Common Device Setup

This chapter provides information to configure common device configurations.

About Common Device Setup

In Cisco Unified Communications Manager Administration, use the**Device** > **Device Settings** > **Common Device Configuration** menu path to configure common device configurations.

A common device configuration comprises user-specific service and feature attributes. Ensure that each device is associated with a common device configuration for user-oriented information.

Note The Device Pool window now contains only location-related information. The Common Device Configuration window records all the user-oriented information.

Common Device Setup Deletion

You cannot delete a common device configuration that a device uses. To find out which devices are using the common device configuration, click the Dependency Records link from the Common Device Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a common device configuration that is in use, Cisco Unified Communications Manager displays a message. Before deleting a common device configuration that is currently in use, you must perform either or both of the following tasks:

- Assign a different common device configuration to any devices that are using the common device configuration that you want to delete.
- Delete the devices that are using the common device configuration that you want to delete.

Common Device Settings

The following table describes the common device settings.

Table 1: Common Device Settings

Field	Description
Common Device Configuration Information	
Name	Enter a name to identify the common device configuration.
Softkey Template	From the drop-down list box, choose the softkey template for the common device configuration.
User Hold MOH Audio Source	Choose the audio source to use for MOH when a user initiates a hold action.
Network Hold MOH Audio Source	Choose the audio source to use for music on hold (MOH) when the network initiates a hold action.
User Locale	From the drop-down list box, choose the locale for the common device configuration. The user locale identifies a set of detailed information to support users, including language and font. **Note** If the user does not choose a user locale, the locale that is specified in the Cisco Unified Communications Manager clusterwide parameters as Default User Locale applies.

Field	Description
IP Addressing Mode	Choose the version of IP address that the device (SIP trunk or phone that runs SCCP) uses to connect to Cisco Unified Communications Manager. From the drop-down list box, choose one of the following options: • IPv4 Only—For both media and signaling events, the device uses an IPv4 address to connect to Cisco Unified Communications Manager. If an IPv4 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv6 address. If you choose this option, the SIP trunk uses an IPv4 address to connect to the peer device. • IPv6 Only—For both media and signaling events, the device uses an IPv6 address to connect to Cisco Unified Communications Manager. If an IPv6 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv4 address. If you choose this option, the SIP trunk uses an IPv6 address to connect to the peer device. • IPv4 and IPv6 (Default)—Choose this option for dual-stack devices, which can have both an IPv4 and IPv6 address. For both media and signaling events, the dual-stack device uses either an IPv4 or an IPv6 address to connect to Cisco Unified Communications Manager. If only an IPv4 or IPv6 is available for a device (not both types of IP addresses), the device uses the available IP address to negotiate the call. If the device has both IP address types for both signaling and media events, Cisco Unified Communications Manager uses the configuration for IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.

Field	Description
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 Cisco Unified Communications Manager during a signaling event. For dual-stack SIP trunks, choose the version of IP address that the SIP trunk uses to connect to the peer device for signaling events. From the drop-down list box, choose one of the following options: • IPv4—The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event. • IPv6—The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event. • Use System Default—The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies.

Field	Description
Allow Auto-Configuration for Phones	This drop-down list box supports IPv6 for Cisco Unified IP Phones that run SCCP. From the drop-down list box, choose one of the following options: • On—Depending on how the M bit is set via 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 Cisco Unified Communications Manager. You can manually configure the TFTP server address via the interface on the phone, or you can obtain it from a DHCPv6 server. **Tip** To indicate to the phone that it needs to use the DHCPv6 server to obtain other information, ensure that the O bit is set via stateless address autoconfiguration on the router. • 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. Although Cisco Unified Communications Manager does not use this configuration, the TFTP file that the phone obtains includes this information.
Allow Duplicate Address Detection	This drop-down list box supports an IPv6 parameter for Cisco IP Phones. From the drop-down list box, choose one of the following options: • 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.

Field	Description
Accept Redirect Messages	This drop-down list box supports an IPv6 parameter for Cisco IP Phones. From the drop-down list box, choose one of the following options: • 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.
Reply Multicast Echo Request	This drop-down list box supports an IPv6 parameter for Cisco IP Phones. From the drop-down list box, choose one of the following options: • 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.
Use Trusted Relay Point	From the drop-down list box, 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.

Field	Description
Use Intercompany Media Engine (IME) for Outbound Calls	Check this check box to enable the devices that associate with this common device configuration to use a trusted relay point. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager inserts a TRP for an endpoint if the Use Trusted Relay Point check box is checked for the endpoint or for the common device configuration with which the endpoint associates. The endpoint device can comprise any device that terminates media, including SIP, H.323, MGCP, and SCCP devices, such as phones that are running SCCP, CTI devices, MoH servers, annunciators, and conference bridges. If the Use Trusted Relay Point setting of a device specifies On or Off, the device setting overrides the Use Trusted Relay Point setting from the common device configuration with which the device associates. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP.
Multilevel Precedence and Preemption Information	

Field	Description
MLPP Indication	This setting specifies whether devices that are capable of playing precedence tones will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices from the following options: • Default—Devices inherit MLPP Indication settings from the MLPP Indication Status enterprise parameter. • Off—Devices do not handle nor process indication of an MLPP precedence call. • On—Devices do handle and process indication of an MLPP precedence call. **Note** Do not configure the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. **Note** Turning on MLPP Indication (at the enterprise parameter or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
MLPP Preemption	This setting specifies whether devices that are capable of preempting calls in progress will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices from the following options: • Default—Devices inherit MLPP Preemption settings from the MLPP Preemption Setting enterprise parameter. • Disabled—Devices do not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—Devices allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

Field	Description
Confidential Access Level	Select the appropriate CAL value from the drop-down list box.

Synchronize Common Device Settings with Devices

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

Procedure

Step 1 Choose **Device** > **Device Settings** > **Common Device Configuration**.

The Find and List Common Device Configurations window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.

The window displays a list of common device configurations that match the search criteria.

Step 4 Click the common device configuration to which you want to synchronize applicable devices. The Common Device Configuration Information window displays.

Step 5 Make any additional configuration changes.

Step 6 Click Save.

Step 7 Click Apply Config.

The Apply Configuration Information dialog displays.

Step 8 Click OK.