Configure Call Control

Call Control Overview

To begin using CMR Hybrid, you must configure the call control product(s) used in your video network.

There are four possible call control scenarios:

- Cisco Cisco Unified Communications Manager with Cisco Expressway-C and Cisco Expressway-E.

  Endpoints are registered and bridges are trunked to Unified Communications Manager only.

- Cisco VCS Control and Cisco VCS Expressway

  Endpoints are registered to Cisco VCS Control and/or Cisco VCS Expressway only and bridges are registered to Cisco VCS Control only.

- Cisco Unified Communications Manager with Cisco Expressway-C and Cisco Expressway-E or Cisco VCS Control and Cisco VCS Expressway

  Endpoints are registered to Unified Communications Manager only and bridges are registered to Cisco VCS Control only.

- Cisco VCS Control and Cisco VCS Expressway with Unified Communications Manager

  Endpoints are registered to Cisco VCS Control/Expressway and Unified Communications Manageronly and bridges are registered to Cisco VCS Control only.

Note Using Unified Communications Manager as the call control solution requires either Cisco Expressway-C and Cisco Expressway-E or Cisco VCS Control and Cisco VCS Expressway to be deployed in order to communicate with WebEx, regardless of whether endpoints are registered to Unified Communications Manager or Cisco VCS.

Cisco Expressway and TelePresence Configuration Tasks

The procedures that follow apply to both VCS and Expressway products. Any step that refers to VCS Control also applies to Expressway-C. Likewise, any step that refers to VCS Expressway, also applies to Expressway-E.

Before You Begin

To configure WebEx in Cisco VCS or Expressway, the following are required:

- Cisco TelePresence Video Communication Server (Cisco VCS) or Expressway must be running firmware X8.5 or a later release.
- Cisco VCS Expressway or Expressway must be assigned a static IP address, DNS and NTP information, and be accessible for management via its web interface.
- Rich media licenses must be installed on the Cisco Expressway Series
- From software Version X8.5.3 we recommend that you configure the default SIP TCP timeout value in the Cisco Expressway / Cisco VCS as described in 'Reduce Default SIP TCP Timeout in Cisco Expressway / Cisco VCS' in Requirements,
- Endpoints in the network are registered to Cisco VCS Control or Expressway and/or Unified Communications Manager

  Note If endpoints are registered to Unified Communications Manager, you must configure a SIP trunk between Unified Communications Manager and Cisco VCS Control. For more information, refer to Configuring Cisco Unified Communications Manager, on page 5.

- Firewall must have port 5061 open to allow access to Cisco VCS Expressway

  If this port is not configured correctly, calls will not take place correctly.

  Note IMPORTANT: Stateful packet inspection used in Check Point Software Technologies, Inc. firewalls is incompatible with Cisco VCS Expressway and Expressway-E.

  - As a result, it is highly recommended to disable SIP and H.323 application layer gateways on routers/firewalls carrying network traffic to or from a VCS Expressway or Expressway-E, because, when these are enabled they can negatively affect the built-in firewall/NAT traversal functionality of the VCS

- Conferencing Bridge(s) to be used (MCU or TelePresence Server) are already operational within the network
- Cisco VCS Control or Expressway-C is in the private network
- Cisco VCS Expressway or Expressway-E is in the DMZ and has access to the Internet
- Set zones and pipes appropriately (according to your network's requirements) to allow a minimum of 2-4 Mbps for WebEx calls. For more information about bandwidth controls, please refer to the "Cisco VCS Administrator Guide" at:

  http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-maintenance-guides-list.html

  or "Cisco Expressway Administrator Guide" at:

  http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html
- If endpoints are registered to Cisco VCS Control, it must be configured as the SIP Registrar/H.323 gatekeeper.

  In order for CMR Hybrid to work with endpoints registered to Cisco VCS Control, it is required to set up a Cisco VCS Control as a SIP registrar, enabling it to register SIP devices and route calls to them. Cisco VCS Control has the capability to be both an H.323 gatekeeper and a SIP registrar.

  Configuring Cisco VCS Control as a SIP registrar is done by configuring one or more SIP domains. The Cisco VCS Control will act as a SIP Registrar and Presence Server for these domains, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes these domains.

  For details on how to configure SIP domains in Cisco VCS Control, refer to the "Cisco VCS and CUCM Deployment Guide" at:

  http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

  or "Cisco Expressway and CUCM via SIP Trunk Deployment Guide" at:

  http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html
- Intercompany TelePresence participants: If you want to allow participants from another company to be able to join via TelePresence, you must have a valid SIP SRV (secure SIP), non-secure SIP SRV or multiple SIP and H.323 SRV records in place that resolve to the Cisco VCS Expressway for your configured SIP Domain so TelePresence participants can route to your Cisco VCS Expressway.

Procedure

	Command or Action	Purpose
Step 1	Create a New DNS Zone, on page 4	Required. Configure a DNS zone on theCisco VCS Expressway for connection to the WebEx cloud.
Step 2	Configure Traversal Zones for MCUs, on page 5	Configure traveral zones to support MCUs that have encryption enabled (the default setting).

Create a New DNS Zone

Connection to the WebEx cloud uses a new DNS zone, which needs to be configured on the Cisco VCS Expressway.

To configure the Expressway-E or Cisco VCS Expressway for CMR Hybrid, do the following:

Procedure

Step 1 Create a new DNS zone:Set H.323 to **Off**.

a) Set SIP Media encryption mode to **Force encrypted**.
b) Turn on TLS Verify mode.
c) In the TLS verify subject name field, enter **sip.webex.com**.
d) Click **Create Zone**.

Step 2 Set up a search rule with a higher priority than the search rule for the existing DNS zone (lower number priority) for the domain of WebEx. The following configuration is required:

- Protocol: SIP
- Source: <Admin Defined>, default: Any
- Mode: Alias Pattern Match
- Pattern Type: Regex
- Pattern String: (.*)@(.*)(\.webex\.com).*
- Pattern Behavior: Replace
- Replace String: \1@\2\3
- On Successful Match: Stop
- Target: <DNS Zone Created for WebEx>
- State: Enabled

For details on how to create and set up search rules for a DNS zone, refer to the "Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide" at:

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf

Step 3 Configure a valid Client/Server Certificate for your company. Typically the CName of the certificate is the routable domain to your company's Cisco VCS Expressway. It must be a CA-level certificate name issued by a public CA that is supported by WebEx.

Note Self-signed certificates are NOT supported.

For a list of supported certificates and details on how to configure a certificate on Cisco VCS Expressway, refer to: Configure Certificates on Cisco Expressway-E and Cisco VCS Expressway.

Configure Traversal Zones for MCUs

This procedure details the configuration necessary in VCS to support MCUs that have encryption enabled (the default setting).

Caution If you choose not to do the following configuration, MCUs with encryption enabled will deliver the presentation content in the main video channel, instead of a separate stream.

Note In the following procedure, tasks for VCS Control are the same as for Expressway-C and tasks for Expressway-E or the same as for VCS Expressway.

To support MCUs that have encryption enabled, do the following

Procedure

Step 1 Set up a new traversal client zone from Cisco VCS Control to Cisco VCS Expressway.

Note Make sure the new zone uses a different port number.

Step 2 Configure the media encryption setting on the traversal client to be **Force unencrypted** or **Best effort**.

Step 3 On Cisco VCS Expressway, set up a new traversal server zone that connects to the Cisco VCS Control traversal zone set up in the previous step.

Step 4 In this new Cisco VCS Expressway traversal server zone, set media encryption to **Force unencrypted**.

Step 5 On Cisco VCS Control set up a search rule (at higher priority than the search rule that uses the default traversal zone) that matches WebEx traffic e.g. match = .*@example.webex.com

Note The above configuration ensures that whether the MCU encryption is enabled or not, that the video and the presentation stay on separate channels. It also ensures the content from WebEx is not encrypted when sent to the MCU (even though it is encrypted across the internet).

Configuring Cisco Unified Communications Manager

The following section describes the steps required for configuring Cisco Unified Communications Manager (Unified Communications Manager) for CMR Hybrid. This configuration also supports deployments where endpoints are registered to Unified Communications Manager only or both Unified Communications Manager and Cisco VCS Control/Cisco VCS Expressway.

This section describes the following tasks:

• Configuring a Routing Rule for Bridges Trunked to Unified Communications Manager, on page 9

Cisco Unified Communications Manager Configuration Prerequisites

To configure WebEx in Cisco Unified Communications Manager (Unified Communications Manager), the following are required:

- Unified Communications Manager 10.5(2)SU1 or SU2
- Endpoints in the network are registered to Unified Communications Manager
- Conferencing Bridge(s) to be used (MCU or Cisco TelePresence Server) are already operational within the network and trunked to Unified Communications Manager or registered to VCS
- Cisco Expressway-C or Cisco VCS Control is deployed in the private network
- To ensure optimum SIP audio and video connectivity between MCU and TelePresence Serverendpoints on Unified Communications Manager and the WebEx cloud, it is recommended to set region to permit a minimum of 2-4 Mbps.
- Cisco Expressway-E or Cisco VCS Expressway is configured with the DNS zone.

SIP Trunks Between Cisco Unified Communications Manager and Cisco Expressway-C or Cisco VCS Control

This section describes how to configure the Cisco Expressway Series X8.5 or later and Cisco Unified Communications Manager (Unified Communications Manager versions 10.5(2)SU1 or later) to interwork via a SIP trunk.

This is required for endpoints registered to Unified Communications Manager to participate in a Cisco Collaboration Meeting Rooms Hybrid meeting and to call endpoints registered to Cisco VCS Control. In addition, make sure that the Unified Communications Manager neighbor zone in Cisco VCS is configured with BFCP enabled.

The configuration steps are detailed in the Cisco Unified Communications Manager with Cisco VCS Deployment Guides at the following location:

http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

Configuring Early Offer for SIP Messaging

Configuring Early Offer is only required for a Unified CM-centric deployment, where bridges are trunked and endpoints are registered to Unified CM.

With Early Offer, the session initiator sends its capabilities in the SIP Invite and the called device chooses the preferred codec. Cisco recommends that all SIP trunks which carry TelePresence calls are configured for Early Offer.

Additionally, Early Offer is required from any direct scheduled bridges to Cisco Expressway or Cisco VCS to support CMR Hybrid calls. The entire path from the calling device to the service must be configured to support Early Offer.

Cisco VCS-centric deployments always run in Early Offer mode and this section is only relevant to Unified CM-centric deployments. It provides the recommended approach for configuring outbound trunks as Early Offer.

Note The default configuration for Unified CM trunks is Delayed Offer.

All trunks between the following Optimized Conferencing elements should be enabled for Early Offer. No media termination point (MTP) resources should be made available to these trunks, directly or indirectly:

- Unified CM to Cisco Expressway-C
- Unified CM to Cisco VCS Control
- Unified CM to TelePresence Server
- Unified CM to MCU
- Unified CM to Unified CM trunks which carry traffic originating from a TelePresence endpoint and any of the network elements listed above should also be enabled for Early Offer, with no media termination point (MTP) resources. For example, in a call flow scenario of EX90 >> UCM1 >> UCM2 >> Conductor >> TelePresence Server, the trunk between UCM1 >> UCM2 and the trunk between UCM2 >> Conductor should be enabled for Early Offer.

To restrict the use of MTPs, all MTP resources should be removed from all Session Management Edition (SME) clusters, and all MTP resources on Unified CM clusters should be placed in Media Resource Groups that are inaccessible both to TelePresence endpoints and to SIP trunks carrying TelePresence traffic.

Some specific points apply in various deployment scenarios:

Scenario 1. Configuring Early Offer in a single Unified CM system

Conference bridges are connected to the Cisco Unified Communications Manager, with Unified Communications Manager trunked to the Cisco Expressway. Endpoints are registered to the Unified Communications Manager. In this scenario the following trunks must be configured for Early Offer:

- Unified Communications Manager to Cisco Expressway-C
- Unified Communications Manager to the TelePresence Conductor

Scenario 2. Configuring Early Offer in a multi-cluster system (TelePresence Conductor connected to Unified Communications Manager SME)

One or more Unified Communications Manager SME clusters with connected leaf Unified CM clusters. The TelePresence Conductor and conference bridges are connected to the Unified Communications Manager SME. The Unified Communications Manager SME is trunked to the Cisco Expressway-C. In this scenario the following trunks must be configured for Early Offer:

- Unified Communications Manager SME to Cisco Expressway-C
- Unified Communications Manager SME to the TelePresence Conductor

Note In multi-cluster systems with three or more clusters, where one Unified CM cluster is a dedicated Unified Communications Manager SME, endpoints never register to the Unified Communications Manager SME but always to a leaf Unified CM cluster.

Scenario 3. Configuring Early Offer in a multi-cluster system (TelePresence Conductor connected to Unified Communications Manager SME)

One or more SME clusters with connected leaf Unified Communications Manager clusters. The conference bridges are connected to the leaf cluster(s). A single trunk connects the SME to the Cisco Expressway-C. In this scenario the following trunks must be configured for Early Offer:

- Unified Communications Manager SME to Cisco Expressway-C
- Leaf Unified Communications Manager clusters to the TelePresence Conductor
- Leaf Unified CM clusters to the Unified Communications Manager SME

Configuring Early Offer (and fallback to Delayed Offer) for SIP trunks

Procedure

Step 1 For each trunk, do one of the following depending on your Unified CM version:

- For Unified CM Version 10.5(2) systems, in the **Early Offer support for voice and video calls** dropdown, select Best Effort (no MTP inserted).

Step 2 Remove all MTP resources from the following elements:

- SME clusters (in the case of Unified Communications Manager SME deployments).
- All TelePresence endpoints and SIP trunks on all Unified CM clusters.

Step 3 Set **SIP Trunk DTMF Signaling Method** to RFC 2833 (the default).

Step 4 Enable the **Accept Audio Codec Preference in Received Offer** option on the following elements:

- All SME SIP trunks (in the case of Unified Communications Manager SME deployments).
- All SIP trunks that carry TelePresence calls on all Unified CM clusters.

Fallback to Delayed Offer

For outgoing calls, the default settings provide for automatic fallback to Delayed Offer in cases where no MTP resource exists. Without fallback, issues may arise in non-Optimized Conferencing areas of the network. For incoming calls, Early Offer is supported with no requirement for MTP resources.

Endpoints

Any TelePresence endpoints registered to Unified CM should be configured with a Media Resource Group List (MRGL) that does not contain any MTP resources. So that when the endpoints place a call that traverses one of the above trunk types an MTP will not be available within the MRGL of the endpoint.

Configuring a Routing Rule for Bridges Trunked to Unified Communications Manager

For Unified Communications Manager-centric deployments, it is required to set up a routing rule for any MCU or TelePresence Server trunked to Unified Communications Manager.

If your MCU or TelePresence Server is trunked to Unified CM, it will dial a long string of characters at your CMR Hybrid site (example: yoursite.webex.com)

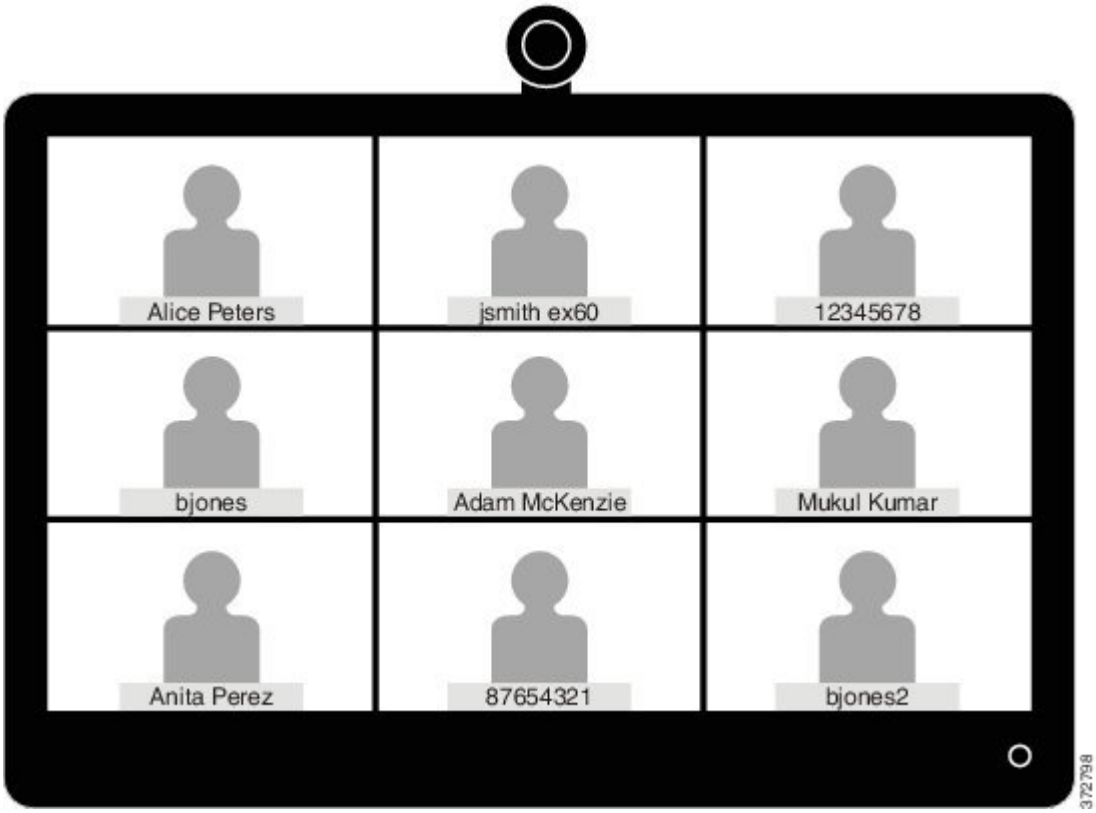
To ensure calls are routed correctly, set up a SIP routing pattern in Unified CM for your site to route to the SIP trunk for Expressway-C. For details, refer to the Unified CM documentation.

Also, make sure that the trunk for each MCU or TelePresence Server trunked to Unified CM has Early Offer enabled, as described in Configuring Early Offer for SIP Messaging, on page 6.

Provisioning Endpoint Display Names

Display names are used across endpoints such as TelePresence to identify a user to other participants.

Figure 1: Display Names Example



The preferred format for this name is to use the first name and last name of the user, for example Alice Peters, or the canonical name of the conference room where the endpoint is installed, such as MDR21-3-#120 (room 120 on the 3rd floor of building 21 in Madrid). However if this name is not explicitly provisioned then the system will choose the display name based on the SIP URI or device number of the endpoint. The result that is displayed will depend on how the particular users and rooms have been provisioned. This can lead to inconsistencies in the names displayed on a conference call, with the individual user information being displayed in different formats, as shown in the example above.

To ensure that names display consistently, these settings need to be provisioned in Unified CM and/or in Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) for Cisco VCS registered endpoints.

If the endpoints you want to provision are Unified CM registered, see Provisioning Display Names on Unified CM, on page 11. If the endpoints you want to provision are Cisco VCS registered, see Provisioning Display Names on Cisco VCS, on page 13.

Provisioning Display Names on Unified CM

This section describes how to update display names in the Cisco Unified CM Administration user interface. It describes how users, devices, and lines are configured in order to allow an administrator to identify the correct fields and locations in which to make those updates, so that the names display correctly. The section titled Trunks, on page 12 describes some optional advanced settings that may be useful to some users.

Users and Devices

On the Cisco Unified CM Administration user interface new users are configured in the User Management > End User window. It is possible to both create new users or to import them through Active Directory (AD) or LDAP.

New devices are configured in the **Device > Phone** window. Users are then associated to a device. The details supplied during this configuration will not be used for display name purposes. The display name must be manually configured on the line under **Call routing > Directory Number**, or by selecting the line configured on the endpoint under **Device > Phone > Line#**.

Line

Display names are configured on the line that is associated with the device. In this way, the display name is set for a particular device to which that user is associated. In the case of shared lines, it is possible to set different display names on each appearance of the shared line. However, it is recommended that the same display name be used across all devices using the first name and the last name of the user or the name of the conference room.

Set Display Names for Unified CM Registered Endpoints using Bulk Administration

Bulk Administration can be used to set the display names for Unified Communications Manager registered endpoints for large numbers of users.

Before You Begin

Ensure that you have users configured and associated to devices. For more information on provisioning users, see Cisco Unified Communications Manager Administration Guide, Release 10.0(1).

Procedure

Step 1 To export user records, see Export User Records in Cisco Unified Communications Manager Cisco Unified Communications Manager Administration Guide, Release 10.0(1).

Step 2 In the CSV file you have downloaded, copy the first name and last name columns into a new CSV file.

Step 3 To upload this CSV file to the correct device, see Update phones using custom file in Cisco Unified Communications Manager Administration Guide, Release 10.0(1).

Manually Set Display Names for Unified CM Registered Endpoints

This procedure explains how to configure the display name for a device that is registered to Unified Communications Manager, whether the device is assigned to a user who is associated with a device, or the device is a shared conference room device.

Before You Begin

Ensure that you have users configured and associated to devices. For more information on provisioning users, see Cisco Unified Communications Manager Administration Guide, Release 10.0(1).

Procedure

Step 1 Log in to the Cisco Unified CM Administration user interface and choose **Device > Phone** to go to the Find and List Phonewindow.

Step 2 Choose the **Device Name(Line)** for the device you want to configure to get to the Phone Configuration window for that device.

Step 3 Choose the line for the device from the Association area on the left hand side of the window. This brings you to the Directory Number Configuration window.

Step 4 In the *Directory Number Information* area, enter the display name in the **Alerting name** and **ASCII (Caller ID)** fields. **Note:** This will be used to display the user's name when communicating with devices that are not in the Unified Communications Manager cluster.

Step 5 In the Line 1 on Device area, enter the display name in the **Display (Caller ID)** and **ASCII Display (Caller ID)** fields. **Note:** This will appear on devices which are on the same cluster as the Cisco Unified CM.

Step 6 If this is a shared line, to ensure changes appear on all devices, check the **Update Shared Device Settings** check box, and click **Propagate selected**. **Note**: Cisco recommends that the display name set in the Alerting Name, ASCII Alerting Name, Display (Caller ID) and ASCII Display (Caller ID) field be the user's full name (for example First Name Last Name), for devices that are associated with a user, or the name of the conference room for endpoints that are in shared conference room spaces.

Step 7 Click **Save**.
The changes are automatically propagated and will take effect immediately, unless the endpoint is on an active call, in which case they will take effect immediately after the active call has ended.

Trunks

If required, the following features can also be configured to further control the behavior of display names. These settings are on the Trunk Configuration window.

- In the Device Information area, checking the **Transmit UTF-8 for Calling Party Name** check box will transmit the ASCII Alerting Name on devices that support UTF-8.
- It is possible to hide display names on a per-trunk basis. This is done in the Inbound Calls area by selecting Restricted from the **Connected Name Presentation** drop-down list.
- In the Caller Information area, individual device display names can also be overridden by setting the **Caller Name** field.

Provisioning Display Names on Cisco VCS

On Cisco VCS there are two methods which can be used to provision display names.

In the first method, Display Names are provisioned using FindMe templates. This method is used to provision individual users. Each template contains the details for each individual user, including their Display Name.

In the second method, Display Names are provisioned using the Direct Manage method. This method is used to provision Conference Room endpoints. This means that each Display Name is individually provisioned for each Conference Room endpoint on the endpoint itself.

FindMe

FindMe is a Cisco TMSPE feature which allows users to specify which video and audio devices should ring when someone calls their ID. As a result, a single ID can be used to reach multiple devices which are associated with that ID.

In FindMe the administrator provisions users with FindMe accounts and provisioning templates that contain attributes, including the display name. Users can be newly added or imported using AD or LDAP.

For more information on FindMe, see Deploying FindMe in Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide.

Setting Caller ID Display Names for Cisco VCS Users

This section describes how to manually set display names for Cisco VCS FindMe users.

Note If you are dealing with large numbers of users we recommend that you import their details using Active Directory or LDAP. Using this method, user display names are imported and set automatically.

Before You Begin

Ensure that you have installed and provisioned Cisco TMSPE. See Configuring Cisco VCS for provisioning, Installing Cisco TMSPE, and Setting up users and provisioning in Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide.

Procedure

Step 1 Log in to Cisco TMS, go to **Systems** > **Provisioning** > **Users**.

Step 2 In the **User Settings** pane, click **Edit**. The **User Settings** dialog box opens.
In the **Display Name** field, enter the first name and last name of the user. **Note**: If the user has been imported using LDAP, the Display Name will be already associated with the user.

Setting Caller ID Display Names for Conference Rooms

Procedure

Step 1 Log in to Cisco TMS, go to **Systems** > **Provisioning** > **Users**.

Step 2 In the Navigator, choose the conference room you want to update from the pane on the left side of the window.

Step 3 Choose the Address of the endpoint that you want to configure. This will bring you to the user interface of the endpoint that you have chosen.

Step 4 Choose **Configuration** > **System Configuration**, and search for the word 'display' using the search field on the left side of the window.

Step 5 Enter the Display Name in the **Profile 1 DisplayName** field. **Note:** Steps 4 and 5 may vary depending on the endpoint model you have chosen.

Step 6 Click **Save**.