Configure Cisco IP Phones

- Cisco IP Phones Overview, on page 1
- Cisco IP Phones Configuration Task Flow, on page 1

Cisco IP Phones Overview

Cisco IP Phones are full-featured telephones that provide voice communication over an IP network. To provide this capability, the IP phones interact with several other key Cisco Unified IP Telephony and network components, such as Unified Communications Manager, DNS and DHCP servers, TFTP servers, media resources, Cisco Power over Ethernet (PoE), and others. These IP phones function much like digital business phones that allow you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because Cisco IP Phones connect to your data network, they offer enhanced IP telephony features, such as access to network information and services and customizable features and services. The phones also support security features that include file authentication, device authentication, signaling encryption, and media encryption.

This chapter describes how to configure a phone to make it operational on your system. To configure features such as Call Park, Call Forward, Busy Lamp Field (BLF), Call Pickup, and Speed Dial, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Cisco IP Phones Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Phones, on page 3	Perform this task to configure a SIP or an SCCP Phone.
Step 2	Configure EnergyWise, on page 7	To reduce power consumption, configure the phone to power down (sleep) and power up (wake) automatically.

	Command or Action	**Purpose**
Step 3	Configure a Client Services Framework Device, on page 9	Perform this procedure to configure a Client Services Framework device. A Client Services Framework device can be any of the following: • Cisco Unified Communications Integration for Microsoft Office Communicator • Cisco Unified Communications Integration for Webex Connect • Cisco Unified Personal Communicator (Release 8.0 and later)
Step 4	Configure a CTI Remote Device, on page 11	Perform this procedure to configure a CTI Remote Device. A CTI remote device is a device type that represents off-cluster phones that users can use with Cisco UC applications. The device type is configured with one or more lines (directory numbers) and one or more remote destinations.
Step 5	Configure a Cisco Spark Remote Device, on page 17	Perform this procedure to configure a Cisco Webex remote device. A Cisco Webex remote device represents a Cisco Webex client that users can use with Cisco UC applications. The device type supports multiple active calls to the configured remote destination. A Cisco Spark remote device requires an enhanced license, except in the following scenario: • When the Owner User ID for the Cisco Spark remote device is also assigned an IP Phone or Jabber client, a single enhanced license is used for both devices. • When the Owner User ID for the Cisco Spark remote device is also assigned a TelePresence device, a single TelePresence license is used for both devices. **Caution** The Cisco Spark remote device is supported only for connecting your on-premises environment to Cisco cloud services. Use of this remote device for any other purpose is not supported.
Step 6	Migrate Phone Data, on page 21	Perform this procedure if you are migrating from one phone to another and you do not need to use the old phone anymore.

Configure Phones

Procedure

	Command or Action	Purpose
Step 1	To configure SIP phones, perform the following procedures: • Configure SIP Phone Secure Port, on page 4 • Restart Services, on page 4 • Configure SIP Profile, on page 4 • Configure Phone Security Profile • Configure a Phone, on page 6 • Configure Cisco IP Phone Services, on page 7 • Configure a VPN client.	Perform these procedures if you have phones that use Session Initiation Protocol (SIP). SIP provides the primary interface between the phone and other network components. In addition to SIP, other protocols are used for various functions such as DHCP for IP address assignment, DNS for domain name to address resolution, and TFTP for downloading image and configuration data. For detailed steps about configuring a VPN client, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
Step 2	To configure SCCP Phones, perform the following procedures: • Configure Phone Security Profile • Configure a Phone, on page 6 • Configure Cisco IP Phone Services, on page 7 • Configure a VPN client	Perform these procedures if you want to configure Cisco IP Phones that use the Skinny Client Control Protocol (SCCP). SCCP uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified Communications Manager. SCCP easily coexists in a multiple protocol environment. During registration, a Cisco Unified IP Phone receives its line and all other configurations from Cisco Unified Communications Manager. For detailed steps about configuring a VPN client, see the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

What to do next

Provide power, verify network connectivity, and configure network settings for the Cisco Unified IP Phone. For more information about configuring network settings, see the *Cisco Unified IP Phone Administration Guide* for your Cisco Unified IP Phone model.

Configure SIP Phone Secure Port

Follow these steps to configure the SIP Phone Secure Port. Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.

Procedure

Step 1	From Cisco Unified CM Administration, choose **System** > **Cisco Unified CM**.
Step 2	In the **Cisco Unified Communications Manager TCP Port Settings for this Server** section, specify a port number in the **SIP Phone Secure Port** field, or leave the field set to default. The default value is 5061.
Step 3	Click **Save**.
Step 4	Click **Apply Config**.
Step 5	Click **Ok**.

Restart Services

Follow these steps to restart Cisco CallManager and Cisco CTL Provider services.

Procedure

Step 1	From the Cisco Unified Serviceability interface, choose **Tools** > **Control Center - Feature Services**.
Step 2	Choose the Cisco Unified Communications Manager server from the **Servers** drop-down list. In the CM Services area, Cisco CallManager displays in the **Service Name** column.
Step 3	Click the radio button that corresponds to the Cisco CallManager service.
Step 4	Click **Restart**. The service restarts and displays the message, `Service Successfully Restarted`.
Step 5	Repeat step 3 and step 4 to restart Cisco CTL Provider service.

Configure SIP Profile

Use this procedure to configure SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks.

Before you begin

Procedure

Step 1	In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.
Step 2	Click **Find**.

Step 3	For the profile that you want to copy, click the file icon in the **Copy** column.
Step 4	Enter the name and description of the new profile.
Step 5	If you have the IPv6 stack configured and you are deploying two stacks, check the **Enable ANAT** check box.

> **Note** This configuration applies whether you have Unity Connection deployed or not.

Step 6	Click **Save**.

What to do next

Configure Phone Security Profile

Configure Phone Security Profile

If you want to enable security features like TLS signaling, CAPF, and digest authentication requirements for the endpoints, you must configure a new security profile that you can apply it to the endpoints.

> **Note** By default, if you don't apply a SIP phone security profile to a provisioned device, the device uses a nonsecure profile.

Procedure

Step 1	From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.
Step 2	Click **Add New**.
Step 3	From the **Phone Security Profile Type** drop-down list, choose the Universal Device Template to create a profile that you can use when provisioning through the device templates.

> **Note** Optionally, you can also create security profiles for specific device models.

Step 4	Select the protocol.
Step 5	Enter an appropriate name for the profile in the **Name** field.
Step 6	If you want to use TLS signaling to connect to the device, set the **Device Security Mode** to **Authenticated** or **Encrypted** and the Transport Type to **TLS**.
Step 7	(Optional) Check the **Enable OAuth Authentication** check box if you want the phone to use digest authentication.
Step 8	(Optional) Check the **TFTP Encrypted Config** check box if you want to use encrypted TFTP.
Step 9	Complete the remaining fields in the Phone Security Profile Configuration window. For help with the fields and their settings, see the online help.
Step 10	Click **Save**.

Configure a Phone

Perform these steps to manually add the phone to the Cisco Unified Communications Manager database. You do not have to perform these steps if you are using autoregistration. If you opt for autoregistration, Cisco Unified Communications Manager automatically adds the phone and assigns the directory number. For more information about enabling autoregistration, see Configure Autoregistration Task Flow.

Before you begin

- Configure Phone NTP References
- Configure Phone Security Profile
- Add a Date/Time Group
- Set Up SIP Dial Rule (when configuring a SIP phone)

Procedure

Step 1	From Cisco Unified CM Administration, choose **Device** > **Phone**.
Step 2	Click **Add New**.
Step 3	From the **Phone Type** drop-down list, select the appropriate Cisco IP Phone model.
Step 4	Click **Next**.
Step 5	From the **Select the device protocol** drop-down list, choose one of the following: • **SCCP** • **SIP**
Step 6	Click **Next**.
Step 7	Configure the fields in the **Phone Configuration** window. See the online help for more information about the fields and their configuration options. **Note** The CAPF settings that are configured in the security profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacturer-installed certificates (MICs) or locally significant certificates (LSC). See the Cisco Unified Communications Manager Security Guide for more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings.
Step 8	Click **Save**.
Step 9	In the **Association** area, click **Line [1] - Add a new DN**.
Step 10	In the **Directory Number** field, enter the directory number that you want to associate with the phone.
Step 11	Click **Save**.

What to do next

For SIP or SCCP phones:

Configure Cisco IP Phone Services, on page 7

Configure Cisco IP Phone Services

Configure services for Cisco IP Phones if you want to provide phone services such as a company directory, visual voicemail, or weather forecasts to the Cisco IP Phones. Cisco provides certain default IP phone services, which install automatically with Cisco Unified Communications Manager. You can also create customized Cisco IP Phone services for your site. Follow these steps to configure the customized services in Unified Communications Manager.

Before you begin

Procedure

Step 1   From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2   Click **Add New**.

Step 3   Configure the fields in the **IP Phone Services Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4   Click **Save**.

What to do next

- Add services to the phones in the database if they are not classified as enterprise subscriptions. You can add services to the phones using Bulk Administration Tool (BAT) or Cisco Unified Communications Self Care Portal. For more information, see *Cisco Unified Communications Manager Bulk Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html and *Cisco Unified Communications Self Care Portal User Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html.

- You can assign the services to the phone buttons, if the phone model supports these buttons. For more information about assigning services, see Cisco IP Phone User Guide for your phone model.

- Configure VPN Client (optional).

Configure EnergyWise

Before you begin

- Ensure that your system includes an EnergyWise controller. For example, a Cisco Switch with the EnergyWise feature enabled.

- See the user documentation for your phone model to check whether your phone model supports the EnergyWise feature.

Procedure

Step 1	From Cisco Unified CM Administration, choose **Device** > **Phone**.
Step 2	Specify the search criteria and click **Find**. A list of phones that are configured on the Cisco Unified Communications Manager is displayed.
Step 3	Choose the phone for which you want to configure the EnergyWise feature.
Step 4	Configure the EnergyWise fields in the **Product Specific Configuration Layout** section. See the Related Topics section for more information about the fields and their configuration options.
Step 5	Click **Save**.

EnergyWise Configuration Fields

Table 1: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Select the day for which you want the phone to automatically power off. You can select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected.
Phone On Time	Enter the time in 24 hour format, where 00:00 is midnight. This value determines when the phone automatically powers on for the days selected in the **Enable Power Save Plus** field. **Note** To wake up the phone before the **Phone On Time**, you must power on the phone from the switch. For more information, see the switch documentation.
Phone Off Time	Enter the time in 24 hour format, where 00:00 is midnight. This value determines when the phone automatically powers down for the days selected in the **Enable Power Save Plus** field. If the **Phone On Time** and the **Phone Off Time** fields contain the same value, the phone does not power down.
Phone Off Idle Timeout	Specify the duration for which the phone must be idle before the phone powers down. You can specify any value from 20 minutes to 1440 minutes. The default value is 60 minutes.

Field	Description
Enable Audible Alert	Check this check box to instruct the phone to play an audible alert 10 minutes, 7 minutes, 4 minutes, and 30 seconds before the time specified in the **Phone Off Time** field. This check box applies only if the **Enable Power Save Plus** list box has one or more days selected.
EnergyWise Domain	Specify the EnergyWise domain that the phone is in. The maximum length allowed is 127 characters.
EnergyWise Secret	Specify the security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length allowed is 127 characters
Allow EnergyWise Overrides	Check this check box to disable Power Save Plus. If you check this check box, the EnergyWise domain controller policy overrides the **Power On Time** and **Power Off Time** values. **Note** Leaving the **Allow EnergyWise Overrides** check box checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.

Configure a Client Services Framework Device

Perform this procedure to configure a Client Services Framework device. A Client Services Framework device can be any of the following:

- Cisco Unified Communications Integration for Microsoft Office Communicator
- Cisco Unified Communications Integration for Webex Connect
- Cisco Unified Personal Communicator (Release 8.0 and later)

Procedure

	Command or Action	Purpose
Step 1	Add a Client Services Framework Device, on page 10	Add a device that uses the Client Services Framework.
Step 2	Associate Device with End User, on page 11	Associate an end user account to the Client Services Framework device.

Add a Client Services Framework Device

Procedure

Step 1	From Cisco Unified CM Administration, choose **Device** > **Phone**.
Step 2	Click **Add New**.
Step 3	From the **Phone Type** drop-down list, choose **Cisco Unified Client Services Framework**.
Step 4	Click **Next**.
Step 5	Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.
Step 6	Click **Save**.
Step 7	In the **Association** area, click **Line [1] - Add a new DN**.
Step 8	In the **Directory Number** field, enter the directory number that you want to associate with the client services framework device.
Step 9	Click **Save**.

Client Services Framework Device Configuration Fields

Table 2: Client Services Framework Device Configuration Fields

Field	Description
Device Name	Enter a name to identify the Client Services Framework device. The name can include up to 15 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). **Note** When you configure the device name for the Cisco Unified Personal Communicator, make sure that the name starts with UPC.
Description	Enter a brief description for the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Device Pool	Choose the device pool to which you want this device assigned.
Phone Button Template	Choose **Standard Client Services Framework**.
Owner User ID	Choose the user ID of the assigned Client Services Framework device user. The user ID is recorded in the call detail record (CDR) for all calls made from this device.

Field	Description
Device Security Profile	Choose **Cisco Unified Client Services Framework - Standard SIP Non-secure Profile**.
SIP Profile	Choose **Standard SIP Profile**.

Associate Device with End User

Use this procedure to associate an end user with the Client Services Framework Device.

Procedure

Step 1   From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2   Click **Find** and select the user whom you want to associate to the device.

Step 3   In the **Device Information** section, click **Device Association** .
The User Device Association window appears.

Step 4   Click **Find** to view a list of available devices.

Step 5   Select the device that you want to associate, and click **Save Selected/Changes**.

Step 6   From **Related Links**, choose **Back to User**, and click **Go**.
The **End User Configuration** window appears, and the associated device that you chose appears in the **Controlled Devices** pane.

Configure CTI Remote Device

Procedure

	Command or Action	**Purpose**
Step 1	Configure a CTI Remote Device, on page 11	Create a CTI Remote Device.
Step 2	Add a Directory Number to a Device, on page 15	To register a CTI Remote Device, you must add a Directory Number to that device.
Step 3	Configure a Remote Destination, on page 15	Configure the remote destinations that you want to associate with the CTI remote device.

Configure a CTI Remote Device

Procedure

Step 1   From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2   Click **Add New**.

Step 3   From the **Phone Type** drop down list, select CTI Remote Device and click **Next**.

Step 4   Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5   Click **Save**.

CTI Remote Device Configuration Fields

CTI Remote Device Information

Table 3: Device Information

Field	Description
Registration	Specifies the registration status of the CTI Remote Device.
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies if the device is trusted.
Active Remote Destination	Specifies if the remote destination which is active. The CTI client can specify one remote destination as 'active' at any one given time. Incoming calls and Dial via Office (DVO) calls are routed to the active remote destination.
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device.
Device Name	Specifies the name for the CTI Remote Device that is automatically populated based on the Owner User ID. The format of the device name is *CTIRD<OwnerUserID>* by default. This field is editable. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the CTI remote device. This field can contain up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Field	Description
Device Pool	Select the device pool which defines the common characteristics for CTI remote devices. For more information on how to configure the device pool, see Device Pool Configuration Settings.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Network Hold MOH Audio Source	From the drop-down list, choose the audio source to use for MOH when the network initiates a hold action.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.

Call Routing Information

Table 4: Inbound/Outbound Calls Information

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.

Table 5: Protocol Specific Information

Field	Description
Presence Group	Configure this field with the Presence feature.
	If you are not using this application user with presence, leave the default (None) setting for presence group.
	From the drop-down list, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user.
	From the drop-down list, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list.
	If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.
	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.
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting.
	The rerouting calling search space of the referrer is used to find the route to the refer-to target. When the Refer message fails due to the rerouting calling search space, the Refer Primitive rejects the request with the "405 Method Not Allowed" message.
	The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.

Table 6: Do Not Disturb Information

Field	Description
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device.
DND Option	When you enable DND on the phone, Call Reject 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.

Add a Directory Number to a Device

To register a CTI Remote Device, you must add a Directory Number to that device. You cannot register a CTI Remote Device without a Directory Number. You can add a maximum of five Directory Numbers to the CTI Remote Device.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Specify the filter criteria and click on the CTI Remote Device for which you want to associate the directory number.

Step 3 In the **Association** pane, click **Add a new DN** link.

Step 4 Configure the fields in the **Directory Number Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Configure a Remote Destination

You can configure one or more remote destinations for a CTI Remote Device. A remote destination is a mobile or other phone that you can configure to perform remote destination pickup (accept transfers from the desk phone of the user) and accept incoming Cisco Unified Mobility calls. The remote destination that is associated with the CTI Remote Device specifies the phone number to reach the remote device. The maximum number of remote destinations that you can configure for a CTI Remote Device is dependent on the Remote Destination limit set for the Owner User ID.

Remote destinations can include any of the following devices:

- Single-mode mobile (cellular) phones
- Smartphones
- Dual-mode phones
- Enterprise IP phones that are not in the same cluster as the desk phone
- Home phone numbers in the PSTN

Procedure

Step 1	From Cisco Unified CM Administration, choose **Device** > **Phone** > **CTI Remote Device** > **Associated Remote Destinations**.
Step 2	Specify the filter criteria and click on the CTI Remote Device for which you want to configure the remote destination.
Step 3	In the **Associated Remote Destinations** pane, select **Add a New Remote Destination**.
	Alternatively, you can also use the **Device** > **Phone** > **Add New** menu path to configure a remote destination.
Step 4	Configure the fields in the **Remote Destination Configuration** window. See the Related Topics section for more information about the fields and their configuration options.
Step 5	Click **Save**.

Remote Destination Configuration Fields

Table 7: Remote Destination Configuration Fields

Field	Description
Name	Enter the name of the remote destination.
Destination Number	Enter the number that you would dial from within the enterprise. Include the area code and any additional digits that are required to reach an outside line. The maximum field length is 24 characters; individual characters can take the values 0-9, *, #, and +. Cisco recommends that you configure the caller ID of the remote destination.
Owner User ID	From the drop-down list, choose the owner of the remote destination.
Enable Unified Mobility features	Check the check box to enable Unified Mobility features.
Remote Destination Profile	From drop-down list, choose the profile that you configured.
Enable Single Number Reach	Check the check box to enable Single-Number_Reach for the remote destination.
Enable Move to Mobile	This is an optional field. If your phone is a mobile phone, check this check box.

Configure a Cisco Spark Remote Device

Procedure

	Command or Action	**Purpose**
Step 1	Configure a Cisco Spark Remote Device, on page 17	Create a Cisco Spark remote device.
Step 2	Add a Directory Number to a Cisco Spark Device, on page 21	To register a Cisco Spark remote device, you must add a Directory Number to that device.

Configure a Cisco Spark Remote Device

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select Cisco Spark Remote Device and click **Next**.

Step 4 Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

Cisco Spark Remote Device Configuration Fields

Table 8: Webex Remote Device Configuration Fields

Field	Description
Device Information	
Registration	Specifies the registration status of the Webex remote device.
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies whether the device is trusted or not trusted.
Active Remote Destination	Specifies if the remote destination is active. The Webex client has only one active remote destination by default. All incoming calls are routed to the active remote destination. This field is to none even though it is associated to an active remote destination.
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device.

Field	Description
Device Name	Specifies the name for the Webex remote device that is automatically populated based on the Owner User ID.
	The format of the device name is *SparkRD<OwnerUserID>* by default. The default device name *SparkRD* must not be changed.
	This field is editable. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the Webex remote device.
	This field can contain up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Select the device pool which defines the common characteristics for Webex remote devices.
	For more information on how to configure the device pool, see Device Pool Configuration Settings.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when you initiate a hold action.
	Caution MOH is currently not supported for Cisco Spark remote device as Hold/Resume feature on the device is not implemented.
Network Hold MOH Audio Source	From the drop-down list, choose the audio source to use for MOH when the network initiates a hold action.
	Caution MOH is currently not supported for Cisco Spark remote device as Hold/Resume feature on the device is not implemented.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.
Call Routing Information	
Inbound and Outbound Calls Information	
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the **Trunk Configuration** window.
Protocol Specific Information	
Presence Group	Configure this field with the Presence feature. If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. **Caution** Presence Group is currently not supported for Cisco Spark remote device.

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user.
	From the drop-down list, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list.
	If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.
	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.
	Caution SUBSCRIBE Calling Search Space is currently not supported for Cisco Spark remote device.
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting.
	The rerouting calling search space of the referrer is used to find the route to the refer-to target. When the Refer message fails due to the rerouting calling search space, the Refer Primitive rejects the request with the "405 Method Not Allowed" message.
	The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
Do Not Disturb Information	
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device.
	Caution The calls are not routed to Cisco Spark clients if the DND option is enabled.
	Caution Do Not Disturb is currently not supported for Cisco Spark remote device .

Field	Description
DND Option	When you enable DND on the phone, Call Reject 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. **Caution** Do Not Disturb is currently not supported for Cisco Spark remote device .

Add a Directory Number to a Cisco Spark Device

To register a Webex remote device, add a Directory Number to that device. You cannot register a Webex remote device without a Directory Number. You can add a maximum of five Directory Numbers to the Webex remote device.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Specify the filter criteria and click the Cisco Spark Remote Device for which you want to associate the directory number.

Step 3 In the **Association** pane, click **Add a new DN** link.

Step 4 Configure the fields in the **Directory Number Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Migrate Phone Data

Procedure

	Command or Action	Purpose
Step 1	Create a Phone Template, on page 22	Create a phone template in Bulk Administration Tool (BAT) for the phone model and protocol to which you want to migrate the data.
Step 2	Migrate Phone Data, on page 22	Migrate phone data to a different phone.

Create a Phone Template

Procedure

Step 1	From Cisco Unified CM Administration, choose **Bulk Administration** > **Phones** > **Phone Template**.
Step 2	Click **Add New**. The **Add a New Phone Template** window displays.
Step 3	From the **Phone Type** drop-down list, choose the phone model for which you are creating the template. Click **Next**.
Step 4	From the **Select the Device Protocol** drop-down list, choose the device protocol. Click **Next**. The **Phone Template Configuration** window appears with fields and default entries for the chosen device type.
Step 5	Configure the fields in the **Phone Template Configuration** window. See the online help for more information about the fields and their configuration options.
Step 6	Click **Save**.

Migrate Phone Data

Before you begin

- Unplug the phone from the network.
- Ensure that there are enough device license units for the new phone.
- Ensure that the phone model supports phone migration.

Procedure

Step 1	From Cisco Unified CM Administration, choose **Device** > **Phone**.
Step 2	Specify the search criteria and click **Find**.
Step 3	Choose and click the phone configuration that you want to migrate.
Step 4	Choose **Migrate Phone** from the **Related Links** drop-down list. The **Phone Migration Configuration** window appears.
Step 5	From the drop-down list, choose the phone template for the phone model to which you want to migrate the phone configuration.
Step 6	Enter the **Media Access Control (MAC) address** for the new Cisco Unified IP Phone to which you are migrating the configuration. The MAC address must contain 12 hexadecimal characters.
Step 7	(Optional) Enter a description for the new phone. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
Step 8	Click **Save**.
Step 9	If a warning displays that the new phone may lose feature functionality, click **OK**.

What to do next

Plug the new phone into the network and register the device.