



Cisco Unified Communications Manager with Cisco VCS

Deployment Guide

**Cisco VCS X7.2
CUCM v6.1, 7.x and 8.x
SIP trunk**

D14602.11

August 2012

Contents

Introduction	5
Objectives and intended audience	5
Deployment scenario.....	5
Summary of configuration process.....	6
Prerequisites for system configuration	6
Enabling calls between endpoints registered on the Cisco VCS Control	7
Cisco VCS Control configuration.....	7
Set up the SIP domain of the Cisco VCS Control	7
Check the Traversal Subzone configuration	8
Create transforms.....	8
CUCM configuration	10
Registering endpoints to the Cisco VCS Control.....	10
Endpoint configuration.....	10
Confirming registrations	10
Test calls	10
Enabling calls between endpoints registered on CUCM	11
Cisco VCS Control configuration.....	11
CUCM configuration	11
Configure the SIP Profile.....	11
Add a phone device.....	13
Device directory number configuration.....	13
Configure phone endpoint to pick up its configuration from CUCM.....	13
Confirming registrations	14
Test calls.....	14
Enabling endpoints registered on VCS Control to call endpoints registered on CUCM	15
CUCM configuration	15
Configure the SIP Trunk security profile	15
Configure the SIP Trunk device	16
Cisco VCS Control configuration.....	19
Create a neighbor zone for CUCM.....	19
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	22
Test calls.....	22
Enabling endpoints registered on CUCM to call endpoints registered on VCS Control	23
Cisco VCS Control configuration.....	23
Set up a transform for CUCM to call the Cisco VCS Local and Neighbor Zones	23
Ensure that VCS stays in the signaling path for calls with CUCM	24
CUCM configuration	25
Allow numeric dialing from Cisco phones to Cisco VCS.....	25
Test calls.....	26

Advanced configuration	27
CUCM SIP Max Incoming Message Size	27
Appendix 1 – Troubleshooting	28
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	28
Check for errors	29
Tracing calls	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	30
Call failures with Cisco TelePresence Server	30
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 VCS.....	31
Failure to join a CUCM endpoint to a conference using Multiway	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
Appendix 2 – Known interworking capabilities and limitations	33
Capabilities	33
SIP and H.323 endpoints making basic calls	33
Cisco TelePresence Conductor.....	33
Limitations.....	33
E20 encryption	33
T150 running L6.0 code	33
H.323 MXP and 9971	33
Appendix 3 – Allow dialing to Cisco VCS domain from Cisco phones.....	34
Appendix 4 – Connecting CUCM to a cluster of Cisco VCS peers.....	35
Configuring the trunk to VCS to specify the DNS SRV address for the VCS cluster	35
Configuring the trunk to Cisco VCS to specify a list of VCS peers	36
Appendix 5 – Connecting Cisco VCS to a cluster of CUCM nodes.....	38
Option 1: Using a single neighbor zone	38
CUCM configuration	38
Cisco VCS Control configuration.....	38
Option 2: Using a DNS zone	39
CUCM configuration	39
DNS server configuration	39
Cisco VCS Control configuration.....	39
Option 3: Using multiple neighbor zones.....	42
Cisco VCS Control configuration.....	42

Appendix 6 – Cisco TelePresence Multiway and CUCM	43
VCS configuration.....	43
CUCM configuration	43
Appendix 7 – Endpoint specific configuration	44
T150 running L6.x.....	44
Other products.....	44
Appendix 8 – Parameters set by the ‘Cisco Unified Communications Manager’ Advanced Zone profile	45
Appendix 9 – CUCM 5 incompatibility	46
Appendix 10 – Connecting Cisco VCS to CUCM using TLS (rather than TCP)	47
Ensure that CUCM trusts the Cisco VCS server certificate	47
Configure a SIP trunk security profile on CUCM	48
Update the CUCM trunk to Cisco VCS to use TLS	48
Update the VCS neighbor zone to CUCM to use TLS	49
Verify that the TLS connection is operational.....	49
Network of VCSs	49
Appendix 11 – Characters allowed in SIP URIs	50
Appendix 12 – Enabling BFCP – Dual video / presentation sharing	51
VCS configuration.....	51
CUCM configuration	51
Document revision history	52

Introduction

Objectives and intended audience

This deployment guide provides guidelines on how to configure the Cisco TelePresence Video Communication Server (Cisco VCS) version X7.2 and Cisco Unified Communications Manager (CUCM) versions 6.1, 7 or 8 to interwork via a SIP trunk.

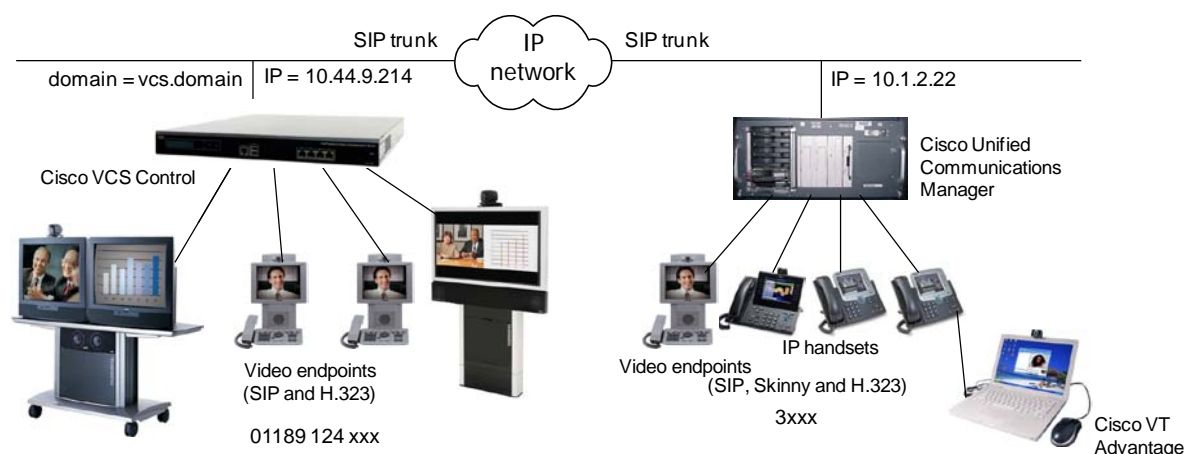
Other ways that Cisco VCS and CUCM can be connected to allow them to interwork include:

- 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 *VCS Basic Configuration (Single 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 breadcrumb trail is 'VCS configuration > Protocols > SIP > Domains > Create domain'. The main form area is titled 'Configuration' and contains a 'Name' field with a red asterisk and a dropdown arrow. Below the field are 'Create domain' and 'Cancel' buttons.

Check the Traversal Subzone configuration

- Go to **VCS configuration > Local Zone > Traversal Subzone**.
 - Port ranges can be left at default values (50000 to 54999), or can be configured as required (see the “Zones and Neighbors” section of *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 *Cisco VCS Administrator Guide* for further details).
- Click **Save**.

The screenshot shows the 'Traversal Subzone' configuration page in the Cisco VCS Administrator GUI. The breadcrumb trail is 'VCS configuration > Local Zone > Traversal Subzone'. The page is organized into three main sections:

- Ports:** Contains two input fields: 'Traversal media port start' with a value of 50000 and 'Traversal media port end' with a value of 54999. Both fields have an information icon to their right.
- Total bandwidth available:** Contains two fields: 'Bandwidth restriction' set to a dropdown menu with 'Unlimited' selected, and 'Total bandwidth limit (kbps)' with a value of 500000. Both have information icons.
- Calls handled by the Traversal Subzone:** Contains two fields: 'Bandwidth restriction' set to a dropdown menu with 'Unlimited' selected, and 'Per call bandwidth limit (kbps)' with a value of 1920. Both have information icons.

At the bottom of the configuration area is a 'Save' button. Below the configuration area is a 'Traversal Subzone status' table:

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.)

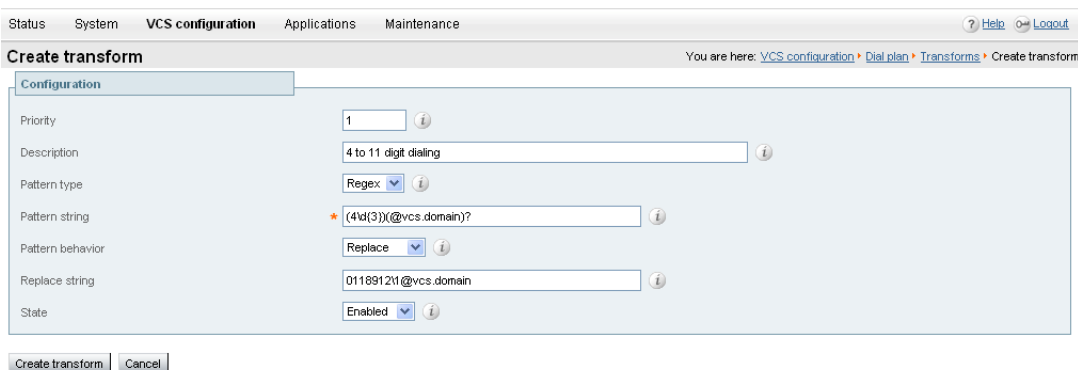
See the Regular Expression Reference in the Appendices section of the *Cisco VCS Administrator Guide* for further details, or alternatively search the world wide web for the term "Regular Expression".

To create the first transform:

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

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

4. Click **Create transform**.



To create the second transform:

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

Priority	2
Description	"add domain where none exists" for example
Pattern type	Regex
Pattern string	([^@]*)
Pattern behavior	Replace

Replace string	\1@vcs.domain
State	<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 with 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. Below the navigation bar, there are 'Help' and 'Logout' links. The main content area is titled 'Create transform' and includes a breadcrumb trail: 'You are here: VCS configuration > Dial plan > Transforms > Create transform'. The configuration form is titled 'Configuration' and contains the following fields:

- Priority: 2
- Description: add domain where none exists
- Pattern type: Regex
- Pattern string: *([*@!]
- Pattern behavior: Replace
- Replace string: \1@vcs.domain
- State: Enabled

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

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 *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 > Calls > 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.

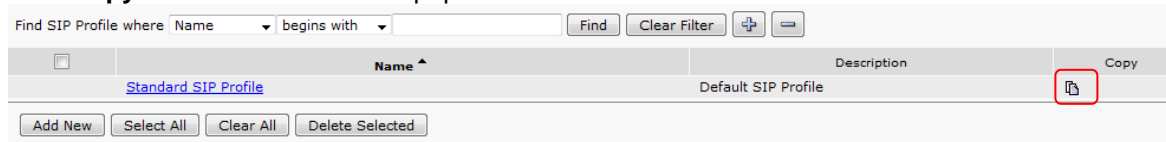
CUCM configuration

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 **Copy** – the double sheets of paper icon in the table.



3. Configure the fields as follows:

Name	Standard SIP Profile – for VCS
Default MTP Telephony Event Payload Type	101
Redirect by Application	Select the check box
Allow Presentation Sharing using BFCP	Select the check box (in CUCM 8.6.1 or later)
Timer Invite Expires	180
Timer Register Delta	5
Timer Register Expires	3600
Timer T1	500
Timer T2	Leave as default (typically 4000 or 5000)
Retry INVITE	6
Retry non-INVITE	10
Start Media Port	16384
Stop Media Port	32766
Call Pickup URI	x-cisco-serviceuri-pickup

Call Pickup Group Other URI	x-cisco-serviceuri-opickup
Call Pickup Group URI	x-cisco-serviceuri-gpickup
Meet Me Service URI	x-cisco-serviceuri-meetme
User Info	None
DTMF DB Level	Nominal
Call Hold Ring Back	Off
Anonymous Call Block	Off
Caller ID Blocking	Off
Do Not Disturb Control	User
Telnet Level for 7940 and 7960	Disabled
Timer Keep Alive Expires	120
Timer Subscribe Expires	120
Timer Subscribe Delta	5
Maximum Redirections	70
Off Hook To First Digit Timer	15000
Call Forward URI	x-cisco-serviceuri-cfwdall
Abbreviated Dial URI	x-cisco-serviceuri-abbrdial
Reroute Incoming Request to new Trunk based on	Never

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

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

Save | Delete | Copy | Reset | Apply Config | Add New

Status

- Status: Ready
- All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name* Standard SIP Profile - for VCS
 Description Default SIP Profile
 Default MTP Telephony Event Payload Type* 101
 Resource Priority Namespace List < None >
 Early Offer for G.Clear Calls* Disabled
 SDP Session-level Bandwidth Modifier for Early Offer and Re-invites* TIAS and AS
 User-Agent and Server header information* Send Unified CM Version Information as User-Agen

Redirect by Application
 Disable Early Media on 180
 Outgoing T.38 INVITE include audio mline
 Enable ANAT
 Require SDP Inactive Exchange for Mid-Call Media Change
 Use Fully Qualified Domain Name in SIP Requests
 Allow Presentation Sharing using BFCP

Parameters used in Phone

Timer Invite Expires (seconds)* 180
 Timer Register Delta (seconds)* 5
 Timer Register Expires (seconds)* 3600
 Timer T1 (msec)* 500
 Timer T2 (msec)* 4000
 Retry INVITE* 6
 Retry Non-INVITE* 10
 Start Media Port* 16384
 Stop Media Port* 32766
 Call Pickup URI* x-cisco-serviceuri-pickup
 Call Pickup Group Other URI* x-cisco-serviceuri-opickup
 Call Pickup Group URI* x-cisco-serviceuri-gpickup

Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
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 URI*	x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*	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	

Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on*	Never
RSVP Over SIP*	Local RSVP
<input checked="" type="checkbox"/> Fall back to local RSVP	
SIP Rel1XX Options*	Disabled
<input type="checkbox"/> Deliver Conference Bridge Identifier <input type="checkbox"/> Early Offer support for voice and video calls (insert MTP if needed) <input type="checkbox"/> Send send-receive SDP in mid-call INVITE	
SIP OPTIONS Ping	
<input type="checkbox"/> Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	
Ping Interval for In-service and Partially In-service Trunks (seconds)*	60
Ping Interval for Out-of-service Trunks (seconds)*	120
Ping Retry Timer (milliseconds)*	500
Ping Retry Count*	6

- Save Delete Copy Reset Apply Config Add New

4. Click **Save**.

Add a phone device

1. Go to **Device > Phone**.
2. Click **Add New**.
3. Configure as required.
If BFCP is to be used, ensure that a SIP profile is used that has the **“Allow Presentation Sharing using BFCP”** check box selected.
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.

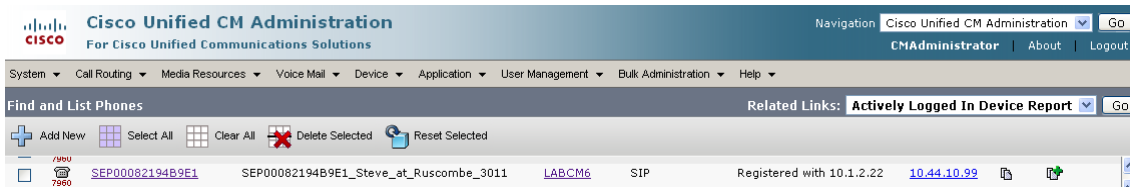
2. Select the Network Configuration section, and check whether the **TFTP Server** is the IP address of CUCM. If not:
 - a. Press the **settings** button twice – to return to SETTINGS menu.
 - b. Select **Unlock** and enter the appropriate password.
 - c. Select the Network Configuration section.
 - 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 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:

Name	Non Secure SIP Trunk Profile
Device Security Mode	Non Secure
Incoming Transport Type	TCP+UDP
Outgoing Transport Type	TCP
Incoming Port	5060
Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box

4. Click **Save**.

The screenshot shows the Cisco Unified CM Administration web interface. The page title is "SIP Trunk Security Profile Configuration". The navigation bar includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The breadcrumb trail is "System > Security > SIP Trunk Security profile". The page contains a "Status" section showing "Status: Ready". Below that is the "SIP Trunk Security Profile Information" section with the following fields:

- Name*: Non Secure SIP Trunk Profile
- Description: Non Secure SIP Trunk Profile authenticated by null Stri
- 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
- Transmit Security Status
- SIP V.150 Outbound SDP Offer Filtering*: Use Default Filter

At the bottom of the configuration area are buttons for "Save", "Delete", "Copy", "Reset", "Apply Config", and "Add New".

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:

Device Name	VCS_location, for example VCS_Ruscombe
Device Pool	(As set up in System > Device Pool)
Call classification	OnNet
Location	(As set up in System > Location)
Packet Capture Mode	None
Media Termination Point Required	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
SRTP Allowed	Select this check box

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:

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

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

Calling Party Selection	Originator
Calling Line ID Presentation	Default
Calling Name Presentation	Default

Caller ID DN	<blank>
Caller Name	<blank>

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

Destination address	<IP address of Cisco VCS> or <Domain of Cisco VCS / Cisco VCS cluster>
Destination address is an SRV	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.
Destination port	5060
Presence Group	Standard Presence Group (or whichever presence group has been configured in System > Presence Group)
SIP Trunk Security Profile	Non Secure SIP Trunk Profile
SIP Profile	Standard SIP Profile – for VCS
DTMF Signaling Method	RFC 2833
Normalization Script (only applies to CUCM 8.6 or later)	vcs-interop (if available)

9. Click **Save**.

10. Click **Reset**.

11. Click **Reset**.

The screenshot shows the 'SIP Trunk Configuration' page in Cisco Unified CM Administration. The 'Device Information' section is expanded, showing the following configuration details:

- Product: SIP Trunk
- Device Protocol: SIP
- Trunk Service Type: None(Default)
- Device Name*: VCS_Ruscombe
- Description: VCS at Ruscombe
- Device Pool*: Default
- Common Device Configuration: LABCMS
- Call Classification*: OnNet
- Media Resource Group List: < None >
- Location*: RestonLABCM6A51
- AAR Group: < None >
- Tunneled Protocol*: None
- QSIG Variant*: No Changes
- ASN.1 ROSE OID Encoding*: No Changes
- Packet Capture Mode*: None
- Packet Capture Duration: 0
- Media Termination Point Required
- Retry Video Call as Audio
- Path Replacement Support
- Transmit UTF-8 for Calling Party Name
- Transmit UTF-8 Names in QSIG APDU
- Unattended Port
- SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
- Consider Traffic on This Trunk Secure*: When using both sRTP and TLS
- Route Class Signaling Enabled*: Default
- Use Trusted Relay Point*: Default
- PSTN Access
- Run On All Active Unified CM Nodes

Intercompany Media Engine (IME)
 E.164 Transformation Profile < None >

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

Call Routing Information
 Remote-Party-Id
 Asserted-Identity
 Asserted-Type* Default
 SIP Privacy* Default

Inbound Calls
 Significant Digits* All
 Connected Line ID Presentation* Default
 Connected Name Presentation* Default
 Calling Search Space LABCMS
 AAR Calling Search Space < None >
 Prefix DN
 Redirecting Diversion Header Delivery - Inbound

Incoming Calling Party Settings
 If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default		< None >	<input checked="" type="checkbox"/>

Connected Party Settings
 Connected Party Transformation CSS < None >
 Use Device Pool Connected Party Transformation CSS

Outbound Calls
 Called Party Transformation CSS < None >
 Use Device Pool Called Party Transformation CSS
 Calling Party Transformation CSS < None >
 Use Device Pool Calling Party Transformation CSS
 Calling Party Selection* Originator
 Calling Line ID Presentation* Default
 Calling Name Presentation* Default
 Caller ID DN
 Caller Name
 Redirecting Diversion Header Delivery - Outbound
 Redirecting Party Transformation CSS < None >
 Use Device Pool Redirecting Party Transformation CSS

SIP Information

Destination
 Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.50.152.7		5060

MTP Preferred Originating Codec* 711ulaw
 Presence Group* Standard Presence group
 SIP Trunk Security Profile* Non Secure SIP Trunk Profile
 Rerouting Calling Search Space < None >
 Out-Of-Dialog Refer Calling Search Space < None >
 SUBSCRIBE Calling Search Space < None >
 SIP Profile* Standard SIP Profile - for VCS
 DTMF Signaling Method* RFC 2833

Normalization Script
 Normalization Script vcs-interop
 Enable Trace

Parameter Name	Parameter Value
1	

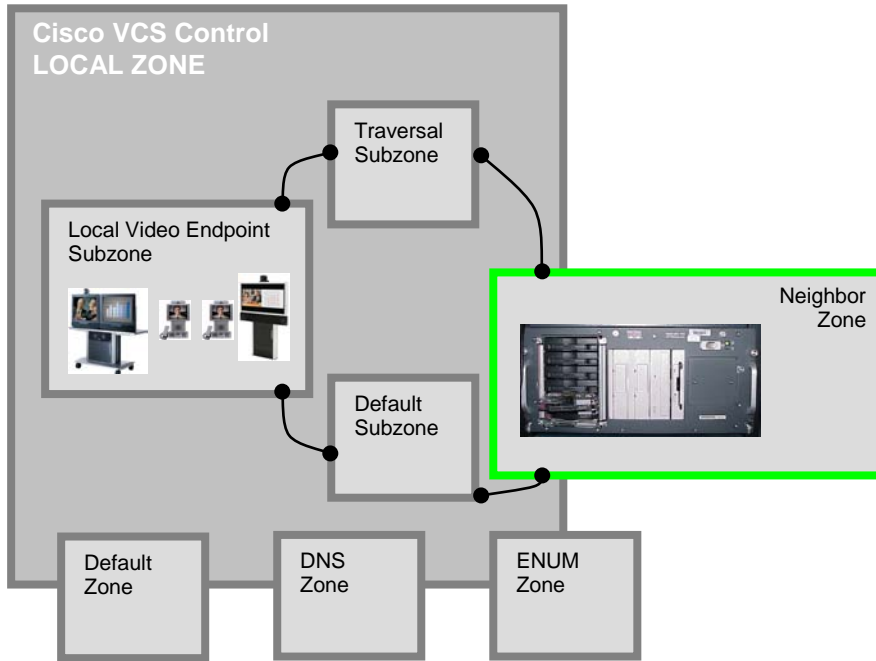
Geolocation Configuration
 Geolocation < None >
 Geolocation Filter < None >
 Send Geolocation Information

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 has 3 steps:

- Configure a neighbor zone that contains the CUCM.
- Configure a search rule to route calls to that zone.
- Configure 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 > Zones**.
2. Click **New**.
3. Configure the fields as follows:

Name	CUCM Neighbor
Type	<i>Neighbor</i>
Hop count	15
H.323 mode	<i>Off</i> (H.323 access is not required for communication with CUCM)
SIP mode	<i>On</i>
SIP port	5060 (if the SIP access port on CUCM is not 5060, change the SIP Port value to be the same as used by CUCM)
Transport	<i>TCP</i>
Accept proxied registrations	<i>Deny</i>
Media encryption mode	<i>Auto</i>
Authentication policy	Configure the authentication settings according to your authentication policy.
SIP authentication trust mode	<i>Off</i>
Peer 1 address	IP address of CUCM, or the domain of CUCM.

Zone profile (Advanced section)	Select Cisco Unified Communications Manager or Custom mode. Custom mode may be required to enable BFCP operation or when using TLS. See 'Appendix 8 – Parameters set by the 'Cisco Unified Communications Manager' Advanced Zone profile' for details on what is configured by the "Cisco Unified Communications Manager" setting, and what values to set up in Custom mode if desired..
--	--

Note: This configures the Cisco VCS Control 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 10 – Connecting Cisco VCS to CUCM using TLS (rather than TCP).

4. Click **Create zone**.

The screenshot shows the 'Create zone' configuration page in Cisco VCS Control. The breadcrumb trail is: [VCS configuration](#) > [Zones](#) > [Zones](#) > [Create zone](#). The page is organized into several sections:

- Configuration:**
 - Name:
 - Type:
 - Hop count:
- H.323:**
 - Mode:
 - Port:
- SIP:**
 - Mode:
 - Port:
 - Transport:
 - Accept proxied registrations:
 - Media encryption mode:
- Authentication:**
 - Authentication policy:
 - SIP authentication trust mode:
- Location:**
 - Peer 1 address:
 - Peer 2 address:
 - Peer 3 address:
 - Peer 4 address:
 - Peer 5 address:
 - Peer 6 address:
- Advanced:**
 - Zone profile:

At the bottom of the page are two buttons: **Create zone** and **Cancel**.

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

Search rules specify the range of telephone numbers / URIs to be 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 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.

1. Go to **VCS configuration > Dial plan > Search rules**.
2. Click **New**.
3. 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:

Rule name	Route to CUCM
Description	For example: Send 3xxx@vcs.doman calls to CUCM
Priority	100
Protocol	Any
Source	Any
Request must be authenticated	Configure this setting according to your authentication policy
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 zone	CUCM Neighbor
State	Enabled

4. Click **Create search rule**.

The screenshot shows the 'Create search rule' configuration page. The breadcrumb trail is: VCS configuration > Dial plan > Search rules > Create search rule. The configuration fields are as follows:

- Rule name: Route to CUCM
- Description: Send 3xxx@vcs.doman calls to CUCM
- Priority: 100
- Protocol: Any
- 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@10.1.2.22
- On successful match: Stop
- Target: CUCM Neighbor
- State: Enabled

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

See the “Zones and Neighbors” section of *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 – this is so that the existing search rule can route the call to CUCM:

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

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

4. Click **Create transform**.

The screenshot shows the 'Create transform' configuration page in the Cisco VCS Administrator GUI. The page is titled 'Create transform' and shows the configuration fields for a new transform. The fields are: 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), and State (Enabled). The 'Create transform' button is highlighted.

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.

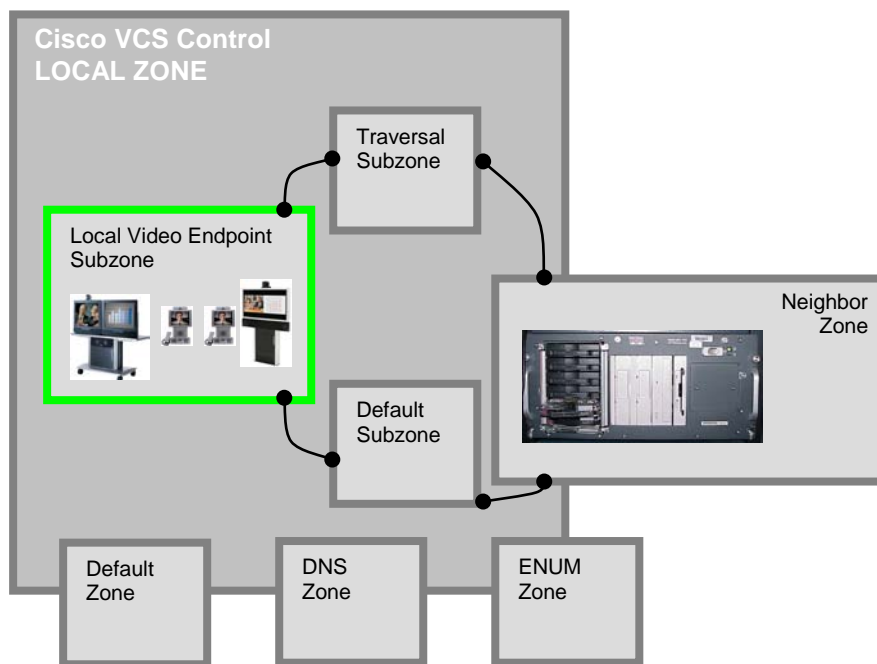
On endpoints registered to the Cisco VCS dial the extension numbers of endpoints registered on CUCM, for example 3000.

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

Cisco VCS Control configuration

The configuration of the Cisco VCS Control needs 2 steps:

- 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.
- (From X7.0.) Ensure that VCS stays in the signaling path for calls with CUCM so that CUCM knows that signaling messages need to go to the video network via the SIP trunk.



Set up a transform for CUCM to call the Cisco VCS Local and Neighbor Zones

This transform will convert URIs received from CUCM to the format used in the VCS’s Local Zone and thus expected within any neighbor zones.

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

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

Note: This search rule will handle all calls to URIs in the format **(0118912)?(4ld{3})@<IP address of VCS>:<port>** 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:

Description	CUCM to registered devices
Priority	5 (for example; note that the priority of this transform should be above any transforms that should be applied for searching local and neighbor zones)
Pattern type	Regex
Pattern string	For example: (0118912)?(4\d{3})@%ip%(:.*)?
Pattern behavior	Replace
Replace string	0118912\2@vcs.domain
State	Enabled

4. Click **Create transform**.

Ensure that VCS stays in the signaling path for calls with CUCM

To handle calls using GRUU, where the contact address is not an IP address, and allow call signaling to be routed properly where the contact IP is non-routable by CUCM (such as when Multiway is in use and the MCU is registered to the VCS), VCS needs to stay in the signaling path. This can be configured by the zone profile, as follows.

- If VCS is version X7.0.n, go to the CUCM neighbor zone and:
 - a. Change the **Advanced Zone profile** from *Cisco Unified Communications Manager* to *Custom*.
 - b. Set the parameters as documented in “Appendix 8 – Parameters set by the ‘Cisco Unified Communications Manager’ Advanced Zone profile”.
 - c. Set **Call signaling routed mode** to *Always*.
- If VCS is version X7.1 or later, these settings are applied by default in the *Cisco Unified Communications Manager* zone profile, so this does not need to be changed.

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:

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

Set Called Party Transformations:

Discard Digits	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:

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

Set Called Party Transformations:

Discard Digits	< None >
-----------------------	----------

The screenshot shows the Cisco Unified CM Administration web interface. The main heading is "Cisco Unified CM Administration" with the Cisco logo. Below it, there's a navigation menu with "Navigation" set to "Cisco Unified CM Administration" and a "Go" button. The user is logged in as "CMAdministrator". The main menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The current page is "Route Pattern Configuration" with a "Related Links" section containing "Back To Find/List" and "Go".

The configuration form is divided into several sections:

- Status:** Status: Ready
- Pattern Definition:**
 - Route Pattern*: 0118912.4XXX
 - 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: [Empty]
 - Prefix Digits (Outgoing Calls): [Empty]
 - 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: [Empty]
 - Prefix Digits (Outgoing Calls): [Empty]
- ISDN Network-Specific Facilities Information Element:**
 - Network Service Protocol: -- Not Selected --
 - Carrier Identification Code: [Empty]
 - Network Service: -- Not Selected --
 - Service Parameter Name: < Not Exist >
 - Service Parameter Value: [Empty]

At the bottom of the form, there are buttons for "Save", "Delete", "Copy", and "Add New". A note at the bottom left states: "i *- 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.

Advanced configuration

CUCM SIP Max Incoming Message Size

SIP messages for video are considerably larger than SIP messages for audio calls. In particular, when a Cisco TelePresence Server is used in the video network, SIP messages can be > 5,000 bytes (which is the default **SIP Max Incoming Message Size** configured in CUCM).

To increase the **SIP Max Incoming Message Size**, on CUCM:

1. Go to **System > Service Parameters**.
2. Select the appropriate server.
3. Select **Cisco CallManager (Active)** as the service.
4. Select **Advanced**.
5. In the Clusterwide Parameters (Device – SIP) configure the field as follows:

SIP Max Incoming Message Size		12000
SIP Station UDP Port Throttle Threshold *	50	50
SIP Trunk UDP Port Throttle Threshold *	200	200
SIP V.150 Outbound SDP Offer Filtering *	No Filtering	No Filtering
SIP Max Incoming Message Size *	12000	5000
SIP Max Incoming Message Headers *	100	100
Send SIP Multicast TTL in SDP *	False	False
Default PUBLISH Expiration Timer *	3600	3600
Minimum PUBLISH Expiration Timer *	60	60

6. Click **Save**.

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 that 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 have only 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

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

Tracing calls

Tracing calls at SIP / H.323 level

X7 or later:

1. Log in to Cisco VCS Control web interface as **admin**.
2. Go to **Maintenance > Diagnostics > Diagnostics logging**.
3. Ensure all log levels are set to *DEBUG* and click **Start new log**.
4. Retry the action for which the problem occurs (such as setting up a call or similar).
5. Click **Stop logging** followed by **Download log**.

The log file will contain information related to the events triggered by the action performed in step 4.

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 Cisco Unified CM Administration interface. The main heading is "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation bar includes "Navigation Cisco Unified CM Administration" and "Go". Below the navigation bar, there are tabs for "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The current page is "Service Parameter Configuration" with a "Related Links: Parameters for All Servers" and a "Go" button. The "Clusterwide Parameters (Device - SIP)" section is displayed, showing a table of parameters. The "SIP Min-SE Value" parameter is highlighted with a red circle, showing a value of 500 in the input field and 1800 in the current value field.

Parameter Name	Current Value	Default Value
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 Rel1XX *	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 Rel1XX Timer *	500	500
SIP Trying Timer *	500	500
SIP Publish Timer *	500	500
SIP Min-SE Value *	500	1800
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.

Call failures with Cisco TelePresence Server

SIP messages from Cisco TelePresence Server can be > 5,000 bytes (which is the default **SIP Max Incoming Message Size** configured in CUCM).

Increase the **SIP Max Incoming Message Size** – see "CUCM SIP Max Incoming Message Size".

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 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.

Failure to join a CUCM endpoint to a conference using Multiway

Ensure that VCS and CUCM are set up as described in “Appendix 6 – Cisco TelePresence Multiway and CUCM”.

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** = *UCM*
 - **Services** = *Cisco CallManager*
 - **Trace File Type** = *sdi*
7. Click **Finish**.

Note that:

- 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.

Cisco TelePresence Conductor

When Cisco VCS is configured to work with Conductor, calls made from CUCM over the SIP trunk may initiate or join conferences controlled by Conductor.

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 – 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:

Pattern Usage	<i>Domain Routing</i>
Pattern	Domain for calls, for example vcs.domain
Route Partition	Default is "<None>"; set according to dial plan restrictions
SIP Trunk	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
CMAAdministrator | 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 (TCP) or NNNN@<IP address of VCS>:5061 (TLS)

Appendix 4 – 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 the DNS SRV address for the VCS cluster
- the trunk to VCS specifies a list of VCS peers

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

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

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

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

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 AS1
 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*: Originator
 Calling Line ID Presentation*: Default
 Calling Name Presentation*: Default
 Caller ID DN:
 Caller Name:

Redirecting Diversion Header Delivery - Outbound

SIP Information

Destination Address*: 10.44.9.214
 Destination Address is an SRV
 Destination Port*: 5060
 MTP Preferred Originating Codec*: 711ulaw
 Presence Group*: Standard Presence group
 SIP Trunk Security Profile*: Non Secure SIP Trunk Profile
 Rerouting Calling Search Space: < None >
 Out-Of-Dialog Refer Calling Search Space: < None >
 SUBSCRIBE Calling Search Space: < None >
 SIP Profile*: Standard SIP Profile
 DTMF Signaling Method*: No Preference

Save | Delete | Reset | Add New

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

- On VCS, ensure that the cluster name is configured as a SIP domain (**VCS Configuration > Protocols > SIP > Domains**).

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

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

4. Configure the SIP Information fields as follows:

Destination address is an SRV	Ensure that this check box is not selected
Destination address 1	IP address or DNS name of VCS peer 1
Destination port 1	5060 or 5061 depending on connectivity (TCP/TLS)
Destination address 2	IP address or DNS name of VCS peer 2
Destination port 2	5060 or 5061 depending on connectivity (TCP/TLS)
Destination address 3	IP address or DNS name of VCS peer 3 – if it exists
Destination port 3	5060 or 5061 depending on connectivity (TCP/TLS)
Destination address 4	IP address or DNS name of VCS peer 4 – if it exists
Destination port 4	5060 or 5061 depending on connectivity (TCP/TLS)
Destination address 5	IP address or DNS name of VCS peer 5 – if it exists
Destination port 5	5060 or 5061 depending on connectivity (TCP/TLS)
Destination address 6	IP address or DNS name of VCS peer 6 – if it exists
Destination port 6	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 5 – 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 be done in 3 ways, in order of preference:

1. With a single neighbor zone in VCS with the CUCM nodes listed as location peer addresses. This option is only available from VCS X7.0 or later.
2. By using DNS SRV records and a Cisco VCS DNS zone.
3. 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).

Options 1 and 2 are recommended as they ensure that the Cisco VCS to CUCM call load is shared across CUCM nodes. Option 3 only provides redundancy; it does not provide load balancing.

Option 1: Using a single neighbor zone

This is only available for a Cisco VCS running version X7.0 or later.

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.

The screenshot shows a configuration window titled 'Clusterwide Domain Configuration'. It contains two input fields: 'Organization Top Level Domain' and 'Cluster Fully Qualified Domain Name'. The 'Cluster Fully Qualified Domain Name' field is highlighted with a red box in the original image.

2. Set the **Cluster Fully Qualified Domain Name** to the same domain as the video network, for example vcs.domain.
This parameter defines one or more Fully Qualified Domain Names (FQDNs) for this cluster. Multiple FQDNs must be separated by a space. Requests containing URLs (for example, SIP calls) whose host portion matches any of the FQDNs in this parameter will be recognized as a request destined for this cluster and/or devices attached to it.

Cisco VCS Control configuration

Cisco VCS configuration requires 1 step:

- Update neighbor zone

Update neighbor zone

1. Go to **VCS configuration > Zones**.
2. Select the CUCM Neighbor zone.
3. Configure the fields as follows:

Peer 1 address	IP address of CUCM node 1, or the domain of CUCM node 1.
Peer 2 address	IP address or the domain of CUCM node 2.

Peer 3 address	IP address or the domain of CUCM node 3, or blank if no CUCM node 3.
Peer 4 address	IP address or the domain of CUCM node 3, or blank if no CUCM node 4.
Peer 5 address	IP address or the domain of CUCM node 3, or blank if no CUCM node 5.
Peer 6 address	IP address or the domain of CUCM node 3, or blank if no CUCM node 6.

Option 2: Using a DNS zone

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.

The screenshot shows the 'Clusterwide Domain Configuration' section with two input fields: 'Organization Top Level Domain' and 'Cluster Fully Qualified Domain Name'.

2. Set the **Cluster Fully Qualified Domain Name** to the same domain as the video network, for example vcs.domain.
This parameter defines one or more Fully Qualified Domain Names (FQDNs) for this cluster. Multiple FQDNs must be separated by a space. Requests containing URLs (for example, SIP calls) whose host portion matches any of the FQDNs in this parameter will be recognized as a request destined for this cluster and/or devices attached to it.

DNS server configuration

Configure the DNS server (that is used by the Cisco VCS) with DNS SRV records for the CUCM cluster.

- `_sips._tcp.fqdn_of_cucm_cluster` records for TLS connectivity (one record for each CUCM node)
or
- `_sip.tcp.fqdn_of_cucm_cluster` records 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 > Zones**.
2. Click **New**.
3. Configure the fields as follows:

Name	CUCM Cluster Neighbor DNS Zone
Type	DNS
Hop count	15

H.323 mode	<i>Off</i> H.323 access is not required for communication with CUCM
SIP mode	<i>On</i>
TLS verify mode	<i>Off</i>
Media encryption mode	<i>Auto</i>
Include address record	<i>Off</i>
Zone profile	Select <i>Cisco Unified Communications Manager</i> . See 'Appendix 8 – Parameters set by the 'Cisco Unified Communications Manager' Advanced Zone profile' for details on what is configured by this setting.

4. Click **Create zone**.

The screenshot shows the 'Create zone' configuration page in the Cisco VCS web interface. The breadcrumb trail indicates the path: VCS configuration > Zones > Zones > Create zone. The form is organized into four sections:

- Configuration:** Name (CUCM Cluster Neighbor DNS Zone), Type (DNS), Hop count (15).
- H.323:** Mode (Off).
- SIP:** Mode (On), TLS verify mode (Off), Media encryption mode (Auto).
- Advanced:** Include address record (Off), Zone profile (Cisco Unified Communications Manager).

Buttons for 'Create zone' and 'Cancel' are located at the bottom left of the form.

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.

Note that 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.

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

Rule name	Route to CUCM
------------------	---------------

Description	For example: 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	Leave
On successful match	Stop
Target zone	CUCM Cluster Neighbor DNS Zone
State	Enabled

4. Click **Save**.

The screenshot shows the 'Edit search rule' configuration page in the Cisco VCS Administrator. The page has a breadcrumb trail: 'You are here: VCS configuration > Dial plan > Search rules > Edit search rule'. The configuration form includes the following fields and values:

- Rule name: * Route to CUCM
- Description: Send 3xxx@vcs.doman calls to CUCM
- Priority: * 100
- Protocol: Any
- 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 are three buttons: Save, Delete, and Cancel.

See the “Zones and Neighbors” section of *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 > Zones**.
2. Select the check box next to the “CUCM Neighbor” zone.
3. Click **Delete**.

Option 3: Using multiple neighbor zones

This option only provides redundancy; it does not provide load balancing.

Cisco VCS Control configuration

- Replicate neighbor zone
- Replicate search rule

Replicate neighbor zone

Replicate the neighbor zone created for the single CUCM peer – once for each node, adjusting the **Name** and **Peer 1 address** for each CUCM node.

Replicate search rule

Replicate the search rule created for the single CUCM peer – once for each node, adjusting the **Priority**, and the **Target** so that each search rule targets a different CUCM neighbor zone.

Appendix 6 – Cisco TelePresence Multiway and CUCM

To enable CUCM registered endpoints to be joined into a Multiway™ conference:

1. Ensure a zone profile with **Call Signaling Routed Mode** set to *Always* is in use on the Zone towards the CUCM on the VCS.
2. Ensure that CUCM will route calls to VCS (using Route Patterns) which have the domain given by the Multiway alias.
3. Ensure that CUCM is configured with “Redirect by Application” selected in the SIP profile used by the SIP trunk to VCS.

VCS configuration

If Cisco VCS X7.0.n is in use, or a custom zone profile is in use, in Cisco VCS, go to the CUCM neighbor zone and:

1. Change the **Advanced Zone profile** from *Cisco Unified Communications Manager* to *Custom*.
2. Set the parameters as documented in “Appendix 8 – Parameters set by the ‘Cisco Unified Communications Manager’ Advanced Zone profile”.
3. Ensure that **Call signaling routed mode** is set to *Always*.

CUCM configuration

Ensure that CUCM will route calls to VCS which have a video domain:

1. Follow the instructions in “Appendix 3 – Allow dialing to Cisco VCS domain from Cisco phones”.

In the SIP profile used by the SIP trunk to VCS, ensure that “Redirect by Application” is selected:

1. Go to **Device > Device Settings > SIP Profile**.
2. Select the check box by Redirect by Application.
3. Click **Save**.
4. Click **Apply Config**.
5. Click **OK**.

SIP Profile Information	
Name*	Standard SIP Profile
Description	Default SIP Profile
Default MTP Telephony Event Payload Type*	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
<input checked="" type="checkbox"/> Redirect by Application	
<input type="checkbox"/> Disable Early Media on 180	
<input type="checkbox"/> Outgoing T.38 INVITE include audio mline	
<input type="checkbox"/> Enable ANAT	
<input type="checkbox"/> Require SDP Inactive Exchange for Mid-Call Media Change	
<input type="checkbox"/> Use Fully Qualified Domain Name in SIP Requests	
<input checked="" type="checkbox"/> Allow Presentation Sharing using BFCP	

You can now test Multiway.

Appendix 7 – 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 8 – Parameters set by the ‘Cisco Unified Communications Manager’ Advanced Zone profile

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

Parameter	Value
Monitor peer status	Yes
Call signaling routed mode	Always (was “Auto” in VCS versions prior to X7.1)
Automatically respond to H.323 searches	Off
Automatically respond to SIP searches	Off
Empty INVITE allowed	On
SIP poison mode	Off
SIP encryption mode	Auto
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 (was “On” in VCS versions prior to X7.2 due to compatibility issues)
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>

Use of BFCP

To use BFCP with endpoints registered to CUCM 8.6.1 or later, select *Custom* for the **Advanced Zone profile**, configure the entries as above, then change **SIP UDP/BFCP filter mode** to *Off*.

Further configuration will be needed on CUCM – see “Appendix 12 – Enabling BFCP”.

Use of Call Signaling Routed Mode (VCS X7.0.n or earlier)

If TLS connectivity is used from Cisco VCS to CUCM, and VCS is configured with optimal routing, either CUCM has to trust the certificates for all VCSs in the network, or, select *Custom* for the **Advanced Zone profile**, configure the entries as above, then change **Call signaling routed mode** to *Always*. This ensures that the VCS neighbored to CUCM will remain in the call signaling path for calls to and from CUCM, so that CUCM only has to trust this VCS cluster’s certificates.

Call signaling routed mode set to *Always* is also important where endpoints are using GRUU contact addresses (from VCS X7.0) or where IP addresses of video devices are unroutable directly from CUCM. It should also be set when interfacing between CUCM and MCUs for Multiway. VCS staying in the signaling path ensures messaging can be routed properly.

Appendix 9 – 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 10 – 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
- update the Cisco VCS search rule to use port 5061 instead of port 5060

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 **Server certificate** page (**Maintenance > Certificate management > Server certificate**).
 - 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:

Certificate Name	CallManager-trust.
Root Certificate	<leave blank>
Description	Enter a textual description as required.
Upload File	Click Browse... 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:

Name	A name indicating that this profile is an encrypted profile for the specific X.509 name(s).
Description	Enter a textual description as required.
Device Security Mode	Select <i>Encrypted</i> .
Incoming Transport Type	Select <i>TLS</i> .
Outgoing Transport Type	Select <i>TLS</i> .
Enable Digest Authentication	Leave unselected.
X.509 Subject Name	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.)
Incoming Port	5061
Other parameters	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	
Device Name	This name must match the subject name of the Cisco VCS certificate (as used in the X.509 Subject Name in the security profile).
Description	Update as required; you may want to indicate that this is now a TLS connection.
SIP Information section	
Destination Port	5061
SIP Trunk Security Profile	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 VCS neighbor zone to CUCM to use TLS

Note: 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 VCS:

1. On the **Edit zone** page (**VCS configuration > Zones > 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 VCS zone reports its status as active and then make some test calls:

1. Check the 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 VCS registered endpoint to a CUCM phone.
3. Make a test call from a CUCM phone to a 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.

Network of VCSs

If there is a network of VCSs behind this VCS neighbored to CUCM, then, either:

- CUCM must trust the certificates of all the VCSs in the network, or
- (From X7.0) configure VCS neighbor zone to 'always' route the signaling

Set VCS to always route signaling to CUCM

With TLS configured between VCS and CUCM, and where VCS is configured for optimal routing (usual case), either:

- CUCM must trust the certificates for all VCSs in the network, or
- If VCS is version X7.0.n, or a custom zone is in use, go to the CUCM neighbor zone and:
 - a. Change the **Advanced Zone profile** from *Cisco Unified Communications Manager* to *Custom*.
 - b. Set the parameters as documented in "Appendix 8 – Parameters set by the 'Cisco Unified Communications Manager' Advanced Zone profile".
 - c. Set **Call signaling routed mode** to *Always*.

Appendix 11 – 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.

Appendix 12 – Enabling BFCP – Dual video / presentation sharing

This requires CUCM version 8.6.1 or later.

VCS configuration

In Cisco VCS, go to the CUCM neighbor zone and:

1. Change the **Advanced Zone profile** from *Cisco Unified Communications Manager* to *Custom*.
2. Set the parameters as documented in “Appendix 8 – Parameters set by the ‘Cisco Unified Communications Manager’ Advanced Zone profile”.
3. Ensure that **SIP UDP/BFCP filter mode** is set to *Off*.

CUCM configuration

In the SIP profile used by the SIP trunk to VCS, select “Allow Presentation Sharing using BFCP”

On CUCM

1. Go to **Device > Device Settings > SIP Profile**.
2. Select the check box by **Allow Presentation Sharing using BFCP**.
3. Click **Save**.
4. Click **Apply Config**.
5. Click **OK**.

SIP Profile Information	
Name*	Standard SIP Profile
Description	Default SIP Profile
Default MTP Telephony Event Payload Type*	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
<input checked="" type="checkbox"/> Redirect by Application	
<input type="checkbox"/> Disable Early Media on 180	
<input type="checkbox"/> Outgoing T.38 INVITE include audio mline	
<input type="checkbox"/> Enable ANAT	
<input type="checkbox"/> Require SDP Inactive Exchange for Mid-Call Media Change	
<input type="checkbox"/> Use Fully Qualified Domain Name in SIP Requests	
<input checked="" type="checkbox"/> Allow Presentation Sharing using BFCP	

You can now test BFCP operation.

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.
8	August 2011	Updated for Cisco VCS X7.0 and BFCP. Updated guidance on connecting Cisco VCS to a cluster of CUCM nodes.
9	October 2011	Updated guidance on configuration for Multiway (Call Signaling Routed Mode).
10	March 2012	Updated for Cisco VCS X7.1
11	August 2012	Updated for Cisco VCS X7.2

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. 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.

© 2012 Cisco Systems, Inc. All rights reserved.