Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 8.x

Create software phone devices so that users can send and receive audio and video on their computers. Create desk phone devices that users can control with Cisco Jabber. Learn how to enable different audio and video features. Understand which server profiles you should create and which user associations you must assign.

Note The client does not support audio and video calling on Cisco Unified Communications Manager Version 8.x when users connect to the corporate network using Expressway for Mobile and Remote Access.

Create Software Phone Devices

Software phones let users send and receive audio and video through their computers.

Create CSF Devices on 8.6(1)

The steps in this section describe how to create CSF devices on Cisco Unified Communications Managerversion 8.6(1). CSF devices provide users with software phone capabilities.

As part of the task of creating CSF devices, you can enable video desktop sharing using Binary Floor Control Protocol (BFCP). Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. For this reason, you configure Cisco Unified Communications Manager to allow BFCP presentation sharing. On Cisco Unified Communications Manager version 8.6(1), you enable BFCP presentation sharing on a SIP profile. You must then apply that SIP profile to the CSF devices.

Note

- Cisco Unified Communications Manager supports BFCP presentation sharing on version 8.6(1) and later only. You cannot enable BFCP, or provision users with video desktop sharing capabilities, on versions earlier than 8.6(1).
- You can enable video desktop sharing only on software phone devices. You cannot enable video desktop sharing on desk phone devices.
- Users must be on active calls to use video desktop sharing capabilities. You can only initiate video desktop sharing sessions from active calls.
- In hybrid cloud-based deployments, both Cisco WebEx and Cisco Unified Communications Manager provide desktop sharing functionality.
    - If users initiate desktop sharing sessions during an instant messaging session, Cisco WebEx provides desktop sharing capabilities.
    - If users initiate desktop sharing sessions during an audio or video conversation, Cisco Unified Communications Manager provides desktop sharing capabilities.

Create SIP Profiles

The first step in creating a software phone device is to create a SIP profile so that you can enable video desktop sharing. You cannot edit or configure the default SIP profile. For this reason, you must create a new SIP profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.
The **Find and List SIP Profiles** window opens.

Step 3 Do one of the following to create a new SIP profile:

- Find the default SIP profile and create a copy that you can edit.
- Select **Add New** and create a new SIP profile.

Enable Video Desktop Sharing on SIP Profiles

You should enable BFCP on the SIP profile before you apply the SIP profile to CSF devices.

Note You cannot migrate a BFCP-enabled SIP profile to Cisco Unified Communications Manager version 8.6(2) or higher. If you configure video desktop sharing on Cisco Unified Communications Manager 8.61 and then upgrade to Cisco Unified Communications Manager 8.62, you must configure video desktop sharing on version 8.6.2.

Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.

Procedure

Step 1 Open the **Cisco Unified Communications Manager Administration** interface.

Step 2 Enable video desktop sharing on the SIP profile.

- For individual profiles, do the following:
  1. Select **Device** > **Device Settings** > **SIP Profile**.
  2. Select your SIP profile.
  3. In the **SIP Profile Information** section, select **Allow Presentation Sharing Using BFCP**.
  4. Select **Save**.
- For multiple profiles, do the following:
  1. Select **Bulk Administration** > **Phones** > **Export Phones** > **All Details**.
  2. Select **Bulk Administration** > **Upload/Download Files** and download the exported `CSV` file.
  3. Open the `CSV` file with any editor.
  4. Insert a column named Allow presentation sharing using BFCP into the `CSV` file.
  5. Set the value of the column to Y for all required devices.
  6. Save the `CSV` file.
  7. Select **Bulk Administration** > **Phones** > **Insert Phones**.
  8. Select the **Override the existing configuration** option.
  9. Import the `CSV` file.
  10. Select **Run Immediately**.
  11. Select **Submit**.

Create CSF Devices

Complete the steps in this task to create CSF devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Specify a name for the CSF device in the **Device Name** field.
You should use the CSF*username* format for CSF device names. For example, you create a CSF device for a user named Tanya Adams, whose username is tadams. In this case, you should specify CSFtadams as the device name.

Step 6 Specify configuration settings on the **Phone Configuration** window as appropriate.
See the *Phone Configuration Settings* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.

Step 7 Select the SIP profile on which you enabled BFCP presentation sharing from the **SIP Profile** drop-down list.

Step 8 Select **Save**.
A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

Add a directory number to the device and apply the configuration.

Create CSF Devices on 8.6(2) and Later

The steps in this section describe how to create CSF devices on Cisco Unified Communications Manager version 8.6(2) and later. CSF devices provide users with software phone capabilities.

As part of the task of creating CSF devices, you can enable video desktop sharing using Binary Floor Control Protocol (BFCP). Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. For this reason, you configure Cisco Unified Communications Manager to allow BFCP presentation sharing. On Cisco Unified Communications Manager version 8.6(2) and later, you must apply a COP file to add an option to allow BFCP presentation sharing on CSF devices. You must then enable BFCP presentation sharing on the CSF devices.

Note

- Cisco Unified Communications Manager supports BFCP presentation sharing on version 8.6(1) and later only. You cannot enable BFCP, or provision users with video desktop sharing capabilities, on versions earlier than 8.6(1).
- You can enable video desktop sharing only on software phone devices. You cannot enable video desktop sharing on desk phone devices.
- Users must be on active calls to use video desktop sharing capabilities. You can only initiate video desktop sharing sessions from active calls.
- In hybrid cloud-based deployments, both Cisco WebEx and Cisco Unified Communications Manager provide desktop sharing functionality.
    - If users initiate desktop sharing sessions during an instant messaging session, Cisco WebEx provides desktop sharing capabilities.
    - If users initiate desktop sharing sessions during an audio or video conversation, Cisco Unified Communications Manager provides desktop sharing capabilities.

Tip As of Cisco Unified Communications Manager version 8.6(2), you must enable BFCP on the SIP trunk to allow video desktop sharing capabilities between nodes in a Cisco Unified Communications Manager cluster. To enable BFCP on the SIP trunk, do the following:

1. Select **Allow Presentation Sharing using BFCP** in the **Trunk Specific Configuration** section of the SIP profile.
2. Select the SIP profile from the **SIP Profile** drop-down list on the CSF device configuration.

Apply COP File for BFCP Capabilities

You must apply `cmterm-bfcp-e.8-6-2.cop.sgn` to configure video desktop sharing on Cisco Unified Communications Manager version 8.6.2 and later. This COP file adds an option to enable BFCP on the CSF device.

Note

- You must install the COP file each time you upgrade. For example, if you configure video desktop sharing on Cisco Unified Communications Manager 8.6.2 .20000-1 and then upgrade to Cisco Unified Communications Manager 8.6.2 .20000-2, you must apply the COP file on Cisco Unified Communications Manager 8.6.2 .20000-2.
- If you configure video desktop sharing on Cisco Unified Communications Manager 8.6.1 and then upgrade to Cisco Unified Communications Manager 8.6.2, you must apply the COP file on Cisco Unified Communications Manager 8.6.2 before you can configure video desktop sharing.

Procedure

Step 1 Download the Cisco Jabber administration package from Cisco.com.

Step 2 Copy `cmterm-bfcp-e.8-6-2.cop.sgn` from the Cisco Jabber administration package to your file system.

Step 3 Open the **Cisco Unified Communications Manager Administration** interface.

Step 4 Upload and apply `cmterm-bfcp-e.8-6-2.cop.sgn`.

Step 5 Restart the server as follows:

a) Open the **Cisco Unified OS Administration** interface.
b) Select **Settings** > **Version**.
c) Select **Restart**.
d) Repeat the preceding steps for each node in the cluster, starting with your presentation server.

The COP add the **Allow Presentation Sharing using BFCP** field to the **Protocol Specific Information** section on the **Phone Configuration** window for CSF devices.

Create CSF Devices

Complete the steps in this task to create CSF devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Specify a name for the CSF device in the **Device Name** field.
You should use the CSF*username* format for CSF device names. For example, you create a CSF device for a user named Tanya Adams, whose username is tadams. In this case, you should specify CSFtadams as the device name.

Step 6 Specify configuration settings on the **Phone Configuration** window as appropriate.
See the *Phone Configuration Settings* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.

Step 7 Select **Allow Presentation Sharing using BFCP** in the **Protocol Specific Information** section to enable video desktop sharing.
Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.

Step 8 Select **Save**.

A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

Add a directory number to the device and apply the configuration.

Set Up Secure Phone Capabilities

You can optionally set up secure phone capabilities for CSF devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

Configure the Security Mode

To use secure phone capabilities, you must configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. You cannot use secure phone capabilities with the nonsecure security mode. At a minimum, you must use mixed mode security.

Mixed mode security:

- Allows authenticated, encrypted, and nonsecure phones to register with Cisco Unified Communications Manager.
- Cisco Unified Communications Manager supports both RTP and SRTP media.
- Authenticated and encrypted devices use secure port 5061 to connect to Cisco Unified Communications Manager.

See the *Cisco Unified Communications Manager Security Guide* for instructions on configuring mixed mode with the Cisco CTL Client.

Related Topics

Cisco Unified Communications Manager Security Guide, Release 8.6(1)
Cisco Unified Communications Manager Security Guide, Release 9.1(1)
Cisco Unified Communications Manager Security Guide, Release 10.0(1)

Create a Phone Security Profile

The first step to setting up secure phone capabilities is to create a phone security profile that you can apply to the device.

Before You Begin

Configure the Cisco Unified Communications Manager security to use mixed mode.

Procedure

Step 1 Select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 Select the appropriate phone security profile from the Phone Security Profile type drop-down list and select **Next**.
The **Phone Security Profile Configuration** window opens.

Configure the Phone Security Profile

After you add a phone security profile, you must configure it to suit your requirements.

Procedure

Step 1 Specify a name for the phone security profile in the Name field on the **Phone Security Profile Configuration** window.

Restriction You must use fully qualified domain name (FQDN) format for the security profile name if users connect remotely to the corporate network through Expressway for Mobile and Remote Access.

Step 2 Specify values for the phone security profile as follows:

- Device Security Mode — Select one of the following:
  - Authenticated
  - Encrypted
- Transport Type — Leave the default value of **TLS**.
- TFTP Encrypted Config — Select this checkbox to encrypt the CSF device configuration file that resides on the TFTP server.
- Authentication Mode — Select By Authentication String.
- Key Size (Bits) — Select the appropriate key size for the certificate.

  Note Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

  The client has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.
- SIP Phone Port — Leave the default value. The client always uses port 5061 to connect to Cisco Unified Communications Manager when you apply a secure phone profile. The port that you specify in this field only takes effect if you select **Non Secure** as the value for Device Security Mode.

Step 3 Select **Save**.

Configure CSF Devices

Add the phone security profile to the devices and complete other configuration tasks for secure phone capabilities.

Procedure

Step 1 Open the CSF device configuration window.

a) Select **Device** > **Phone**.
The **Find and List Phones** window opens.

b) Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

c) Select the CSF device from the list.
The **Phone Configuration** window opens.

Step 2 Select **Allow Control of Device from CTI** in the Device Information section.

Step 3 Select **Save**.

Step 4 Locate the Protocol Specific Information section.

Step 5 Select the phone security profile from the Device Security Profile drop-down list.

Step 6 Select **Save**.

At this point in the secure phone set up, existing users can no longer use their CSF devices. You must complete the secure phone set up for users to be able to access their CSF devices.

What to Do Next

Specify the certificate settings and generate the authentication string for users.

Specify Certificate Settings

Specify certificate settings in the CSF device configuration and generate the authentication strings that you provide to users.

Procedure

Step 1 Locate the Certification Authority Proxy Function (CAPF) Information section on the **Phone Configuration** window.

Step 2 Specify values as follows:

- Certificate Operation — Select **Install/Upgrade**.
- Authentication Mode — Select **By Authentication String**.
- Key Size (Bits) — Select the same key size that you set in the phone security profile.
- Operation Completes By — Specify an expiration value for the authentication string or leave as default.

Step 3 Select **Save**.

Step 4 To create the authentication string you can do one of the following:

- Select **Generate String** in the Certification Authority Proxy Function (CAPF) Information section.
- Enter a custom string in the Authentication String field.

What to Do Next

Provide users with the authentication string.

Provide Users with Authentication Strings

Users must specify the authentication string in the client interface to access their devices and securely register with Cisco Unified Communications Manager.

When users enter the authentication string in the client interface, the CAPF enrollment process begins.

Note The time it takes for the enrollment process to complete can vary depending on the user's computer or mobile device and the current load for Cisco Unified Communications Manager. It can take up to one minute for the client to complete the CAPF enrollment process.

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's device and then provide it to the user.

- Users do not enter the authentication string before the expiration time you set in the Operation Completes By field.

  In this case, you must generate a new authentication string on the user's device. The user must then enter that authentication string before the expiration time.

Important When you configure the end users in Cisco Unified Communications Manager, you must add them to the following user groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Users must not belong to the Standard CTI Secure Connection user group.

Secure Phone Details for Cisco Jabber for Windows

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between CSF devices and Cisco Unified Communications Manager are over TLS.
    - If you select Authenticated as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption.
    - If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using AES 128/SHA encryption.
- Mutual TLS ensures that only CSF devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, CSF devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their CSF device connections to Cisco Unified Communications Manager are secure. If the other end point also has a secure connection to Cisco Unified Communications Manager, then the call can be secure. However, if the other end point does not have a secure connection to Cisco Unified Communications Manager, then the call is not secure.

Encrypted Media

If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the client uses Secure Realtime Transport Protocol (SRTP) to offer encrypted media streams as follows:

Media Stream	Encryption
Main video stream	Can be encrypted
Main audio stream	Can be encrypted
Presentation video stream Refers to video desktop sharing using BFCP.	Can be encrypted
BFCP application stream Refers to BFCP flow control.	Not encrypted

The ability to encrypt media depends on if the other end points also encrypt media, as in the following examples:

- You enable media encryption for user A and user B. In other words, Device Security Mode is set to Encrypted on the phone security profile for the users' CSF devices.
- You do not enable media encryption for user C. In other words, Device Security Mode is set to Authenticated on the phone security profile for the user's CSF device.
- User A calls user B. The client encrypts the main video stream and audio stream.
- User A calls user C. The client does not encrypt the main video stream and audio stream.

- User A, user B, and user C start a conference call. The client does not encrypt the main video stream or audio stream for any user.

Note The client displays the following lock icon when it can use SRTP for encrypted media streams to other secured clients or conference bridges:

However, not all versions of Cisco Unified Communications Manager provide the ability to display the lock icon. If the version of Cisco Unified Communications Manager you are using does not provide this ability, the client cannot display a lock icon even when it sends encrypted media.

Using Expressway for Mobile and Remote Access

Users cannot complete the enrollment process or use secure phone capabilities from outside the corporate network. This limitation also includes when users connects through Expressway for Mobile and Remote Access; for example,

1. You configure a user's CSF device for secure phone capabilities.
2. That user connects to the internal corporate network through Expressway for Mobile and Remote Access.
3. The client notifies the user that it cannot use secure phone capabilities instead of prompting the user to enter an authentication string.

When users connect to the internal network through Expressway for Mobile and Remote Access and participate in a call:

- Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
- Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager.

Note If you change the phone security profile while the client is connected through Expressway for Mobile and Remote Access, you must restart the client for that change to take effect.

Stored Files

The client stores the following files for secure phone capabilities:

- Certificate trust list (`.tlv`)
- Locally significant certificate (`.lsc`)
- Private key for the CSF device (`.key`)

The client downloads and stores certificate trust lists whenever you configure Cisco Unified Communications Manager security as mixed mode. Certificate trust lists enable the client to verify the identity of Cisco Unified Communications Manager nodes.

The client saves the locally significant certificates and private keys after users successfully enter the authentication code and complete the enrollment process. The locally significant certificate and private key enable the client to establish mutual TLS connections with Cisco Unified Communications Manager.

Note The client encrypts the private key before saving it to the file system.

The client stores these files in the following folder:
`%User_Profile%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Security`

Because the client stores the files in the user's `Roaming` folder, users can sign in to any Microsoft Windows account on the Windows domain to register their CSF devices.

Conference Calls

On conference, or multi-party, calls, the conferencing bridge must support secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

CSF device security reverts to the lowest level available on multi-party calls. For example, user A, user B, and user C join a conference call. User A and user B have CSF devices with secure phone capabilities. User C has a CSF device without secure phone capabilities. In this case, the call is not secure for all users.

Sharing Secure CSF Devices between Clients

Clients that do not support secure phone capabilities cannot register to secure CSF devices.

For example, you set up secure phone capabilities on a CSF device to which both Cisco Jabber for Windows version 9.2 and Cisco Jabber for Windows version 9.1 register. However, Cisco Jabber for Windows version 9.1 does not support secure phone capabilities. In this scenario, you must create two different CSF devices, one secure CSF device for Cisco Jabber for Windows version 9.2 and another CSF device that is not secure for Cisco Jabber for Windows version 9.1.

Multiple Users on a Shared Microsoft Windows Account

Multiple users can have unique credentials for the client and share the same Windows account. However, the secure CSF devices are restricted to the Windows account that the users share. Users who share the same Windows account cannot make calls with their secure CSF devices from different Windows accounts.

You should ensure that multiple users who share the same Windows account have CSF devices with unique names. Users cannot register their CSF devices if they share the same Windows account and have CSF devices with identical names, but connect to different Cisco Unified Communications Manager clusters.

For example, user A has a CSF device named CSFcompanyname and connects to cluster 1. User B has a CSF device named CSFcompanyname and connects to cluster 2. In this case, a conflict occurs for both CSF devices. Neither user A or user B can register their CSF devices after both users sign in to the same Windows account.

Multiple Users on a Shared Computer

The client caches the certificates for each user's secure CSF device in a location that is unique to each Windows user. When a user logs in to their Windows account on the shared computer, that user can access only the

secure CSF device that you provision to them. That user cannot access the cached certificates for other Windows users.

Add Directory Number to the Device for Desktop Applications

You must add directory numbers to devices in Cisco Unified Communications Manager. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point display. See the Cisco Unified Communications Manager documentation for more information about different options to configure directory numbers.

Procedure

Step 1 Locate the Association Information section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the Directory Number field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.

b) Select **Associate End Users**.
The **Find and List Users** window opens.

c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

d) Select the appropriate users from the list.

e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.
The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Create Desk Phone Devices

Users can control desk phones on their computers to place audio calls.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.

The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select the appropriate device from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Complete the following steps in the **Device Information** section:

a) Enter a meaningful description in the **Description** field.
The client displays device descriptions to users. If users have multiple devices of the same model, the descriptions help users tell the difference between multiple devices.

b) Select **Allow Control of Device from CTI**.
If you do not select **Allow Control of Device from CTI**, users cannot control the desk phone.

Step 6 Complete the following steps to enable desk phone video capabilities:

a) Locate the **Product Specific Configuration Layout** section.

b) Select **Enabled** from the **Video Capabilities** drop-down list.

Note If possible, you should enable desk phone video capabilities on the device configuration. However, certain phone models do not include the **Video Capabilities** drop-down list at the device configuration level. In this case, you should open the **Common Phone Profile Configuration** window and then select **Enabled** from the **Video Calling** drop-down list.

See *Desk Phone Video Configuration* for more information about desk phone video.

Step 7 Specify all other configuration settings on the **Phone Configuration** window as appropriate.
See the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

Step 8 Select **Save**.
An message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

Add a directory number to the device and apply the configuration.

Desk Phone Video Configuration

Desk phone video capabilities let users receive video transmitted to their desk phone devices on their computers through the client.

Set Up Desk Phone Video

To set up desk phone video, you must complete the following steps:

1 Physically connect the computer to the computer port on the desk phone device.

You must physically connect the computer to the desk phone device through the computer port so that the client can establish a connection to the device. You cannot use desk phone video capabilities with wireless connections to desk phone devices.

Tip If users have both wireless and wired connections available, they should configure Microsoft Windows so that wireless connections do not take priority over wired connections. See the following Microsoft documentation for more information: *An explanation of the Automatic Metric feature for Internet Protocol routes*.

2. Enable the desk phone device for video in Cisco Unified Communications Manager.
3. Install Cisco Media Services Interface on the computer.

   Cisco Media Services Interface provides the Cisco Discover Protocol (CDP) driver that enables the client to do the following:

   - Discover the desk phone device.
   - Establish and maintain a connection to the desk phone device using the CAST protocol.

Note Download the **Cisco Media Services Interface** installation program from the download site on `Cisco.com`.

Desk Phone Video Considerations

Review the following considerations and limitations before you provision desk phone video capabilities to users:

- You cannot use desk phone video capabilities on devices if video cameras are attached to the devices, such as a Cisco Unified IP Phone 9971. You can use desk phone video capabilities if you remove video cameras from the devices.
- You cannot use desk phone video capabilities with devices that do not support CTI.
- Video desktop sharing, using the BFCP protocol, is not supported with desk phone video.
- It is not possible for endpoints that use SCCP to receive video only. SCCP endpoints must send and receive video. Instances where SCCP endpoints do not send video result in audio only calls.
- 7900 series phones must use SCCP for desk phone video capabilities. 7900 series phones cannot use SIP for desk phone video capabilities.
- If a user initiates a call from the keypad on a desk phone device, the call starts as an audio call on the desk phone device. The client then escalates the call to video. For this reason, you cannot make video calls to devices that do not support escalation, such as H.323 endpoints. To use desk phone video capabilities with devices that do not support escalation, users should initiate calls from the client.
- A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. You must upgrade your firmware to version SCCP45.9-3-1 to use desk phone video capabilities.
- Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets, which disables desk phone video capabilities. You should configure your antivirus or firewall application to allow inbound CDP packets.

  See the following Symantec technical document for additional details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*.

- You must not select the **Media Termination Point Required** checkbox on the SIP trunk configuration for Cisco Unified Communications Manager. Desk phone video capabilities are not available if you select this checkbox.

If you encounter an error that indicates desk phone video capabilities are unavailable or the desk phone device is unknown, do the following:

1. Ensure you enable the desk phone device for video in Cisco Unified Communications Manager.
2. Reset the physical desk phone.
3. Exit the client.
4. Run services.msc on the computer where you installed the client.
5. Restart Cisco Media Services Interface.
6. Restart the client.

Related Topics

Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection

Add Directory Number to the Device for Desktop Applications

You must add directory numbers to devices in Cisco Unified Communications Manager. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point display. See the Cisco Unified Communications Manager documentation for more information about different options to configure directory numbers.

Procedure

Step 1 Locate the Association Information section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the Directory Number field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.
b) Select **Associate End Users**.
The **Find and List Users** window opens.
c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
d) Select the appropriate users from the list.
e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Enable Video Rate Adaptation

The client uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video quality based on network conditions.

To use video rate adaptation, you must enable Real-Time Transport Control Protocol (RTCP) on Cisco Unified Communications Manager.

Note RTCP is enabled on software phone devices by default. However, you must enable RTCP on desk phone devices.

Enable RTCP on Common Phone Profiles

You can enable RTCP on a common phone profile to enable video rate adaptation on all devices that use the profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.
The **Find and List Common Phone Profiles** window opens.

Step 3 Specify the appropriate filters in the **Find Common Phone Profile where** field and then select **Find** to retrieve a list of profiles.

Step 4 Select the appropriate profile from the list.
The **Common Phone Profile Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

Step 6 Select **Enabled** from the **RTCP** drop-down list.

Step 7 Select **Save**.

Enable RTCP on Device Configurations

You can enable RTCP on specific device configurations instead of a common phone profile. The specific device configuration overrides any settings you specify on the common phone profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of phones.

Step 4 Select the appropriate phone from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

Step 6 Select **Enabled** from the **RTCP** drop-down list.

Step 7 Select **Save**.

Set Up a CTI Gateway

The client requires a CTI gateway to communicate with Cisco Unified Communications Manager and perform certain functions such as desk phone control.

Add a CTI Gateway Server

The first step in setting up a CTI gateway is to add a CTI gateway server on Cisco Unified Presence.

Procedure

Step 1 Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **Application** > **Cisco Jabber** > **CTI Gateway Server**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Server**.

The **Find and List CTI Gateway Servers** window opens.

Step 3 Select **Add New**.
The **CTI Gateway Server Configuration** window opens.

Step 4 Specify the required details on the **CTI Gateway Server Configuration** window.

Step 5 Select **Save**.

Create a CTI Gateway Profile

After you add a CTI gateway server, you must create a CTI gateway profile and add that server to the profile.

Procedure

Step 1 Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **Application** > **Cisco Jabber** > **CTI Gateway Profile**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Profile**.

The **CTI Gateway Profile Configuration** window opens.

Step 3 Specify the required details on the **CTI Gateway Profile Configuration** window.

Step 4 Select **Add Users to Profile** and add the appropriate users to the profile.

Step 5 Select **Save**.

Configure Silent Monitoring and Call Recording

You can set up additional audio path functions for devices such as silent monitoring and call recording.

Note This feature is currently supported on Cisco Jabber for Windows only.

To enable silent monitoring and call recording, you configure Cisco Unified Communications Manager. See the *Monitoring and Recording* section of the *Cisco Unified Communications Manager Features and Services Guide* for step-by-step instructions.

Notes:

- Cisco Jabber does not provide any interface to initiate silent monitoring or call recording. You must use the appropriate software to silently monitor or record calls.
- Cisco Jabber does not currently support monitoring notification tone or recording notification tone.
- You can use silent monitoring and call recording functionality only. Cisco Jabber does not support other functionality such as barging or whisper coaching.
- You might need to download and apply a device package to enable monitoring and recording capabilities on the device, depending on your version of Cisco Unified Communications Manager. Before you start configuring the server, do the following:

  1 Open the **Phone Configuration** window for the device on which you plan to enable silent monitoring and call recording.

  2 Locate the **Built In Bridge** field.

  If the **Built In Bridge** field is not available on the **Phone Configuration** window, you should download and apply the most recent device packages.

Related Topics

v8.6(1): Monitoring and Recording
v9.1: Monitoring and Recording

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

Step 4 Select the appropriate user from the list.
The **End User Configuration** window opens.

Step 5 Locate the **Device Information** section.

Step 6 Select **Device Association**.
The **User Device Association** window opens.

Step 7 Select the devices to which you want to associate the user.

Step 8 Select **Save Selected/Changes**.

Step 9 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 10 Find and select the same user from the list.
The **End User Configuration** window opens.

Step 11 Locate the **Permissions Information** section.

Step 12 Select **Add to User Group**.
The **Find and List User Groups** dialog box opens.

Step 13 Select the groups to which you want to assign the user.
At a minimum you should assign the user to the following groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional groups, as follows:

- Cisco Unified IP Phone 9900 or 8900 series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 14 Select the groups to which you want to assign the user.

Step 15 Select **Add Selected**.

The **Find and List User Groups** window closes.

Step 16 Select **Save** on the **End User Configuration** window.

Reset Devices

After you create and associate users with devices, you should reset those devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

Step 4 Select the appropriate device from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Association Information** section.

Step 6 Select the appropriate directory number configuration.
The **Directory Number Configuration** window opens.

Step 7 Select **Reset**.
The **Device Reset** dialog box opens.

Step 8 Select **Reset**.

Step 9 Select **Close** to close the **Device Reset** dialog box.

Specify Your TFTP Server Address

The client gets device configuration from the TFTP server. For this reason, you must specify your TFTP server address when you provision users with devices.

Attention If the client gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service.

You do not need to specify your TFTP server address if you deploy the `_cisco-uds` SRV record.

Specify Your TFTP Server on Cisco Unified Presence

If you are using Cisco Unified Communications Manager Version 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Presence. If you are using Cisco Unified Communications Manager Version 9.x, then you do not need to follow the steps below.

Procedure

Step 1 Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **Application** > **Cisco Jabber** > **Settings**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Settings**.

The **Cisco Jabber Settings** window opens.

Step 3 Locate the fields to specify TFTP servers in one of the following sections, depending on your version of Cisco Unified Presence:

- **Cisco Jabber Security Settings**
- **CUPC Global Settings**

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**
- **Backup TFTP Server**

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

If you deploy the client in phone mode you can provide the address of the TFTP server as follows:

- Users manually enter the TFTP server address when they start the client.
- You specify the TFTP server address during installation with the TFTP argument.

Specify TFTP Servers with the Cisco WebEx Administration Tool

If the client connects to the Cisco WebEx Messenger service, you specify your TFTP server address with the Cisco WebEx Administration Tool.

Procedure

Step 1 Open the Cisco WebEx Administration Tool.

Step 2 Select the **Configuration** tab.

Step 3 Select **Unified Communications** in the **Additional Services** section.
The **Unified Communications** window opens.

Step 4 Select the **Clusters** tab.

Step 5 Select the appropriate cluster from the list.
The **Edit Cluster** window opens.

Step 6 Select **Advanced Server Settings** in the **Cisco Unified Communications Manager Server Settings** section.

Step 7 Specify the IP address of your primary TFTP server in the **TFTP Server** field.

Step 8 Specify the IP address of your backup TFTP servers in the **Backup Server #1** and **Backup Server #2** fields.

Step 9 Select **Save**.
The **Edit Cluster** window closes.

Step 10 Select **Save** in the **Unified Communications** window.

Create a CCMCIP Profile

The client gets device lists for users from the CCMCIP server.

Procedure

Step 1 Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **Application** > **Cisco Jabber** > **CCMCIP Profile**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **CCMCIP Profile**.

The **Find and List CCMCIP Profiles** window opens.

Step 3 Select **Add New**.
The **CCMCIP Profile Configuration** window opens.

Step 4 Specify service details in the CCMCIP profile as follows:

a) Specify a name for the profile in the **Name** field.

b) Specify the hostname or IP address of your primary CCMCIP service in the **Primary CCMCIP Host** field.

c) Specify the hostname or IP address of your backup CCMCIP service in the **Backup CCMCIP Host** field.

d) Leave the default value for **Server Certificate Verification**.

Step 5 Add users to the CCMCIP profile as follows:

a) Select **Add Users to Profile**.
The **Find and List Users** dialog box opens.

b) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

c) Select the appropriate users from the list.
d) Select **Add Selected**.
The selected users are added to the CCMCIP profile.

Step 6 Select **Save**.

Dial Plan Mapping

You configure dial plan mapping to ensure that dialing rules on Cisco Unified Communications Manager match dialing rules on your directory.

Application Dial Rules

Application dial rules automatically add or remove digits in phone numbers that users dial. Application dialing rules manipulate numbers that users dial from the client.

For example, you can configure a dial rule that automatically adds the digit 9 to the start of a 7 digit phone number to provide access to outside lines.

Directory Lookup Dial Rules

Directory lookup dial rules transform caller ID numbers into numbers that the client can lookup in the directory. Each directory lookup rule you define specifies which numbers to transform based on the initial digits and the length of the number.

For example, you can create a directory lookup rule that automatically removes the area code and two-digit prefix digits from 10-digit phone numbers. An example of this type of rule is to transform `4089023139` into `23139`.

Publish Dial Rules

Cisco Unified Communications Manager version 8.6.1 or earlier does not automatically publish dial rules to the client. For this reason, you must deploy a COP file to publish your dial rules. This COP file copies your dial rules from the Cisco Unified Communications Manager database to an XML file on your TFTP server. The client can then download that XML file and access your dial rules.

Remember You must deploy the COP file every time you update or modify dial rules on Cisco Unified Communications Manager version 8.6.1 or earlier.

Before You Begin

1. Create your dial rules in Cisco Unified Communications Manager.
2. Download the Cisco Jabber administration package from `Cisco.com`.
3. Copy `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the Cisco Jabber administration package to your file system.

Procedure

Step 1 Open the **Cisco Unified OS Administration** interface.

Step 2 Select **Software Upgrades** > **Install/Upgrade**.

Step 3 Specify the location of `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.

Step 4 Select **Next**.

Step 5 Select `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the **Available Software** list.

Step 6 Select **Next** and then select **Install**.

Step 7 Restart the TFTP service.

Step 8 Open the dial rules XML files in a browser to verify that they are available on your TFTP server.

a) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/AppDialRules.xml`.

b) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/DirLookupDialRules.xml`.

If you can access `AppDialRules.xml` and `DirLookupDialRules.xml` with your browser, the client can download your dial rules.

Step 9 Repeat the preceding steps for each Cisco Unified Communications Manager instance that runs a TFTP service.

What to Do Next

After you repeat the preceding steps on each Cisco Unified Communications Manager instance, restart the client.