



# Cisco Unified Communications Manager v6.1, 7 and 8

Cisco TelePresence Deployment Guide

---

Cisco VCS X6  
SIP trunk

D14602.07

June 2011

# Contents

<b>Document revision history .....</b>	<b>5</b>
<b>Introduction .....</b>	<b>6</b>
Objectives and intended audience .....	6
Deployment scenario.....	6
Summary of configuration process.....	7
Prerequisites for system configuration .....	7
<b>Enabling calls between endpoints registered on the Cisco VCS Control.....</b>	<b>8</b>
Cisco VCS Control configuration.....	8
Set up the SIP domain of the Cisco VCS Control .....	8
Check the Traversal Subzone configuration .....	9
Create transforms.....	9
CUCM configuration .....	11
Registering endpoints to the Cisco VCS Control .....	11
Endpoint configuration.....	11
Confirming registrations .....	11
Test calls .....	11
<b>Enabling calls between endpoints registered on CUCM .....</b>	<b>12</b>
Cisco VCS Control configuration.....	12
CUCM configuration .....	12
Configure the SIP Profile.....	12
Add a phone device.....	14
Device directory number configuration.....	14
Configure phone endpoint to pick up its configuration from CUCM.....	14
Confirming registrations .....	15
Test calls.....	15
<b>Enabling endpoints registered on Cisco VCS Control to call endpoints registered on CUCM .....</b>	<b>16</b>
CUCM configuration .....	16
Configure the SIP Trunk security profile .....	16
Configure the SIP Trunk device .....	17
Cisco VCS Control configuration.....	20
Create a neighbor zone for CUCM.....	20
Create a search rule to route calls to the CUCM neighbor zone .....	21
Create a transform that converts number@<IP address of cucm> to number@vcs.domain .....	23
Test calls.....	23
<b>Enabling endpoints registered on CUCM to call endpoints registered on the Cisco VCS Control .....</b>	<b>24</b>
Cisco VCS Control configuration.....	24
Set up a search rule for CUCM to call the Cisco VCS Local Zone .....	24
CUCM configuration .....	26
Allow numeric dialing from Cisco phones to Cisco VCS.....	26
Test calls.....	27

<b>Appendix 1 – Troubleshooting.....</b>	<b>28</b>
Problems connecting Cisco VCS Control local calls .....	28
Look at “Search history” to check the applied transforms .....	28
Look at “Call history” to check how the call progressed.....	29
Check for errors.....	29
Event Log .....	29
Real time detailed event log .....	29
Tracing calls .....	29
Tracing calls at SIP / H.323 level .....	29
H.323 to SIP CUCM calls do not work .....	29
422 Session Timer too small.....	29
Cisco VCS reports SIP decode error.....	30
CUCM 5 and 6.....	30
CUCM 7.....	31
In-call problems .....	31
Calls remain up for a maximum of 15 minutes.....	31
Calls clear down when a call transfer from a video phone on CUCM transfers a call to Cisco VCS .....	31
Taking a trace on CUCM using RTMT .....	31
Configure CUCM to enable tracing .....	31
Installing RTMT – Real Time Monitoring Tool.....	31
Running RTMT .....	32
Taking a trace using RTMT .....	32
<b>Appendix 2 – Known interworking capabilities and limitations .....</b>	<b>33</b>
Capabilities .....	33
SIP and H.323 endpoints making basic calls .....	33
Limitations .....	33
E20 encryption .....	33
T150 running L6.0 code .....	33
H.323 MXP and 9971 .....	33
<b>Appendix 3 – Benefits of using Cisco VCS with CUCM.....</b>	<b>34</b>
Separate management and operation of video systems and CUCM telephony systems.....	34
Duo Video .....	34
Bandwidth management.....	34
FindMe™ .....	34
<b>Appendix 4 – Allow dialing to Cisco VCS domain from Cisco phones .....</b>	<b>35</b>
<b>Appendix 5 – Connecting CUCM to a cluster of Cisco VCS peers .....</b>	<b>36</b>
Configuring the trunk to VCS to specify the DNS SRV address for the VCS cluster.....	36
Configuring the trunk to VCS to specify a list of VCS peers .....	37
<b>Appendix 6 – Connecting Cisco VCS to a cluster of CUCM nodes .....</b>	<b>38</b>
Configuration for Cisco VCS to use a DNS Zone to contact a cluster of CUCM nodes .....	38
CUCM configuration .....	38
DNS Server configuration.....	38
Cisco VCS Control configuration.....	38
<b>Appendix 7 – Cisco TelePresence Multiway™ and CUCM .....</b>	<b>41</b>

---

<b>Appendix 8 – Endpoint specific configuration .....</b>	<b>42</b>
T150 running L6.x.....	42
Other products .....	42
<b>Appendix 9 – Advanced parameters set by the “Cisco Unified Communications Manager” zone profile .....</b>	<b>43</b>
<b>Appendix 10 – CUCM 5 incompatibility.....</b>	<b>44</b>
<b>Appendix 11 – Connecting Cisco VCS to CUCM using TLS (rather than TCP).....</b>	<b>45</b>
Ensure that CUCM trusts the Cisco VCS server certificate .....	45
Configure a SIP trunk security profile on CUCM .....	45
Update the CUCM trunk to Cisco VCS to use TLS .....	46
Update the Cisco VCS neighbor zone to CUCM to use TLS .....	46
Verify that the TLS connection is operational.....	47
<b>Appendix 12 – Characters allowed in SIP URIs.....</b>	<b>48</b>

## Document revision history

The following table summarizes the changes that have been applied to this document.

Revision	Date	Description
1	January 2010	Initial release.
2	April 2010	Updated for Cisco VCS X5.1 Additional troubleshooting information.
3	June 2010	Added Appendix 10 - Connecting Cisco VCS to CUCM using TLS.
4	July 2010	Document title updated to refer to Cisco Unified Communications Manager. Added this document revision history table. General updates applied to reflect user interface differences in CUCM v8.
5	October 2010	Additions for Clustered CUCMs. Additions to handle returning call to CUCM callback URI. Updates to handle call transfer.
6	March 2011	Updates to Appendix 5 for CUCM version 8.5 regarding connecting CUCM to a cluster of Cisco VCS peers. Added Appendix 12 – Characters allowed in SIP URIs.
7	June 2011	Updated for Cisco VCS X6.

# Introduction

## Objectives and intended audience

This deployment guide provides guidelines on how to configure the Cisco TelePresence Video Communication Server (Cisco VCS) version X6 and Cisco Unified Communications Manager (CUCM) versions 6.1, 7 or 8 to interwork via a SIP trunk.

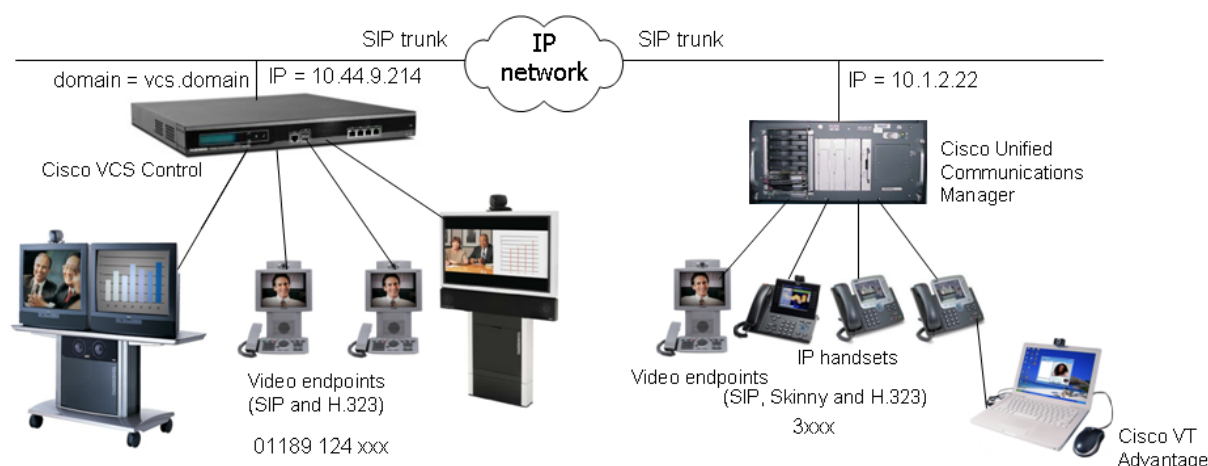
Other ways that Cisco VCS and CUCM can be connected to allow them to interwork include:

- ▶ use of an H.323 trunk
- ▶ configuring CUCM to register to the Cisco VCS as a gateway (typically used with CUCM version 4.1 and earlier)

## Deployment scenario

A company already has CUCM running their telephone system. They want to integrate this with a Cisco VCS Control which connects their existing (or new) video conferencing systems, so that voice and video terminals can communicate with one another across one unified network.

The existing telephone system uses telephone numbers to specify who to call. This functionality is to be extended into the video system, so that all endpoints will be contactable by telephone numbers.



For the purposes of this example, endpoints connected to the CUCM are identified by their extension numbers **3xxx** and endpoints connected to the Cisco VCS Control are identified by telephone numbers **01189 124 xxx**. 4-digit extension number dialing and full 11-digit dialing of endpoints registered to the Cisco VCS Control are supported.

CUCM and the Cisco VCS Control are connected together using a SIP trunk across an IP network; the Cisco VCS Control domain is **vcs.domain**. Calls sent to CUCM need the domain portion to be `<ip address of cucm>`; calls from CUCM to Cisco VCS will arrive with the domain portion set as `<ip address of vcs>:5060`

It is assumed that the Cisco VCS Control is running version X6 or later code and has at least the following option keys installed:

- ▶ H323-SIP interworking
- ▶ Traversal calls
- ▶ Non-traversal calls

It is assumed that CUCM is running IOS v6.1, 7 or 8.

## Summary of configuration process

This document specifies how to configure both the CUCM (IOS v6.1, 7 or 8) and the Cisco VCS Control so that calls can be made:

- ▶ from video endpoints connected to the Cisco VCS to other video endpoints connected to that same Cisco VCS
- ▶ from IP handsets or other devices connected to CUCM to other IP handsets or devices connected to that same CUCM
- ▶ from video endpoints connected to the Cisco VCS to IP handsets or other devices connected to CUCM
- ▶ from IP handsets or other devices connected to CUCM to video endpoints connected to the Cisco VCS

The configuration process describes each of these stages separately, so that individual stages can be implemented and tested before moving on to the next.

## Prerequisites for system configuration

Before using this document to configure the Cisco VCS Control and CUCM to interwork, make sure that the following is configured and operational:

- ▶ CUCM contains a basic configuration and has already set up at least:
  - System > Server
  - System > Cisco Unified CM
  - System > Cisco Unified CM Group
  - System > Date / Time Group
  - System > Presence Group
  - System > Region
  - System > Device Pool
  - System > DHCP
  - System > Location
  - System > Physical location
  - System > Enterprise parameters
  - System > Licensing
- ▶ The Cisco VCS Control is configured with IP address, DNS and NTP information, and is accessible for management via its web browser interface. See document D14524 *Basic configuration - Single Cisco VCS Control* deployment guide.

# Enabling calls between endpoints registered on the Cisco VCS Control

## Cisco VCS Control configuration

Configuration of the Cisco VCS Control to enable calls to be made between devices that register to it can be broken down into the following steps:

1. Set up the SIP domain of the Cisco VCS Control. This is needed for SIP registration.
2. Check the Traversal Subzone configuration. The Traversal Subzone handles the interworking of H.323 endpoints with SIP endpoints.
3. Create transforms to:
  - Ensure that domain information is added to dialed numbers that do not have it. This forces dialed number information from SIP and H.323 endpoints into a common format: number@domain
  - Expand 4-digit Cisco VCS extension numbers (4xxx) to full 11-digit numbers. Both SIP and H.323 endpoints will register on the Cisco VCS Control with a URI (H323 ID) in the format **11\_digit\_number@domain** (that is, their full 11-digit telephone number followed by domain information). The transforms will convert 4-digit (4xxx) or 11-digit numbers, with or without domain information to be transformed into the correct 11-digit URI format for routing. Calls to 3xxx will be formatted to 3xxx@domain.

## Set up the SIP domain of the Cisco VCS Control

SIP endpoints register with the Cisco VCS Control with an AOR (Address Of Record) in the format **11\_digit\_number@vcs.domain**. The Cisco VCS Control must be configured with the SIP domain information so that it will accept these registrations.

1. Go to **VCS configuration > Protocols > SIP > Domains**.
2. Click **New**.
3. Configure the field as follows:

Name	Required domain, for example vcs.domain
------	---

4. Click **Create Domain**.

The screenshot shows the 'Create domain' configuration page in the Cisco VCS Control web interface. The navigation bar includes 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The breadcrumb trail indicates the current path: 'VCS configuration > Protocols > SIP > Domains > Create domain'. The main form area is titled 'Create domain' and has a 'Configuration' tab selected. There is a 'Name' field with a red asterisk indicating it is required, and a 'Create domain' button at the bottom left.



## Check the Traversal Subzone configuration

- Go to **VCS configuration > Local Zone > Traversal Subzone**.
  - Port ranges can be left at default values (50000 to 52399), or can be configured as required (see the “Zones and Neighbors” section of the *Cisco VCS Administrator Guide* for further details).
  - Bandwidth values can be left at default values (Unlimited), or can be configured as required (see the “Bandwidth Control” section of the *Cisco VCS Administrator Guide* for further details).
- Click **Save**.

Traversal Subzone status	
Number of registrations	0
Number of calls	0
Bandwidth used on this VCS	0 kbps
Total bandwidth used across this cluster	0 kbps

## Create transforms

In this deployment scenario, users want to be able to dial other endpoints registered to the Cisco VCS Control using either an 11-digit E.164 number (01189 124 xxx) or a 4-digit extension number (4xxx). CUCM endpoints are to be dialed using a 4 digit number (3xxx). This dialing model can be supported by H.323 (if the endpoint registers both 4-digit and 11-digit E.164 aliases), however, SIP does not support dialing by numbers alone. If a number (without a domain appended) is dialed from a SIP endpoint the endpoint will automatically append its own domain.

For consistency with both SIP and H.323 dialing, this deployment scenario always uses the URI form for routing calls (that is, **dialed\_digits@domain**).

For call requests received by the Cisco VCS Control the dialed number:

- ▶ may or may not include the first 7 digits of the 11-digit (Cisco VCS registered endpoint) number - (not included when just the 4-digit extension number is dialed)
- ▶ will always have the last 4 digits (extension number part) of the dialed number that identifies the specific endpoint to route to
- ▶ may or may not include a domain - (only included when a SIP endpoint is making the call)

Transforms are needed to ensure that the dialed number (in whatever format it is received) is transformed into a consistent form, in this case:

- ▶ domain added (i.e. **dialed\_digits@domain**).  
(In this example the **domain** to be appended, is the Cisco VCS Control's domain **vcs.domain**.)

- ▶ calls to 4xxx have the prefix 0118912 added to convert them to a full 11 digit number

To achieve this, two regex expressions are used:

- ▶ `(4\d{3})(@vcs.domain)?` transforms to `0118912\1@vcs.domain`
- ▶ `([^\@]*)` transforms to `\1@vcs.domain`

(In the first, a 4xxx number with or without '@vcs.domain' is transformed to 01189124xxx@vcs.domain, in the second any dialed information which does not contain a domain – does not contain an '@' – has the '@vcs.domain' added.)

See the Regular Expression Reference in the Appendices section of the *Cisco VCS Administrator Guide* for further details, or alternatively search the world wide web for the term "Regular Expression".

#### To create the first transform:

1. Go to **VCS configuration > Dial plan > Transforms**.
2. Click **New**.
3. Configure the fields as follows:

<b>Priority</b>	1
<b>Description</b>	"4 to 11 digit dialing" for example
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	<code>(4\d{3})(@vcs.domain)?</code>
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	<code>0118912\1@vcs.domain</code>
<b>State</b>	<i>Enabled</i>

4. Click **Create transform**.

The screenshot shows the 'Create transform' form in the Cisco VCS Administrator interface. The form is titled 'Create transform' and has a breadcrumb trail: 'You are here: VCS configuration > Dial plan > Transforms > Create transform'. The form fields are as follows:

- Priority:** 1
- Description:** 4 to 11 digit dialing
- Pattern type:** Regex
- Pattern string:** `(4\d{3})(@vcs.domain)?`
- Pattern behavior:** Replace
- Replace string:** `0118912\1@vcs.domain`
- State:** Enabled

At the bottom of the form, there are two buttons: 'Create transform' and 'Cancel'.

#### To create the second transform:

1. Go to **VCS configuration > Dial plan > Transforms**.
2. Click **New**.
3. Configure the fields as follows:

<b>Priority</b>	2
<b>Description</b>	"add domain where none exists" for example
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	<code>([^\@]*)</code>
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	<code>\1@vcs.domain</code>
<b>State</b>	<i>Enabled</i>

#### 4. Click **Create transform**.

The screenshot shows the 'Create transform' configuration page in the Cisco VCS Control interface. The page has a navigation bar at the top with 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. Below the navigation bar, there's a breadcrumb trail: 'You are here: VCS configuration > Dial plan > Transforms > Create transform'. The main configuration area is titled 'Configuration' and contains the following fields:

- Priority:** 2
- Description:** add domain where none exists
- Pattern type:** Regex
- Pattern string:** \*([0-9]\*)
- Pattern behavior:** Replace
- Replace string:** 11@vcs.domain
- State:** Enabled

At the bottom of the form, there are two buttons: 'Create transform' and 'Cancel'.

## CUCM configuration

No configuration is required on CUCM for the Cisco VCS Control to route calls between endpoints registered locally to the Cisco VCS Control.

## Registering endpoints to the Cisco VCS Control

### Endpoint configuration

For H.323, configure the endpoints as follows:

- ▶ H.323 ID (for example 01189124000@vcs.domain, 01189124001@vcs.domain and so on)
- ▶ H.323 Call Setup = Gatekeeper
- ▶ Gatekeeper IP address = IP address of the Cisco VCS Control

For SIP, configure the endpoints as follows:

- ▶ SIP Address (URI) (for example 01189124000@vcs.domain, 01189124001@vcs.domain and so on)
- ▶ Server Address (Proxy address) = IP address of the Cisco VCS Control

### Confirming registrations

Registration status can be confirmed by checking the Cisco VCS Control via **Status > Registrations**.

By default the Cisco VCS Control will accept all H.323 registrations and all SIP registrations within the specified SIP domain. It is possible to limit registrations by explicitly allowing or denying individual registrations. See the "Cisco VCS Configuration" section of the *Cisco VCS Administrator Guide* for further details.

### Test calls

Make some test calls using both 4-digit dialing and 11-digit dialing.

Your call history can be seen on the Cisco VCS Control via **Status > Call history**.

# Enabling calls between endpoints registered on CUCM

## Cisco VCS Control configuration

No configuration is required on the Cisco VCS Control for CUCM to route calls between endpoints registered locally to the CUCM.

## CUCM configuration

The configuration of CUCM and Cisco phones to enable calls to be made between the phones consists of setting up a SIP Profile, specifying the phones on CUCM, giving the phones phone numbers and getting the phones to load their configuration. This comprises the following steps:

- ▶ Configure the SIP Profile.
- ▶ Add a phone device: add the new phone device to the list of supported endpoints on CUCM.
- ▶ Configure the device directory number: specify the telephone number that will cause this phone endpoint to ring.
- ▶ Configure the phone endpoint to pick up its configuration from CUCM. Then reboot the phone to activate the configuration process.

## Configure the SIP Profile

1. On CUCM, go to **Device > Device Settings > SIP Profile**.
2. Click **Add New**.
3. Configure the fields as follows:

<b>Name</b>	Standard SIP Profile
<b>Default MTP Telephony Event Payload Type</b>	101
<b>Timer Invite Expires</b>	180
<b>Timer Register Delta</b>	5
<b>Timer Register Expires</b>	3600
<b>Timer T1</b>	500
<b>Timer T2</b>	Leave as default (typically 4000 or 5000)
<b>Retry INVITE</b>	6
<b>Retry non-INVITE</b>	10
<b>Start Media Port</b>	16384
<b>Stop Media Port</b>	32766
<b>Call Pickup URI</b>	x-cisco-serviceuri-pickup
<b>Call Pickup Group Other URI</b>	x-cisco-serviceuri-opickup
<b>Call Pickup Group URI</b>	x-cisco-serviceuri-gpickup
<b>Meet Me Service URI</b>	x-cisco-serviceuri-meetme
<b>User Info</b>	None
<b>DTMF DB Level</b>	Nominal

<b>Call Hold Ring Back</b>	Off
<b>Anonymous Call Block</b>	Off
<b>Caller ID Blocking</b>	Off
<b>Do Not Disturb Control</b>	User
<b>Telnet Level for 7940 and 7960</b>	Disabled
<b>Timer Keep Alive Expires</b>	120
<b>Timer Subscribe Expires</b>	120
<b>Timer Subscribe Delta</b>	5
<b>Maximum Redirections</b>	70
<b>Off Hook To First Digit Timer</b>	15000
<b>Call Forward URI</b>	x-cisco-serviceuri-cfwdall
<b>Abbreviated Dial URI</b>	x-cisco-serviceuri-abbrdial
<b>Reroute Incoming Request to new Trunk based on</b>	Never

**Cisco Unified CM Administration** For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration  CMAdministrator | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

**SIP Profile Configuration** Related Links: [Back To Find/List](#)

**Status**

Status: Ready

**SIP Profile Information**

Name\*

Description

Default MTP Telephony Event Payload Type\*

☐ Redirect by Application

☐ Disable Early Media on 180

**Parameters used in Phone**

Timer Invite Expires (seconds)\*

Timer Register Delta (seconds)\*

Timer Register Expires (seconds)\*

Timer T1 (msec)\*

Timer T2 (msec)\*

Retry INVITE\*

Retry Non-INVITE\*

Start Media Port\*

Stop Media Port\*

Call Pickup URI\*

Call Pickup Group Other URI\*

Call Pickup Group URI\*

Meet Me Service URI\*

User Info\*  ▾

DTMF DB Level\*  ▾

Call Hold Ring Back\*  ▾

Anonymous Call Block\*  ▾

Caller ID Blocking\*  ▾

Do Not Disturb Control\*  ▾


Telnet Level for 7940 and 7960\*  ▾

Timer Keep Alive Expires (seconds)*	120
Timer Subscribe Expires (seconds)*	120
Timer Subscribe Delta (seconds)*	5
Maximum Redirections*	70
Off Hook To First Digit Timer (milliseconds)*	15000
Call Forward UR1*	x-cisco-serviceuri-cfwdall
Abbreviated Dial UR1*	x-cisco-serviceuri-abbrdial
<input checked="" type="checkbox"/> Conference Join Enabled <input type="checkbox"/> RFC 2543 Hold <input checked="" type="checkbox"/> Semi Attended Transfer <input type="checkbox"/> Enable VAD <input type="checkbox"/> Stutter Message Waiting <input type="checkbox"/> Call Stats	

<b>Trunk Specific Configuration</b>	
Reroute Incoming Request to new Trunk based on*	Never

 \*- indicates required item.

## Add a phone device

1. Go to **Device > Phone**.
2. Click **Add New**.
3. Configure as required.
4. Click **Save**.

Alternatively, if there is already another phone configured, copy its configuration by selecting “super copy”, entering the new phone’s MAC address and then changing the description (especially correct the MAC address part of the description).

## Device directory number configuration

1. Go to **Device > Phone**.
2. Select the relevant device name.
3. On the left hand side, select a line.
4. Set up the required directory number (for this example use a 3xxx number).

## Configure phone endpoint to pick up its configuration from CUCM

On the Cisco phone:

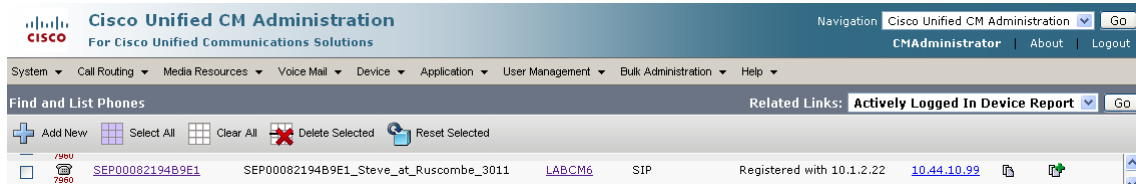
1. Press the **settings** button.
2. Select the Network Configuration section, and check whether the **TFTP Server** is the IP address of CUCM. If not:
  - a. Press the **settings** button twice – to return to SETTINGS menu.
  - b. Select **Unlock** and enter the appropriate password.
  - c. Select the Network Configuration section.
  - d. Set **Alternate TFTP** = YES.
  - e. Set **TFTP Server** = <IP address of CUCM>.
  - f. Select **Accept**.
  - g. Select **Save**.
3. Reboot the phone (unplug and re-connect the power).

The phone should now indicate that Line 1 is the phone number specified on CUCM (for example 3001).

Calls can now be made between handsets registered on CUCM.

## Confirming registrations

Registration status of phones connected to CUCM can be seen on the **Device > Phone** page.



## Test calls

Make some test calls by dialing the numbers of the registered phones (for example, 3001).

# Enabling endpoints registered on Cisco VCS Control to call endpoints registered on CUCM

## CUCM configuration

Configuration of CUCM to enable calls to be made between devices that register to it can be broken down into 2 steps:

- ▶ Configure the SIP Trunk security profile.
- ▶ Configure the SIP Trunk device.

### Configure the SIP Trunk security profile

1. On CUCM, go to **System > Security > SIP Trunk Security profile**.
2. Click **Add New**.
3. Configure the fields as follows:

<b>Name</b>	Non Secure SIP Trunk Profile
<b>Device Security Mode</b>	Non Secure
<b>Incoming Transport Type</b>	TCP+UDP
<b>Outgoing Transport Type</b>	TCP
<b>Incoming Port</b>	5060

4. Click **Save**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go  
CMAdministrator | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

**SIP Trunk Security Profile Configuration** Related Links: Back To Find/List | Go

Save | Delete | Copy | Reset | Add New

**Status**  
Status: Ready

**SIP Trunk Security Profile Information**

Name\* Non Secure SIP Trunk Profile  
Description Non Secure SIP Trunk Profile authenticated by null Str  
Device Security Mode Non Secure  
Incoming Transport Type\* TCP+UDP  
Outgoing Transport Type TCP

☐ Enable Digest Authentication  
Nonce Validity Time (mins)\* 600  
X.509 Subject Name  
Incoming Port\* 5060

☐ Enable Application Level Authorization  
☐ Accept Presence Subscription  
☐ Accept Out-of-Dialog REFER  
☐ Accept Unsolicited Notification  
☐ Accept Replaces Header

Save | Delete | Copy | Reset | Add New

\*- indicates required item.



## Configure the SIP Trunk device

1. On CUCM, go to **Device > Trunk**.
2. Click **Add New**.
3. Select a **Trunk Type** of *SIP Trunk*.
  - **Device Protocol** displays *SIP*.
  - If asked for a **Trunk Service Type**, select *None(Default)*.
4. Click **Next**.
5. Configure the **Device Information** fields as follows:

<b>Device Name</b>	VCS_location, for example VCS_Ruscombe
<b>Device Pool</b>	(As set up in System > Device Pool)
<b>Call classification</b>	OnNet
<b>Location</b>	(As set up in System > Location)
<b>Packet Capture Mode</b>	None
<b>Media Termination Point Required</b>	Select this check box if only audio devices are registered to CUCM Clear this check box if any video phones registered to CUCM are to make or receive video calls with endpoints registered to Cisco VCS

**Note:** The use of the Media Termination Point has been found to be beneficial in the following circumstances:

- ▶ When calls from a CUCM phone to a SIP video device registered on Cisco VCS fail due to CUCM not providing a SIP sdp as required (seen with CUCM 6.1).
- ▶ When calls from a CUCM phone to an H.323 video device registered on Cisco VCS fail due to INVITEs with no sdp not being interworked correctly by Cisco VCS (note that this issue is fixed in Cisco VCS X5.1.1 and later).

The Media Termination Point may however cause problems when making video calls between CUCM and Cisco VCS (seen with CUPC).

6. Configure the **Call Routing Information > Inbound Calls** fields as follows:

<b>Significant digits</b>	All
<b>Connected Line ID Presentation</b>	Default
<b>Connected Name Presentation</b>	Default
<b>Calling Search Space</b>	(As set up in Call Routing > Class of Control > Calling Search Space)
<b>Prefix DN</b>	<blank>
<b>Redirecting Diversion Header Delivery – Inbound</b>	Select this check box

7. Configure the **Call Routing Information > Outbound Calls** fields as follows:

<b>Calling Party Selection</b>	Originator
<b>Calling Line ID Presentation</b>	Default
<b>Calling Name Presentation</b>	Default

<b>Caller ID DN</b>	<blank>
<b>Caller Name</b>	<blank>

8. Configure the **SIP Information** fields as follows:

<b>Destination address</b>	<IP address of Cisco VCS> or <Domain of Cisco VCS / Cisco VCS cluster>
<b>Destination address is an SRV</b>	Only select this check box if a domain is specified for the destination address, and the DNS server uses DNS SRV records to direct the domain to a Cluster of Cisco VCSs. Do not select this check box if an IP address is specified.
<b>Destination port</b>	5060
<b>Presence Group</b>	Standard Presence Group (or whichever presence group has been configured in System > Presence Group)
<b>SIP Trunk Security Profile</b>	Non Secure SIP Trunk Profile
<b>SIP Profile</b>	Standard SIP Profile
<b>DTMF Signaling Method</b>	RFC 2833

9. Click **Save**.  
 10. Click **Reset**.  
 11. Click **Reset**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | CMAdministrator | About | Logout

System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Administration > Help

**Trunk Configuration** Related Links: [Back To Find/List](#)

Save Delete Reset Add New

**Status**  
Status: Ready

**Device Information**

Product: SIP Trunk  
 Device Protocol: SIP  
 Device Name\*: VCS\_Ruscombe  
 Description: VCS at Ruscombe  
 Device Pool\*: LABCM6  
 Common Device Configuration: < None >  
 Call Classification\*: OnNet  
 Media Resource Group List: < None >  
 Location\*: Reston LABCM6 A51  
 AAR Group: < None >  
 Packet Capture Mode\*: None  
 Packet Capture Duration: 0

☐ Media Termination Point Required  
☒ Retry Video Call as Audio  
☐ Transmit UTF-8 for Calling Party Name  
☐ Unattended Port

**Multilevel Precedence and Preemption (MLPP) Information**  
 MLPP Domain: < None >

**Call Routing Information**

**Inbound Calls**

Significant Digits\*: All  
 Connected Line ID Presentation\*: Default  
 Connected Name Presentation\*: Default  
 Calling Search Space: LABCM6  
 AAR Calling Search Space: < None >  
 Prefix DN:

☐ Redirecting Diversion Header Delivery - Inbound

**Outbound Calls**  
Calling Party Selection\*   
Calling Line ID Presentation\*   
Calling Name Presentation\*   
Caller ID DN   
Caller Name   
☐ Redirecting Diversion Header Delivery - Outbound

**SIP Information**  
Destination Address\*   
☐ Destination Address is an SRV  
Destination Port\*   
MTP Preferred Originating Codec\*   
Presence Group\*   
SIP Trunk Security Profile\*   
Rerouting Calling Search Space   
Out-Of-Dialog Refer Calling Search Space   
SUBSCRIBE Calling Search Space   
SIP Profile\*   
DTMF Signaling Method\*

\*- indicates required item.

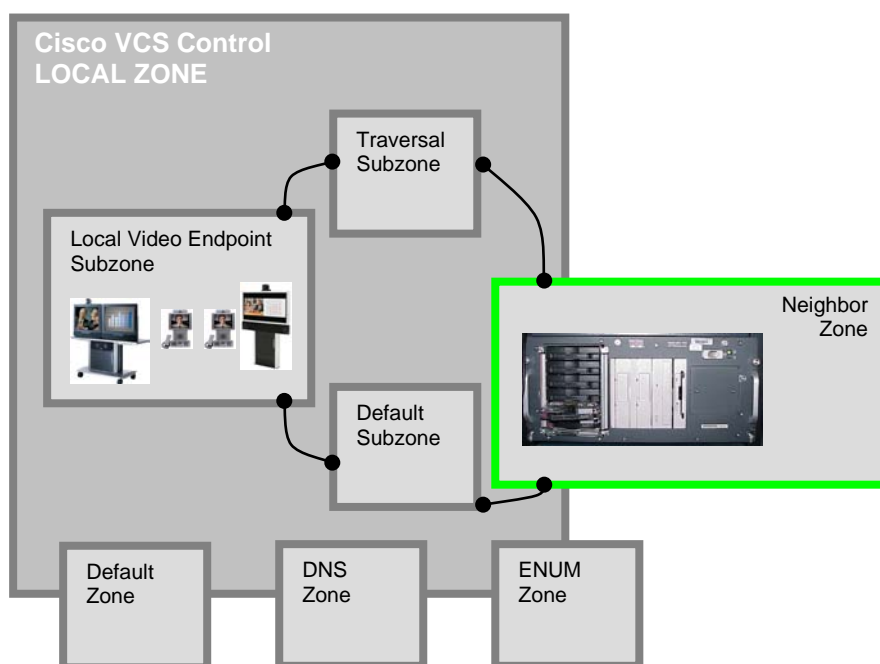
\*\*- Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

Calls can now be made between handsets registered on the Cisco VCS Control to handsets registered on CUCM.

## Cisco VCS Control configuration

The configuration of the Cisco VCS Control needs 3 steps:

- ▶ Configure the Cisco VCS Control with a neighbor zone that contains the CUCM.
- ▶ Configure the Cisco VCS Control with a search rule to route calls to that zone.
- ▶ Configure the Cisco VCS Control with a transform that converts number@<IP address of cucm> to number@vcs.domain.



### Create a neighbor zone for CUCM

1. Go to **VCS configuration > Zones**.
2. Click **New**.
3. Configure the fields as follows:

<b>Name</b>	CUCM Neighbor
<b>Type</b>	<i>Neighbor</i>
<b>Hop count</b>	15
<b>H.323 mode</b>	<i>Off</i> H.323 access is not required for communication with CUCM.
<b>SIP mode</b>	<i>On</i>
<b>SIP port</b>	5060 If the SIP access port on CUCM is not 5060, change the SIP Port value to be the same as used by CUCM.
<b>Transport</b>	<i>TCP</i>
<b>Accept proxied registrations</b>	<i>Deny</i>
<b>Authentication policy</b>	Configure the authentication settings according to your authentication policy.
<b>SIP authentication trust mode</b>	<i>Off</i>

<b>Peer 1 address</b>	IP address of CUCM, or the domain of CUCM.
<b>Zone profile (Advanced section)</b>	Select Cisco Unified Communications Manager. See 'Appendix 9 – Advanced parameters set by the “Cisco Unified Communications Manager” zone profile’ for details on what is configured by this setting.

**Note:** The Cisco VCS Control is to use SIP over TCP to communicate with the CUCM. If you want to use TLS, complete the configuration as described here for TCP and then refer to Appendix 11 – Connecting Cisco VCS to CUCM using TLS (rather than TCP).

#### 4. Click **Create zone**.

The screenshot shows the 'Create zone' configuration page in the Cisco VCS web interface. The page has a navigation bar with tabs: Status, System, VCS configuration (selected), Applications, and Maintenance. Below the navigation bar, the breadcrumb trail reads: You are here: VCS configuration > Zones > Create zone. The form is organized into several expandable sections:

- Configuration:** Contains fields for Name (CUCM Neighbor), Type (Neighbor), and Hop count (15).
- H.323:** Contains Mode (Off) and Port (1719).
- SIP:** Contains Mode (On), Port (5060), Transport (TCP), and Accept proxied registrations (Deny).
- Authentication:** Contains Authentication policy (Do not check credentials) and SIP authentication trust mode (Off).
- Location:** Contains Peer 1 address (192.0.2.0) and five empty fields for Peer 2 through Peer 6 addresses.
- Advanced:** Contains Zone profile (Cisco Unified Communications Manager).

At the bottom of the form are two buttons: 'Create zone' and 'Cancel'.

### Create a search rule to route calls to the CUCM neighbor zone

1. Go to **VCS configuration > Dial plan > Search rules**.
2. Click **New**.

**Note:** Search rules are used to specify the range of telephone numbers / URIs that will be handled by this neighbor CUCM. Search rules can also be used to transform URIs before they are sent to the neighbor.

In this implementation the transforms set up in the “Create transforms” section above have already made sure that dial strings are in URI format **number@vcs.domain**. As CUCM requires dialed numbers to be in the form 3xxx@<IP address of CUCM> a transform will be required to convert calls to CUCM which are addressed 3xxx@vcs.domain to that format.

- Configure the fields as follows to convert called IDs in the format **3xxx@vcs.domain** to 3xxx@<IP address of CUCM> and then route the call to CUCM:

<b>Rule name</b>	Route to CUCM
<b>Description</b>	For example: Send 3xxx@vcs.doman calls to CUCM
<b>Priority</b>	100
<b>Source</b>	Any
<b>Request must be authenticated</b>	Configure this setting according to your authentication policy
<b>Mode</b>	Alias pattern match
<b>Pattern type</b>	Regex
<b>Pattern string</b>	(3\d{3})@vcs.domain(.*)
<b>Pattern behavior</b>	Replace
<b>Replace string</b>	\1@<ip address of CUCM>\2, for example \1@10.1.2.22
<b>On successful match</b>	Stop
<b>Target zone</b>	CUCM Neighbor
<b>State</b>	Enabled

- Click **Create search rule**.

Status System **VCS configuration** Applications Maintenance [Help](#) [Logout](#)

**Create search rule** You are here: [VCS configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

**Configuration**

Rule name \* Route to CUCM ⓘ

Description Send 3xxx@vcs.doman calls to CUCM ⓘ

Priority \* 100 ⓘ

Source Any ⓘ

Request must be authenticated No ⓘ

Mode Alias pattern match ⓘ

Pattern type Regex ⓘ

Pattern string \* (3\d{3})@vcs.domain(.\*) ⓘ

Pattern behavior Replace ⓘ

Replace string \1@<ip address of CUCM>\2, for example \1@10.1.2.22 ⓘ

On successful match Stop ⓘ

Target \* CUCM Neighbor ⓘ

State Enabled ⓘ

Create search rule Cancel

See the “Zones and Neighbors” section of the *Cisco VCS Administrator Guide* for further details.

## Create a transform that converts number@<IP address of cucm> to number@vcs.domain

When a call is made from CUCM to Cisco VCS, the callback address is presented as number@<ip address of cucm>. For Cisco VCS to route this back to CUCM the domain portion should have the IP address removed and the video domain added:

1. Go to **VCS configuration > Dial plan > Transforms**.
2. Click **New**.
3. Configure the fields as follows:

<b>Priority</b>	3
<b>Description</b>	"CUCM IP to domain" for example
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	(.*)@<ip address of CUCM>(: ; .)*?
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	\1@vcs.domain\2
<b>State</b>	<i>Enabled</i>

4. Click **Create transform**.

The screenshot shows the 'Create transform' configuration page in the Cisco VCS web interface. The page has a top navigation bar with 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. Below this is a breadcrumb trail: 'You are here: VCS configuration > Dial plan > Transforms > Create transform'. The main form area is titled 'Configuration' and contains the following fields:

- Priority:** 3
- Description:** CUCM IP to domain
- Pattern type:** Regex
- Pattern string:** (.\* )@<ip address of CUCM>(:|;|.)\*?
- Pattern behavior:** Replace
- Replace string:** \1@vcs.domain\2
- State:** Enabled

At the bottom of the form are two buttons: 'Create transform' and 'Cancel'.

## Test calls

Make some test calls from endpoints registered on the Cisco VCS Control to endpoints registered on CUCM by dialing the required CUCM extension number (3xxx) on the Cisco VCS endpoint.

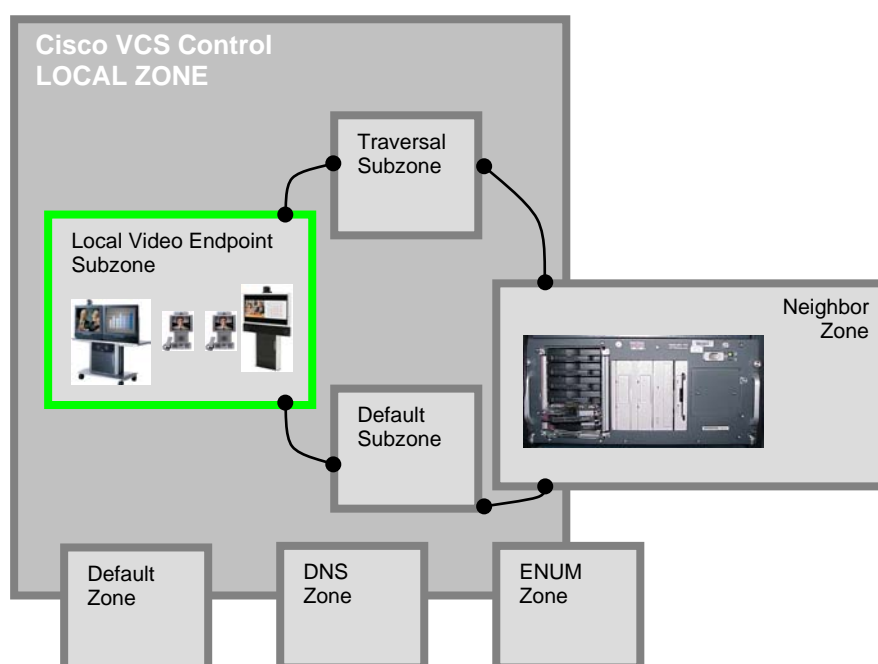
On endpoints registered to the Cisco VCS dial the extension numbers of endpoints registered on CUCM, for example 3000.

# Enabling endpoints registered on CUCM to call endpoints registered on the Cisco VCS Control

## Cisco VCS Control configuration

The configuration of the Cisco VCS Control needs 1 step:

- Configure the Cisco VCS Control with a search rule that takes the incoming domain information put on by CUCM (IP address of VCS:IP port) and converts it to the sip domain used by the registered endpoints and routes the call to the Local Zone. The transform must expand a received “short” 4 digit number to a full 11 digit phone number, as endpoints register with their full 11 digits.



## Set up a search rule for CUCM to call the Cisco VCS Local Zone

**Note:** The search rule must match and transform the URI received from CUCM (0118912)?(4xxx@<ip address of vcs>:5060) into 01189124xxx@vcs.domain

1. Go to **VCS configuration > Dial plan > Search rules**.
2. Click **New**.

**Note:** This search rule will handle all calls to URIs in the format **(0118912)?(4ld{3})@<IP address of VCS>:5060** and transform them to 0118912\2@vcs.domain, for example in this scenario, 01189124000@10.44.9.214:5060 will be converted to 01189124000@vcs.domain and 4000@10.44.9.214:5060 will also be converted to 01189124000@vcs.domain

3. Configure the fields as follows:

<b>Rule name</b>	CUCM to registered devices
<b>Description</b>	For example: (0118912)? 4xxx@10.44.9.214:5060 to call registered endpoints



<b>Priority</b>	40
<b>Source</b>	Any
<b>Request must be authenticated</b>	Configure this setting according to your authentication policy
<b>Mode</b>	Alias pattern match
<b>Pattern type</b>	Regex
<b>Pattern string</b>	(0118912)?(4\d{3})@<IP address of VCS>:<IP port on VCS> For example: (0118912)?(4\d{3})@10.44.9.214:5060
<b>Pattern behavior</b>	Replace
<b>Replace string</b>	0118912\2@vcs.domain
<b>On successful match</b>	Stop
<b>Target zone</b>	LocalZone
<b>State</b>	Enabled

4. Click **Create search rule**.

Status System **VCS configuration** Applications Maintenance [Help](#) [Logout](#)

**Create search rule** You are here: [VCS configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

**Configuration**

Rule name \* CUCM to registered devices ⓘ

Description 2)? 4xxx@10.44.9.214:5060 to call registered endpoints ⓘ

Priority \* 40 ⓘ

Source Any ⓘ

Request must be authenticated No ⓘ

Mode Alias pattern match ⓘ

Pattern type Regex ⓘ

Pattern string \* (0118912)?(4\d{3})@10.44.9.214:5060 ⓘ

Pattern behavior Replace ⓘ

Replace string 0118912\2@vcs.domain ⓘ

On successful match Stop ⓘ

Target \* LocalZone ⓘ

State Enabled ⓘ

Create search rule Cancel

## CUCM configuration

### Allow numeric dialing from Cisco phones to Cisco VCS

CUCM can be configured to take a prefix and route calls to a sip trunk based on a specific prefix.

Configure CUCM to route calls dialed as 01189124xxx and 4xxx to the Cisco VCS as 4xxx:

1. On CUCM, go to **Call Routing > Route/Hunt > Route Pattern**.
2. Click **Add New**.
3. Configure a Route Pattern as indicated above to route calls dialed 01189124xxx to the Cisco VCS trunk after stripping off the leading 0118912 (leaving 4xxx).

Set Pattern definitions:

<b>Route Pattern</b>	0118912.4XXX
<b>Route Partition</b>	(As set up in <b>System &gt; Device Pool</b> )
<b>Description</b>	As required, for example "Route 01189 124 xxx to VCS SIP trunk"
<b>Gateway/Route List</b>	Required Trunk to route calls to the Cisco VCS Control
<b>Call Classification</b>	<i>OnNet</i>
<b>Provide Outside Dial Tone</b>	Not selected

Set Called Party Transformations:

<b>Discard Digits</b>	PreDot
-----------------------	--------

4. Configure a second Route Pattern to route calls dialed 4xxx to the Cisco VCS trunk (no change to dialed number).

Set Pattern definitions:

<b>Route Pattern</b>	4XXX
<b>Route Partition</b>	(As set up in <b>System &gt; Device Pool</b> )
<b>Description</b>	As required, for example "Route 4 xxx to VCS SIP trunk"
<b>Gateway/Route List</b>	Required Trunk to route calls to the Cisco VCS Control
<b>Call Classification</b>	<i>OnNet</i>
<b>Provide Outside Dial Tone</b>	Not selected

Set Called Party Transformations:

<b>Discard Digits</b>	< None >
-----------------------	----------

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go  
CMAdministrator | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

**Route Pattern Configuration** Related Links: Back To Find/List | Go

Save | Delete | Copy | Add New

**Status**  
Status: Ready

**Pattern Definition**

Route Pattern\* 01189124XXX  
Route Partition LABCM6  
Description Route 01189 124 xxx to VCS SIP trunk  
Numbering Plan -- Not Selected --  
Route Filter < None >  
MLPP Precedence\* Default  
Gateway/Route List\* VCS\_Ruscombe (Edit)  
Route Option  
☒ Route this pattern  
☐ Block this pattern No Error  
Call Classification\* OnNet  
☐ Allow Device Override ☐ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority  
☐ Require Forced Authorization Code  
Authorization Level\* 0  
☐ Require Client Matter Code

**Calling Party Transformations**

☐ Use Calling Party's External Phone Number Mask  
Calling Party Transform Mask  
Prefix Digits (Outgoing Calls)  
Calling Line ID Presentation\* Default  
Calling Name Presentation\* Default

**Connected Party Transformations**

Connected Line ID Presentation\* Default  
Connected Name Presentation\* Default

**Called Party Transformations**

Discard Digits PreDot  
Called Party Transform Mask  
Prefix Digits (Outgoing Calls)

**ISDN Network-Specific Facilities Information Element**

Network Service Protocol -- Not Selected --  
Carrier Identification Code  
Network Service Service Parameter Name Service Parameter Value  
-- Not Selected -- < Not Exist >

Save | Delete | Copy | Add New

\* - indicates required item.

Calls can now be made from CUCM to endpoints on Cisco VCS registered as 01189124xxx@vcs.domain.

## Test calls

Make some test calls from endpoints registered on CUCM to endpoints registered on the Cisco VCS Control by dialing the 4 digit extension number 4xxx and also the full 11 digit number 01189124xxx.

On endpoints registered to CUCM dial the 4 digit extension number and 11 digit full number of registered endpoints, for example 4000 and 01189124000.

# Appendix 1 – Troubleshooting

## Problems connecting Cisco VCS Control local calls

### Look at “Search history” to check the applied transforms

Search history entries report on any searches initiated from a SETUP/ARQ /LRQ in H323 and from an INVITE/OPTIONS in SIP.

1. Go to **Status > Search history**.  
The summary shows the source and destination call aliases, and whether the destination alias was found.
2. Select the relevant search attempt.

The search history for that search attempt shows:

- ▶ the incoming call's details
- ▶ any transforms applied by admin or user policy or CPL
- ▶ and in priority order, zones which matched the required (transformed) destination, reporting on:
  - any transforms the zone may apply
  - found or not found status
  - if not found, the error code as seen in the zone's search response
  - repeated until a zone is found that can accept the call, or all prioritized zone matches have been attempted  
(the search may be “not found” due to lack of bandwidth or because the search from the zone resulted in an H.323 rejection reason or a non 2xx response to a SIP request)

If the search indicates:

- ▶ Found: False
- ▶ Reason: 480 Temporarily Not Available

this could be because the Cisco VCS Control's zone links are not correctly set up. From the command line execute:

```
xcommand DefaultLinksAdd
```

to set up the required links for the Cisco VCS Control's default zones; also check the links for other zones that have been created.

---

**Note:** Each H.323 call will have two entries in the search history:

- ▶ The first for an ARQ to see if the endpoint can be found.
- ▶ The second for the Setup to actually route the call.

The ARQ search does not worry about links or link bandwidth, and so if links do not exist or link bandwidth is insufficient it may still pass, even though the Setup search will subsequently fail.

- 
- ▶ Each SIP call will usually only have a single search history entry for the SIP INVITE.
-

## Look at “Call history” to check how the call progressed

1. Go to **Status > Call history**.  
The summary shows the source and destination call aliases, the call duration and whether the call is a SIP, H.323 or SIP< -- >H.323 interworking call.
2. Select the relevant call attempt.  
The entry will show the incoming and outgoing call leg details, the call's status and the zones that the Cisco VCS Control used to route the call.

## Check for errors

### Event Log

Check the Event Log which is accessible from the web browser: **Status > Logs > Event Log**.

### Real time detailed event log

To obtain a more detailed log of key events and errors, start up syslog level 1 logging and then try the call or initiate a presence action.

Log in to the Cisco VCS Control as **admin** using an SSH or Telnet connection.

At the prompt type:

```
syslog 1
```

To turn off tracing, at the prompt type:

```
syslog off
```

- Information displayed between typing syslog 1 and syslog off will contain the key events and error messages that occurred between those two times.

## Tracing calls

### Tracing calls at SIP / H.323 level

Log in to the Cisco VCS Control as **admin** using an SSH or Telnet connection.

At the prompt type:

```
syslog 2
```

To turn off tracing, at the prompt type:

```
syslog off
```

- Information displayed between typing syslog 2 and syslog off will contain the SIP and H.323 messaging received and sent out by the Cisco VCS Control.
- Information displayed by syslog 2 includes the key event and error message information reported by syslog 1. Viewing syslog 1 and syslog 2 information separately can be useful so that syslog 1 messages are not lost within the detailed SIP / H.323 messaging.

## H.323 to SIP CUCM calls do not work

### 422 Session Timer too small

When interworking a call from H.323 to SIP, Cisco VCS in X4 and earlier versions of code would not handle the SIP “422 Session Timer too small” response from CUCM. If an H.323 call is interworked to a SIP call to CUCM and CUCM sends the ‘422 Session Timer too small’ message Cisco VCS clears the call.

From X5.0, setting the neighbor zone to “Cisco Unified Communications Manager” enables Cisco VCS to handle session timer exchanges with CUCM, and so the changes to configuration in CUCM documented below should be unnecessary.

For X4.x and earlier versions of Cisco VCS code, the workaround is to set CUCM to support a Minimum Session Expires time that matches that requested by endpoints.

Video endpoints typically request a Session-Expires: 500 and CUCM has a default Min-SE (Minimum Session Expires): 1800

To configure CUCM to have a Minimum Session Expires time <= 500:

1. Go to **System > Service Parameters**.
2. Select **Server** = current server, for example “<IP> (Active)”.
3. Select **Service** = Cisco CallManager (Active).
4. Search for **SIP Min-SE Value** and set it to 500.
5. Click **Save**.

The screenshot shows the 'Service Parameter Configuration' page for SIP parameters. The 'SIP Min-SE Value' parameter is highlighted with a red circle. The input field contains '500' and the 'Current Value' column shows '1800'.

Clusterwide Parameters (Device - SIP)		
SIP Interoperability Enabled *	True	True
Retry Count for SIP Bye *	10	10
Retry Count for SIP Cancel *	10	10
Retry Count for SIP Invite *	6	6
Retry Count for SIP PRACK *	6	6
Retry Count for SIP ReliXX *	10	10
Retry Count for SIP Publish *	6	6
Retry Count for SIP Response *	6	6
SIP Connect Timer *	500	500
SIP Disconnect Timer *	500	500
SIP Expires Timer *	180000	180000
SIP PRACK Timer *	500	500
SIP ReliXX Timer *	500	500
SIP Trying Timer *	500	500
SIP Publish Timer *	500	500
<b>SIP Min-SE Value *</b>	<b>500</b>	<b>1800</b>
SIPS URI Handling *	Reject	Reject
SIP statistics Periodic update Timer *	2	2
SIP Session Expires Timer *	1800	1800
SIP Trunk TspReq Retry *	2	2

## Cisco VCS reports SIP decode error

### CUCM 5 and 6

When CUCM is not configured to connect to Cisco VCS, CUCM responds to the OPTIONS pings that Cisco VCS sends to it with a 503 “Service unavailable”.

- ▶ The 503 message contains a warn header which should be constructed as:  
“Warning” 3 digit warn code <space> warn agent <space> warn text  
CUCM wrongly misses out the warn agent.
- ▶ The 503 message contains a warn header which has a text section opened by “ and closed by ‘.  
Both open and close should be “.

Cisco VCS rightfully reports this as an illegal construct.

## CUCM 7

When CUCM is not configured to connect to Cisco VCS, CUCM responds to the OPTIONS pings that Cisco VCS sends to it with a 503 “Service unavailable”.

- ▶ The 503 message contains a warn header which should be constructed as:  
`"Warning" 3 digit warn code <space> warn agent <space> warn text`  
 CUCM wrongly misses out the warn agent.

Cisco VCS correctly reports this as an illegal construct.

## In-call problems

### Calls remain up for a maximum of 15 minutes.

If a call is made from CUCM (version 8.0 or earlier) to a Cisco VCS FindMe that has CallerID set to FindMe ID, CUCM does not handle the session refresh messages Cisco VCS sends to it (the message has an updated From: header) and so session refreshes fail and the call is cleared by the session refresh timer.

This is not a problem in CUCM versions later than 8.0.

### Calls clear down when a call transfer from a video phone on CUCM transfers a call to Cisco VCS

Even if use of a media termination point (MTP) is not requested on the SIP trunk between CUCM and Cisco VCS, if DTMF signaling method is configured as “No preference” on the SIP trunk on CUCM, CUCM will try and use a Media Transfer Point and the call will fail.

To resolve this, ensure that DTMF signaling method is configured as “RFC 2833” on CUCM on the SIP trunk from CUCM to Cisco VCS.

## Taking a trace on CUCM using RTMT

RTMT is a tool that lets you monitor system health, view graphs and collect logs from CUCM. There are versions for both Linux and Windows. CUCM must also be configured to specify what can be traced.

### Configure CUCM to enable tracing

1. Log in to CUCM.
2. In the **Navigation** drop-down select **Cisco Unified Serviceability** and click **Go**.
3. Go to the **Troubleshooting Trace Settings** page (**Trace > Troubleshooting Trace Settings**).
4. Select the **Check All Services** check box.
5. Click **Save**.

### Installing RTMT – Real Time Monitoring Tool

1. Log in to CUCM using a Linux or Windows PC.
2. Go to **Application > Plugins**.
3. Select **Find** with ‘**Name begins with** <blank>’ and ‘**Plugin Type equals** **Installation**’.
4. Scroll down to the entry for ‘Cisco Unified CM Real-Time Monitoring Tool – Linux’ or ‘Cisco Unified CM Real-Time Monitoring Tool – Windows’, as required.
5. Click on the [Download](#) link.
6. When downloaded, run the downloaded install file.
7. Follow the instructions in the install wizard.

8. When complete, click **Done** to exit the installer.

## Running RTMT

1. Run RTMT.  
For example, under windows this is in **Start > All Programs > Cisco > CallManager Serviceability > Real-Time Monitoring Tool**.
2. In the Login window enter the **Host IP Address**, **User Name** and **Password**.
3. Click **OK**.

## Taking a trace using RTMT

1. Select **Trace & Log Central**.
2. Double-click on **Real Time Trace**.
3. Double-click View **Real Time Data**.
4. Select a Node – the CUCM instance that is to have the trace run on it.
5. Click **Next >**.
6. Select:
  - **Products** = *CCM*
  - **Services** = *Cisco CallManager*
  - **Trace File Type** = *sdi*
7. Click **Finish**.

---

### Note:

- ▶ Logs can take a while to download.
  - ▶ The sdi (System Diagnostic Interface) trace contains alarms, error information and SIP stack trace information.
-



## Appendix 2 – Known interworking capabilities and limitations

### Capabilities

#### SIP and H.323 endpoints making basic calls

- ▶ SIP and H.323 endpoints can make calls via the Cisco VCS Control to endpoints registered to CUCM.
- ▶ Endpoints registered to CUCM can make calls to SIP and H.323 endpoints on the Cisco VCS Control.

### Limitations

#### E20 encryption

If E20 has Encryption Mode = Best Effort then calls from CUCM clear when E20 answers them. Set Encryption Mode = Off.

#### T150 running L6.0 code

If a SIP call is made from a T150 running L6.0 code to CUCM 8.0 (and earlier), CUCM does not handle the UPDATE message that the T150 sends immediately after the call is answered, and so on call answer the call is cleared down immediately.

If xConfiguration Conference H239 is set to Off then no BFCP is offered and CUCM handles the UPDATE from the T150 and the call completes as desired.

#### H.323 MXP and 9971

When an MXP registered to Cisco VCS is in a call with a 9971 registered to CUCM and the MXP call is H.323, the video on the MXP will be CIF (small picture) rather than VGA (full size picture).

(Seen on MXP F9.0 and 9971 version 9.0.2)

If the MXP call is SIP, a full size picture will be seen.

## Appendix 3 – Benefits of using Cisco VCS with CUCM

### Separate management and operation of video systems and CUCM telephony systems

The video network with its high bandwidth requirements and requirements to control how many calls can be sent down specific IP links can be controlled and managed independently from the telephony systems, which typically are more relaxed about these issues.

### Duo Video

Sharing presentations in a conference is not supported in CUCM, but it is supported by Cisco VCS.

### Bandwidth management

The Cisco VCS uses the concept of pipes which allow you to apply bandwidth restrictions to a link. This ensures that calls are not attempted if they would overload a link's bandwidth. If a link's bandwidth would be exceeded, the call may be diverted to a different zone (link), downspeeded to a lower bandwidth or rejected – depending on configuration.

### FindMe™

FindMe provides the ability for users to set up groups of video endpoints / phones to ring when a call arrives so that for instance the video phone can ring at the office, in the home office and on the laptop soft video phone at the same time – giving the highest likelihood of the person being able to answer their video call.

FindMe also allows devices to be called if the primary set are not answered or are busy, for example to route them through to a mobile phone or video mail so that the call can always be handled.

From Cisco VCS version X5, calls made by devices in a FindMe will present the FindMe ID as the caller ID, so whichever endpoint you called from, people returning your call, will make all your currently selected FindMe devices ring.

## Appendix 4 – Allow dialing to Cisco VCS domain from Cisco phones

Configure a SIP route pattern that tells CUCM that anything with a domain vcs.domain needs to be sent down the Cisco VCS SIP trunk

1. On CUCM, go to **Call Routing > SIP Route Pattern**.
2. Click **Add New**.
3. Configure the fields as follows:

<b>Pattern Usage</b>	<i>Domain Routing</i>
<b>Pattern</b>	Domain for calls, for example vcs.domain
<b>Route Partition</b>	(As set up in <b>System &gt; Device Pool</b> )
<b>SIP Trunk</b>	Required Trunk to route calls to the Cisco VCS Control

4. Click **Save**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go  
CMAdministrator | About | Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

**SIP Route Pattern Configuration** Related Links: Back To Find/List Go

Save Delete Copy Add New

**Status**  
Status: Ready

**Pattern Definition**  
 Pattern Usage: Domain Routing  
 Pattern\*: vcs.domain  
 Description: Ruscombe VCS domain  
 Route Partition: LABCM6  
 SIP Trunk\*: VCS\_Ruscombe  
☐ Block Pattern

**Calling Party Transformations**  
☐ Use Calling Party's External Phone Mask  
 Calling Party Transformation Mask:  
 Prefix Digits (Outgoing Calls):  
 Calling Line ID Presentation\*: Default  
 Calling Line Name Presentation\*: Default

**Connected Party Transformations**  
 Connected Line ID Presentation\*: Default  
 Connected Line Name Presentation\*: Default

Save Delete Copy Add New

\* - indicates required item.

When NNNN@vcs.domain is dialed by an endpoint registered to CUCM, CUCM will route the call to the Cisco VCS as NNNN@<IP address of VCS>:5060.

## Appendix 5 – Connecting CUCM to a cluster of Cisco VCS peers

From CUCM version 8.5, to connect CUCM with a cluster of Cisco VCS peers there are 2 methods of providing CUCM with the addresses of the VCS cluster peers:

- ▶ the trunk to VCS specifies a list of VCS peers
- ▶ the trunk to VCS specifies the DNS SRV address for the VCS cluster

Prior to CUCM 8.5, there was only 1 method; the trunk to VCS had to specify the DNS SRV address for the VCS cluster.

### Configuring the trunk to VCS to specify the DNS SRV address for the VCS cluster

Ensure that in the DNS server used by CUCM a DNS SRV record exists for the cluster of VCS peers; in the DNS SRV record each peer should be set with equal priority and equal weight.

1. On CUCM, go to **Device > Trunk**.
2. Select the previously configured Trunk.
3. Scroll down to the SIP Information section
4. Configure the SIP Information fields as follows:

<b>Destination address is an SRV</b>	Select this check box.
<b>Destination address</b>	<DNS SRV name of VCS cluster>

5. Click **Save**.
6. Click **Reset**.
7. Click **Reset**.

The screenshot displays the Cisco Unified CM Administration web interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'Trunk Configuration' and shows the configuration for a SIP Trunk named 'VCS\_Ruscombe'. The 'Device Information' section includes fields for Product (SIP Trunk), Device Protocol (SIP), Device Name (VCS\_Ruscombe), Description (VCS at Ruscombe), Device Pool (LABCM6), Common Device Configuration (< None >), Call Classification (OnNet), Media Resource Group List (< None >), Location (Reston LABCM6 AS1), AAR Group (< None >), Packet Capture Mode (None), and Packet Capture Duration (0). There are checkboxes for 'Media Termination Point Required' (unchecked), 'Retry Video Call as Audio' (checked), 'Transmit UTF-8 for Calling Party Name' (unchecked), and 'Unattended Port' (unchecked). The 'Multilevel Precedence and Preemption (MLPP) Information' section shows 'MLPP Domain' set to '< None >'. The 'Call Routing Information' section includes 'Inbound Calls' with fields for Significant Digits (All), Connected Line ID Presentation (Default), Connected Name Presentation (Default), Calling Search Space (LABCM6), AAR Calling Search Space (< None >), and Prefix DN.

☐ Redirecting Diversion Header Delivery - Inbound

**Outbound Calls**

Calling Party Selection\*

Calling Line ID Presentation\*

Calling Name Presentation\*

Caller ID DN

Caller Name

☐ Redirecting Diversion Header Delivery - Outbound

**SIP Information**

Destination Address\*

☐ Destination Address is an SRV

Destination Port\*

MTP Preferred Originating Codec\*

Presence Group\*

SIP Trunk Security Profile\*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile\*

DTMF Signaling Method\*

\*: indicates required item.

\*\*: Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

## Configuring the trunk to VCS to specify a list of VCS peers

1. On CUCM, go to **Device > Trunk**.
2. Select the previously configured Trunk.
3. Scroll down to the SIP Information section.

**SIP Information**

**Destination**

☐ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text"/>	<input type="text"/>	<input type="text"/>

4. Configure the SIP Information fields as follows:

<b>Destination address is an SRV</b>	Ensure that this check box is not selected
<b>Destination address 1</b>	IP address or DNS name of VCS peer 1
<b>Destination port 1</b>	5060 or 5061 depending on connectivity (TCP/TLS)
<b>Destination address 2</b>	IP address or DNS name of VCS peer 2
<b>Destination port 2</b>	5060 or 5061 depending on connectivity (TCP/TLS)
<b>Destination address 3</b>	IP address or DNS name of VCS peer 3 – if it exists
<b>Destination port 3</b>	5060 or 5061 depending on connectivity (TCP/TLS)
<b>Destination address 4</b>	IP address or DNS name of VCS peer 4 – if it exists
<b>Destination port 4</b>	5060 or 5061 depending on connectivity (TCP/TLS)
<b>Destination address 5</b>	IP address or DNS name of VCS peer 5 – if it exists
<b>Destination port 5</b>	5060 or 5061 depending on connectivity (TCP/TLS)
<b>Destination address 6</b>	IP address or DNS name of VCS peer 6 – if it exists
<b>Destination port 6</b>	5060 or 5061 depending on connectivity (TCP/TLS)

To obtain additional destination address entries select the “+”.

5. Click **Save**.
6. Click **Reset**.
7. Click **Reset**.

## Appendix 6 – Connecting Cisco VCS to a cluster of CUCM nodes

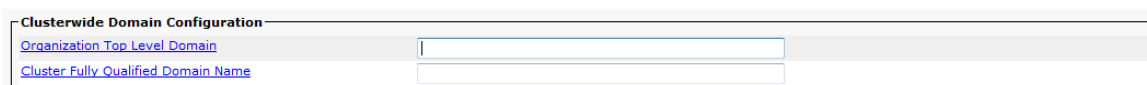
When connecting Cisco VCS to a cluster of CUCM nodes, Cisco VCS needs to be able to route calls to each of these CUCM nodes. This can either be done by setting up multiple zones – one per CUCM node, then setting up a set of prioritized search rules to route calls to each of the zones in the preferred order (priority values different for each search rule). An alternative method is to use DNS SRV records and a Cisco VCS DNS zone. This is a better approach because call load can be shared across CUCM nodes.

### Configuration for Cisco VCS to use a DNS Zone to contact a cluster of CUCM nodes

#### CUCM configuration

When in a cluster, CUCM needs to accept calls routed to number@domain (instead of number@<ip address of CUCM>) so that Cisco VCS can send the call to any CUCM node without having to make sure that the domain portion matches the IP address of the node that the call is being sent to.

1. Go to System > Enterprise parameters, and find the **Clusterwide Domain Configuration** section.



2. Set the **Organization Top Level Domain** to the same domain as the video network, vcs.domain for example.

#### DNS Server configuration

Configure the DNS server that Cisco VCS has been configured to use with DNS SRV records for the CUCM cluster.

- ▶ `_sips._tcp.fqdn_of_cucm_cluster` for TLS connectivity (one record for each CUCM node)
- or
- ▶ `_sip.tcp.fqdn_of_cucm_cluster` for TCP connectivity (one record for each CUCM node)

#### Cisco VCS Control configuration

Cisco VCS configuration requires 3 steps:

- ▶ Create a CUCM DNS zone
- ▶ Adjust search rule
- ▶ Delete the old CUCM neighbor zone

##### Create a CUCM DNS zone

1. Go to **VCS configuration > Zones**.
2. Click **New**.
3. Configure the fields as follows:

<b>Name</b>	CUCM Cluster Neighbor DNS Zone
<b>Type</b>	DNS
<b>Hop count</b>	15

<b>H.323 mode</b>	<i>Off</i> H.323 access is not required for communication with CUCM
<b>SIP mode</b>	<i>On</i>
<b>TLS verify mode</b>	<i>Off</i>
<b>Include address record</b>	<i>Off</i>
<b>Zone profile</b>	Select <i>Cisco Unified Communications Manager</i> . See 'Appendix 9 – Advanced parameters set by the “Cisco Unified Communications Manager” zone profile’ for details on what is configured by this setting.

#### 4. Click **Create zone**.

#### Adjust search rule

Change the search rule to point to this CUCM DNS zone. Also, instead of using an IP address, set the domain as used in the DNSSRV record.

1. Go to **VCS configuration > Dial plan > Search rules**.
2. Select the existing “Route to CUCM” search rule.

**Note:** Search rules are used to specify the range of telephone numbers / URIs that are handled by this neighbor CUCM. They can also be used to transform URIs before they are sent to the neighbor. In this implementation the transforms set up in the “Create transforms” section have already made sure that dial strings are in URI format **number@vcs.domain**.

Previously CUCM required dialed numbers to be in the form 3xxx@<IP address of CUCM>. A transform converted calls to CUCM from 3xxx@vcs.domain into that format. This transform is no longer needed.

3. Modify the fields as follows to leave called IDs in the format **3xxx@vcs.domain** and then route the call to CUCM (the dimmed fields retain their existing values):

<b>Rule name</b>	Route to CUCM
<b>Description</b>	For example: Send 3xxx@vcs.doman calls to CUCM

<b>Priority</b>	100
<b>Source</b>	Any
<b>Request must be authenticated</b>	No
<b>Mode</b>	Alias pattern match
<b>Pattern type</b>	Regex
<b>Pattern string</b>	(3\d{3})@vcs.domain(.*)
<b>Pattern behavior</b>	Leave
<b>On successful match</b>	Stop
<b>Target zone</b>	CUCM Cluster Neighbor DNS Zone
<b>State</b>	Enabled

4. Click **Save**.

The screenshot shows the 'Edit search rule' configuration page in the Cisco VCS Administrator. The page has a navigation bar with 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The 'VCS configuration' tab is selected. The page title is 'Edit search rule'. The configuration form includes the following fields:

- Rule name: Route to CUCM
- Description: Send 3xxx@vcs.domain calls to CUCM
- Priority: 100
- Source: Any
- Request must be authenticated: No
- Mode: Alias pattern match
- Pattern type: Regex
- Pattern string: (3\d{3})@vcs.domain(.\*)
- Pattern behavior: Leave
- On successful match: Stop
- Target: CUCM Cluster Neighbor DNS Zone
- State: Enabled

At the bottom of the form, there are three buttons: 'Save', 'Delete', and 'Cancel'. The 'Save' button is highlighted.

See the “Zones and Neighbors” section of the *Cisco VCS Administrator Guide* for further details.

### Delete the old CUCM neighbor zone

Delete the now unused neighbor zone “CUCM Neighbor”.

1. Go to **VCS configuration > Zones**.
2. Select the check box next to the “CUCM Neighbor” zone.
3. Click **Delete**.

The screenshot shows the 'Zones' configuration page in the Cisco VCS Administrator. The page has a navigation bar with 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The 'VCS configuration' tab is selected. The page title is 'Zones'. The table below shows the list of zones:

Name	Type	Calls	Bandwidth used	Status	Actions
<a href="#">DefaultZone</a>	Default Zone	0	0 kbps	Active	<a href="#">View/Edit</a>
<input type="checkbox"/> <a href="#">CUCM Cluster Neighbor DNS Zone</a>	DNS	0	0 kbps	Active	<a href="#">View/Edit</a>
<input checked="" type="checkbox"/> <a href="#">CUCM Neighbor</a>	Neighbor	0	0 kbps	Active	<a href="#">View/Edit</a>

At the bottom of the table, there are four buttons: 'New', 'Delete', 'Select all', and 'Unselect all'. The 'Delete' button is highlighted.



## Appendix 7 – Cisco TelePresence Multiway™ and CUCM

To enable CUCM registered endpoints to be joined into a Multiway™ conference set the Conference Factory Template to use the IP address of the Cisco VCS as the domain, 55501%%@<IPofVCS> for example.

Also configure a SIP Route pattern in CUCM that routes the domain @<IPofVCS> to the SIP trunk connecting to Cisco VCS.

## Appendix 8 – Endpoint specific configuration

### T150 running L6.x

Duo Video enabled on the T150 causes the call to be dropped when a 7960 answers the call from the T150.

To disable Duo Video on the T150 set:

- ▶ xConfiguration Conference H239: Off

### Other products

There are no other known special requirements for endpoint configuration for devices registering to Cisco VCS.

## Appendix 9 – Advanced parameters set by the “Cisco Unified Communications Manager” zone profile

Selecting a **Zone profile** of **Cisco Unified Communications Manager** sets the following Advanced zone parameters:

Parameter	Value
Searches are automatically responded to	Off
Empty INVITE allowed	On
SIP poison mode	Off
SIP encryption mode	On
SIP SDP attribute line limit mode	Off
SIP SDP attribute line limit length	130
SIP multipart MIME strip mode	Off
SIP UPDATE strip mode	Off
Interworking SIP Search Strategy	OPTIONS
SIP UDP/BFCP filter mode	On
SIP Duo Video filter mode	Off
SIP record route address type	IP
SIP Proxy-Require header strip list	<Blank>

## Appendix 10 – CUCM 5 incompatibility

- ▶ CUCM 5 does not work with Cisco VCS; CUCM 5 responds incorrectly to OPTIONS messages that Cisco VCS sends to it.
- ▶ CUCM 6.1 and later does correctly respond to the Cisco VCS OPTIONS messages and so CUCM 6.1 or later must be used when integrating with Cisco VCS.

## Appendix 11 – Connecting Cisco VCS to CUCM using TLS (rather than TCP)

These instructions explain how to take a system that is already configured and working using a TCP interconnection between Cisco VCS and CUCM, and to convert that connection to use TLS instead.

The process involves:

- ▶ ensuring that CUCM trusts the Cisco VCS server certificate
- ▶ configuring a SIP trunk security profile on CUCM
- ▶ updating the CUCM trunk to Cisco VCS to use TLS
- ▶ updating the Cisco VCS neighbor zone to CUCM to use TLS

### Ensure that CUCM trusts the Cisco VCS server certificate

For CUCM to make a TLS connection to Cisco VCS, CUCM must trust the VCS's server certificate. CUCM must therefore have a root certificate that trusts the VCS's certificate.

If VCS and CUCM have both been loaded with valid certificates from the same certificate authority and the root CA is already loaded onto CUCM, then no further work is required.

If VCS does not have a certificate from an authority that is accepted by the root CA certificate on CUCM:

- ▶ The preferred solution is to obtain a valid certificate for the Cisco VCS from an authority accepted by the CUCM root CA certificate, and then load this new certificate onto Cisco VCS (see the *Certificate creation and use with Cisco VCS* deployment guide).
- ▶ An alternative solution is to have CUCM validate the Cisco VCS's existing server certificate. You can do this by taking the server certificate off the VCS and loading it into CUCM. To do this:
  - a. Copy the server certificate from VCS to a text file and save the file with a suffix of **.pem**.
    - i. Go to the Cisco VCS's **Security certificates** page (**Maintenance > Certificate management > Security certificates**).
    - ii. Click **Show server certificate**.
    - iii. Copy all the information displayed including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines into a text file named in the format, for example, VCS<IPaddress>-cert.pem.
  - b. On CUCM, select **Cisco Unified OS Administration**, click **Go** and log in.
  - c. Go to **Security > Certificate management** then **Upload Certificate**.
  - d. Configure the fields as follows:

<b>Certificate Name</b>	CallManager-trust.
<b>Root Certificate</b>	<leave blank>
<b>Description</b>	Enter a textual description as required.
<b>Upload File</b>	Click <b>Browse...</b> and select the .pem file you created in step 1.

- e. Click **Upload File**.
- f. Click **Close**.

### Configure a SIP trunk security profile on CUCM

On CUCM:

1. Select **Cisco Unified CM Administration**, click **Go** and log in.

2. Go to **System > Security > SIP Trunk Security Profile**.
3. Click **Add New**.
4. Configure the fields as follows:

<b>Name</b>	A name indicating that this profile is an encrypted profile for the specific X.509 name(s).
<b>Description</b>	Enter a textual description as required.
<b>Device Security Mode</b>	Select <i>Encrypted</i> .
<b>Incoming Transport Type</b>	Select <i>TLS</i> .
<b>Outgoing Transport Type</b>	Select <i>TLS</i> .
<b>Enable Digest Authentication</b>	Leave unselected.
<b>X.509 Subject Name</b>	The subject name or an alternate subject name provided by the Cisco VCS in its certificate. (Multiple X.509 names can be added if required; separate each name by a space, comma, semicolon or colon.)
<b>Incoming Port</b>	5061
<b>Other parameters</b>	Leave all other parameters unselected.

5. Click **Save**.

## Update the CUCM trunk to Cisco VCS to use TLS

On CUCM:

1. Go to **Device > Trunk**.
2. Using Find, select the Device Name previously set up for the trunk to the Cisco VCS.
3. Configure the following fields:

Device Information section	
<b>Device Name</b>	This name must match the subject name of the Cisco VCS certificate (as used in the X.509 Subject Name in the security profile).
<b>Description</b>	Update as required; you may want to indicate that this is now a TLS connection.
SIP Information section	
<b>Destination Port</b>	5061
<b>SIP Trunk Security Profile</b>	Select the trunk profile set up above.

Leave other parameters as previously configured.

4. Click **Save**.
5. Click **Apply Config**.
6. Click **OK**.

## Update the Cisco VCS neighbor zone to CUCM to use TLS

**Note:** Cisco VCS will report that the CUCM zone is active even while it is communicating with CUCM over TCP. The changes below are necessary to allow communications to happen over TLS.

On Cisco VCS:

1. On the **Edit zone** page (**VCS configuration > Zones**, then select the zone to CUCM).

2. Configure the following fields:

SIP section	
Port	5061
Transport	TLS
TLS verify mode	Off
Authentication trust mode	Off

Leave other parameters as previously configured.

3. Click **Save**.

## Verify that the TLS connection is operational

To verify correct TLS operation, check that the Cisco VCS zone reports its status as active and then make some test calls:

1. Check the Cisco VCS zone is active:
  - a. Go to **VCS configuration > Zones**.
  - b. Check the Status of the zone.

If the zone is not active, try resetting or restarting the trunk again on CUCM.

2. Make a test call from a Cisco VCS registered endpoint to a CUCM phone.
3. Make a test call from a CUCM phone to a Cisco VCS registered endpoint.

---

**Note:** CUCM 8.0.2 and earlier do not handle received crypto tags properly; the receipt of them may cause CUCM to clear the call. If this occurs, configure endpoints with Encryption = Off.

---

## Appendix 12 – Characters allowed in SIP URIs

The following character set is allowed in SIP URIs (further details may be found in RFC 3261):

a-z / A-Z / 0-9 / "-" / "\_" / "." / "!" / "~" / "\*" / "'" / "(" / ")" / "&" /  
"=" / "+" / "\$" / ", " / ";" / "?" / "/"

If other characters are needed they must be 'escaped' using "%" HexDigit HexDigit

where HexDigit HexDigit is the ASCII value for the required character.

For example, firstname%20lastname@company.com - %20 is the space character.



---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.