Infrastructure Configuration Product Fields

- Infrastructure Data Object Fields, on page 1

Infrastructure Data Object Fields

To create Configuration Templates, you must add infrastructure Configuration Products to the Configuration Template.

Not all fields in an infrastructure configuration template are applicable on all Cisco Unified Communications Manager versions.

Note All the Infrastructure Configuration Product fields, where you manually enter text, are case sensitive.

CTI Route Point Configuration Product Fields

Table 1: CTI Route Point Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Device Pool	List of available device pools. The device pool specifies a collection of properties for this device, including Unified CM Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Common Device Config	Configuration of common device settings, such as the softkey template and user locale.
Call Search Space	Specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed.

Field	Description
Location	Specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the location feature does not keep track of the bandwidth that this route point consumes.
Directory Numbers	Enter directory numbers. These directory numbers must not exist on the Cisco Unified Communications Manager.
Route Partition for Directory Numbers	Available route partitions.
Media Resource Group List	Provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If this field is left blank, the Media Resource Group that is defined in the device pool is used.
User Locale	User location associated with the user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
User Hold MOH Audio Source	The audio source that plays Music On Hold when the user initiates a hold action.
Network Hold Audio Source	The audio source that plays when the network initiates a hold action.

Call Park Infrastructure Configuration Product Fields

Table 2: Call Park Infrastructure Configuration Product Fields

Field	Description
Number/Range	Enter the call park extension number or a range of numbers. **Note** Call Park template allows you to add the same range of numbers in different partitions.
Description	Optional description.
Route Partition	List of available route partitions.

Field	Description
Unified CM	List of available Cisco Unified Communications Managers.

Call Pickup Group Infrastructure Configuration Product Fields

Table 3: Call Pickup Group Infrastructure Configuration Product Fields

Field	Description
Call Pickup Group Information	
Name	Infrastructure Configuration Product name.
Number	Unique directory number (integers).
Description	Optional description.
Route Partition	List of available route partitions.
Call Pickup Group Notification Settings	
Call Pickup Group Notification Policy	From the drop-down list box, choose one of the following notification types: • No Alert • Audio Alert • Visual Alert • Audio and Visual Alert
Call Pickup Group Notification Timer (seconds)	Enter the seconds of delay (integer in the range of 1 to 300) between the time that the call first comes into the original called party and the time that the notification to the rest of the call pickup group is to occur.
Associated Call Pickup Group Information - Find Pickup Numbers by Numbers/Partition	
Partition	See Partition in Call Pickup Group Information in this table.
Call Pickup Group Numbers Contain	Enter the DN or part of the DN of the call pickup group that you want to find; then, click Find.
Available Call Pickup Groups	To add a member to the associated call pickup group list in the Current Associated Call Pickup Groups area.
Associated Call Pickup Group Information - Current Associated Call Pickup Groups	

Field	Description
Selected Call Pickup Groups	To change order of the Call Pickup Groups listings, use the Up and Down arrows on the right side of this box to move the listings.
Removed Call Pickup Groups	Use the Up and Down arrows above this box to move a call pickup group from this box to the Selected Call Pickup Groups box.
Call Information Display For Call Pickup Group Notification	
Calling Party Information	Check the check box if you want the visual notification message to the call pickup group to include identification of the calling party.
Called Party Information	Check the check box if you want the visual notification message to the call pickup group to include identification of the original called party.

Call Search Space Infrastructure Configuration Product Fields

Table 4: Call Search Space Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Available Route Partitions	List of available route partitions. The route partitions list is not strictly required, but you should provide at least one value. You must reference a route partition that already exists on the Cisco Unified Communications Manager, or define one in the same Configuration Template before to this call search space.

Called Party Transformation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 5: Called Party Transformation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Pattern	Enter the transformation pattern, including numbers and wildcards (do not use spaces).

Field	Description
Partition	Choose the desired partition to restrict access to the transformation pattern from the drop-down list box.
Description	Optional description.
Numbering Plan	Choose a numbering plan.
Route Filter	Choosing an optional route filter restricts certain number patterns.
Urgent Priority	Check this check box to interrupt interdigit timing and route the call immediately.
MLPP Preemption Disabled	Check this check box to make the numbers in a transformation pattern nonpreemptable.
Called Party Transformation	
Discard Digits	Choose the discard digit instructions that you want to be associated with this calling party transformation pattern.
Called Party Transformation Mask	Enter a transformation mask value.
Prefix Digits	Enter the prefix digits.
Called Party Number Type	Choose the format of the number type in called party directory numbers.
Called Party Numbering Plan	Choose the format of the numbering plan in called party directory numbers.

Calling Party Transformation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 6: Calling Party Transformation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Pattern	Enter the transformation pattern, including numbers and wildcards (do not use spaces).
Partition	choose the desired partition to restrict access to the transformation pattern from the drop-down list box.
Description	Optional description.

Field	Description
Numbering Plan	Choose a numbering plan.
Route Filter	Choosing an optional route filter restricts certain number patterns.
Urgent Priority	Check this check box to interrupt interdigit timing and route the call immediately.
MLPP Preemption Disabled	Check this check box to make the numbers in a transformation pattern nonpreemptable.
Calling Party Transformations	
Using calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Discard Digit Instructions	Choose the discard digit instructions that you want to be associated with this calling party transformation pattern.
Calling Party Transformation Mask	Enter a transformation mask value.
Prefix Digits	Enter the prefix digits.
Calling Line ID Presentation	Used as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis.
Calling Party Number Type	Choose the format of the number type in calling party directory numbers.
Calling Party Numbering Plan	Choose the format of the numbering plan in calling party directory numbers.

Common Device Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 7: Common Device Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Softkey Template	Softkey template that determines the configuration of the softkeys on Cisco IP Phones.
User Hold MOH Audio Source	The audio source that plays Music On Hold when the user initiates a hold action.

Field	Description
Network Hold Audio Source	The audio source that plays when the network initiates a hold action.
User Locale	User location associated with the user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
IP Addressing Mode	Choose the version of IP address that the device (SIP trunk or phone that runs SCCP) uses to connect to the system.
IP Addressing Mode Preference for Signaling	For dual-stack phones, which support both IPv4 and IPv6 addresses, choose the version of IP address that the phone prefers to establish a connection to the system during a signaling event.
Use Trusted Relay Point	Choose one of the following options: • On—To allow the IP Phones to send multicast echo request messages. • Off—To disable sending multicast echo request messages. • Default—To use the configuration for the Reply Multicast Echo Request enterprise parameter, choose this option.
Use Intercompany Media Services (IMS) for Outbound Calls	Check this check box to enable the devices that associate with this common device configuration to use a trusted relay point.

Field	Description
Allow Auto-Configuration for Phone	This drop-down list box supports IPv6 for dual-stack Cisco Unified IP Phones that run SCCP: • On—Depending on how the M bit is set through stateless address autoconfiguration on the router, the phone is allowed to use the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address. Phones also require a TFTP server address to register with the system. You can manually configure the TFTP server address through the interface on the phone, or you can obtain it from a DHCPv6 server. • Off—The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server. • Default—To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option.
Allow Duplicate Address Detection	This drop-down list box supports an IPv6 parameter for Cisco IP Phone: • On—The phone performs duplicate address detection on each of the addresses in all the identity associations that it receives in the Reply message. • Off—The phone does not perform duplicate address detection. • Default—To use the configuration for the Allow Duplicate Address Detection enterprise parameter, choose this option.
Accept Redirect Messages	This drop-down list box supports an IPv6 parameter for Cisco IP Phones: • On—The phone accepts the redirect messages from the same router that is used for the destination number. • Off—The phone ignores the redirect messages. • Default—To use the configuration for the Accept Redirect Messages enterprise parameter, choose this option.

Field	Description
Reply Multicast Echo Request	This drop-down list box supports an IPv6 parameter for Cisco IP Phones: • On—The phone sends an Echo Reply message in response to an Echo Request message sent to an IPv6 address. • Off—The phone does not send Echo Reply messages. • Default—To use the configuration for the Reply Multicast Echo Request enterprise parameter, choose this option.
MLPP Indication	Specifies whether devices in the device pool that are capable of playing precedence tones use the capability when the devices place an MLPP precedence call.
MLPP Preemption	Specifies whether devices in the device pool that are capable of preempting calls in progress use the capability when the devices place an MLPP precedence call.
MLPP Domain	Multilevel Precedence and Preemption (MLPP) Domain that is associated with this device.
Confidential Access Mode	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.
Confidential Access Level	Select the appropriate CAL value.

Common Phone Profile Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 8: Common Phone Profile Infrastructure Configuration Product Fields

Field	Description
Common Phone Profile Information	
Name	Enter a name to identify the common phone profile; for example, CPP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.

Field	Description
Description	Identify the purpose of the common phone profile; for example, common phone profile for the 7905 phone. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Local Phone Unlock Password	Enter the password that is used to unlock a local phone. Valid values comprise 1 to 15 characters.
DND Option	When you enable Do Not Disturb (DND) on the phone, this parameter allows you to specify how the DND features handle incoming calls: • Call Reject—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. • Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so that you can accept the call. **Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

Field	Description
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • Disable—This option disables both beep and flash notification of a call, but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display, and no information gets sent to the device. • Beep Only—For an incoming call, this option causes the phone to beep. • Flash Only—For an incoming call, this option causes the phone to display a flash alert.
Enable End User Access to Phone Background Image Setting	Check this check box to change the background image on phones that use this common phone profile.
Feature Control Policy	You can choose a feature control policy that has already been configured in the Feature Control Policy configuration.
Wi-Fi Hotspot Profile	Select a Wi-Fi Hotspot Profile from the drop-down list.
Secure Shell Information	
Secure Shell User	Enter a user ID for the secure shell user. The Engineering Team uses secure shell for troubleshooting and debugging. Contact the Engineering Team for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH credentials to the phone in the clear.
Secure Shell User Password	Enter the password for a secure shell user. Contact the Engineering Team for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH passwords to the phone in the clear.

Field	Description
Phone Personalization Information	
Phone Personalization	The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. From the Phone Personalization drop-down list box, choose one of the following options: • Disabled—You cannot customize the Cisco Unified IP Phone by using Phone Designer. • Enabled—You can use Phone Designer to customize the phone. • Default—The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window. Install and configure Phone Designer to customize the phone. Before that, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer documentation. For more information on Phone Designer, see the Phone Designer documentation.
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Services Provisioning	From the drop-down list, choose how the phone will support the services: • Internal—The phone uses the phone configuration file to support the service. Choose this option or Both for Cisco-provided default services where the Service URL has not been updated; that is, the service URL indicates Application:Cisco/<name of service>; for example, Application:Cisco/CorporateDirectory. Choose Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file. • External URL—Choosing External URL indicates that the phone ignores the services in the phone configuration file and retrieves the services from a Service URL. If you configured a custom Service URL for a service, choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the phone. • Both—Choosing Both indicates that the phone support both the services that are defined in the configuration file and external applications that are retrieved from custom service URLs. If you have phones in your network that can obtain the service information from the phone configuration file and phones in your network that can only use custom service URLs for obtaining the information, choose **Both**.
VPN Information	
VPN Group	From the drop-down list, choose the VPN Group for the phone. For information about creating VPN groups, see the Virtual Private Network Configuration chapter in the Cisco Unified Communications Manager Security Guide.
VPN Profile	From the drop-down list, choose the VPN profile for the phone. For information about creating VPN profiles, see the Virtual Private Network Configuration chapter in the Cisco Unified Communications Manager Security Guide.
Service Specific Configuration Layout	

Field	Description
Disable USB	Disable the USB ports on the device and dock. This is a required field. Default: False **Note** A reset of the device is required for this parameter to take effect.
Back USB Port	Indicates whether the back USB port on the phone is enabled or disabled. This is a required field. Default: Enabled
Side USB Port	Indicates whether the side USB port on the phone is enabled or disabled. This is a required field. Default: Enabled
Enable/Disable USB Classes	Indicates which the USB Classes on the phone are enabled or disabled. Default: Audio Class
SDIO	Indicates whether the SDIO device on the phone is enabled or disabled. This is a required field. Default: Disabled
Bluetooth	Indicates whether the Bluetooth device on the phone is enabled or disabled. This is a required field. Default: Enabled
Bluetooth Profiles	Indicates which bluetooth profiles on the phone are enabled or disabled. This is a required field. Default: Handsfree
Allow Bluetooth Contacts Import	Indicates whether the Bluetooth device on the phone is allowed to sync the contacts from the phone. This is a required field. Default: Enabled

Field	Description
Allow Bluetooth Mobile Handsfree Mode	Indicates whether the user is allowed to enable or disable 2 way audio between devices with HFP. This is a required field. Default: Enabled
Console Access	Indicates whether the USB serial console is enabled or disabled. This is a required field. Default: Disabled
Cisco Camera	Indicates whether the Cisco Camera on the phone is enabled or disabled. This is a required field. Default: Disabled
Enable Power Save Plus	To enable the Power Save Plus feature, select the day(s) that you want the phone to power off on schedule. You can select multiple days by pressing and holding the Control key. while clicking on the days that you want Power Save Plus to operate. The default is disabled (no days selected). Power Save Plus mode turns off the phone for the time period specified in the Phone Off Time and Phone On Time fields. This time period is usually outside of your organization's regular operating hours. Power Save Plus mode turns on the phone automatically when Phone On Time arrives. When you select day(s) in this field, the following notice displays to indicate e911 concerns. By enabling Power Save Plus, you are agreeing to the terms specified in this Notice. While Power Save Plus Mode is in effect, endpoints configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: • You are taking full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect. • Cisco has no liability with your selection of the mode and all liability with enabling the mode is your responsibility. • Users should be aware of the effects of the mode on calls, calling and otherwise.

Field	Description
Enable Audible Alert	This check box, when enabled, instructs the phone to play an audible alert ten minutes prior to the time specified in the field, Phone Off Time. To also audibly alert the user, enable this check box. The default is disabled. This check box only applies if the Enable Power Save Plus list box has one or more days selected. This is a required field. Default: False
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. A few conditions apply; first, one or more days must be selected in the Enable Power Save Plus field. If the Enable Power Save Plus list box does not have any days selected, the phone ignores the EnergyWise directive to turn off the phone. Second, the settings in Unified CM Administration takes effect on schedule even if EnergyWise sends an override. For example, assume the Display Off Time is set to 22:00 (10 p.m.), the value in the Display On Time field is 06:00 (6 a.m.), and the Enable Power Save Plus has one or more days selected. If EnergyWise directs the phone to turn off at 20:00 (8 p.m.), that directive will remain in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6 a.m. At 6 a.m., the phone will turn on and resume receiving its power level changes from the settings in Unified CM Administration. To change the power level on the phone again, EnergyWise must reissue a new power level change command. Also, any user interaction will take effect so if a user presses the select softkey after EnergyWise has directed the phone to power off, the phone will power on as a result of the user action. The default is unchecked. This is a required field. Default: False
EnergyWise Domain	This field defines the EnergyWise domain in which the phone is participating. An EnergyWise domain is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, provide an EnergyWise domain. The default is blank. Maximum length: 127

Field	Description
EnergyWise Endpoint Security Secret	This field defines the password (shared secret) used to communicate within the EnergyWise domain. An EnergyWise domain and secret is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, provide an EnergyWise domain and secret. The default is blank. Maximum length: 127
Phone On Time	This field determines the time that the phone turns on automatically on the days that are selected in the Enable Power Save Plus list box. Enter the time in 24 hour format, where 00:00 represents midnight. For example, to automatically turn the phone on at 7:00 a.m., (0700), enter 07:00. To turn the phone on at 2:00 p.m. (1400), enter 14:00. If this field is blank, the phone automatically turns on at 00:00. Default: 00:00 Maximum length: 5
Phone Off Time	This field determines the time of day that the phone will turn itself off on the days that are selected in the Enable Power Save Plus list box. Enter the time in the following format hours: minutes. If this field is blank, the phone automatically turns off at midnight (00:00). **Note** If Phone On Time is blank (or 00:00) and Phone Off Time is blank (or 24:00), the phone will remain on continuously, effectively disabling the Power Save Plus feature unless you allow EnergyWise to send overrides. Default: 24:00 Maximum length: 5

Field	Description
Phone Off Idle Timeout	This field represents the number of minutes that the device must be idle before the device will request the power sourcing equipment (PSE) to power down the device. The value in this field takes effect: • When the device was in Power Save Plus mode as scheduled and was taken out of Power Save Plus mode via some user interactions. • When the phone is repowered by the attached switch. • When the Phone Off Time is met but the phone is in use. The unit is minutes. The range is 20 to 1440. This is a required field. Default: 60 Minimum: 20 Maximum: 1440
Days Display Not Active	This field allows the user to specify the days that the backlight is to remain off by default. Typically this would be Saturday and Sunday for US corporate customers. Saturday and Sunday should be the default. The list contains all of the days of the week. To turn off backlight on Saturday and Sunday the User would hold down Control and select Saturday and Sunday.
Display On Time	This field indicates the time of day the display is to automatically turn itself on for days listed in the off schedule. The value should be in a 24 hour format. Where 0:00 is the beginning of the day and 23:59 is the end of the day. Leaving this field blank will activate the display at the beginning of the day (e.g. - "0:00"). To set the display to turn on at 7:00AM the user would enter "07:00" without the quotes. If they wanted the display to turn on at 2:00PM they would enter "14:00" without the quotes. Default: 07:30 Maximum length: 5

Field	Description
Display On Duration	This field indicates the amount of time the display is to be active for when it is turned on by the programmed schedule. No value indicates the end of the day. Maximum value is 24 hours. This value is in free form hours and minutes. "1:30" would activate the display for one hour and 30 minutes. Default: 10:30 Maximum length: 5
Display Idle Timeout	This field indicates how long to wait before the display is turned off when it was turned on by user activity. This inactivity timer will continually reset itself during user activity. Leaving this field blank will make the phone use a pre-determined default value of one hour. Maximum value is 24 hours. This value can be in free form hours and minutes. "1:30" would turn off the display after one hour and 30 minutes of inactivity. Default: 01:00 Maximum length: 5
Display On When Incoming Call	When the device is in screen saver mode, this will turn the display on when a call is ringing. This is a required field. Default: Enabled
Incoming Call Toast Timer	This parameter specifies the maximum time in seconds that the toast displays a new incoming call notification. This is a required field. Default: 5
Enable Mute Feature	Enable mute feature to provide Mute softkey on 7906/7911. This is a required field. Default: False
Join And Direct Transfer Policy	This field indicates join and direct transfer policy for same line and across line. This is a required field. Default: Same line, across line enable
Medianet Statistics Interval	Medianet statistics reports are updated periodically during active media sessions. Set stats collection interval in seconds. Default: 15

Field	Description
RTCP	Maintains statistic for audio. This is a required field. Default: Disabled
Advertise G.722 and iSAC Codecs	Indicates whether Cisco Unified IP Phones will advertise the G.722 codec to Cisco Unified CallManager. Codec negotiation involves two steps: first, the phone must advertise the supported codec(s) to Cisco Unified CallManager (not all endpoints support the same set of codecs). Second, when Cisco Unified CallManager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. Valid values specify Use System Default (this phone will defer to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (this phone will not advertise G.722 to Cisco Unified CallManager) or Enabled (this phone will advertise G.722 to Cisco Unified CallManager). This is a required field. Default: Use System Default
Video Calling	When enabled, indicates that the phone will participate in video calls when connected to an appropriately equipped PC. This is a required field. Default: Enabled
Wifi	Indicates whether the Wi-Fi on the phone is enabled or disabled. This is a required field. Default: Enabled

Field	Description
Wi-Fi Hotspot	Indicates whether the personal Wi-Fi Hotspot capability on the phone is enabled or disabled. In order for a phone to provide a hotspot, at least three conditions must be met: • This flag must be enabled. • Phone must provide a hotspot. • An appropriate Wi-Fi Hotspot Profile must be given on the Device Pool Configuration or the Phone Configuration page. This is a required field. Default: Disabled
PC Port	Indicates whether the PC port on the phone is enabled or disabled. The port labeled "10/100 PC" on the back of the phone connects a PC or workstation to the phone so they can share a single network connection. This is a required field. Default: Enabled
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the Phone Port to the PC Port. Select Enabled if an application is being run on the PC Port that requires monitoring of the IP Phone's traffic such as monitoring and recording applications (common in call center environments) or network packet capture tools used for diagnostic purposes. To use this feature PC Voice VLAN access must be enabled. This is a required field. Default: Disabled
PC Voice VLAN Access	Indicates whether the phone will allow a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the phone. Set this setting to Enabled if an application is being run on the PC that requires monitoring of the phones traffic. These could include monitoring and recording applications and use of network monitoring software for analysis purposes. This is a required field. Default: Enabled

Field	Description
PC Port Remote Configuration	Allows remote configuration of the speed and duplex for the PC port of the phone, which overrides any manual configuration at the phone. This is a required field. Default: Disabled
Switch Port Remote Configuration	Allows remote configuration of the speed and duplex for the switch port of the phone, which overrides any manual configuration at the phone. Be aware that configuring this port may cause the phone to lose network connectivity. This is a required field. Default: Disabled
Automatic Port Synchronization	Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds. This is a required field. Default: Disabled
Cisco Discovery Protocol (CDP) Switch Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the switch port. This is a required field. Default: Enabled **Note** CDP should only be disabled on the Network port if this phone is connected to a non-Cisco switch. For further details, see the *Cisco Unified Communications Manager Administration Guide*.
Cisco Discovery Protocol (CDP) PC Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the PC port. This is a required field. Default: Enabled **Note** Disabling CDP on the PC port will prevent Cisco VT Advantage or Unified Video Advantage from working properly on this phone. For further details, see the *Cisco Unified Communications Manager Administration Guide*.

Field	Description
LLDP-MED- Switch Port	Media Endpoint Discover (LLDP-MED): Switch Port: Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the switch port. This is a required field. Default: Enabled
Link Layer Discovery Protocol (LLDP)- PC Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the PC port. This is a required field. Default: Enabled
LLDP Asset ID	Allows administrator to set Asset ID for Link Layer Discovery Protocol. Maximum length: 32
LLDP Power Priority	Allows administrator to set Power Priority for Link Layer Discovery Protocol. This is a required field. Default: Unknown
Power Negotiation	Allows administrator to enable or disable Power Negotiation. This is a required field. Default: Enabled
802.1x Authentication	Specifies the 802.1x authentication feature status. This is a required field. Default: User Controlled
FIPS Mode	This parameter sets the Federal Information Processing Standards (FIPS) mode for the phone. The phone is a FIPS 140-2 level 1 compliant device when this option is enable. This is a required field. Default: Disabled
80-bit SRTCP	Enable 80-bit authentication tag for SRTCP. This is a required field. Default: Disabled

Field	Description
Always On VPN	Indicates whether the device starts the VPN AnyConnect client and establish a connection with the configured VPN profile from the Cisco Unified Communications Manager. This is a required field. Default: False
Store VPN Password on Device	This parameter controls whether VPN password can be stored on the device. Its value is used only when Password Persistence is set to true. If disabled, the user's VPN password is stored in memory and is automatically resubmitted upon subsequent connects. However, when the device reboots, the user has to re-enter their VPN password again. If enabled, the user's VPN password is stored on the device and persist across reboots. This is a required field. Default: False
Allow User-Defined VPN Profiles	This parameter controls whether the user can use the AnyConnect VPN client to create VPN profiles. If disabled, the user cannot create VPN profiles. This is a required field. Default: True
Require Screen Lock	This parameter indicates whether screen lock is required on the device. If "User Controlled" is selected, the device will not prompt for a PIN or password. The "PIN" and "Password" options require the user to enter a password to unlock the screen. A "PIN" is a numeric password that is at least four digits long. A "Password" is an alphanumeric password, consisting of at least 4 alphanumeric characters, one of which must be a nonnumeric number, and one must be a capital letter. This is a required field. Default: PIN

Field	Description
Screen Lock Timeout	Maximum idle time in seconds before the device automatically locks the screen. After the screen is locked, the user password is required to unlock it. This is a required field. Default: 600 Minimum: 15 Maximum: 1800
Enforce Screen Lock During Display-On Time	This parameter provides an unobtrusive lock policy that allows users to work freely with their device throughout the workday, without the device locking after the interval that is set in Cisco Unified Communications Manager. After work, the device locks as defined in the policy, to prevent unauthorized users from accessing it. The device always supports the user-controlled manual lock option (power button), for meetings or lunch breaks. The device remains locked until the user enters the PIN/password on next use. • ON—Device locks during the workday or during display-on time (default setting). • OFF—Device locks only during display-off time or after work hours, based on day or time settings listed above. This is a required field. Default: True
Lock Device During Audio Call	When the device is in a charging state and an active voice call is in progress, an administrator can override the screen lock PIN enforcement timer to keep the screen active during an audio call. Screen lock timer takes effect after audio call is completed and timer is exceeded. This is a required field. Default: Disabled
Kerberos Server	Authentication server for web proxy Kerberos. Maximum length: 256
Kerberos Realm	Realm for web proxy Kerberos. Maximum length: 256

Field	Description
TLS Resumption Timer	This parameter controls the maximum number of seconds that a peer can reuse the TLS session without doing a full handshake authentication. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. Only apply to TLS session for HTTPS on Cisco IP phones. This is a required field. Default: 3600 Minimum: 0 Maximum: 3600
User Credentials Persistent For Expressway Sign in	This parameter enables the phone to persistently store user credentials used for authentication with Expressway Sign in. This is a required field. Default: Disabled
WLAN SCEP Server	Indicates the SCEP Server the phone uses to obtain certificates for WLAN authentication. Enter the hostname or the IP address (using standard IP addressing format) of the server. Maximum length: 256
WLAN Root CA Fingerprint (SHA256 or SHA1)	Indicates the SHA256 or SHA1 fingerprint of the Root CA to use for validation during the SCEP process when issuing certificates for WLAN authentication. It is recommended to utilize the SHA256 fingerprint, which can be obtained via OpenSSL (i.e. openssl x509 -in rootca.cer -noout -sha256 -fingerprint) or using a Web Browser to inspect the certificate details. Enter the 64 hexadecimal character value for the SHA256 fingerprint or the 40 hexadecimal character value for the SHA1 fingerprint with a common separator (colon, dash, period, space) or without a separator. If using a separator, then the separator should be consistently placed after every 2, 4, 8, 16, or 32 hexadecimal characters for an SHA256 fingerprint or every 2, 4, or 8 hexadecimal characters for an SHA1 fingerprint. Maximum length: 95
Outbound Rollover	When the number of calls on the line is exceeded, a new created call will roll over to the next line. This is a required field. Default: Disabled

Field	Description
Detect Unified CM Connection Failure	This field determines the sensitivity that the phone application has for detecting a connection failure to Cisco Unified Communications Manager, which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. The precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing. This only applies to the wired Ethernet connection. Default = Normal. This is a required field. Default: Normal
Time to Wait for Seamless Reconnect After TCP Drop or Roaming	This field indicates a grace period to establish a new TCP connection via keep-alive registration after the original TCP connection is torn down. The Seamless Reconnect is disabled if the value is set to 0. Default: 5 Minimum: 0 Maximum: 300
Load Server	Indicates that the phone uses an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IP address (using standard IP addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades. Maximum length: 256

Field	Description
IPv6 Load Server	Indicates that the phone will use an alternative IPv6 server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local IPv6 server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IPv6 address (using standard IPv6 addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades. Maximum length: 25
Peer Firmware Sharing	Enables or disables Peer to Peer image distribution in order to allow a single phone in a subnet to retrieve an image firmware file then distribute it to its peers; thus reducing TFTP bandwidth and providing for a faster firmware upgrade time. This is a required field. Default: Enabled
Log Server	Specifies an IP address and port of a remote system where log messages are sent. Maximum length: 32
IPv6 Log Server	Specifies an IPv6 address and port of a remote system where log messages are sent. The format is: [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]:ppppp@@options. Options will be format as: • base=x (value range is 0~7) (default value is 7) • pfs=y (value range is 0~1) (default value is 0) And the two parameters are optional.
Log Profile	Run the pre-defined debug command remotely. Default: Preset
Remote Log	This parameter specifies where to send the log data by serviceability. If enabled, the log data is copied by serviceability to the place specified by Log Server/IPV6 Log Server. If disabled, the log data will not be copied by serviceability to the place specified by Log Server/IPV6 Log Server.

Field	Description
HTTPS Server	Allows Administrator to permit http and https or https only connections if Web Access is enabled. This is a required field. Default: http and https Enabled
Web Access	This parameter indicates whether the phone accepts connections from a web browser or other HTTP client. Disabling the web server functionality of the phone blocks access to the phones internal web pages. These pages provide statistics and configuration information. Features, such as Quality Report Tool (QRT), will not function properly without access to the phones web pages. This setting will also affect any serviceability application such as CiscoWorks 2000 that relies on web access. This is a required field. Default: Disabled
Settings Access	Indicates whether the Settings button on the phone is functional. When Settings Access is enabled, you can change the phone network configuration, ring type, and volume on the phone. When Settings Access is disabled, the Settings button is disabled; no options appear when you press the button. Also, you cannot adjust the ringer volume or save any volume settings. This is a required field. Default: Enabled
SSH Access	This parameter indicates whether the device accepts SSH connections. Disabling the SSH server functionality of the device blocks access to the device. This is a required field. Default: Disabled
Ring Locale	IP Phone has distinctive ring for On-net/Off-net or line based, but its ring cadence is fixed, and it is based on US standard only. Ring cadence in US standard is opposite to Japan standard. To support Japan ring cadence, the ring cadence is be configurable according to Ring Locale. This is a required field. Default: Default

Field	Description
Android Debug Bridge or ADB	This parameter enables or disables the Android Debug Bridge (ADB) on the device. This is a required field. Default: Disabled
Customer support upload URL	This URL is used to upload problem report files when the user has run the "Problem Reporting Tool" on the endpoint. Maximum length: 256
Allow Applications from Unknown Sources	This parameter controls whether the user can install Android applications on the device from a URL or from Android packages (APK) that are received through email, instant message (IM), or from a Secure Digital (SD) card. This is a required field. Default: Disabled
Allow Applications from Android Market	This parameter controls whether the user can install Android applications from the Google's Android Market. This is a required field. Default: False
Allow Applications from Cisco AppHQ	This parameter controls whether the user can install Android applications from the Cisco AppHQ. This is a required field. Default: False
AppHQ Domain	The fully qualified domain name to use when users log into AppHQ. If empty, the user will specify their own domain name along with their username. The AppHQ domain is used to associate the user to a given Custom AppHQ store, if it exists. Example: cisco.com. Maximum length: 256
Enable Cisco UCM App Client	This parameter controls whether the Application Client runs on the device. When the Application Client is enabled, you can select the applications they want to install from the Cisco Unified Communications Manager. This is a required field. Default: False

Field	Description
Company Photo Directory	This parameter specifies the URL which the device can query for a user and get the image associated with that user. Maximum length: 256
Voicemail Server (Primary)	Hostname or IP address of the primary mailstore voicemail server. Maximum length: 256
Voicemail Server (Backup)	Hostname or IP address of the backup mailstore voicemail server. Maximum length: 256
Presence and Chat Server (Primary)	Hostname or IP address of the primary presence server. Maximum length: 256
Alternate phone book server type	By default the endpoint uses the UDS server on the UCM it's registered to, but if you wish to use an alternate phone book server, this parameter combined with an alternate phone book address overrides the default setting of the endpoint. UDS sets the alternate phone book type as UDS. This is a required field. Default: UDS
Alternate phone book server address	By default the endpoint uses the UDS server on the UCM it's registered to, but if you wish to use an alternate phone book server, this parameter combined with the alternate phone book type will override the default setting of the endpoint. The field requires a full URL for the phone book servers. Example for UDS server url: https://uds-host-name:8443/cucm-uds/users. Maximum length: 256
Presence and Chat Server Type	This parameter indicates the type of server specified in the "Presence and Chat Server" field. This is a required field. Default is Cisco WebEx Connect.
Presence and Chat Single Sign-On (SSO) Domain	The enterprise domain used by Cisco WebEx Connect Cloud to perform Single-Sign-On (SSO) authentication against an enterprise. Maximum length: 256

Field	Description
Device UI Profile	Changes the device's user interface characteristics to optimize for specific user personas such as basic video callers (Simple), public space phone(Public) or general collaboration users (Enhanced). This is a required field. Default: Simple
Multi-User	This parameter indicates whether multi-user is enabled or disabled on the device. This is a required field. Default: Disabled
Multi-User URL	This parameter specifies the URL of the extension mobility server. Maximum length: 256
Email address for customer support	This sets an email address to which you can send problem report files from the 'Problem Reporting Tool' on the phone. Maximum length: 256
PSTN Mode	Enable PSTN Mode for IP Phone 6921/6941/6961. This is a required field. Default: Disabled
Background Image	This parameter specifies the default wallpaper file. Only the administrator disables end user access to phone wallpaper list, could this parameter take effect. Maximum length: 64
Simplified New Call UI	This parameter specifies if use simplified call UI style when the phone is Off-hook. Those who like the New Call Window can continue to use that at the same time that those who prefer the Simplified New Call Session can use that method. This is a required field. Default: Disabled
Revert to All Calls	When enabled, phone will revert to All Calls after any call is ended if the call is on a filter other than Primary line or All Calls. This is a required field. Default: Disabled

Field	Description
RTCP for Video	RTCP enable for both Video and audio RTP streams which for RTP statistic and lip sync purpose. With this disable, video lipsync relays on free run mode. This is a required field. This is a required field. Default: Enabled
Provide Dial Tone from Release Button	Indicates whether Dial Tone is provided when Release Button is pressed. If the value is true, then in "Off Hook Dialing/RingingOut/Connected" state, a new Call Windows will be brought out after Release Button is pressed. If "Revert To All Calls" feature was enabled, it should be active first before "Dial Tone" feature. This is a required field. Default: Disabled
Hide Video By Default	This field provides an additional flexibility of hiding video window by default if "Hide Video By Default" is enabled. This is a required field. Default: Disabled With "Hide Video by default" feature enabled, the video window is initially hidden on video calls. If "Auto Transmit Video" is "on," the phone displays a "Hide Video View", while the video is being transmitted to the remote party. This may make distinguishing video calls from voice calls more difficult for end users. The benefit of "Hide Video by default" is that, in work environments where users are more likely to mute their video or close the shutters on the camera, the far end user will see the audio call plane rather than a black "mute" box on their phone. "Hide Video by Default" is not recommended for work environments where video calling is used often with cameras open, enabled, and unmuted.

Field	Description
VXC VPN Option	This field indicates how VXC VPN is supported. If "Dual Tunnel" is selected, phone establishes two VPN tunnels, one for Phone and another for VXC device. If "Single Tunnel" is selected, phone establishes only one VPN tunnel for phone and VXC-device to share. Where uncompromised voice or video quality is required the dual VPN tunnel solution is recommended. Dual Tunnel—Through the use of two VPN tunnels the host Cisco IP Phone is able to provide prioritization of its CPU and memory resources to the data associated with the Phones Voice or video functions over that of the data associated with the VXC VPN tunnel. This approach requires two manual login entries (dependent on security parameters), one for Phone's Voice or Video VPN and another for VXC VPN. The two tunnel approach also requires two VPN concentrator ports and two IP addresses adding potential costs. Single Tunnel—A single VPN tunnel option is implemented for those customers willing to trade off potential voice/video quality for a simplified operating model. The solution consists of operating over a single VPN tunnel by sharing the available 89/99xx processor and memory resources across the voice, video and VDI services. The IP Phone is unable to prioritize data handing of one service over another. This is a required field. Default: Dual Tunnel

Field	Description
VXC Challenge	This field indicates whether or not to challenge VXC device. If "Challenge" is selected, VXC device will be challenged. For "Single Tunnel" VXC VPN Option, Phone VPN Sign In window will pop up for user to input credentials and re-establish Phone VPN tunnel. For "Dual Tunnel" VXC VPN Option, VXC VPN Sign In window will pop up for user to input credentials and re-establish VXC VPN tunnel. If "No Challenge" is selected, VXC challenge will be bypassed. For "Single Tunnel" VXC VPN Option, VXC traffic will silently be permitted to go over phone VPN without VXC challenge. For "Dual Tunnel" VXC VPN Option, credentials of Phone VPN tunnel will be reused to re-establish VXC VPN tunnel. This is a required field. Default: Challenge
VXC-M Servers	VXC Management Server IP address list, separated with comma. Maximum length: 255
Record Call Log from Shared Line	This field indicates whether to record call log from shared line. This is a required field. Default: Disabled
Show Call History for Selected Line Only	When enabled, the phone shows call history for selected line only. This is a required field. Default: Disabled
Actionable Incoming Call Alert	Show an Alert with Answer, Divert, and Ignore softkeys when there is an incoming call alerting for user to act. This is a required field. Default: Show for all Incoming Call
DF bit	Configure the DF bit in IP header. This is a required field. Default: 0

Field	Description
Separate Audio and Video Mute	Indicates whether separate audio and video mute. When enabled this parameter, the Mute key affects only the audio; When disabled this parameter, the Mute key affects the audio and the video. By default, Separate Audio and Video is disabled. This is a required field. Default: Disabled
Softkey Control	Indicates whether phone softkeys are controlled by Feature Control Policy or Softkey Template. This is a required field. Default: Feature Control Policy
Start Video Port	This field defines the beginning of video RTP port
Stop Video Port	This field defines the end of video RTP port
Lowest Alerting Line State Priority	When disabled, if there is an incoming call alerting on the shared line, the LED/Line state icon reflects the alerting state instead of Remote-In-Use. When enabled, you see the Remote-In-Use state when there is call alerting on the shared line. This is a required field. Default: Disabled
One Column Display for KEM	When disabled. The KEM displays 18 Line/Button configured. Each line item uses half of the KEM screen width. When enabled, each line item will occupy entire KEM screen width for being able to show more characters. Total 9 Line/Button configured is displayed on one KEM. This is a required field. Default: Disabled
Audio EQ	This field configures handset or handsfree mode audio equalization setting. This is a required field.
Customer Support Use	This parameter specifies some special issue. Please split the special issue ID with semicolon." Maximum length: 64

Field	Description
Energy Efficient Ethernet(EEE): PC Port	This parameter indicates enable or disable Energy Efficient Ethernet(EEE) on PC port. This is a required field. Default is Enable.
Energy Efficient Ethernet(EEE): SW Port	This parameter indicates enable or disable Energy Efficient Ethernet(EEE) on switch port This is a required field. Default is Disabled.
WLAN Authentication Attempts	This parameter specifies the number of authentication attempts when there is explicit failure due to invalid credentials. This is a required field. Default: 2
WLAN Profile 1 Prompt Mode	This parameter enables or disables WLAN prompt mode, where user is prompted to re-enter password on device start-up or reboot. This is a required field. Default: Disabled
Line Mode	This parameter allows admin to switch between Session Line Mode and Enhanced Line Mode. While in Session Line Mode, the buttons on the left of the screen can be configured as programmable line keys and the buttons on the right of the screen are always session keys. While in Enhanced Line Mode, all the buttons can be configured as programmable line keys. This is a required field. Default: Session Line Mode
Interactive Connectivity Establishment (ICE)	

Field	Description
ICE	Specifies if clients use the ICE protocol to choose optimal paths for sending and receiving media. If you select Enabled, clients use the ICE protocol to choose optimal media paths. Using the ICE protocol can improve the quality of audio and video calls for users outside the corporate network. If you select Disabled, clients do not use the ICE protocol or attempt to communicate using optimal media paths. If you select Disabled as the value, no other ICE settings take effect. Select Disabled if your network does not include TURN servers or if all client communication takes place within the corporate network. Default: Enabled
Default Candidate Type	Defines the initial method that clients use to communicate with each other. Choose one of the following values: The default setting controls the initial communication path for the first few seconds of a call. If the ICE protocol can establish a more optimal media path than the default candidate type, clients use that path. For example, if you specify Server Reflexive as the default, clients communicate through NAT enabled routers when calls start. If clients can use the Host candidate type, they stop communicating through NAT enabled routers and communicate directly with each other. If clients cannot establish communication using the default candidate type, they use the next candidate type in order of performance. For example, you leave the default value of Host. For the initial attempt to establish communication, clients try to communicate directly. If clients cannot communicate directly with each other, clients use the Server Reflexive candidate type and attempt to communicate through NAT enabled routers. If clients cannot communicate through NAT enabled routers, they use the Relay candidate type. Default: Host

Field	Description
Server Reflexive Address	Specifies if clients can communicate through NAT enabled routers. If you enable this setting, clients can communicate directly with each other, through NAT enabled routers, or through TURN servers. Enable this setting if you specify Server Reflexive as the default candidate type. If you disable this setting, clients can communicate directly with each other or through a TURN server. You should disable this setting if your TURN servers apply Quality of Service (QoS) settings to improve media quality. Default: Enabled
Primary TURN Server Host Name or IP Address	Specifies the primary Traversal Using Relay for NAT (TURN) server. The ICE protocol uses TURN servers to provide addresses and ports to clients so that they can establish optimal media paths. Usually, TURN servers relay media between clients and the corporate network when calls begin. If clients can establish a more optimal media path using the ICE protocol, clients stop relaying media through TURN servers and use the optimal media path. You do not need to specify a TURN server address if your edge device includes a built-in TURN server. In other words, you do not need to specify a TURN server address if that address is the same as the address for your edge server. If your edge device does not include a built-in TURN server, and you do not specify a TURN server address, the ICE protocol does not take effect. You can specify either an IP address or FQDN. Maximum length: 1024
Secondary TURN Server Host Name or IP Address	Specifies the secondary TURN Server that the ICE protocol uses. You can specify either an IP address or FQDN. Maximum length: 1024
TURN Server Transport Type	Defines the protocol the client uses to send requests to TURN servers. Clients can send requests over UDP, TCP, or TLS over TCP. Select Auto to allow clients to set an appropriate transport type. Default: Auto

Field	Description
TURN Server Username	If you do not specify a username or do not apply this parameter, clients attempt to authenticate to TURN servers with the users' Cisco Unified Communications Manager username. If your deployment uses single sign-on (SSO), you must specify a username. TURN servers do not support SSO. Maximum length: 127
TURN Server Password	If you do not specify a password or do not apply this parameter, clients attempt to authenticate to TURN servers with the users' Cisco Unified Communications Manager password. If your deployment uses single sign-on (SSO), you must specify a password. TURN servers do not support SSO. Maximum length: 127
Instant Messaging	
File Types to Block in File Transfer	A semicolon separated list of file types to block during file transfer operations. Maximum length: 1024
URLs to Block in File Transfer	A semicolon separated list of URLs to block during file transfer operations. Maximum length: 1024
Desktop Client Settings	
Automatically Start in Phone Control	If enabled, the client starts in desktop phone control mode. This is a required field. Default: Disabled
Automatically Control Tethered Desk Phone	If enabled, the client automatically controls the tethered desktop phone. This is a required field. Default: Disabled
Extend and Connect Capability	Indicates if Extend and Connect capabilities are enabled for the client. This allows the client to monitor and control calls on Third party PBX, PSTN, and other remote phones. This is a required field. Default: Enabled

Field	Description
Display Contact Photos	Indicates if contact photo retrieval and display are enabled or disabled for the client. This is a required field. Default: Enabled
Number Lookups on Directory	Indicates if phone number lookups using the Corporate Directory are enabled or disabled for the client. This is a required field. Default: Enabled
Jabber For Windows Software Update Server URL	The URL of the Software Update Server that the Jabber For Windows Client uses when the User selects the Update Jabber link. The default is blank. Maximum length: 1024
Analytics Collection	Indicates if analytics collection is enabled or disabled for the client. This is a required field. Default: Disabled
Problem Report Server URL	The URL of the Problem Report Server that is used by the client. The default is blank. Maximum length: 1024
Analytics Server URL	The URL of the analytics server that is used by the client. The default is blank. Maximum length: 1024
Cisco Support Field	A semicolon separated list of custom settings that are used by the client to assist with deployment. This field is used only with the assistance of Cisco Support personnel. The default is blank. Maximum length: 1024

Conference Bridge Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 9: Conference Bridge Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.

Cisco IOS Enhanced Conference Bridge

For Cisco Prime Collaboration Release 11.5 and later

Table 10: Cisco IOS Enhanced Conference Bridge Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Device Security Mode	This field displays for Cisco IOS Enhanced Conference Bridge only. If you choose non-secure Conference Bridge, the non-secure conference establishes a TCP port connection to Cisco Unified Communications Manager on port 2000. **Note** Ensure that this setting matches the security setting on the conference bridge, or the call fails. The Encrypted Conference Bridge setting supports the secure conference feature.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • 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.

Cisco Conference Bridge Hardware

For Cisco Prime Collaboration Release 11.5 and later

Table 11: Cisco Conference Bridge Hardware Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Hardware Conference Bridge Info	
MAC Address	Enter a unique device MAC address.
Description	Enter a description for your conference bridge.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • 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.
Special Load Information	Enter any special load information or leave blank to use system default.

Cisco IOS Conference Bridge

For Cisco Prime Collaboration Release 11.5 and later

Table 12: Cisco IOS Conference Bridge Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.

Field	Description
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • 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.

Cisco TelePresence MCU

For Cisco Prime Collaboration Release 11.5 and later

Table 13: Cisco TelePresence MCU Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Device Information	
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Conference Bridge Prefix	Conference Bridge Prefix is used only for centralized deployments when the conference resources are deployed across a Small Medium Enterprise (SME). HTTP and SIP signaling are intended for different destinations. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
SIP Trunk	Select a SIP trunk to use for this conference bridge from a list of existing SIP trunks.

Field	Description
Allow Conference Bridge Control of the Call Security Icon	Check this check box to allow the Cisco TelePresence Conductor to control the display of the call security icon.
HTTP Interface Info	
Override SIP Trunk Destination as HTTP Address	Check this check box to override the SIP trunk destination. Use this feature if the HTTP and SIP signaling are intended for different destination IP addresses. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
Host Name IP Address	
Username	Enter the Cisco TelePresence Conductor administrator username.
Password	Enter the Cisco TelePresence Conductor administrator password
Confirm Password	Re-enter the Cisco TelePresence Conductor administrator password
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence Conductor. The default HTTPS port is 443.
HTTP Port	Enter the Cisco TelePresence Conductor HTTP port. The default port is 80.

Cisco TelePresence Conductor

For Cisco Prime Collaboration Release 11.5 and later

Table 14: Cisco TelePresence Conductor Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Select the conference bridge type.
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Conference Bridge Prefix	Conference Bridge Prefix is used only for centralized deployments when the conference resources are deployed across a Small Medium Enterprise (SME). HTTP and SIP signaling are intended for different destinations. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.

Field	Description
SIP Trunk	Select a SIP trunk to use for this conference bridge from a list of existing SIP trunks.
Allow Conference Bridge Control of the Call Security Icon	Check this check box to allow the Cisco TelePresence Conductor to control the display of the call security icon.
HTTP Interface Info	
Override SIP Trunk Destination as HTTP Address	Check this check box to override the SIP trunk destination. Use this feature if the HTTP and SIP signaling are intended for different destination IP addresses. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
Host Name IP Address	Enter one or more hostnames or IP addresses for the HTTP signaling destination if you have selected to override the SIP trunk destination.
Username	Enter the Cisco TelePresence Conductor administrator username.
Password	Enter the Cisco TelePresence Conductor administrator password
Confirm Password	Re-enter the Cisco TelePresence Conductor administrator password
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence Conductor. The default HTTPS port is 443.
HTTP Port	Enter the Cisco TelePresence Conductor HTTP port. The default port is 80.

Cisco Conference Bridge (WS-SVC-CMM)

For Cisco Prime Collaboration Release 11.5 and later

Table 15: Cisco Conference Bridge (WS-SVC-CMM) Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Choose Cisco Conference Bridge (WS-SVC-CMM).
Media Server Conference Bridge Info	
MAC Address	Enter a unique device MAC address.
Subunit	From the drop-down list box, choose the value for the daughter card for a given slot on the Communication Media Module card.
Description	Enter a description for your conference bridge.

Field	Description
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • 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.
Maximum Capacity	Choose the maximum number of streams for a given service on a daughter card. Possible values include 32, 64, 96, and 128 streams. Ensure that each daughter card has as many ports as the value that you choose.
Service Specific Configuration Layout	
General	
RTP Timeout (sec)	This defines the RTP timeout value.
Signaling Diffserv Code Points (DSCP)	This defines DSCP for signaling.
Audio Diffserv Code Points (DSCP)	This defines DSCP for audio.
Enable G.729 Voice Activity Detection	This enables or disables the Voice Activity Detection(VAD) for G.729 codec. When music is played in the transcoding session, the quality is degraded since VAD is enabled by default in G.729. VAD can be disabled to address this issue.
Codec Packetization Rate	
G.711ulaw	This defines the packetization rate for codec G.711ulaw. "None" defaults to 60ms.
G.711alaw	This defines the packetization rate for codec G.711alaw. "None" defaults to 60ms.

Field	Description
G.729/G.729b	This defines the packetization rate for codec G.729/G.729b. "None" defaults to 60ms.
G.729a/G.729ab	This defines the packetization rate for codec G.729a/G.729ab. "None" defaults to 60ms.
G.723	This defines the packetization rate for codec G.723. "None" defaults to 60ms.
Connection Options	
Switchover Method	Timing mechanism to switch over to a backup CallManager. • Graceful—The switchover happens only after all the active sessions are terminated. • Immediate—The switchover to the backup CallManager happens immediately.
Switchback Method	Timing mechanism to switch back to a primary CallManager. • Graceful—The CallManager switchback happens only after all the active sessions are terminated. • Guard (graceful guard)—The CallManager switchback happens when either the active sessions are terminated gracefully or when the guard timer expires, whichever happens first. • Immediate—Switchback to the higher order CallManager happens immediately. • Scheduled—The CallManager switchback happens during the scheduled time. • Uptime—The uptime timer is started once the higher order CallManager comes alive; once this timer expires, the CallManager switchback happens.
Switchback Interval (sec)	The Switchback Interval timer is used to control the polling of the primary or higher order CallManager(s). If attempt to switchback to a higher order CallManager fails, the Switchover Interval timer is started. When the timer expires, another attempt to switchback to a higher order CallManager is initiated.
Switchback guard timeout	This defines the guard timeout value. With the guard (graceful guard) method, the CallManager switchback happens when either the active sessions are terminated gracefully or when the guard timer expires, whichever happens first.
Switchback uptime timeout	This defines the uptime timeout value. With the uptime method, the uptime timer is started once the higher order CallManager comes alive; once this timer expires, the CallManager switchback happens.

Field	Description
Switchback scheduled timeout	This defines the scheduled time value. With the scheduled method, the CallManager switchback happens during the scheduled time.
CallManager Connect Retries	This defines the number of polling retries before connectivity to the CallManager is considered down. When the number of polling attempts reaches the Connect Retries value, connection to the next CallManager is attempted.
CallManager Connect Interval (sec)	The Connect Interval timer is used to control the polling interval of the CallManager. If the current CallManager connection fails, the Connect Interval timer is started. When the timer expires, another attempt to connect to the CallManager is initiated.
Keepalive Retries	This defines the number of keepalive retries before connectivity to the CallManager is considered down. When the number of unacknowledged keepalive messages reaches the Keepalive Retries value, CallManager switchover happens.
Keepalive Timeout (sec)	This defines the keepalive timeout value. A timer is started whenever a keepalive message is sent to the CallManager. Once the timeout occurs, the next keepalive message is sent unless the number of unacknowledged keepalive messages reaches the Keepalive Retries value.
Registration Retries	This defines the number of registration retries with one CallManager before registering to the next CallManager in the CallManager group.
Registration Timeout (sec)	This defines the registration timeout value. A timer is started whenever a registration message is sent to the CallManager. Once the timeout occurs, the next registration message is sent unless the number of unacknowledged registration messages reaches the Registration Retries value.

Cisco Video Conference Bridge (IPVC-35xx) Configuration Settings

For Cisco Prime Collaboration Release 11.5 and later

Table 16: Cisco Video Conference Bridge (IPVC-35xx) Infrastructure Configuration Product Fields

Field	Description
IOS Conference Bridge Info	
Conference Bridge Type	Choose Cisco Conference Bridge(IPVC-35xx).
Media Server Conference Bridge Info	
MAC Address	Enter a unique device MAC address.
Description	Enter a description for your conference bridge.
Device Pool	Choose a device pool or choose Default.

Field	Description
Common Device Configuration	Choose the common device configuration to assign to the conference bridge.
Location	From the drop-down list box, choose the appropriate location for this conference bridge.
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • 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.
Service Specific Configuration Layout	
General	
DSCP for Control Messages	This parameter specifies the Quality of Service field to be used in the IP packets of the SCCP protocol from the Conference Bridge to the Call Manager.
Local Base Port	The Local Base Port parameter chooses the first port used by the Conference Bridge to connect to its Cisco CallManager(s). The connection is used for SCCP messaging.
Registration Info	
Failover Recovery Mode	Failover recovery occurs when a new TCP connection to a higher priority Cisco CallManager is opened, while the Conference Bridge is connected to a lower priority Cisco CallManager. The recovery mode determines when the Conference Bridge registers to the new Cisco CallManager. • Immediate—As soon as the new connection is opened. • Graceful—Only when the Conference Bridge is free of active calls. • Timeout—When the Conference Bridge is free of active calls or when the timer expires.
Failover Recovery Timeout	This value is only active when the Failover Recovery Mode is set to Timeout. This parameter determines the time that the Conference Bridge waits before performing failover recovery regardless of the existence of active calls.

Field	Description
Keepalive Message Timeout	The keepalive message to the Cisco CallManager is typically answered by an Acknowledge Message to the Conference Bridge. The Keepalive Message Timeout determines how long the Conference Bridge should wait for the Acknowledge message before assuming that the Acknowledge will not arrive.
Keepalive Retries	The keepalive message to the Cisco Call Manager should be followed by an Acknowledge Message to the Conference Bridge. The Keepalive Message Retries determines the number of times that the keepalive message is sent (without receiving an acknowledgment) before the connection will be considered dead.
Register Messages Retries	The register and unregister messages to the Cisco CallManager should be followed by an Acknowledge message to the Conference Bridge. The Register Message Retries determines how many times the Conference Bridge retries registration before giving up on the currently configured Cisco CallManager and turning to a lower priority one if such a Cisco CallManager exists.
Register Messages Timeout	The register and unregister messages to the Cisco Call Manager should be followed by an Acknowledge message to the Conference Bridge. The Register Message Timeout determines how long the Conference Bridge should wait for an Acknowledge message before retrying the registration.
Wait For Primary Cisco CallManager Timeout	When the Conference Bridge is not connected to any Cisco CallManager, this parameter specifies how much time the bridge should wait for the primary Call Manager, before connecting to the backup Call Manager.

BLF Presence Group Fields Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 17: BLF Presence Group Fields Infrastructure Configuration Product Fields

Field	Description
BLF Presence Group Information	
Name	Enter the name of the BLF presence group that you want to configure.
Description	Enter a description for the BLF presence group that you are configuring.
Modify Relationship to Other BLF Presence Groups	
BLF Presence Group	Select one or more BLF presence groups to configure the permission settings for the named group to the selected groups.

Field	Description
Subscription Permission	For the selected BLF presence groups, choose one of the following options from the drop-down list box: • Use System Default—Set the permissions setting to the Default Inter-Presence Group Subscription cluster-wide service parameter setting (Allow Subscription or Disallow Subscription). • Allow Subscription—Allow members in the named group to view the real-time status of members in the selected groups. • Disallow Subscription—Block members in the named group from viewing the real-time status of members in the selected groups.

Unity Distribution List Infrastructure Configuration Product Fields

Table 18: Unity Distribution List Infrastructure Configuration Product Fields

Field	Description
Alias	Alias name of the distribution list.
Display Name	Name of the distribution list.
Extension	Extension that the phone system uses to connect.
Owner	Owner of the Call Handler for any user or distribution list.
Owner Type	Type of the owner.
Show Distribution List in Email Server Address Book	Displays the distribution list name in the email server's address book.
Member List	List of members associated with the distribution list. Use the format Alias/MemberType. **Note** You cannot remove the default system distribution list.

Unity Connection Distribution List Infrastructure Configuration Product Fields

Table 19: Unity Connection Distribution List Infrastructure Configuration Product Fields

Field	Description
Alias	Alias name of the distribution list.
Display Name	Name of the distribution list.

Field	Description
Extension	Extension that the phone system uses to connect.
Partition	Partition that is used to define the scope of the distribution list that a user or outside caller can reach.
Allow Contacts	Specifies whether contacts can be added as members of the distribution list.
Accept Messages from Foreign Systems	Allows users on remote voice messaging systems that are configured as VPIM locations to send messages to this distribution list.
Member List	List of users associated with the distribution list. Use the format Alias/MemberType. You are allowed to add, modify, or delete only 200 members at a time. For better performance, we recommend a maximum of 20 distribution lists, each with 500 members. If you want to manage more than 500 members, you can use a nested distribution list.

Directed Call Park Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 20: Directed Call Park Infrastructure Configuration Product Fields

Field	Description
Directed Call Park Configuration	
Number	Enter the directed call park number.
Description	Provide a brief description of this directed call park number or range.
Partition	If you want to use a partition to restrict access to the directed call park numbers, choose the desired partition from the dropdown list. If you do not want to restrict access to the directed call park numbers, leave the partition to use system default.
Reversion Number	Enter the number to which you want the parked call to return if not retrieved, or leave the field blank.
Reversion Calling Search Space	Choose the calling search space from the dropdown list or leave the calling search space to use the system default.

Field	Description
Retrieval Prefix	This required field, enter the prefix for retrieving a parked call.

Device Pool Infrastructure Configuration Product Fields

Table 21: Device Pool Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Cisco Unified CM Group	List of available Cisco Unified Communications Manager groups.
Date/Time Group	The date/time group to assign to devices in this device pool.
Region	The Cisco Unified Communications Manager region to assign to devices in this device pool.
Softkey Template	Softkey template that determines the configuration of the softkeys on Cisco IP Phones.
SRST Reference	A survivable remote site telephony (SRST) reference to assign to devices in this device pool.
Calling Search Space for Auto-Generation	The calling search space to assign to devices in this device pool that auto-registers with Cisco Unified Communications Manager.
Local Route Group	List of available local route groups.
Media Resource Group List	Provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If this field is left blank, the Media Resource Group that is defined in the device pool is used.
Network Hold MOH Audio Source	The audio source that plays when the network initiates a hold action.
User Hold MOH Audio Source	The audio source that plays Music On Hold when the user initiates a hold action.
Network Locale	The locale that is associated with endpoints and gateways.

Field	Description
User Locale	User location associated with the user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Connection Monitor Duration	Defines the amount of time that the IP phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and re-registers to Cisco Unified Communications Manager.
MLPP Indication	Specifies whether devices in the device pool that are capable of playing precedence tones will use the capability when the devices place an Multilevel Precedence and Preemption (MLPP) call.
MLPP Preemption	Specifies whether devices in the device pool that are capable of preempting calls in progress will use the capability when the devices place an MLPP call.
MLPP Domain	MLPP Domain that is associated with this device.
Emergency Location (ELIN) Group	Choose the ELIN group to associate with the device pool. **Note** This setting is applicable only if the Emergency Location Service is enabled in the Cisco Unified Communications Manager.

Feature Control Policy Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 22: Feature Control Policy Infrastructure Configuration Product Fields

Field	Description
Feature Control Policy Info	
Name	Name of the Feature Control Policy.
Description	Optional description.
Feature Control Section	

Field	Description
Enable Setting	For each feature listed, choose whether you want to enable or disable the setting: • Check the **Enable Setting** check box to enable the setting for the feature. • Uncheck the **Enable Setting** check box to disable the setting for the feature.

Feature Group Template Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 23: Feature Group Template Infrastructure Configuration Product Fields

Field	Description
Feature Group Template	
Name	Enter the feature group template name.
Description	Optional description.
Features	
Home Cluster	Check this check box if the end user is homed to this cluster.
Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)	Check this check box to enable the end user (on the home cluster) for IM and Presence
Include meeting information in Presence (Requires Exchange Presence Gateway to be configured on Unified Communications Manager IM and Presence server)	Check this checkbox to enable the end user to include meeting and calendar information in IM and Presence Service.
Service Profile	Choose a service profile.
User Profile	Choose a user profile.
Enable End User to Host Conference Now	Check this check box to allow the user to host a conference.
Allow Control of Device from CTI	Check this check box to allow control of the device from Computer Telephony Integration (CTI) applications.
Enable Extension Mobility Cross Cluster	Check this check box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature.

Field	Description
Enable Mobility	Check this check box to activate Cisco Unified Mobility.
Enable Mobile Voice Access	Check this check box to allow the user to access the Mobile Voice Access Integrated Voice Response (IVR) system.
Maximum Wait Time for Desk Pickup	Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call.
Remote Destination Limit	Enter the maximum number of phones to which the user is permitted to transfer calls.
BLF Presence Group	Choose a BLF presence group for the end user.
SUBSCRIBE Calling Search	Choose the SUBSCRIBE calling search space that is used to route the presence requests from the end user.
User Locale	Choose the locale that is associated with the user.

H323 Gateway Infrastructure Configuration Product Fields

Table 24: H323 Gateway Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Device Pool	List of available device pools. The device pool specifies a collection of properties for this device including Unified CM Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Call Classification	Determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet).
Media Resource Group List	Provides a prioritized grouping of media resource groups.
Location	Location for this device.
Media Termination Point Required	If Media Termination Point is used to implement features that H.323 does not support (such as hold and transfer), select Yes.
Retry Video Call As Audio	Applies to video endpoints that receive calls.

Field	Description
Wait for Far End H.245 Terminal Capability Set	Specifies that Cisco Unified Communications Manager needs to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set.
MLPP Domain	Multilevel Precedence and Preemption (MLPP) Domain to associate with this device.
Significant Digits Value	Represents the number of final digits that are retained on inbound calls.
Calling Search Spaces	Specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed.
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	The prefix digits that are appended to the called party number on incoming calls.
Redirecting Number IE Delivery - Inbound	Selecting Yes accepts the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent.
Calling Party Presentation	Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number.
Called Party IE Number Type Unknown	Choose the format for the number type in called party directory numbers.
Calling Party IE Number Type Unknown	Choose the format for the number type in calling party directory numbers.
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers.
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers.
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits.

Field	Description
Display IE Delivery	Enables delivery of the display IE in Setup, Connect, and Notify messages for the calling and called party name delivery service.
Redirecting Number IE Delivery - Outbound	Includes the Redirecting Number IE in the outgoing Setup message from the Cisco Unified Communications Manager to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded.
Packet Capture Mode	Configure this field if you need to troubleshoot encrypted signaling information for the H.323 gateway.
Common Device Config	Configuration of common device settings, such as the softkey template and user locale.
SRTP Allowed	Select Yes if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the gateway.
Enable Outbound FastStart	Select Yes to enable the H323 FastStart feature for outgoing calls.
AAR Group	Select an alternate routing group if there is insufficient bandwidth.
Packet Capture Duration	Configure this field if you need to troubleshoot encrypted signaling information for the H.323 gateway.

Hunt List Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 25: Hunt List Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Cisco Unified CM Group	List of available Cisco Unified Communications Manager groups.
Enable this Hunt List	Check this check box to enable the hunt list.
For Voice Mail Usage	If this hunt list is used for voicemail, check this check box.

Field	Description
Hunt List Member Information	
Line Group	Select one or more line groups from the **Available** list.

Hunt Pilot Infrastructure Configuration Product Fields

Table 26: Hunt Pilot Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Hunt Pilot	The hunt pilot, including numbers and wildcards (do not use spaces). You can enter + or \+ to indicate the international escape character. **Note** Ensure that the directory hunt pilot, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the hunt pilot, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries.
Route Partition	If you want to use a partition to restrict access to the hunt pilot, choose the desired partition.
Description	Enter a description of the hunt pilot. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Numbering Plan	Choose a numbering plan.
Route Filter	If your hunt pilot includes the @ wildcard, you may choose a route filter.
MLPP Precedence	MLPP precedence setting.
Hunt List	Choose the hunt list for which you are adding a hunt pilot.
Call Pickup Group	Choose the number that can be dialed to answer calls to this directory number (in the specified partition).
Alerting Name	Enter an alerting name for the hunt pilot in UNICODE format.

Field	Description
ASCII Alerting Name	Enter an alerting name for the hunt pilot in ASCII format.
Route Option	The Route Option designation indicates whether you want this hunt pilot to be used for routing calls or for blocking calls.
Provide Outside Dial Tone	Check this check box for each hunt pilot that routes the call off the local network and provides outside dial tone to the calling device.
Urgent Priority	To interrupt inter digit timing and route the call immediately.
Hunt Call Treatment Settings	
Forward Hunt No Answer	When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded.
Forward Hunt Busy	When the call that is distributed through the hunt list is busy in a specific period of time, this field specifies the destination to which the call gets forwarded.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Select Yes if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transformation Mask	Enter a transformation mask value.
Calling Party Prefix Digits (Outgoing Calls)	Enter the prefix digits.
Calling Line ID Presentation	Used as a supplementary service to allow or restrict the originating caller's phone number on a call basis.
Display Line Group Member DN as Connected Party	Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.
Calling Name Presentation	Used as a supplementary service to allow or restrict the originating caller's name on a call-by-call basis.
Calling Party Number Type	Choose the format for the number type in calling party directory numbers.
Calling Party Numbering Plan	Choose the format for the numbering plan in calling party directory numbers.

Field	Description
Connected Party Transformations	
Connected Line ID Presentation	Used as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis.
Display Line Group Member DN as Connected Party	Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.
Connected Name Presentation	Used as a supplementary service to allow or restrict the called party's name on a call-by-call basis.
Called Party Transformations	
Called Party Discard Digits	Select the discard digits instructions that you want to associate with this hunt pilot.
Called Party Transformation Mask	Enter a transformation mask value.
Called Party Prefix Digits (Outgoing Calls)	Enter the prefix digits.
Called Party Number Type	Choose the format for the number type in called party directory numbers.
Called Party Numbering Plan	Choose the format for the numbering plan in called party directory numbers.
AAR Group Settings	
AAR Group	Choose an Automated Alternate Routing (AAR) group from the drop-down list box.
External Number Mask	Enter an external number mask value for the hunt pilot.
Queuing **Note** Forward Hunt No Answer or Forward Hunt Busy settings are designed to move calls through the route list. Queuing, on the other hand, is used to hold callers in a route list. Therefore, if queuing is enabled, both Forward Hunt No Answer and Forward Hunt Busy are automatically disabled. Conversely, if Forward Hunt No Answer or Forward Hunt Busy are enabled, queuing is automatically disabled.	
Queue Calls	Check this check box to enable Call Queuing.
Network Hold/MOH Source and Announcements	Choose the audio source file that contains the music on hold and announcement to be played when a call is held in a queue.

Field	Description
Maximum Number of Callers Allowed in a Queue	Enter a value that specifies the maximum number of callers to be queued per hunt pilot. Call Queuing allows up to 100 callers to be queued per hunt pilot. Once this limit is reached on a particular hunt pilot, subsequent calls can be routed to an alternate number.
Maximum Wait Time in Queue	Enter a value (in seconds) that specifies the maximum wait time for each call in a queue. Each caller can be queued for up to 3600 seconds per hunt pilot. Once this limit is reached, that caller is routed to an alternate number.
When No Hunt Members are Logged In or registered	Check this check box to route the calls to an alternate number when none of the hunt members are logged in or registered.
Park Monitoring	
Park Monitoring Forward No Retrieve Destination	When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) to forward the parked call when the service parameter Park Monitoring Forward No Retrieve Timer expires. If the parameter value of the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter is blank, then the call will be forwarded to the destination configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires. Specify the following values • Destination-This setting specifies the directory number to which a parked call is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination. • Calling Search Space-A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

Intercom Calling Search Space Infrastructure Configuration Product Fields

Table 27: Intercom Calling Search Space Infrastructure Configuration Product Fields

Field	Description
Intercom Calling Search Space Information	
Name	Enter the intercom calling search space name.
Description	Optional description.
Intercom Route Partitions for this Calling Search Space	
Available Intercom Partitions	Choose an intercom partition in the Available Intercom Partitions list box and add it to the Selected Intercom Partitions list box by clicking the arrow button between the two list boxes.
Selected Intercom Partitions(Ordered by highest priority)	Displays all the selected intercom partition. To change the priority of an intercom partition, choose an intercom partition name in the Selected Intercom Partitions list box. Move the intercom partition up or down in the list by clicking the arrows on the right side of the list box.

Intercom Directory Number Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 28: Intercom Directory Number Infrastructure Configuration Product Fields

Field	Description
Intercom Directory Number Information	
Intercom Directory Number	Enter a phone number.
Route Partition	Choose the intercom partition to which the intercom directory number belongs.
Description	Enter a description of the intercom directory number and intercom route partition.
Alerting Name	Enter a name that you want to display on the phone of the caller.
ASCII Alerting Name	Enter the same information as the Alerting Name field, but limit input to ASCII characters.
Intercom Directory Number Settings	
Calling Search Space	Choose an intercom calling search space.
BLF Presence Group	Choose a BLF Presence Group for this intercom directory number.

Field	Description
Auto Answer	Choose the required auto answer feature for this intercom directory number.
Default Activate Device	Choose a default activated device for this intercom directory number.

Intercom Route Partition Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 29: Intercom Route Partition Infrastructure Configuration Product Fields

Field	Description
Intercom Partition Information	
Name	Enter the intercom partition name.
Description	Optional description.
Time Schedule	Choose the required time schedule.
Time Zone	Choose the required time zone. If you want the time zone to be same as that of the originating device, choose Originating Device. By default Originating Device option is selected.

Intercom Translation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 30: Intercom Translation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Intercom Translation Pattern	Intercom Translation Pattern, including numbers and wildcards (do not use spaces).
Partition	Choose an intercom partition.
Description	Optional description.
Numbering Plan	Choose a numbering plan.
Route Filter	Choosing an optional route filter restricts certain number patterns.
Calling Search Space	Choose the intercom calling search space for which you are adding an intercom translation pattern.

Field	Description
Pattern Definition	
Block this pattern	Choose the reason for which you want this intercom translation pattern to block calls.
Provide Outside Dial Tone	Check this check box to routes the calls off the local network.
Urgent Priority	Check this check box to interrupt interdigit timing and route the call immediately.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transform Mask	Enter a transformation mask value.
Prefix Digits (Outgoing Calls)	Enter the prefix digits.
Calling Line ID Presentation	Used as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis.
Calling Name Presentation	Used as a supplementary service to allow or restrict the originating caller's name on a call-by-call basis.
Connected Party Transformations	
Connected Line ID Presentation	Used as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis.
Connected Name Presentation	Used as a supplementary service to allow or restrict the called party's name on a call-by-call basis.
Called Party Transformations	
Discard Digits	Choose the discard digits instructions that you want to be associated with this intercom translation pattern.
Called Party Transform Mask	Enter a transformation mask value.
Prefix Digits (Outgoing Calls)	Enter the prefix digits.

Line Group Infrastructure Configuration Product Fields

Table 31: Line Group Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
RNA Reversion Timeout	Enter a time, in seconds, after which Cisco Unified Communications Manager will distribute a call to the next available or idle member of this line group or to the next line group if the call is not answered and if the first hunt option, "Try next member; then, try next group in Hunt List" is chosen.
Distribution Algorithm	Select a distribution algorithm, which applies at the line group level.
Hunt Algorithm No Answer	For a given distribution algorithm, select a hunt option for Cisco Unified Communications Manager to use if a call is distributed to a member of a line group that does not answer.
Hunt Algorithm Busy	For a given distribution algorithm, select a hunt option for Cisco Unified Communications Manager to use if a call is distributed to a member of a line group that is busy.
Hunt Algorithm Not Available	For a given distribution algorithm, select a hunt option for Cisco Unified Communications Manager to use if a call is distributed to a member of a line group that is not available.
Directory Numbers	Enter a directory number that already exists in Cisco Unified Communications Manager.

Local Route Group Names Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 32: Local Route Group Names Infrastructure Configuration Product Fields

Field	Description
Local Route Group Names	
Name	Enter a unique local route group name in this required field.
Description	Enter a description that will help you to distinguish between local route group names.

Location Infrastructure Configuration Product Fields

Table 33: Location Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kbps) that is available for all audio calls on the link between this location and other locations. **Note** This option is available for Cisco Unified Communications Manager 9.0 or higher versions.
Video Bandwidth	Enter the maximum amount of video bandwidth (in kbps) that is available for all video calls on the link between this location and other locations. Use 0 for Unlimited and -1 for None. **Note** This option is available for Cisco Unified Communications Manager 9.0 or higher versions.
Links	Bandwidth Between This Location and Adjacent Locations.
Location	Select a location from the list.
Weight	Enter the relative priority of this link in forming the Effective Path between any pair of Locations. The Effective Path has the least cumulative of all possible paths. Valid values are 0-100.

Media Termination Point Infrastructure Configuration Product Fields

Table 34: Media Termination Point Fields

Field	Description
Media Termination Point Type	Choose Cisco Enhanced Software Termination Point.
Media Termination Point Name	Enter a name for the media termination point upto 15 alphanumeric characters. **Note** You cannot use special characters as the MTP name, for example: !, @, #, $, or %.
Description	Enter any description for the media termination point.
Device Pool	Choose a device pool that has the highest priority.

Trusted Relay Point	Check this checkbox to designate this media termination point (MTP) as a trusted relay point (TRP) that Cisco Unified Communications Manager can use in a network virtualization environment.

Message Waiting Infrastructure Configuration Product Fields

Table 35: Message Waiting Fields

Field	Description
Message Waiting Number	Enter the Cisco Message Waiting directory number.You may use the following characters: 0 to 9, ?, [,], +, -, *, ^, #, !.
Partition	If partitions are being used, choose the appropriate partition from the drop-down list box.
Description	Enter up to 50 characters for a description of the message-waiting directory number. You may use any characters except the following: "", <, >, &, %.
Message Waiting Indicator	Click On or Off.
Calling Search Space	If partitions and calling search spaces are used, from the drop-down list box, choose a calling search space that includes the partitions of the DNs on all phones whose lamps you want to turn on (the partition that is defined for a phone DN must be in a calling search space that the MWI device uses).

Media Resource Group Infrastructure Configuration Product Fields

Table 36: Media Resource Group Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Available Devices	The available media resources that can be selected.
Is Multicast for MOH Audio	Click Yes to use multicast for Music On Hold Audio.

Media Resource Group List Infrastructure Configuration Product Fields

Table 37: Media Resource Group List Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.
Available Media Resource Group Names	The available media resource groups that can be selected.

Meet-Me Number/Pattern Configuration Product Fields

Table 38: Meet-Me Number/Pattern Configuration Product Fields

Field	Description
Directory Number or Pattern	Enter Meet-Me number/pattern or a range of numbers. To configure a range, the dash must appear within brackets and follow a digit; for example, to configure the range 1000 to 1050, enter 10[0-5]0. This field allows up to 24 characters.
Description	The description can include up to 50 characters. The following characters are not allowed: double-quotes ("), backslash (\), dash (-), percentage sign (%), ampersand (&), or angle brackets (<>).
Partition	To use a partition to restrict access to the Meet-Me number/pattern, choose the desired partition from the drop-down list.
Minimum Security Level	Choose the minimum security level for this Meet-Me number/pattern from the drop-down list. • Choose Authenticated to block participants with nonsecure phones from joining the conference. • Choose Encrypted to block participants with nonsecure phones from joining the conference. • Choose Non Secure to allow all participants to join the conference.

Partition Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 39: Partition Infrastructure Configuration Product Fields

Field	Description
Partition Information	
Name	Enter a partition name.
Description	Enter a description for the partition.
Time Schedule	Choose a time schedule to associate with this partition.
Time Zone	Choose one of the following options to associate a partition with a time zone: • Originating Device—If you choose this option, the system checks the partition against the associated time schedule with the time zone of the calling device. • Specific Time Zone—If you choose this option, the system checks the partition against the associated time schedule at the time that is specified in this time zone.

Recording Profile Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and later

Table 40: Recording Profile Infrastructure Configuration Product Fields

Field	Description
Name	Enter a the recording profile name.
Recording Calling Search Space	Choose the calling search space that contains the partition of the route pattern that is associated with the SIP trunk that is configured for the recorder.
Recording Destination Address	Enter the directory number (DN) or the URL of the recorder that associates with this recording profile.

Region Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 41: Region Infrastructure Configuration Product Fields

Field	Description
Region Information	
Name	Enter a unique name for this region.
Modify Relationship to other Regions	
Region	The entries in this column display all regions for which non-default relationships have been configured.
Audio Codec Preference List	For each region that is specified in the Regions window pane, choose the corresponding value from the drop-down list box in this column to set the Audio Codec Preference list describing the network conditions between this region and the specified region. • Use System Default—Choose this value to use the system default value for link loss type. • Factory Default Low Loss—Choose this value to specify a low-loss link loss type. • Factory Default Lossy—Choose this value to specify a lossy link loss type.
Maximum Audio Bit Rate	For each region that is specified in the Regions window pane, choose the value from the drop-down list box in this column to set the maximum bit rate to use for audio between this region and the specified region. This setting applies to both audio and video calls and serves as an upper limit for the audio bit rate, which means that audio codecs with higher bit rates than the one that you specify are not used for these calls.
Maximum Session Bit Rate for Video Calls	Enter Kbps value or select either one of the below option in this column: • Use System Default—Select this option to use the default value. • None—If you select this option, the system does not allow video calls.
Maximum Session Bit Rate for Immersive Video Calls	Enter Kbps value or select either one of the below option in this column: • Use System Default—Click this button to use the default value. The default value normally specifies 2000000000 kbps. • None—If you select this option, the system does not allow immersive video calls.

Restriction Table Infrastructure Configuration Product Fields

Table 42: Restriction Table Infrastructure Configuration Product Fields

Field	Description
Remove-Restriction-Pattern	To delete a restriction pattern from a restriction table. The value is restriction pattern alone. This could have multiple values separated by semicolon (;) .For Example : +#99;+91.
Pattern	Enter specific numbers or patterns of numbers that can be permitted or restricted. Include external and long-distance access codes. Use digits 0 through 9 and the following special characters: • * to match zero or more digits. • ? to match exactly one digit. Each ? serves as a placeholder for one digit. • # to correspond to the # key on the phone. • + to call from one country to other country.
Display Name	Enter a descriptive name for the restriction table.
Update-Restriction-Pattern	To update a restriction pattern of a restriction table.This is combination of both restriction pattern and blocked attribute.This could have multiple values separated by semicolon (;) .For Example : +#99/False;+91/true.
New Restriction Patterns are Blocked by Default	Indicate whether new restriction patterns should be flagged as Blocked by default.Default setting: Check box not checked.
Minimum Length of Dial String	Enter the minimum number of digits-including access codes-in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits greater than or equal to the Minimum Length of Dial String value are checked against the restriction table. Dial strings that contain fewer than the Minimum Length of Dial String value are not permitted. For example, to prohibit users from using four-digit numbers, enter 5 in the Minimum Length of Dial String field. Default setting: 1 digit.
Blocked	Check this check box to have Unity Connection prohibit use of phone numbers that match the pattern.

Field	Description
Maximum Length of Dial String	Enter the maximum number of digits-including access codes-in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits fewer than or equal to the Maximum Length of Dial String value are checked against the restriction table. Dial strings that contain more than the Maximum Length of Dial String value are not permitted. For example, if local calls in your area are seven digits long, and you want to prevent users from using long distance phone numbers, enter 8 in the Maximum Length of Dial String field. (A local number plus the access code for the phone system equals 8 digits.)Default setting: 30 digits.
Add-Restriction-Pattern	To add a new restriction pattern to a restriction table.This is combination of both restriction pattern and blocked attribute.This could have multiple values separated by semicolon (;) .For Example : +#99/True;+91/false.

Route Group Infrastructure Configuration Product Fields

Table 43: Route Group Infrastructure Configuration Product Fields

Field	Description
Route Group Information	
Name	Infrastructure Configuration Product name.
Distribution Algorithm	The available options can be chosen.
Ports	If the device supports individually configurable ports, choose the port.
Route Group Member Information	
Find Devices to Add to Route Group	
Device Name contains	Enter the character(s) that are found in the device name that you are seeking and click the Find button. Device names that match the character(s) that you entered display in the Available Devices box.
Available Devices	Choose a device in the Available Devices list box and add it to the Selected Devices list box by clicking Add to Route Group.

Field	Description
Port(s)	If this device supports individually configurable ports, choose the port. (Devices that allow you to choose individual ports include Cisco Access Analog and Cisco MGCP Analog gateways and T1 CAS.) Otherwise, choose the default value (All or None Available, depending upon the device that is chosen). For a device that has no ports available (None Available), the device may already be added to the Route Group or cannot be added to the route group.
Current Route Group Members	
Selected Devices	To change the priority of a device, choose a device name in the Selected Devices list box.
Removed Devices	Choose a device in the Selected Devices list box and add it to the Removed Devices list box.
Route Group Members	
List of devices	This pane displays links to the devices that have been added to this route group. **Note** When you are adding a new route group, this list does not display until you save the route group.

Route List Infrastructure Configuration Product Fields

Table 44: Route List Infrastructure Configuration Product Fields

Field	Description
Route List Information	
Route List Name	Infrastructure Configuration Product name.
Description	Optional description.
Cisco Unified CM Group	List of available Cisco Unified Communications Manager groups.
Enable this Route List	Select Yes to enable the route list.
Run On All Active Unified CM Nodes	To enable the active route list to run on every node, check this check box.
Save	When you click this button to save a route list, a popup message reminds you that you must add at least one route group to this route list for it to accept calls.

Field	Description
Add Route Group	To add a route group to this route list, click this button and perform the procedure to add a route group to a route list.

Route Partition Infrastructure Configuration Product Fields

Table 45: Route Partition Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Description	Optional description.

Route Pattern Infrastructure Configuration Product Fields

Table 46: Route Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Pattern	A valid route pattern, including numbers and wildcards.
Route Partition	If you want to use a partition to restrict access to the route pattern, select the desired partition.
Description	Optional description.
Numbering Plan	Numbering plan. The default setting is North American Numbering Plan (NANP).
Route Filter	If your route pattern includes the @ wildcard, you may choose a route filter.
MLPP Precedence	MLPP precedence setting.
For Cisco Prime Collaboration Release 11.5 and later Apply Call Blocking Percentage	Check this check box to enable the Destination Code Control (DCC) feature.
For Cisco Prime Collaboration Release 11.5 and later Blocked Call Percentage	Enter the percentage of calls to be blocked for this destination in numerals. **Note** The Blocked Call Percentage (%) field gets enabled only if the Apply Call Blocking Percentage check box is checked.

Field	Description
For Cisco Prime Collaboration Release 11.5 and later Resource Priority Namespace Network Domain	Choose a Resource Priority Namespace Network Domain from the drop-down list box.
For Cisco Prime Collaboration Release 11.5 and later Route Class	The route class is a DSN code that identifies the class of traffic for a call.
Gateway, Route List, or SIP Trunk	Choose the gateway or route list for which you are adding a route pattern. You can also enter a value that does not appear in the list. If you enter a custom value, specify whether it is a gateway, route list, or SIP trunk. After the name, add one of the following: • [GW]—Gateway • [RL]—Route list • [ST]—SIP trunk For example, gatewayname[GW].
Release Cause	Dependent on the Block Enabled field. If a release cause is selected, then Block Enabled must be set to True.
Allow Device Override	If Yes is selected, the system uses the Call Classification setting that is configured on the associated gateway or trunk to consider the outgoing call as OffNet or OnNet.
Urgent Priority	If Yes is selected, the interdigit timing is interrupted when Cisco Unified Communications Manager must route a call immediately.
For Cisco Prime Collaboration Release 11.5 and later Is an Emergency Service Number	Check this check box, if you are configuring an emergency service number. **Note** This setting is applicable only if the Emergency Location Service is enabled in the call manager.
Call Classification	Indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network.
Provide Outside Dial Tone	If Yes is selected, an outside dial tone is provided.
For Cisco Prime Collaboration Release 11.5 and later External Call Control Profile	Choose the external call profile that you want to assign to the route pattern.

Field	Description
For Cisco Prime Collaboration Release 11.5 and later Allow Overlap Sending	Check this check box to configure Allow Overlap Sending flag in the Route Pattern.
For Cisco Prime Collaboration Release 11.5 and later Require Forced Authorization Code	If you want to use forced authorization codes with this route pattern, check this check box.
For Cisco Prime Collaboration Release 11.5 and later Authorization Level	Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that needs to successfully route a call through this route pattern.
For Cisco Prime Collaboration Release 11.5 and later Require Client Matter Code	If you want to use client matter codes with this route pattern, check this check box.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Select Yes if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transformation Mask	Transformation mask value.
Calling Party Prefix Digits (Outgoing Calls) This field renamed as Prefix Digits (Outgoing Calls) from Cisco Prime Collaboration 11.5 and later.	Prefix digits.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this route pattern.
Calling Name Presentation	Determines whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party's name on the called party's phone display for this route pattern.
For Cisco Prime Collaboration Release 11.5 and later Calling Party Number Type	Format for the number type in calling party directory numbers.
For Cisco Prime Collaboration Release 11.5 and later Calling Party Numbering Plan	Format for the numbering plan in calling party directory numbers.
Connected Party Transformations	

Field	Description
Connected Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this route pattern.
Connected Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's name on the calling party's phone display for this route pattern.
Called Party Transformation	
Called Party Discard Digits (Outgoing Calls)	Determines the discard digits instructions that you want to associate with this route pattern.
Called Party Transformation Mask	Transformation mask value.
For Cisco Prime Collaboration Release 11.5 and later Prefix Digits (Outgoing Calls)	Prefix digits.
For Cisco Prime Collaboration Release 11.5 and later Called Party Number Type	Format for the number type in calling party directory numbers.
For Cisco Prime Collaboration Release 11.5 and later **For Cisco Prime Collaboration Release 11.5 and later** Called Party Numbering Plan	Format for the numbering plan in calling party directory numbers.
For Cisco Prime Collaboration Release 11.5 and later Network Service Protocol	Choose the PRI protocol that matches the protocol of the terminating gateway.
For Cisco Prime Collaboration Release 11.5 and later Carrier Identification Code	Carrier identification codes allow you to reach the services of interexchange carriers.
Network Service	Network Service.
Service Parameter Value	Service parameter value, valid entries include the digits 0 to 9.

Service Profile Infrastructure Configuration Product Fields

Table 47: Service Profile Infrastructure Configuration Product Fields

Field	Description
Name	Enter the name of the service profile. Maximum characters: 50 (ASCII only). Allowed Values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Description	(Optional) Enter a description that helps you to distinguish between service profiles when you have more than one configured. Allowed Values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Default profile	Check this check box to make this service profile the default option for the system. If you specify a default service profile, end users that do not have an associated service profile automatically inherit the default service profile settings.
Voicemail Profile	
Primary	Select the primary voicemail server with which you want to associate this service profile.
Secondary	Select a secondary voicemail server, if applicable.
Tertiary	Select a tertiary voicemail server, if applicable.
Credentials source for voicemail service	If user credentials for the voicemail service are shared with another service, select the appropriate service. The user credentials automatically synchronize from the service that you select. Default Setting: Not set
Mailstore Profile	
Primary	Select the primary mailstore server with which you want to associate this service profile.
Secondary	Select a secondary mailstore server, if applicable.
Tertiary	Select a tertiary mailstore server, if applicable.
Inbox folder	The name of the folder on the mailstore server in which to store new messages. Only change this value if the mailstore server uses a different folder name from the default folder. Default: Inbox
Trash folder	The name of the folder on the mailstore server in which to store deleted messages. Only change this value if the mailstore server uses a different folder name from the default folder. Default: Deleted Items

Polling Interval (in seconds)	The time (in seconds) that can elapse between polls of the IMAP server for new voice messages, when IDLE is not supported by the mailstore or when a connection failure occurs. Allowed values: 60 - 900 Default: 60
Allow dual folder mode	This dual folder setting is checked by default for use with mailstores that support the IMAP UIDPLUS extensions (RFC 2359 and 4315). By default, the Client Services Framework (CSF) detects if UIDPLUS is not supported and automatically reverts to Single Folder mode. Uncheck this check box if you know that UIDPLUS is not supported and you want to force the system to use Single Folder mode. Default: True
Conferencing Profile	
Primary	Select the primary conferencing server with which you want to associate this service profile.
Secondary	Select a secondary conferencing server, if applicable.
Tertiary	Select a tertiary conferencing server, if applicable.
Server Certificate Verification	Specify how the conferencing server associated with this profile supports TLS connections. This setting is for TLS verification of the conferencing servers listed for this conferencing profile. Select from the following options: • Any Certificate: Cisco Jabber accepts all valid certificates. • Self Signed or Keystore: Cisco Jabber accepts the certificate if the certificate is self-signed, or the signing Certificate Authority certificate is in the local trust store. **Note** A keystore is a file that stores authentication and encryption keys. Cisco Jabber accepts only certificates that are defined in the keystore. You must import the certificate or its Certificate Authority signing certificate into the local trust store.
Credentials source for web conferencing service	If user credentials for the meeting service are shared with another service, select the appropriate service. The user credentials automatically synchronize from the service that you select. Default Setting: Not set
Directory Profile	
Primary	Select the primary directory server with which you want to associate this service profile.
Secondary	Select a secondary conferencing server, if applicable. If you do not set up any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.

Tertiary	Select a tertiary conferencing server, if applicable. If you do not set up any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.
Use UDS for contact resolution	Check this check box if you want to use the UDS service provided in Cisco Unified Communications Manager for the directory lookup instead of external directory.
Use Logged On User Credential	Check this check box to prevent anonymous queries and force the user to enter credentials to sign in to the LDAP server.
Username	Enter the distinguished name for the user ID that is authorized to run queries on the LDAP server, in the format useraccount@domain.com. Maximum length: 128
Password	Enter the password for the Username that is authorized to run queries on your LDAP server. Maximum length: 128
Search Base	This field allows you to narrow your Cisco Unified Personal Communicator contact search queries to a certain part of the LDAP directory. Enter the container or directory on the LDAP server where you have configured your LDAP users. Example for the search base wtih Microsoft Active Directory integration: cn=users,DC=EFT-LA,DC=cisco,DC=com. Maximum length: 256
Recursive Search on All Search Bases	Check this check box to perform a recursive search of the directory starting at the search base. Recursive search allows for Cisco Unified Personal Communicator contact search queries to search all of the LDAP directory tree from a given search context (search base).
Search Timeout (seconds)	Set the default timeout for searches (default is 5 seconds).
Base Filter (Only used for Advance Directory)	Use this option only if the object type that you want to retrieve with queries that you execute against Active Directory is not a user object. Maximum length: 256
IM and Presence Profile	
Primary	Select the primary IM and Presence server with which you want to associate this service profile.
Secondary	Select a secondary conferencing server, if applicable.
Tertiary	Select a tertiary conferencing server, if applicable.
CTI Profile	
Primary	Select the primary CTI server with which you want to associate this service profile.
Secondary	Select a secondary CTI server, if applicable.
Tertiary	Select a tertiary CTI server, if applicable.

SIP Route Pattern Infrastructure Configuration Product Fields

Table 48: SIP Route Pattern Infrastructure Configuration Product Fields

Field	Description
Use Calling Party's External Phone Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.
Description	For this optional entry, enter a description of the SIP Route Pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Calling Line ID Presentation	Uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want your system to allow or restrict the display of the calling party phone number on the called party phone display for this SIP route pattern. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want to allow the display of the calling number. Choose Restricted if you want to block the display of the calling number.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9 and the wildcard characters asterisk (*) and octothorpe (#). The appended prefix digit does not affect which directory numbers route to the assigned device.
SIP Trunk/Route List	(Required) From the drop-down list choose the SIP trunk or route list to which the SIP route pattern should be associated. Click Edit to open the trunk or route list in the Trunk or Route List Configuration window. URI dialing is available over SIP trunks only. If you are using URI dialing and you select a route list from this drop-down list box, the route list must contain route groups with SIP trunks only.

Field	Description
IPv6 Pattern	Uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6. If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv4 Pattern in addition to the IPv6 Pattern.
IPv4 Pattern	(Required) Enter the domain, sub-domain, IPv4 address, or IP subnetwork address. For DomainRouting pattern usage, enter adomain name IPv4 Pattern field that can resolve to an IPv4 address. The domain namecan contain the following characters: [, -, ., 0-9, A-Z, a-z, *, and]. For IPAddress Routing pattern usage, enter an IPv4 address the IPv4 Pattern field that follows the format X.X.X.X, where X representsa number between 0 and 255. For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, X.X.X.X/Y; where Y is the network prefix that denotes the number of bits in the address that will be the network address. If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.
Connected Line ID Presentation	Uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want your system to allow or restrict the display of the connected party phone number on the calling party phone display for this SIP route pattern. Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want to display the connected party phone number. Choose Restricted if you want your system to block the display of the connected party phone number. If a call that originates from an IP phone on your system 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.

Field	Description
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9 and the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not checked, no calling party transformation takes place.
Connected Line Name Presentation	Uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want your system to allow or restrict the display of the connected party name on the calling party phone display for this SIP route pattern. Choose Default if you do not want to change the connected name presentation. Choose Allowed if you want your system to display the connected party name. Choose Restricted if you want your system to block the display of the connected party name.
Calling Line Name Presentation	Uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis. Choose whether you want your system to allow or restrict the display of the calling party name on the called party phone display for this SIP route pattern. Choose Default if you do not want to change calling name presentation. Choose Allowed if you want your system to display the calling name information. Choose Restricted if you want your system to block the display of the calling name information.
Block Pattern	If you do not want this pattern to be used for routing calls, click the Block Pattern check box.
Pattern Usage	(Required) From the drop-down list, choose either Domain Routing or IP Address Routing.

Field	Description
Route Partition	If you want to use a partition to restrict access to the SIP route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the SIP route pattern, choose <None> for the partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more than 250 partitions are specified by using the Max List Box Items enterprise parameter, the Find button displays next to the drop-down list box. Click the Find button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click Add Selected. To set the maximum list box items, choose System>> Enterprise Parameters>> and choose CCMAdmin Parameters. Make sure that the combination of SIP route pattern, route filter, and partition is unique within the cluster.

SIP Trunk Infrastructure Configuration Product Fields

Table 49: SIP Trunk Infrastructure Configuration Product Fields

Field	Description
AAR Group	The Automated Alternate Routing (AAR) group provides the prefix digits that are used to route calls that are otherwise blockedbecause of insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Call Classification	Determines whether an incoming call that is using this trunk is considered off the network (OffNet) or on the network (OnNet), or should use the system default setting.

Field	Description
Common Device Config	Choose the common device configuration for 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 page.
Connected Party Transformation CSS	Choose to transform the connected party number on the device in order 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. Ensure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. If you configure the Connected Party Transformation CSS as None, the transformation does not match and is not applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Device Name	Object name.
Description	Optional description.
Device Pool	List of available device pools. The device pool specifies a collection of properties for this device, including Unified CM Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Location	Specifies the total bandwidth that is available for calls between this location and the central location (or hub). A location setting of Hub_None specifies unlimited available bandwidth.
Media Resource Group List	Provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List.

Field	Description
Media Termination Point Required	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. Deselect the Media Termination Point Required check box if you do not want to use a media termination point to implement features. Check 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 either device is a video endpoint, the call operates as audio only.
Retry Video Call as Audio	Applies to video endpoints that receive calls. For trunks, it 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 will not try to establish an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and (or) route or hunt list.
Unattended Port	If selected, calls can be redirected, transferred, or forwarded to an unattended port, such as a voice mail port. The default value is deselected.

Field	Description
SRTP Allowed	Select 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. If you check this check box, it is recommended 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, you must consider signaling between Cisco Unified Communications Manager and the gateway as nonsecure.

Field	Description
Use Trusted Relay Point	From the list, 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—The device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Disables 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—Enables 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 TRP device designates an MTP or transcoder device that is labeled as a TRP. 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 is used as the required MTP. 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.
Incoming Calling Party Unknown Number Prefix	If this is set to Default, the Call Processor uses the prefix at the next level setting (Device Pool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty, in which case no prefix is assigned.

Field	Description
MLPP Domain	Choose an MLPP Domain to associate with this device. If you leave this field empty, the 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.
Remote-Party-Id	Allows 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 select Yes, the SIP Trunk always sends the RPID header.
Asserted-Identity	Allows the SIP Trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you select Yes, 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 you select No, 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.

Field	Description
Asserted-Type	Specifies the type of Asserted Identity header that SIP Trunk messages should include. Select one of the following values: • Default—Represents the default value. Screening indication information that the SIP Trunk receives from Cisco Unified Communications Manager Call Control determines the type of header the SIP Trunk sends. • PAI—The Privacy-Asserted Identity (PAI) header is 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 is sent in outgoing SIP Trunk messages. This value overrides the screening indication value that comes from Cisco Unified Communications Manager. **Note** These headers are sent only if the Asserted Identity check box is checked.

Field	Description
SIP Privacy	Specifies the type of SIP privacy header for SIP Trunk messages to include. Select one of the following values: • Default—Represents the default value. Name and number presentation values that the SIP Trunk receives from the Cisco Unified Communications Manager Call Control compose the SIP Privacy header. For example: • If the name and number presentation is restricted, the SIP Trunk sends the SIP Privacy header. • If the name and number presentation is allowed, the SIP Trunk does not send the Privacy header. • None—The SIP Trunk includes the header Privacy:none, which means that presentation is allowed. This value overrides the Presentation information that comes from Cisco Unified Communications Manager. • ID—The SIP Trunk includes the header Privacy:id, which means that the presentation is 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 header Privacy:id;critical, which means that presentation is restricted for both name and number. The critical label means that privacy services that are requested for this message are critical, and if the network cannot provide these privacy services, this request should be rejected. This value overrides the presentation information that comes from Cisco Unified Communications Manager. **Note** These headers are sent only if the Asserted Identity check box is checked.

Field	Description
Significant Digits	Represents the number of final digits that are retained on inbound calls. It is used 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. Select the number of significant digits to collect (0 to 32). Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called.
Connected Party 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 is Default, which translates to Allowed. Select Default if you want Cisco Unified Communications Manager to send connected line information. Select Restricted if you do not want Cisco Unified Communications Manager to send connected line information.
Connected Name Presentation	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 is Default, which translates to Allowed. Select Default if you want Cisco Unified Communications Manager to send connected name information. Select Restricted if you do not want Cisco Unified Communications Manager to send connected name information.
Calling Search Space	Available calling search spaces.
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	The prefix digits that are appended to the called party number on incoming calls.

Field	Description
Redirecting Diversion Header Delivery - Inbound	Select Yes (the default) to accept the Redirecting Number in the incoming invite message to the Cisco Unified Communications Manager. Select No 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 select Yes.
Called Party Transformation CSS	Allows you to localize the called party number on the device. The Called Party Transformation CSS that you choose must contain the called party transformation pattern that you want to assign to this device. If you configure the Called Party Transformation CSS as None, the transformation does not match and is not applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Called Party Transformation CSS	Select Yes to use the Called Party Transformation CSS that is configured in the device pool that is assigned to this device. If you select No, the device uses the Called Party Transformation CSS that was configured for the device in the Trunk Configuration page.
Calling Party Transformation CSS	Enables you to localize the calling party number on the device. Ensure 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 Calling Party Transformation CSS as None, the transformation will not match and will not be applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

Field	Description
Calling Party Selection	Select 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—Sends the directory number of the redirecting device. • Last Redirect Number—Sends the directory number of the last device to redirect the call. • First Redirect Number (External)—Sends the external directory number of the redirecting device. • Last Redirect Number (External)—Sends the external directory number of the last device to redirect the call.
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. Select one of the following options: • Default—If you do not want to change the presentation setting. • Allowed—If you want the calling number information to be displayed. • Restricted—If you do not want the calling number information to be displayed.

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. Select one of the following options: • Default—If you do not want to change the presentation setting. • Allowed—If you want Cisco Unified Communications Manager to send calling name information. • Restricted—If you do not want Cisco Unified Communications Manager to send the calling name information.
Caller ID DN	Enter the pattern (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 appends the number with the area code if it is not specified. • 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 central office appends the number with the area code if it is not specified.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP device.
Redirecting Diversion Header Delivery - Outbound	If Yes is selected, the redirecting number is included in the outgoing invite message from Cisco Unified Communications Manager to indicate the original called party number and the redirecting reason for the call when the call is forwarded. If No is selected, the first redirecting number and the redirecting reason are excluded from the outgoing invite message. The redirecting number is used for voice messaging integration only. If your configured voice messaging system supports redirecting Number, you should select Yes.

Field	Description
Destination Address	The remote SIP peer with which this trunk will communicate. The allowed values for this field are a valid V4 IP address, a fully qualified Domain name, or a DNS SRV record (applies only if *yes* is selected in the Destination Address is an SRV field). SIP trunks only accept incoming requests from the configured destination address and the 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, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster.
Destination Address is an SRV	Specifies that the configured Destination Address is an SRV record.
Destination Port	Enter the destination port. Ensure that the value you enter specifies a port between 1024 and 65535 (the default value is 5060). You can specify the same port number for multiple trunks. Do not enter a value if the destination address is a DNS SRV port. The default port number 5060 indicates a SIP port.
Geolocation	An unspecified geolocation, which designates that this device does not associate with a geolocation. You can also select a geolocation that has been configured.
Geolocation Filter	Specifies the geolocation filter for the device.
Incoming Port	Incoming port number.
Outgoing Transport Type	Outgoing transport type (TCP or UDP).
MTP Preferred Originating Codec	Indicates the preferred outgoing codec. To configure G.711/G.729 codecs for use with a SIP Trunk, you must use a hardware MTP or transcoder that supports the G.711/G.729 codec.
Send Geolocation Information	Sends the geolocation information for the associated device.

Field	Description
SIP Trunk Security Profile	Select 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, on Cisco Unified Communications Manager choose **System > Security Profile > SIP Trunk Security Profile**. For information on how to configure security profiles, see *Cisco Unified Communications Manager Security Guide*.
Rerouting Calling Search Space	Determines where a SIP user (A) can refer another user (B) to a third party (C). After the referral 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).
Out-Of-Dialog Refer Calling Search Space	Used when a Cisco Unified Communications Manager refers a call (B) coming in to a SIP user (A) to a third party (C) when there is no involvement of a SIP user (A). In this case, the system uses the out-of-dialog calling search space of the SIP user (A).

Field	Description
Packet Capture Mode	Exists only for troubleshooting encryption. Packet capturing may cause high CPU usage or call-processing interruptions. Select one of the following options: • None—This option, which is 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 non encrypted 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 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. You do not have to reset the trunk after enabling or disabling Packet Capture.
Packet Capture Duration	Exists only for troubleshooting encryption. Packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes allotted for one session of packet capturing. The default setting is 0, and the range is 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” is displayed.

Field	Description
Presence Group	Configures the Unified Presence features. Select a Presence group for the SIP trunk. The selected group specifies the destinations that the device, application, or server that is connected to the SIP trunk can monitor. The default value for Presence Group specifies Standard Presence group, which is 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.
PSTN Access	Indicates that the 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.
Route Class Signaling Enabled	From the drop-down list, enable or disable route class signaling for the port. Select 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
Subscribe Calling Search Space	Determines how Cisco Unified Communications Manager routes presence requests from the device, server, or 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. Select a 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 appear 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 can configure a calling search space as you do all calling search spaces.
SIP Profile	Select the SIP profile that is to be used for this SIP Trunk.

Field	Description
Trunk Service Type	Specifies the type of the Trunk Service. Select one of the following options: • None—Select 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—Selecting 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. • Extension Mobility Cross Cluster—Select 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. • Cisco Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field.

Field	Description
Transmit UTF-8 for Calling Party Name	Specifies 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. The default value for Transmit UTF-8 for Calling Party Name leaves the check box unchecked.
Use Device Pool Connected Party Transformation CSS	Enables you to use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device. 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.

Field	Description
DTMF Signaling Method	Select one of the following options: • No Preference (default)—Cisco Unified Communications Manager will pick the DTMF method to negotiate DTMF, so an MTP is not required for the call. If Cisco Unified Communications Manager does not have a choice but to allocate an MTP (if the Media Termination Point Required check box is checked), SIP Trunk will negotiate DTMF to RFC 2833. • RFC 2833—Select this configuration if the preferred DTMF method to be used across the trunk is RFC 2833. Cisco Unified Communications Manager makes every effort to negotiate RFC 2833 regardless of MTP usage. Out-of-band provides the fallback method if the peer endpoint supports it. • OOB and RFC 2833—Select this configuration if both out-of-band and RFC 2833 should be used for DTMF. If the peer endpoint supports both out-of-band and RFC 2833, Cisco Unified Communications Manager will negotiate both out-of-band and RFC 2833 DTMF methods. As a result, two DTMF events are sent for the same DTMF keypress (one out-of-band and the other RFC 2833).

Note You can provision SIP Trunk infrastructure Configuration Products in Session Management Edition (SME) devices if you add the SME device as a Call Processor in Provisioning.

SIP Profile Infrastructure Configuration Product Fields

Table 50: SIP Profile Infrastructure Configuration Product Fields

Field	Description
Name	Name of the SIP profile.
Description	Description of the SIP profile.

Field	Description
Default MTP Telephony Event Payload Type	Specifies the default payload type for RFC2833 telephony event.
Resource Priority Namespace List	Select a configured Resource Priority Namespace Network Domain list.
Early Offer for G Clear Calls	It supports both standards-based G.Clear (Clearmode) and proprietary Cisco Session Description Protocols (SDP).
SDP Session-level Bandwidth Modifier	Bandwidth needed when all the media streams are used. There are three Session Level Bandwidth Modifiers: Transport Independent Application Specific (TIAS), Application Specific (AS), and Conference Total (CT). Select one of the following options to specify which Session Level Bandwidth Modifier to include in the SDP portion of SIP Early Offer or Reinvite requests. • TIAS and AS • TIAS only • AS only • CT only Supported only for Cisco Unified Communications Manager 8.6.2 and above.

Field	Description
User-Agent and Server header information	This feature indicates how Cisco Unified Communications Manager handles the User-Agent and Server header information in a SIP message. Choose one of the following three options: • Send Unified CM Version Information as User-Agent Header—For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Cisco Unified Communications Manager passes through any contact headers untouched. This is the default behavior. • Pass Through Received Information as Contact Header Parameters —If this option is selected, the User-Agent or Server header information is passed as Contact header parameters. The User-Agent or Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent or Server headers. • Pass Through Received Information as User-Agent and Server Header—If this option is selected, the User-Agent or Server header information is passed as User-Agent or Server headers. The User-Agent or Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent or Server headers. Supported only for Cisco Unified Communications Manager 8.6.2 and above.
Accept Audio Codec Perferences in Received Offer	Select On to enable Cisco Unified Communications Manager to honor the preference of audio codecs in received offer and preserve it while processing. Select Off to enable Cisco Unified Communications Manager to ignore the preference of audio codecs in received offer and apply the locally configured Audio Codec Preference List. The default will select the service parameter configuration.

Field	Description
Dial String Interpretation	Cisco Unified Communications Manager uses the Dial String Interpretation policy to determine if the SIP identity header is a directory number or directory URI. Because directory numbers and directory URIs are saved in different database lookup tables, Cisco Unified Communications Manager examines the characters in the SIP identity header's user portion, which is the portion of the SIP address that is before the @ sign (for example, user@IP address or user@domain). To configure the Dial String Interpretation, choose one of the following options from the drop-down list box: • Always treat all dial strings as URI addresses—Cisco Unified Communications Manager treats the address of incoming calls as if they were URI addresses. • Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI. • Phone number consists of characters 0-9, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI. **Note** If the user=phone tag is present in the Request URI, Cisco Unified Communications Manager always treats the dial string as a number regardless of what option you choose for the Dial String Interpretation field.

Field	Description
Redirect by Application	Check this check box to configure this SIP Profile on the SIP trunk, which allows the Cisco Unified Communications Manager administrator to: • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the call is routed correctly. • Prevent DOS attack by limiting the number of redirections (recursive redirections) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place.
Disable Early Media on 180	Check this check box to play local ringback on the calling phone and connect the media upon receipt of the 2000K response.
Outgoing T.38 INVITE include audio mline	Allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, you must configure a SIP trunk with this SIP profile.
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media.
Assured Services SIP conformance	This checkbox should be checked for third-party AS-SIP endpoints as well as AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.
MLPP User Authorization	Check this box to enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password.
Timer Invite Expires	The time, in seconds, after which a SIP Invite expires.
Timer Register Delta	Specifies the parameter is in conjunction with the Timer Register Expires setting. The phone re-reregisters Timer Register Delta seconds before the registration period ends. The registration period is determined by the value of the SIP Station KeepAlive Interval service parameter.

Field	Description
Timer Register Expires	The value that the phone that is running SIP sends in the Expires header of the Register message. Valid values include any positive number; however, 3600 (1 hour) is the default value. In the 2000K response to Register message, Cisco Unified Communications Manager will include an Expires header with the configured value of the SIP Station KeepAlive Interval service parameter. This value in the 2000K determines the time, in seconds, after which the registration expires. The phone refreshes the registration Timer Register Delta seconds before the end of this interval.
Timer T1	The lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number.
Timer T2	The highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number.
Retry INVITE	The maximum number of times that an Invite request will be transmitted. Valid values include any positive number.
Retry Non-INVITE	The maximum number of times that an Invite request will be retransmitted. Valid values include any positive number.
Start Media Port	The start real-time protocol (RTP) port for media. The ranges is from 16384 to 32767.
Stop Media Port	The stop real-time protocol (RTP) port for media. The ranges is from 16384 to 32767.
Call Pickup URL	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call pickup feature.
Call Pickup Group Other URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call pickup group other feature.
Call Pickup Group URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call pickup group feature.

Field	Description
Meet Me Service URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the meet me conference feature.
User Info	Configures the user = parameter in the Register message.
DTMF DB Level	Specifies in-band DTMF digit tone level.
Call Hold Ring Back	Allows the system to ring to let you know that you still have another party on hold.
Anonymous Call Block	Configures anonymous call block.
Caller ID Blocking	Configures the caller ID blocking.
Do No Disturb Control	Enables the Do Not Disturb feature.
Telnet Level for 7940 and 7960	Controls the telnet level configuration parameter for phones that support Telnet.
Timer Keep Alive Expires	Specifies the interval between keepalive messages that are sent to the backup Cisco Unified Communications Manager to ensure that it is available in the event that a failover is required.
Timer Subscribe Expires	Specifies the time, in seconds, after which a subscription expires. This value is inserted into the Expires header field.
Timer Subscribe Delta	Resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires.
Maximum Redirections	Specifies the maximum number of times that the phone will allow a call to be redirected before dropping the call.
Off Hook To First Digit Timer	Specifies the time, in microseconds, that passes when the phone goes off hook and the first digit timer is set. The range is from 0 - 150,000 microseconds.
Call Forward URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the call forward feature.
Abbreviated Dial URI	Specifies a unique address that the phone that is running SIP will send to Cisco Unified Communications Manager to invoke the abbreviated dial feature.

Field	Description
Conference Join Enabled	Specifies whether the Cisco Unified IP Phones 7940 or 7960, when the conference initiator that is using that phone hangs up, should attempt to join the remaining conference attendees.
RFC 2543 Hold	Specifies whether to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Cisco Unified Communications Manager. This allows backward compatibility with endpoints that do not support RFC3264.
Semi Attended Transfer	Specifies whether the Cisco Unified IP Phones 7940 or 7960 caller can transfer the second leg of an attended transfer while the call is ringing. Check the check box if you want semi attended transfer enabled; leave it unchecked if you want semi attended transfer disabled.
Enable VAD	Specifies whether you want voice activation detection (VAD) enabled; leave it unchecked if you want VAD disabled. When VAD is enabled, no media are transmitted when voice is detected.
Stutter Message Waiting	Specifies whether you want stutter dial tone when the phone goes off hook and a message is waiting; leave unchecked if you do not want a stutter dial tone when a message is waiting.
Incoming Requests FROM URI Settings	
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: • 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 55000 = Fixed calling line ID, where 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 also enter the international escape character +.
Caller Name	Enter a caller name to override the caller name that is received from the originating SIP Device.
Trunk Specific Configuration	

Field	Description
Reroute Incoming Request to new Trunk based on	Specifies the method that Cisco Unified Communications Manager uses to identify the SIP trunk where the call is rerouted.
RSVP Over SIP	Specifies the method that Cisco Unified Communications Manager uses to configure RSVP over SIP trunks.
Fall back to local RSVP	Allows failed end-to-end RSVP calls to fall back to local RSVP to establish the call.
SIP Rel1XX Options	Configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) are sent reliably to the remote SIP endpoint.
Video Call Traffic Class	Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list box, select one of the following three options • Immersive—High-definition immersive video. • Desktop—Standard desktop video. • Mixed—A mix of immersive and desktop video. Cisco Unified Communications Manager Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, Video Bandwidth or Immersive Bandwidth, depending on the type of call determined by the Video Call Traffic Class. Please refer to the Call Admission Control chapter of the Cisco Unified Communications Manager System Guide for more information.
Calling Line Identification Presentation	Select Strict From URI presentation Only to select the network provided identity. Select Strict Identity Headers presentation Only to select the user provided identity.

Field	Description
Deliver Conference Bridge Identifier	Check this check box for the SIP trunk to pass the b-number that identifies the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require that this field be enabled. Checking this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Enabling this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference. Supported only for Cisco Unified Communications Manager 8.5 and above.
Early Offer support for voice and video calls (insert MTP if needed)	Check this check box if you want to create a trunk that supports early offer. Supported only for Cisco Unified Communications Manager 8.5 and above.
Send send-receive SDP in mid-call Invite	Check this check box to prevent Cisco Unified Communications Manager from sending an Invite a=inactive SDP message during call hold or media break during supplementary services. Supported only for Cisco Unified Communications Manager 8.5 and above.
Allow Presentation Sharing using BFCP	If the box is checked, Cisco Unified Communications Manager is configured to allow supported SIP endpoints to use the Binary Floor Control Protocol to enable presentation sharing.
Allow iX Application	Check this check box to enable support for iX media channel.
Allow Passthrough of Configured Line Device Caller Information	Check this box to allow passthrough of configured line device caller information from the SIP trunk.
Reject Anonymous Incoming Calls	Check this box to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Check this box to reject anonymous outgoing calls.
SIP Options Ping	

Field	Description
Enable Options Ping to monitor destination status for Trunks with service type “None (Default)”	Check this check box if you want to enable the SIP Options feature. Supported only for Cisco Unified Communications Manager 8.5 and above.
Ping Interval for In-service and Partially In-service Trunks (seconds)	This field configures the time duration between SIP options requests when the remote peer is responding and the trunk is marked as In Service. Supported only for Cisco Unified Communications Manager 8.5 and above versions.
Ping Interval for Out-of-service SIP Trunks (seconds)	This field configures the time duration between SIP Options requests when the remote peer is not responding and the trunk is marked as Out of Service. Supported only for Cisco Unified Communications Manager 8.5 and above versions.
Ping Retry Timer (milliseconds)	This field specifies the maximum waiting time before retransmitting the Options request. Supported only for Cisco Unified Communications Manager 8.5 and above versions.
Ping Retry Count	This field specifies the number of times that Cisco Unified Communications Manager resends the Options request to the remote peer. Supported only for Cisco Unified Communications Manager 8.5 and above versions.

SIP Realm Infrastructure Configuration Product Fields

Table 51: SIP Realm Infrastructure Configuration Product Fields

Field	Description
Realm	Enter the domain name of the realm that connects to the SIP trunk.
User	Enter the username of the SIP user agent in this realm.
Digest Credentials	Enter the password that the Cisco Unified CM uses to respond to a challenge from this realm and user.

Softkey Template Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 52: Softkey Template Infrastructure Configuration Product Fields

Field	Description
Softkey Template Information	
Name	Enter a unique name to identify the softkey template.
Description	Enter a description that describes the use of the template.
Base SoftKey Template Name	Select the base SoftKey template name from the drop-down list.
Is Default SoftKey Template	Check the **Is Default Softkey Template** check box to designate this softkey template as the standard softkey template,

SRST Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 53: SRST Infrastructure Configuration Product Fields

Field	Description
SRST Reference Information	
Name	Enter a name in the SRST Reference Name field.
Port	Enter the port number for this SRST reference.
IP Address	Enter the IP address of the gateway for devices in a device pool to use as an SRST reference.
SIP Network/IP Address	Enter the IP address of the server that the phones that are running SIP will use when in SRST mode.
SIP Port	Enter the SIP port of the SRST gateway.
SRST Certificate Provider Port	This port monitors requests for the Certificate Provider service on the SRST-enabled gateway.
Is SRST Secure?	After you verify that the SRSTenabled gateway contains a self-signed certificate, check this check box.

Transfer Rule Infrastructure Configuration Product Fields

Table 54: Transfer Rule Infrastructure Configuration Product Fields

Field	Description
Tell Me Who the Call Is For	Check this check box to have Unity Connection say “call for ” or “call for ” when the user answers the phone. Use this setting when users share a phone or a user takes calls from more than one dialed extension. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.
If Extension is Busy	Indicate how Unity Connection handles calls when the phone is busy. You may want to use holding options sparingly, because calls on hold can tie up ports. • Send Callers to Voicemail—Unity Connection plays the busy greeting and allows the caller to leave a voice message. • Put Callers on Hold Without Asking—Unity Connection puts callers on hold. • Ask Callers to Hold—Unity Connection gives the caller the option of holding. These options are unavailable when Release to Switch is selected or when Transfer Calls To is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly.

Field	Description
Rings to Wait For	Select the number of times the extension rings before Unity Connection plays the user or handler greeting. Set this value to at least three to give users a chance to answer. Avoid setting to more than four, especially if the call may be transferred to another extension, where the caller might have to wait for another set of rings. This value should be at least two rings fewer than the phone system setting for forwarding calls. This option is unavailable when Transfer Incoming Calls is set to the Greeting option or when Release to Switch is selected. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly.
Ask Me If I Want to Take the Call	Check this check box to have Unity Connection ask users whether they want to take a call before transferring the call. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.
Transfer Rule Type	The name of the transfer rule.Select the Rule Name to go to the specific page for the transfer rule. • Alternate • Closed • Standard

Field	Description
Ask for Caller's Name	Check this check box to have Unity Connection prompt callers to say their names. When answering the phone, the user hears "Call from..." before Unity Connection transfers the call. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.
Call Handler	Name of the Call Handler for which Transfer Rules needs to be updated.
Extension	Enter an extension or URI to which the call is forwarded.
Play the Wait While I Transfer Your Call Prompt	Check this check box to have Unity Connection play “Wait while I transfer your call” to callers while performing the transfer. This option is unavailable when Transfer Incoming Calls is set to the Greeting option. Default setting: Check box checked.
Tell Me When the Call Is Connected	Check this check box to have Unity Connection say "transferring call" when the user answers the phone. This option is unavailable when Release to Switch is selected or when the Transfer Calls To setting is set to the Greeting option. **Note** Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly. Default setting: Check box not checked.

Field	Description
Status	Indicate whether the transfer option is enabled and for how long: • Disabled—The transfer option is not in effect. • Enabled With No End Date and Time(Enabled Always)—The transfer option is enabled until you disable it. • Enabled Until—Unity Connection performs the selected transfer option until the specified date and time arrives. Select Enabled Until, and then select the month, day, year, and time at which Unity Connection will automatically disable the transfer option. **Note** By design, the standard transfer rule cannot be disabled.
Time Expire	Select Enabled Until, and then select the month, day, year, and time at which Unity Connection will automatically disable the transfer option.

Transfer Calls	Select one of the following settings:
	• Greeting-When this option is selected, the call is transferred as follows:
	  • For user settings-to the user greeting, without ringing the user phone.
	  • For call handler settings-to the call handler greeting.
	• Extension or URI-Enter an extension or URI to which the call is forwarded.

Field	Description
Transfer Type	Select how Unity Connection transfers calls. Use this setting with caution and only if you understand its implications on the phone and voice messaging systems. • Release to Switch—Unity Connection puts the caller on hold, dials the extension, and releases the call to the phone system. When the line is busy or is not answered, the phone system—not Unity Connection—forwards the call to the user or handler greeting. This transfer type allows Unity Connection to process incoming calls more quickly. Use Release to Switch only when call forwarding is enabled on the phone system. • Supervise Transfer—Unity Connection acts as a receptionist, handling the transfer. If the line is busy or the call is not answered, Unity Connection—not the phone system—forwards the call to the user or handler greeting. You can use supervised transfer whether or not the phone system forwards calls. The Transfer Type option is unavailable when Transfer Incoming Calls is set to the My Personal Greeting option. Transfer options apply only to indirect calls; they do not apply when an unidentified caller or another user dials a user extension directly.

Translation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 55: Translation Pattern Infrastructure Configuration Product Fields

Field	Description
Pattern Definition	
Translation Pattern	Translation pattern, including numbers and wildcards.
Partition	Available route partitions.
Description	Optional description.
Numbering Plan	Numbering plan.
Route Filter	Optional route filter.

Field	Description
MLPP Precedence	Multilevel Precedence and Preemption (MLPP) precedence settings.
Resource Priority Namespace Network Domain	Configured Resource-Priority Namespace Network Domain.
Route Class	Route class setting for the translation pattern.
Use Originator's Calling Search Space	To use the originator's calling search space for routing a call.
External Call Control Profile	External call profile that you want to assign to the translation pattern.
Call Search Space	Available calling search spaces.
Block Enabled	Enables or disables block.
Provide Outside Dial Tone	For each translation pattern that you consider to be off network.
Urgent Priority	Interrupts interdigit timing when the system must route a call immediately.
Do Not Wait For Interdigit Timeout On Subsequent Hops	When the Urgent Priority check box is checked and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), the system does not start the interdigit timer after it matches any of the subsequent patterns.
Route Next Hop By Calling Party Number	Enables routing based on the calling party number, which is required for call screening based on caller ID information to work between clusters.
Release Cause	Dependent on the Block Enabled field. If a release cause is selected, then Block Enabled must be set to True.
Is an Emergency Service Number	Check this check box, if you are configuring an emergency service number. **Note** This setting is applicable only if the Emergency Location Service is enabled in the call manager.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Determines whether to use the calling party's external phone number mask.
Calling Party Transform Mask	Transformation mask value.

Field	Description
Prefix Digits (Outgoing Calls)	Prefix digits.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern.
Calling Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's name on the called party's phone display for this translation pattern.
Calling Party Number Type	The format for the number type in calling party directory numbers.
Calling Party Numbering Plan	The format for the numbering plan in calling party directory numbers.
Connected Party Transformations	
Connected Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this translation pattern.
Connected Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's name on the calling party's phone display for this translation pattern.
Called Party Transformations	
Discard Digits	The discard digits instructions that you want to be associated with this translation pattern.
Called Party Transform Mask	Transformation mask value.
Prefix Digits (Outgoing Calls)	Prefix digits.
Called Party Number Type	The format for the number type in called party directory numbers.
Called Party Numbering Plan	The format for the numbering plan in called party directory numbers.

Translation Pattern Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.2 and earlier

Table 56: Translation Pattern Infrastructure Configuration Product Fields

Field	Description
Translation Pattern	Translation pattern, including numbers and wildcards.
Route Partition	Available route partitions.
Description	Optional description.
Dial Plan	Numbering plan.
Route Filter	Optional route filter.
MLPP Precedence	Multilevel Precedence and Preemption (MLPP) precedence settings.
Call Search Space	Available calling search spaces.
Block Enabled	Enables or disables block.
Release Cause	Dependent on the Block Enabled field. If a release cause is selected, then Block Enabled must be set to True.
Is an Emergency Service Number	Check this check box, if you are configuring an emergency service number. **Note** This setting is applicable only if the Emergency Location Service is enabled in the call manager.
Use Calling Party's External Phone Number Mask	Determines whether or not to use the calling party's external phone number mask.
Calling Party Transform Mask	Transformation mask value.
Calling Party Prefix Digits (Outgoing Calls)	Prefix digits.
Calling Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern.
Calling Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the calling party's name on the called party's phone display for this translation pattern.

Field	Description
Connected Line ID Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this translation pattern.
Connected Name Presentation	Determines whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party's name on the calling party's phone display for this translation pattern.
Called Party Discard Digits	The discard digits instructions that you want to be associated with this translation pattern.
Called Party Transform Mask	Transformation mask value.

Unified Call Manager Group Infrastructure Configuration Product Fields

Table 57: Unified Call Manager Group Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Unified CMs	List of available Cisco Unified Communications Managers.
Auto-Registration Unified CM Group	Select Yes if you want this Cisco Unified Communications Manager group to be the default Cisco Unified Communications Manager group when auto-registration is enabled.

UC Service Infrastructure Configuration Product Fields

Table 58: UC Service Infrastructure Configuration Product Fields

Field	Description
Voicemail	
Product Type	Select a product type. Available options are Unity and Unity Connection. Default setting: Unity.
Name	Enter the name of the voicemail service. Ideally, the voicemail service name should be descriptive enough for you to instantly recognize it.

Field	Description
Description	(Optional) Enter a description that helps you to distinguish between voicemail services. You can change the description if required. Maximum characters: 100.
Hostname/IP Address	Enter the address of the voicemail service in one of the following forms: • Hostname • IP address • Fully qualified domain name (FQDN) This field value must exactly match the hostname, IP address, or FQDN of the associated voicemail service. If the hostname or IP address of the voicemail service changes, change this field value accordingly.
Port	Enter the port to connect with the voicemail service. Default port: 443 This field value must match the available port on the voicemail service. Change the port number only if it conflicts with other services.
Protocol	Select the protocol to route voicemail messages securely. Available options: HTTP, HTTPS We recommend that you use HTTPS as the voicemail transport protocol for Cisco Unity Connection servers. Only change to HTTP if your network configuration does not support HTTPS.
Conferencing	
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required.

Field	Description
Hostname/IP Address	Enter the address of the conferencing service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the conferencing service so that users can contact the service when they sign in to web conferences. Default Port: 80 Allowed Values: 1- 65535 **Note** Use port 80 for HTTP and port 443 for HTTPS communications. **Note** This value must match the available port on the conferencing service. Change the port number only if it conflicts with other services.

Field	Description
Protocol	Select the protocol to route web conference communications. Available Options: HTTP, HTTPS Default Setting: HTTP. Change this setting to suit your network configuration, IM and Presence settings and security needs as follows: HTTP— Selects Hypertext Transfer Protocol as the standard method for transferring data between the server, Cisco Jabber, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express server does not have SSL enabled. HTTPS— Selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server, Cisco Jabber, and the browser. Select this option if the Unified MeetingPlace or the Unified MeetingPlace Express server has SSL enabled.
Mailstore	
UC Service Type	Specifies the UC service type as Mailstore.
Product Type	Specifies the product type as Exchange.
Name	Enter the name of the mailstore service. Ideally the mailstore service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between mailstore services. You can change the description if required.

Field	Description
Hostname/IP Address	Enter the address of the mailstore service in one of the following forms: • Hostname • IP address • FQDN This field value must exactly match the hostname, IP address, or FQDN of the associated mailstore service. If the address of the mailstore service changes, change this field value accordingly. Cisco Unity creates subscriber mailboxes for message storage on the Microsoft Exchange server. **Note** Cisco Unity Connection usually provides a mailstore service, and hosts themailstore service on the same server.
Port	Specify the port number configured for the service. Default Port: 143 Allowed Values: 1 - 65535 **Note** For secure voice messaging with Cisco Unity Connection, use port 7993. **Note** This value must match the available port on the mailstore service. Change the port number only if it conflicts with other services.
Protocol	Select the corresponding protocol to use when Cisco Jabber clients contact this service. Available Options: TCP, SSL, TLS, UDP Default Setting: TCP, which is the most commonly used networkconfiguration. Change this setting to suit your deployment, Unified CM settings, and security needs. **Note** For secure voice messaging with Cisco Unity Connection, use TLS.
Directory	
Service Type	Specifies directory as the UC service type.

Field	Description
Product Type	Select a supported directory product type from this list that applies to your network configuration. Available Options: Directory, Enhanced Directory Default Setting: Directory
Name	Enter the name of the directory service. Ideally the directory service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only). Allowed values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required. Allowed values: All characters allowed except quotes ("), angle brackets (< >), backslash (\), ampersand (&), and percent (%).
Hostname/IP Address	Enter the address of the directory service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the directory service. Default Port: 389 Allowed Values: 1- 65535 This value must match the available port on the directory service. **Note** Change the port number only if it conflicts with other services.

Field	Description
Protocol	Select the protocol to route communications between the directory service and Cisco Jabber clients. Available Options: TCP, UDP, TLS Default Setting: TCP. This is the most commonly used network configuration. Change this setting to suit your network configuration, Unified CM settings, and security needs.
Connection Type	Specifies the directory server type to connect to Global Catalog server that is optimized for searching or a Domain Controller (or any server running an Ldap service) which may not be optimized for searching. This is a required field. Default: Global Catalog server
Use Secure Connection	Define whether to send credentials in clear text (default is not to send in clear text i.e. use a secure connection). This is a required field. Default: True
Use Wildcards	Use wildcards when doing number lookups. This is a required field. Default: False
Disable Secondary Number Lookups	Disables queries using home, mobile and other numbers. This is a required field. Default: False
Uri Prefix	Specify the Uri scheme name e.g. 'im:' or 'sip:' Maximum length: 32
Phone Number Masks	Allows a mask to be defined which can be used when doing resolution by telephone number. E.g. the mask +353|+(###) ## ## #### could be used to resolve numbers in the format +35311221234 to +(353) 11 22 1234. Multiple masks can be defined by using the '|' operator. For example: +353|+(###) ## ## ####|+44|+44 (##)## #####) ## ## #### could be used to resolve numbers in the format +35311221234 to +(353) 11 22 1234. Maximum length: 1024
IM and Presence	

Field	Description
Service Type	Specifies IM and Presence as the UC service type.
Product Type	Select a supported IM and Presence product type from this list that applies to your network configuration. Available options: Unified CM (IM and Presence), WebEx (IM and Presence) Default setting: Unified CM (IM and Presence)
Name	Enter the name of the IM and Presence service. Ideally the IM and Presence service name should be descriptive enough for you to recognize it instantly. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between IM and Presence services. You can change the description if required.
Hostname/IP Address	Enter the address of the IM and Presence service in one of the following forms: • Hostname • IP address • DNS SRV Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore(_). **Note** This field value must exactly match the host name, IP address, or DNS SRV of the associated IM and Presence service. If the address of the IM and Presence service changes, change this field value accordingly. Cisco recommends DNS SRV to help the client find the correct IM and Presence service for the user
Conferencing	
UC Service Type	Specifies conferencing as the UC service type.
Product Type	Select a product type that applies to your network configuration. Available Options: MeetingPlace Classic, MeetingPlace Express, WebEx

Field	Description
Name	Enter the name of the coferencing service. Ideally the service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required.
Hostname/IP Address	Enter the address of the conferencing service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly. Allowed values: Alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
Port	Enter the port for the conferencing service so that users can contact the service when they sign in to web conferences. Default Port: 80 Allowed Values: 1- 65535 **Note** Use port 80 for HTTP and port 443 for HTTPS communications. **Note** This value must match the available port on the conferencing service. Change the port number only if it conflicts with other services.

Field	Description
Protocol	Select the protocol to route web conference communications. Available Options: HTTP, HTTPS Default Setting: HTTP. Change this setting to suit your network configuration, IM and Presence settings and security needs as follows: HTTP— Selects Hypertext Transfer Protocol as the standard method for transferring data between the server, Cisco Jabber, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express server does not have SSL enabled. HTTPS— Selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server, Cisco Jabber, and the browser. Select this option if the Unified MeetingPlace or the Unified MeetingPlace Express server has SSL enabled.
CTI	
Service Type	Specifies CTI as the UC service type.
Product Type	Specifies CTI as the product type.
Name	Enter the name of the CTI service. Ideally the CTI service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).
Description	(Optional) Enter a description that helps you to distinguish between CTI services when you have more than one configured. You can change the description if required.

Field	Description
Hostname/IP Address	Enter the address of the CTI service in one of the following forms: • Hostname • IP address • FQDN This field must exactly match the, hostname, IP address, or FQDN of the associated CTI service. If the address of the CTI service changes, change this field value accordingly.
Port	Enter the port for the CTI service. Default port: 2748 Allowed ports: 1-65535 **Note** This value must match the available port on the CTI service. Change the port number only if it conflicts with other services.
Protocol	Specifies TCP as the default protocol.

Voice Region Infrastructure Configuration Product Fields

Table 59: Voice Region Infrastructure Configuration Product Fields

Field	Description
Name	Infrastructure Configuration Product name.
Audio Codec	Codec setting. For Cisco Unified Communications Manager higher versions (4.1 and above) , the Default Codec field is set to the option selected.

Voicemail Pilot Infrastructure Configuration Product Fields

Table 60: Voicemail Pilot Infrastructure Configuration Product Fields

Field	Description
Number	Voicemail pilot number.
Description	Optional description.

Field	Description
Calling Search Space	Available calling search spaces.
Is Default	Indicates whether this pilot number is the default Voice Mail Pilot for the system.

Voicemail Profile Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.5 and later

Table 61: Voicemail Profile Infrastructure Configuration Product Fields

Field	Description
Voice Mail Profile Name	Profile name.
Description	Optional description.
Voice mail Pilot	Available voicemail pilots.
Voice mail Box Mask	The mask that is used to format the voice mailbox number for autoregistered phones.
Is Default	Indicates whether this voicemail profile is the default for the system.

Voice Gateway Infrastructure Configuration Product Fields

Table 62: VG202, VG204, VG224, and VG350 Infrastructure Configuration Product Fields

Field	Description
Gateway Name	Name of the gateway.
Protocol	Protocol associated with the gateway.
MAC Address (Last 10 Characters)	MAC address of the selected device. Updating the MAC Address field will update all associated phones' MAC addresses. However, to update MAC addresses in the user records, you must perform a Domain synchronization.
Description	Description of the device.
Cisco Unified Communications Manager Group	The group of the Cisco Unified Communications Manager.
Module in Slot <Number>	Module that is in the slot number.
Subunit <Number>	Subunit's number.

Field	Description
Modem Passthrough	Enables or disables the modem passthrough.
Cisco Fax Relay	Enables and disables the Cisco fax relay.
T38 Fax Relay	Enables and disables the T-38 fax relay.
RTP Package Capability	Enables or disables RTP Package Capability.
MT Package Capability	Enables or disables MT Package Capability.
RES Package Capability	Enables or disables RES Package Capability.
PRE Package Capability	Enables or disables PRE Package Capability.
SST Package Capability	Enables or disables SST Package Capability.
RTP Unreachable OnOff	Enables or disables RTP unreachable timeout.
RTP Unreachable timeout (ms)	RTP unreachable timeout in milliseconds.
RTP Report Interval (secs)	RTP Report Interval in seconds.
Simple SDP	Enables or disables simple SDP.

VG450, VG310 and VG320 Infrastructure Configuration Product Fields

VG450, VG310 and VG320 infrastructure configuration product fields are almost similar to VG350. VG450, VG310 and VG320 infrastructure configuration products have the following additional fields that are not available in VG350:

Field	Description
Global ISDN Switch Type	Choose the ISDN switch type.
Switchback Timing	Choose the timing mechanism that is used to switch back to a primary Cisco Unified Communications Manager.
Switchback Uptime-Delay	Choose the delay, in minutes, that applies when delayed switchback is used. You must make an entry in this field if you chose “Delayed” in the Switchback Timing field.
Switchback Schedule	Specify the schedule, in hours and minutes, that applies when scheduled switchback is used. You must make an entry in this field if you chose “Scheduled” in the Switchback Timing field.
Type of DTMF Relay	Choose the type of DTMF (Dual-tone multifrequency) that you want to use.

For VG450, VG310 and VG320, Prime Collaboration Provisioning supports only FXS model cards for provisioning analog phones. Cisco Unified Communications Manager supports both FXS and BRI cards for VG310 and VG320. You cannot provision ISDN BRI phones using Prime Collaboration Provisioning.

For Cisco Prime Collaboration Release 12.6SU1 and later

VG450 supports MGCP protocol. You can select MGCP protocol in **Gateway Details** from the **Protocol** drop-down list. For MGCP, you need to provide the domain name instead of MAC address.

Application User Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 11.6 and later

Table 63: Application User Infrastructure Configuration Product Fields

Field	Description
Application User Information	
UserId	Enter a unique application user identification name.
Password	Enter alphanumeric or special characters for the application user password.
BLF Presence Group	Choose a Presence group for the application user.
Accept Presence Subscription	Configure this field with the Presence feature for presence authorization.
Accept Out-of-dialog REFER	Check this box to authorize the system Cisco Unified Communications Manager to accept Out-of-Dialog REFER requests that come from this SIP trunk application user.
Accept Unsolicited Notification	Check this box to authorize the system to accept unsolicited notifications that come from this SIP trunk application user.
Accept Replaces Header	Check this box to authorize Cisco Unified CM to accept header replacements in messages from this SIP trunk application user.
Device Information	
Associated Devices	Displays the list of devices that are associated with the application user. Click **Add**, to add a new controlled device. You can also edit and delete the associated devices. **Note** If a user has more than 50 associated devices, and Prime Collaboration Provisioning displays performance issues, restrict the number of associated devices to 50 per user by splitting the devices between multiple users.
CTI Controlled Device Profiles	This field lists the devices that are associated with the application user.

Field	Description
Associated Groups	Displays the groups to which the application user belongs. Click **Add**, to associate a group. You can also edit and delete the associated groups.

Port Group Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 64: Port Group Infrastructure Configuration Product Fields

Field	Description
Authentication Username	User name that Unity Connection uses to authenticate with the SIP server.
Call Process IP Address	IP Address for the Call Process.
Retry Interval After Successful Attempt	Wait time, in milliseconds, between MWI retries that occur after success is reported.
Delay between Requests	Minimum length of wait time, in milliseconds, between subsequent MWI requests.
Maximum Concurrent Requests	Maximum number of messaging waiting indicator (MWI) requests that are attempted at the same time so that a spike in MWI requests does not demand a large portion of Unity Connection resources.
Register with SIP Server	This is a checkbox. Check this check box so that Unity Connection registers with the SIP server.
SIP Transport Protocol	Lists the SIP transport protocols. Select the SIP transport protocol that Unity Connection uses .
Authenticate with SIP Server	This is a checkbox. Check this check box so that Unity Connection authenticates with the SIP server.
MWI On Extension	Extension specified in Cisco Unified CM Administration for turning MWIs on.
Enable Message Waiting Indicators	This is a checkbox that is checked by default. If checked, voice messaging ports in the port group are enabled to turn message waiting indicators (MWIs) on and off. If unchecked, turning message waiting indicators (MWIs) on and off is disabled for all voice messaging ports in the port group.
Display Name	Port Group Name.

Field	Description
SIP Contact Line Name	Voice messaging line name (or pilot number) that users use to contact Unity Connection and that further register with the SIP server.
Retries After Successful Attempt	Number of times an MWI request is retried after success is reported so that MWI success is assured.
Device Name Prefix	Prefix that Cisco Unified Communications Manager adds to the device name for voice ports. This prefix must match the prefix used by Cisco Unified CM.
Authentication Password	Password that Unity Connection uses to authenticate with the SIP server.
MWI Off Extension	Extension that you specified in Cisco Unified CM Administration for turning MWIs off.
Port Group Type	Type of the port group. Unity Connection creates the new port group based on the type that is selected from the list. The new port group has default settings as specified in the port group type.

Unified Communications Manager Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 65: Unified Communications Manager Server Infrastructure Configuration Product Fields

Field	Description
Password	The password used by the Expressway to access the Unified CM publisher. Range: 1 to 1024 characters.
Username	The username used by the Expressway to access the Unified CM publisher. The user must have the Standard AXL API Access role. Range: 1 to 1024 characters.
Unified CM publisher address	The FQDN or IP address of a Unified CM publisher. Range: 1 to 1024 characters.
CucmServer setting URL to Expressway Server	The Unified Communications Manager Server setting URL for the Expressway Server.

Field	Description
TLS verify mode	State of the TLS verify mode. If TLS verify mode is enabled, the Unified CM system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.

IMP Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 66: IMP Server Infrastructure Configuration Product Fields

Field	Description
IM and Presence Service database publisher node	The FQDN or IP address of the IM and Presence Service database publisher node.
Password	IP Address for the Call ProcessIP Address for the Call Process.
TLS verify mode	State of the TLS verify mode. If TLS verify mode is enabled, the IM and Presence Service node's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.
Username	The username used by the Expressway to access the IM and Presence publisher. The user must have the Standard AXL API Access role.
IMPServer setting URL to Expressway Server	The IMP Server setting URL for the Expressway Server.

DNS Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 67: DNS Infrastructure Configuration Product Fields

Field	Description
Domain name	The name to be appended to an unqualified host name before querying the DNS server. Used when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers. Can also be used along with the local System host name to identify references to this system in SIP messaging .
DNS requests port range	Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure.
DNS requests port range start	The lower source port in the range used for sending DNS queries. Requests choose a random port from this range. **Warning** Setting a small source port range increases your vulnerability to DNS spoofing attacks.
System host name	Defines the DNS hostname that this system is known by. The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit. **Note** This is not the fully-qualified domain name, just the host label portion.
DNS requests port range end	The upper source port in the range used for sending DNS queries. Requests choose a random port from this range. **Warning** Setting a small source port range increases your vulnerability to DNS spoofing attacks.
DNS setting URL to Expressway Server	The DNS setting URL for the Expressway Server.

DNS per Domain Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 68: DNS per Domain Server Infrastructure Configuration Product Fields

Field	Description
Address1	The Address 1 of the Domain Server.
Address2	The Address 2 of the Domain Server.
Address3	The Address 3 of the Domain Server.

Field	Description
Address4	The Address 4 of the Domain Server.
Address5	The Address 5 of the Domain Server.
DNSPerDomainServer setting URL to Expressway Server	The DNS per Domain Server setting URL for the Expressway Server.

DNS Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 69: DNS Server Infrastructure Configuration Product Fields

Field	Description
Address1	The Address 1 of the DNS Server.
Address2	The Address 2 of the DNS Server.
Address3	The Address 3 of the DNS Server.
Address4	The Address 4 of the DNS Server.
Address5	The Address 5 of the DNS Server.
DNSServer setting URL to Expressway Server	The DNS Server setting URL for the Expressway Server.

DNS Zone Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 70: DNS Zone Infrastructure Configuration Product Fields

Field	Description
Automatically respond to SIP searches	Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. • **Off:** a SIP OPTIONS message is sent to the zone. • **On:** Searches are responded to automatically, without being forwarded to the zone.

Field	Description
SIP UDP/IX filter mode	Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. • **On:** any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. • **Off:** INVITE requests are not modified.
SIP record route address type	Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway.
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including inter-worked calls) to and from this zone.
TLS verify inbound mapping	Switch Inbound TLS mapping On to map inbound TLS connections to this zone if the peer certificate contains the TLS verify subject name. If the received certificate does not contain the TLS verify subject name (as CN or SAN), then the connection is not mapped to this zone. Switch Inbound TLS mapping Off to prevent the Expressway from attempting to map inbound TLS connections to this zone.
Fallback transport protocol	Determines which transport type is used for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. RFC 3263 suggests that UDP should be used.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.
Modify DNS request	Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. This option is primarily intended for use with Cisco Spark Call Service. See www.cisco.com/go/hybrid-services.

Field	Description
Send empty INVITE for inter-worked calls	Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. • **On:** SIP INVITEs with no SDP are generated and sent to this neighbor. • **Off:** SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor.
Preloaded SIP routes support	Enable this zone to to process or reject SIP INVITE requests that contain Route header.
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified.
H323 Mode	Determines whether H.323 calls will be allowed to and from this zone.
Zone profile	Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.
SIP parameter preservation	Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. • **On:** preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. • **Off:** allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.
Name	Name of the zone.

Field	Description
SIP UDP/BFCP filter mode	Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. • **On:** any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled • **Off:** INVITE requests are not modified.
DnsZone setting URL to Expressway Server	The DNS Zone setting URL for the Expressway Server.
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or sub-zone. When there is a mismatch of settings i.e. • **On:** 'On' on one side and 'Off' on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. • **Off:**Off by default.
NewName	The new name of zone.
TLS verify subject name	The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).
Include address record	Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS records. • **On:** the Expressway will query for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones. • **Off:** the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

Field	Description
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
Domain to search for	Enter a FQDN to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected. • **On:** SIP requests sent out via this zone that are received again by this Expressway will be rejected. • **Off:** SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.

MRA Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 71: MRA Infrastructure Configuration Product Fields

Field	Description
SSODefaulted	Default SSO availablity.

Field	Description
Enabled	Enable or disable Mobile and Remote Access (MRA). MRA allows endpoints such as Cisco Jabber to have their registration, call control, messaging and provisioning services provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.
SSO	Controls SSO access.
IOSSafariPlugin	IOS Jabber client using safari plugin.
MRA setting URL to Expressway Server	The MRA setting URL for the Expressway Server.

Domain In Expressway Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 72: Domain In Expressway Infrastructure Configuration Product Fields

Field	Description
XMPP federation	Indicates that XMPP federated services will be provided for this local domain. **Note** If static routes for federated foreign domains are required, these are configured on Expressway-E.
IM and Presence Service	Instant messaging and presence services for this SIP domain are provided by Cisco Unified Communications Manager IM and Presence Service.
Domain setting URL to Expressway Server	The Domain setting URL to Expressway Server.
SIP registrations and provisioning on Unified CM	Endpoint registration, call control and provisioning for this SIP domain is serviced by Cisco Unified Communications Manager. The Expressway acts as a Cisco Unified Communications Manager gateway to provide secure firewall traversal and line-side support for Cisco Unified Communications Manager registrations.

Field	Description
Domain name	The name of the domain managed by this Expressway. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot).A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters
NewDomain name	The name of the new domain. You must configure which services are supported for this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is 100.example-name.com. Range: 1 to 1024 characters

NTP Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 73: NTP Server Infrastructure Configuration Product Fields

Field	Description
Address1	The Address 1 of the NTP Server.
Address2	The Address 2 of the NTP Server.
Address3	The Address 3 of the NTP Server.
Address4	The Address 4 of the NTP Server.
Address5	The Address 5 of the NTP Server.
NTPServer setting URL to Expressway Server	The NTP Server setting URL for the Expressway Server.

Neighbor Zone Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 74: Neighbor Zone Infrastructure Configuration Product Fields

Field	Description
Peer address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or host names are therefore not recommended. If the traversal server is a cluster of Expressway-Es, this is the FQDN of one of the peers in that cluster.
NewName	The new name of zone.
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. Best effort: use encryption if available, otherwise fall back to unencrypted media. ForceEncrypted (Force encrypted): all media must be encrypted. ForceunEncrypted (Force unencrypted): all media must be unencrypted.
Send empty INVITE for interworked calls	Determines whether the Expressway generates a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. • **On:** SIP INVITEs with no SDP are generated and sent to this neighbor. • **Off:** SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent to this neighbor.

Field	Description
SIP authentication trust mode	Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. On: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Expressway. Unauthenticated messages are challenged if the Authentication Policy is set to Check credentials. Off: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the Authentication Policy is set to Check credentials.
H.323 call signaling port	Specifies the port on the neighbor to be used for H.323 calls to and from this Expressway.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Zone profile	Determines how the zone's advanced settings are configured. Default: uses the factory default profile. Custom: allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.
Automatically respond to SIP searches	Determines what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. • **Off:** a SIP OPTIONS message is sent to the zone. • **On:** searches are responded to automatically, without being forwarded to the zone.
SIP poison mode	Determines whether SIP requests sent out to this zone will be poisoned such that if they are received by the local Expressway again they will be rejected.
Interworking SIP search strategy	Determines how the Expressway searches for SIP endpoints when interworking an H.323 call. • **Options:** the Expressway sends an OPTIONS request. • **Info:** the Expressway sends an INFO request.

Field	Description
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
Call signaling routed mode	Specifies how the Expressway handles the signaling for calls to and from this neighbor. Auto: signaling is taken as determined by the Call routed mode configuration. Always: signaling is always taken for calls to or from this neighbor, regardless of the Call routed mode configuration.
Transport	The transport protocol to use for SIP calls to and from the traversal client.
SIP Proxy-Require header strip list	A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified.
SIP encryption mode	Determines whether or not the Expressway allows encrypted SIP calls on this zone. • **Auto:** SIP calls are encrypted if a secure SIP transport (TLS) is used. • **Microsoft:** SIP calls are encrypted using MS-SRTP. • **Off:** SIP calls are never encrypted.
SIP UPDATE strip mode	Determines whether or not the Expressway strips the UPDATE method from the Allow header of all requests and responses received from, and sent to, this zone.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.

Field	Description
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
Automatically respond to H.323 searches	Determines what happens when the Expressway receives an H.323 search, destined for this zone. • **Off:** an LRQ message is sent to the zone. • **On:** searches are responded to automatically, without being forwarded to the zone.
Preloaded SIP routes support	Enable this zone to to process or reject SIP INVITE requests that contain Route header.
H323 Mode	Determines whether H.323 calls will be allowed to and from this zone.
Name	Name of the zone.
Neighborzone setting URL to Expressway Server	The Neighbor zone setting URL for the Expressway Server.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.
SIP multipart MIME strip mode	Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007.
SIP record route address type	Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway.
SIP REFER mode	Determines how SIP REFER requests are handled. Forward: SIP REFER requests are forwarded to the target. Terminate: SIP REFER requests are terminated by the Expressway.
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone. • **On:** allow Multistream. • **Off:** disallow Multistream.

Field	Description
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings. For example, On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off
SIP parameter preservation	Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed via this zone.
SIP UDP/IX filter mode	Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. • **On:** any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. • **Off:** INVITE requests are not modified.
Monitor peer status	Specifies whether the Expressway monitors the status of the zones peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive.
SIP UDP/BFCP filter mode	Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. • **On:** any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. • **Off:** INVITE requests are not modified.

Search Rule Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 75: Search Rule Infrastructure Configuration Product Fields

Field	Description
Source	The sources of the requests for which this rule applies. Any: locally registered devices, neighbor or traversal zones, and any non-registered devices. • **AllZones:** locally registered devices plus neighbor or traversal zones. • **LocalZone:** locally registered devices only. Named: a specific zone or subzone.
SearchRule setting URL to Expressway Server	Search Rule setting URL for the Expressway Server.
State	Indicates if the search rule is enabled or disabled. Disabled search rules are ignored.
Replace string	The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only.)
Pattern type	How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) • **Exact:** The entire string must exactly match the alias character for character. • **Prefix:** the string must appear at the beginning of the alias. • **Suffix:** the string must appear at the end of the alias. • **Regex:** the string is treated as a regular expression.
Protocol	The source protocol for which this rule applies.
On successful match	Specifies the ongoing search behavior if the alias matches all of the search rule's conditions. Continue: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. Stop: any remaining search rules with a lower priority are not applied, even if the endpoint identified by the alias is ultimately not found.
Description	A free-form description of the search rule.

Field	Description
Priority	The order in the search process that this rule is applied, when compared to the priority of the other search rules. All priority 1 search rules are applied first, followed by all priority 2 search rules, and so on.
NewRule name	The name of the SearchRule.
Pattern string	The pattern against which the alias is compared. (Applies to Alias pattern match mode only.) Note: if the pattern string is a Regex, you can refer to the regular expressions reference table in the online help.
Target	The zone name or policy service name to query if the alias matches the search rule.
Request must be authenticated	Specifies whether this search rule applies only to authenticated search requests.
SIP variant	Select which type of SIP messages this search rule will process. Choose MicrosoftAny if you want the search rule to route MicrosoftSIP and MicrosoftIMP. Choose Standard to ignore Microsoft types and route standards-compliant SIP, or choose Any to route all types.
Mode	The type of alias for which this search rule applies. • **AliasPatternMatch:** the alias must match the specified pattern type and string. • **AnyAlias:** any alias (providing it is not an IP address) is allowed. • **AnyIPAddress:** the alias must be an IP address.
Source Name	The specific source zone or subzone for which this rule applies. Choose from the Default Zone, Default Subzone or any other configured zone or subzone.
Pattern behavior	Determines whether the matched part of the alias is modified before being sent to the target zone or policy service. (Applies to Alias Pattern Match mode only.) • **Leave:** the alias is not modified. • **Strip:** the matching prefix or suffix is removed from the alias. • **Replace:** the matching part of the alias is substituted with the text in the replace string.
Rule name	The name of the SearchRule.

Time Zone Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 76: Time Zone Infrastructure Configuration Product Fields

Field	Description
TimeZone setting URL to Expressway Server	The Time Zone setting URL for the Expressway Server.
Time Zone	The Time Zone.

Transform Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 77: Transform Infrastructure Configuration Product Fields

Field	Description
Pattern string	The pattern against which the alias is compared.
Priority	Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform.
Description	A free-form description of the transform.
NewPriority	Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform.
State	Indicates if the transform is enabled or disabled. Disabled transforms are ignored.
Pattern behavior	How the alias is modified. Strip: removes the matching prefix or suffix from the alias. Replace: substitutes the matching part of the alias with the text in the replace string. • AddPrefix: Prepends the Additional text to the alias. • AddSuffix: Appends the Additional text to the alias.
Transform setting URL to Expressway Server	The Transform setting URL for the Expressway Server.

Field	Description
Pattern type	How the pattern string must match the alias for the transform to be applied. • **Exact:** the entire string must exactly match the alias character for character. • **Prefix:** the string must appear at the beginning of the alias. • **Suffix:** the string must appear at the end of the alias. • **Regex:** the string is treated as a regular expression.
Replace string	The text string to use in conjunction with the selected Pattern behavior.

Traversal Client Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 78: Traversal Client Infrastructure Configuration Product Fields

Field	Description
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings. That is, 'On' on one side and 'Off' on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone. • **On:** allow Multistream. • **Off:** disallow Multistream.

Field	Description
Peer address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Expressway-Es, this is the FQDN of one of the peers in that cluster.
Password	The Password used by the Expressway when connecting to the traversal server.
SIP parameter preservation	Determines whether the Expressways B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. • **On:** Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. • **Off:** Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.
NewName	The new name of zone.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected. • **On:** SIP requests sent out through this zone that are received again by this Expressway will be rejected. • **Off:** SIP requests sent out through this zone that are received by this Expressway again will be processed as normal.

Field	Description
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
TraversalClient setting URL to Expressway Server	The Traversal Client setting URL for the Expressway Server.
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
Username	The user name used by the Expressway when connecting to the traversal server.
H323 Protocol	Determines which of the two firewall traversal protocols will be used for H323 calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. will be used for H323 calls to and from the traversal client.
Retry interval	Specifies the interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. establish a connection to the traversal server should be retried.
Name	Name of the zone.
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified.
Transport	The transport protocol to use for SIP calls to and from the traversal client.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.

Field	Description
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Auto: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on endpoint requests. • **Best effort:** Use encryption if available, otherwise fall back to unencrypted media. • **ForceEncrypted (Force encrypted):** all media must be encrypted. • **ForceunEncrypted (Force unencrypted):** ForceunEncrypted (Force unencrypted): all media must be unencrypted
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.

Traversal Server Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 79: Traversal Server Infrastructure Configuration Product Fields

Field	Description
H.460.19 demultiplexing mode	Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client
TLS verify subject name	The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).
Name	Name of the zone.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected.

Field	Description
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.
Media encryption mode	Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone.
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off.
Transport	The transport protocol to use for SIP calls to and from the traversal client.
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
NewName	The new name of zone.
SIP parameter preservation	Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed through this zone.
H323 Protocol	Determines which of the two firewall traversal protocols will be used for H323 calls to and from the traversal client.
UDP retry count	Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway.
UDP keep alive interval	Set the frequency until which the UDP probe is sent to the Expressway.

Field	Description
UDP retry interval	Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway.
TLS verify mode	Controls X.509 certificate checking and mutual authenticationbetween this Expressway and the traversal client. If enabled, aTLS verify subject name must be specified.
Username	The user name used by the Expressway when connecting to the traversal server.
SIP Mode	Determines whether SIP calls will be allowed to and from this zone.
TCP Retry interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
H323 Port	Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this Expressway. If the traversal server is a Expressway-E, this must be the port number that has been configured on the Expressway-Es Traversal Server zone associated with this Expressway. Will be used for H323 calls to and from the traversal client.
TraversalServer setting URL to Expressway Server	The Traversal Server setting URL for the Expressway Server.
TCP retry count	Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway.
TCP keep alive interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
H323 Mode	Determines whether H.323 calls will be allowed to and from this zone.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.

XMPP Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 80: XMPP Infrastructure Configuration Product Fields

Field	Description
Privacy mode	Controls whether restrictions are applied to the set of federated domains.
Use static routes	Indicates whether a controlled list of static routes, rather than DNS lookup, are used to locate federation XMPP addresses.
XMPP federation support	Enable or disable support for XMPP federation.
Require client-side security certificates	Controls whether the certificate presented by the client is verified against Expressway's current trusted CA list and the revocation list if loaded.
Dialback secret	The dialback secret used for identity verification with federated XMPP servers.
XMPP setting URL to Expressway Server	The XMPP setting URL for the Expressway Server.
Security mode	Indicates if a TLS connection to servers is required, preferred, or not required.

Unified Communications Traversal Core Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 81: Unified Communications Traversal Core Infrastructure Configuration Product Fields

Field	Description
Username	The user name used by the Expressway when connecting to the traversal server.
Password	The Password used by the Expressway when connecting to the traversal server.
SIP parameter preservation	Determines whether the Expressways B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. • **On:** Preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. • **Off:** Allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.

Field	Description
UnifiedCommunications Traversal Core setting URL to Expressway Server	The Unified Communications Traversal Core setting URL for the Expressway Server.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone. • **On:** Allow Multistream. • **Off:** Disallow Multistream.
Peer Address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal servers certificate. IP addresses or hostnames are therefore not recommended. If the traversal server is a cluster of Expressway-Es, this is the FQDN of one of the peers in that cluster.
Name	Name of the zone.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.
NewName	The new name of zone.
Retry interval	Specifies the interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. establish a connection to the traversal server should be retried.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.

Field	Description
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected. • On: SIP requests sent out through this zone that are received again by this Expressway will be rejected. • Off: SIP requests sent out through this zone that are received by this Expressway again will be processed as normal.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.

Unified Communications Traversal Edge Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 82: Unified Communications Traversal Edge Infrastructure Configuration Product Fields

Field	Description
TCP retry interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
SIP Port	The port on the neighbor to use for outgoing SIP messages initiated from the Expressway. Default: 5061, Range: 1024 to 65534.
Username	The user name used by the Expressway when connecting to the traversal server.

Field	Description
TCP keep alive interval	Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway.
TLS verify subject name	The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).
Multistream mode	Controls if the Expressway allows Multistream to and from devices in this zone.
UDP retry count	Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway.
Authentication policy	Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected.
UnifiedCommunications Traversal Edge setting URL to Expressway Server	The Unified Communications Traversal Edge setting URL for the Expressway Server.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.
ICE support	Controls how the Expressway supports ICE messages to and from the devices in this zone. The behavior depends upon the configuration of the ICE support setting on the incoming (ingress) and outgoing (egress) zone or subzone. When there is a mismatch of settings i.e. On on one side and Off on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host. When ICE support is enabled, you can also configure the TURN servers to offer as ICE candidates, if necessary. Default: Off.
Preloaded SIP routes support	Enable this zone to process or reject SIP INVITE requests that contain Route header.
SIP poison mode	Determines whether SIP requests sent out to this zone are poisoned such that if they are received by the local Expressway again they will be rejected.
UDP retry interval	Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway.
UDP keep alive interval	Set the frequency until which the UDP probe is sent to the Expressway.

Field	Description
Hop count	Specifies the hop count to be used when sending an alias search request to this zone. **Note** If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
Name	Name of the zone.
NewName	The new name of zone.
SIP parameter preservation	Determines whether B2BUA in this node preserves or rewrites the parameters in SIP requests routed through this zone.
TCP retry count	Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway.

Restart Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 83: Restart Infrastructure Configuration Product Fields

Field	Description
Restarting the Expressway Server	Restarting the Expressway Server.
Message	Message on restarting the Server.

Credential Infrastructure Configuration Product Fields

For Cisco Prime Collaboration Release 12.1 and later.

Table 84: Credential Infrastructure Configuration Product Fields

Field	Description
Credential setting URL to Expressway Server	The Credential setting URL for the Expressway Server.
NewName	Change the existing credential name to another name.
Password	The password required for this entry in the local authentication database.The maximum plaintext length is 128 characters, which will then be encrypted.
Name	The name required for entry in the local authentication database.