SIP user (A). The default value for Out-of-Dialog Refer Calling Search Space specifies None.

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests from the device/server/application that connects to the SIP trunk. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the SIP trunk. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the SIP trunk. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the SIP trunk from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.
SIP Profile	From the drop-down list box, choose the SIP profile that is to be used for this SIP trunk. The default value for SIP Profile specifies None Selected.

Field	Description
DTMF Signaling Method	Choose from the following options: No Preference (default)—Cisco Unified Communications Manager will pick the DTMF method to negotiate DTMF, so the call does not require an MTP. If Cisco Unified Communications Manager has no choice but to allocate an MTP (if the Media Termination Point Required check box is checked), SIP trunk will negotiate DTMF to RFC2833. RFC 2833—Choose this configuration if the preferred DTMF method to be used across the trunk is RFC2833. Cisco Unified Communications Manager makes every effort to negotiate RFC2833, regardless of MTP usage. Out of band provides the fallback method if the peer endpoint supports it. OOB and RFC 2833—Choose this configuration if both out of band and RFC2833 should be used for DTMF. **Note** If the peer endpoint supports both out of band and RFC2833, Cisco Unified Communications Manager will negotiate both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events would get sent for the same DTMF keypress (one out of band and the other, RFC2833).
Normalization Script	
Normalization Script	From the drop-down list box, choose the script that you want to apply to this trunk. To import another script, go to the SIP Normalization Script Configuration window (**Device** > **Device Settings** > **SIP Normalization Script**), and import a new script file.

Field	Description
Parameter Name/Parameter Value	Optionally, enter parameter names and parameter values. Valid values include all characters except equals signs (=), semi-colons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value. Example: Parameter Name Parameter Value CCA-ID 11223344 pbx location RTP You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values. To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button.
Enable Trace	Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces SDI trace. **Note** Cisco recommends that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.
Recording Information	
None	To disable the trunk for call recording, click the **None**radio button.
This trunk connects to a recording-enabled gateway	To establish the recording session using the recording enabled Cisco gateway directly connected by this trunk, click **This trunk connects to a recording-enabled gateway** radio button. **Note** Ensure that the gateway used for recording has media forking capabilities.
This trunk connects to other clusters with trunk	To establish recording session in the other cluster connected by this trunk, **This trunk connects to other clusters with trunk** radio button.
Geolocation Configuration	

Field	Description
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System** > **Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.
Geolocation Filter	From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System** > **Geolocation Filter**menu option. For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.
Send Geolocation Information	Check this check box to send geolocation information for this device. For an overview and details of how logical partitioning uses geolocation information, see the the Cisco Unified Communications Manager Features and Services Guide.

Find Trunk

Because you might have multiple trunks in your network, Cisco Unified Communications Manager lets you search for trunks on the basis of specified criteria. Follow these steps to search for a specific trunk in the Cisco Unified Communications Manager database.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your trunk search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your trunk search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Device** > **Trunk**.

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

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 95.

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 3 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.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4 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.

Set Up Trunk

Perform the following procedure to add a new trunk device or update an existing trunk device.

Note You can configure multiple trunk devices per Cisco Unified Communications Manager cluster.

Before you begin

Configure SIP Trunk Security Profiles and SIP Profiles before you configure a SIP Trunk. For more information, see the related topics and the *Cisco Unified Communications Manager Security Guide*.

Procedure

Step 1 Choose **Device** > **Trunk**.

The Find and List Trunks window displays.

Step 2 Perform one of the followings tasks:

a) To add a new trunk device, click the Add New button. The Trunk Configuration window displays. Continue with Step 3, on page 96.
b) To update trunk settings, locate the appropriate trunk. Click the name of the trunk that you want to update. Continue with Step 7, on page 97.

Step 3 From the Trunk Type drop-down list, choose the type of trunk.

Step 4 If applicable, from the Device Protocol drop-down list, choose the device protocol.

Step 5 For SIP trunks, choose one of the following options from the Trunk Service Type drop-down list box:

a) None—Choose this option if the trunk will not be used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine.
b) Call Control Discovery—Choosing this option enables the trunk to support call control discovery. If you assign this trunk to the CCD advertising service in the Advertising Service window, the trunk handles inbound calls from remote call-control entities that use the SAF network. If you assign this trunk to the CCD requesting service in the Requesting Service window, the trunk handles outgoing calls to learned patterns. For more information on the call control discovery feature, see the *Cisco Unified Communications Manager Features and Services Guide*.
c) Extension Mobility Cross Cluster—Choosing this option enables the trunk to support the Extension Mobility Cross Cluster feature. For more information on the Extension Mobility Cross Cluster feature, see the *Cisco Unified Communications Manager Features and Services Guide*.
d) Cisco Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field.

Tip After you choose Call Control Discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine for the trunk service type and click Next, you cannot change the trunk to a different type.

Step 6 Click Next.

Step 7 On the Trunk Configuration window that displays, enter the appropriate settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks as described in H.225 and Intercluster Trunks Settings , on page 2. For SIP trunks, enter the appropriate settings as described in Table 2: SIP Trunk Settings, on page 50.

Step 8 To add the new trunk, click Save.

The trunk gets added to the database.

If you are updating an existing trunk, click Apply Config to apply the new settings (this may also restart the device) and synchronize a trunk.

Note Resetting a trunk drops any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting/restarting an H.323 or SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

After the name of the SIP Trunk is changed, SIP Trunk stops processing calls as the Cisco Unified Communications Manager fails to find the correct device.

Delete Trunk

Perform the following steps to delete a trunk.

Before you begin

You cannot delete a trunk that is assigned to one or more route patterns. To find out which route patterns are using the trunk, in the Trunk Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a trunk that is in use, Cisco Unified Communications Manager displays a message. Before deleting a trunk that is currently in use, you must perform either or both of the following tasks:

- Assign a different trunk to any route patterns that are using the trunk that you want to delete.
- Delete the route patterns that are using the trunk that you want to delete.

Procedure

Step 1 Choose **Device** > **Trunk**.

The Find and List Trunks window displays.

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

A list of trunks that match the search criteria displays.

Step 3 Perform one of the following actions:

a) Check the check boxes next to the trunks that you want to delete and click Delete Selected.
b) Delete all trunks in the window by clicking Select All and then clicking Delete Selected.

c) From the list, choose the name of the trunk that you want to delete to display its current settings and click Delete.

A confirmation dialog displays.

Step 4 To delete the trunk, click OK.

Reset Trunk

Perform the following procedure to reset the trunk.

⚠ **Caution** Resetting devices can cause them to drop calls.

Procedure

Step 1 Choose **Device** > **Trunk**.

The Find and List Trunks window displays.

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

A list of trunks that match the search criteria displays.

Step 3 From the list, click the name of the trunk that you want to reset.

The Trunk Configuration window displays.

Step 4 After you change any settings for the Trunk Device, click Reset.

The Device Reset dialog displays.

Step 5 Click one of the following choices:

a) Restart—Restarts the trunk device without shutting it down first.
b) Reset—Shuts down, then restarts, the internal trunk device. The Cisco Unified Communications Manager cluster unregisters (URQ) and then reregisters (RRQ) with the trunk if the trunk is gatekeeper controlled.
c) Close—Closes the Reset Device dialog without performing any action.

Note For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed. Trunks do not have to undergo a Restart or Reset when Packet Capture is enabled or disabled.

Synchronize Trunk

To synchronize a trunk 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** > **Trunk**.

The Find and List Trunks window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.

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

Step 4 Check the check boxes next to the trunks that you want to synchronize. To choose all trunks 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.

Note Active calls may get disconnected during a restart.