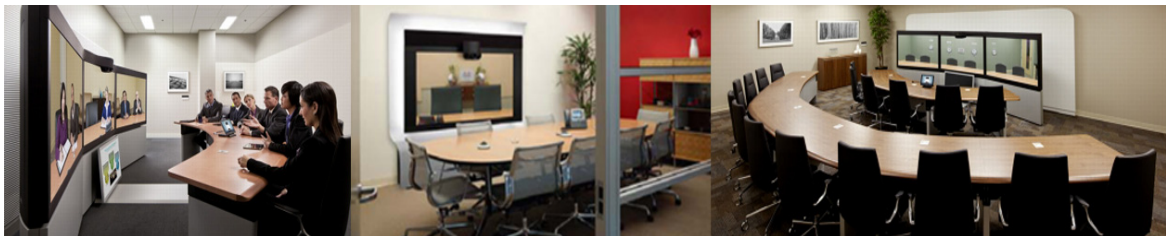

CHAPTER 4

Configuring Call Control

Revised: October 2013

Introduction

This chapter describes how to configure call control for Cisco WebEx Enabled TelePresence meetings.

To begin using Cisco WebEx Enabled TelePresence, you must configure the call control product(s) used in your video network.

There are three possible call control scenarios:

- Cisco TelePresence VCS Control and Expressway

  Endpoints are registered to VCS Control and/or Expressway only.
- Cisco Unified CM with VCS Control and Expressway

  Endpoints are registered to Unified CM only.
- Cisco TelePresence VCS Control and Expressway with Unified CM

  Endpoints are registered to VCS Control/Expressway and Unified CM.

Note Using Unified CM as the call control solution requires VCS Control and Expressway to be deployed in order to communicate with WebEx, regardless of whether endpoints are registered to VCS Control and Expressway or not.

Configuring Cisco TelePresence Video Communication Server Control and Expressway

The following section describes the steps required for configuring Cisco TelePresence Video Communication Server Control and Expressway for Cisco WebEx Enabled TelePresence.

This section describes the following tasks:

Prerequisites

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

- Cisco TelePresence Video Communication Server (VCS) must be running firmware X7.2.2 or a later release.
- Endpoints in the network are registered to VCS Control or Expressway and/or Unified CM

  Note If endpoints are registered to Unified CM, you must configure a SIP trunk between Unified CM and VCS Control. For more information, refer to Configuring Cisco Unified Communications Manager, page 4-5.

- Expressway must be assigned a static IP address
- Firewall must have port 5061 open to allow access to Expressway
  - **If this port is not configured correctly, calls will not take place correctly.**
- Conferencing Bridge(s) to be used (MCU or TelePresence Server) are already operational within the network
- VCS Control is in the private network
- VCS Expressway 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 1.1 Mbps for WebEx calls. For more information about bandwidth controls, please refer to the Cisco VCS Administrator Guide at:

  http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/admin_guide/Cisco_VCS_Administrator_Guide_X7-2.pdf
- VCS Control is configured as the SIP Registrar/H.323 gatekeeper.

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

  Configuring VCS as a SIP registrar is done by configuring one or more SIP domains. The VCS 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 VCS Control, refer to the "Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide" at:

  https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-2.pdf
- 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 H323 SRV records in place that resolve to the VCS Expressway for your configured SIP Domain so TelePresence participants can route to your VCS Expressway.

Creating a New DNS Zone on VCS Expressway for WebEx

By default, a VCS solution will handle local domains, and route calls to non-local domains to the VCS Expressway to route them to the Internet via a DNS zone.

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

To configure the VCS Expressway for Cisco WebEx Enabled TelePresence, do the following:

Step 1 Create a new DNS zone:

a. Set H.323 to **Off**.

b. Set SIP Media encryption mode to **Force encrypted**.

c. Turn on TLS Verify mode.

d. In the TLS verify subject name field, enter **sip.webex.com**.

e. 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: https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-1.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 VCS Expressway. It must be a CA-level certificate name issued by a public CA that is supported by WebEx. For a list of supported public CAs, see the list below.

Note Self-signed certificates are NOT supported.

WebEx supports only the following certificates that use SHA-1 encryption issued by common certificate authorities. SHA-2 is not currently supported. You must choose one of the following certificates or the call from VCS Expressway will not be authorized by WebEx:

- entrust_ev_ca

- digicert_global_root_ca
- verisign_class_2_public_primary_ca_-_g3
- godaddy_class_2_ca_root_certificate
- Go Daddy Root Certification Authority - G2
- verisign_class_3_public_primary_ca_-_g5
- verisign_class_3_public_primary_ca_-_g3
- dst_root_ca_x3
- verisign_class_3_public_primary_ca_-_g2
- equifax_secure_ca
- entrust_2048_ca
- verisign_class_1_public_primary_ca_-_g3
- ca_cert_signing_authority
- geotrust_global_ca
- globalsign_root_ca
- thawte_primary_root_ca
- geotrust_primary_ca
- addtrust_external_ca_root

Note This list may change over time. For the most current information, contact WebEx.

For details on how to configure a certificate, refer to: Chapter 5, "Configuring Certificates on Cisco VCS Expressway".

Configuring Traversal Zones for MCUs with Encryption Enabled

This section 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.

To support MCUs that have encryption enabled, do the following

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

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

Step 2 On VCS Expressway, set up a new traversal server zone that connects to the VCS Control traversal zone set up in the previous step.

Step 3 In this new VCS Expressway traversal server zone, set media encryption to **Force unencrypted**.

Step 4 On 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 CM) for Cisco WebEx Enabled TelePresence. This configuration also supports a deployments where endpoints are registered to Unified CM only or both Unified CM and VCS Control/Expressway.

This section describes the following tasks:

- Prerequisites, page 4-5
- Configuring a SIP Trunk Between Unified CM and VCS Control, page 4-5

Prerequisites

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

- Cisco Unified CM 8.6.2 or 9.1.1.
- Endpoints in the network are registered to Unified CM
- Conferencing Bridge(s) to be used (MCU or TelePresence Server) are already operational within the network and registered to VCS
- VCS Control is deployed in the private network
- To ensure optimum SIP audio and video connectivity between MCU and TelePresence Server and the WebEx cloud, it is recommended to set region to permit a minimum of 1.3 Mbps.
- VCS expressway configured with the DNS zone.

Configuring a SIP Trunk Between Unified CM and VCS Control

This section describes how to configure the Cisco TelePresence Video Communication Server (Cisco VCS) version X7.2.1 or later and Cisco Unified Communications Manager (Unified CM versions 6.1, 7 or 8 to interwork via a SIP trunk.

This is required for endpoints registered to Unified CM to participate in a Cisco WebEx Enabled TelePresence meeting and to call endpoints registered to VCS Control. In addition, make sure that the Unified CM neighbor zone in Cisco VCS is configured with BFCP enabled.

The configuration steps are detailed in the Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide at the following location:

Cisco VCS and Unified CM Deployment Guide (Unified CM 8.6.x, 9.x and VCS X7.2).