Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

MIDSIZE

COLLABORATION

VCS and UCM Video Integration Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

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

What's In This SBA Guide

About SBA

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

For more information, see the *How to Get Started with Cisco SBA* document:

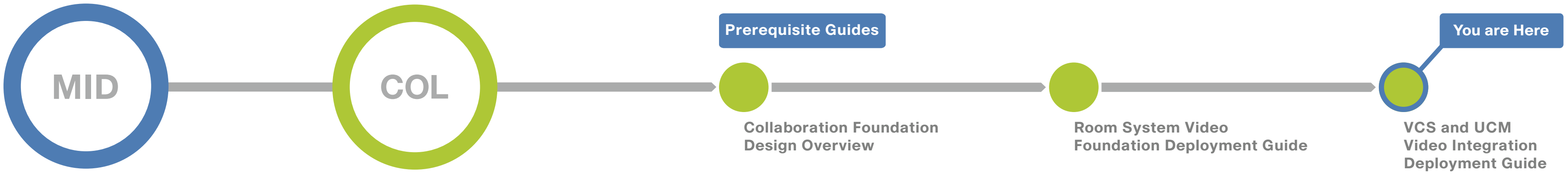
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *additional deployment guide* includes the following sections:

- Business Overview—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- Technology Overview—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- Deployment Details—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.


MID
COL
Prerequisite Guides
You are Here
Collaboration Foundation Design Overview
Room System Video Foundation Deployment Guide
VCS and UCM Video Integration Deployment Guide

Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

Business Overview

Organizations often choose between two distinct types of video solutions based on their immediate needs, without giving much thought about connecting the disparate platforms. *General-purpose systems* are set up quickly when an organization needs to see and hear remote participants, and the quality of the experience is not that much of a concern. The units are designed to move from room to room. *Immersive systems* take longer to deploy because they create a virtual room experience when high-quality video and spatial audio is important. These high-end systems are not moved between rooms, but they offer a consistently greater level of video and audio capability to the participants.

General-purpose video endpoints are less expensive and more versatile. They are normally purchased with rolling carts, so they are easy to relocate and use by a larger number of people in different conference rooms. They are the true workhorses of the video world, and they have been around for many years in countless organizations. On the other hand, immersive systems are deployed as an extension of the boardroom or as an executive conferencing solution. These solutions give the users the sense of being in the same room, and they are meant to make participants to feel as if they are meeting each other in person.

Just like the varied problems they are trying to solve, the underlying technologies are different between the two types of solutions. These walls of separation are acceptable when the deployments are small, but as video collaboration continues to grow, organizations need the individual siloes to communicate with each other on a regular basis. They want the general-purpose workrooms to connect with the boardroom, and they want remote workers in remote offices to communicate with executives in conference rooms at the headquarters location. The technology barriers between the two systems are not easy to overcome without proper guidance.

The biggest issues faced by organizations who want to combine their disparate video solutions are as follows:

- Endpoints require specific features to operate at their highest capabilities
- Advanced features do not interoperate between solutions
- Endpoint identification is difficult to manage
- Incorrect settings can adversely affect the network

Users of general-purpose video conferencing have grown accustomed to advanced features within their products. They do not mind configuring the system with a multi-button remote control because they need a higher level of sophistication to run effective meetings. The video conferencing endpoints handle most of the difficult functions themselves. By contrast, immersive users walk into a conference room, sit down and push a single button to virtually extend their meeting to other locations around the world. This level of simplicity hides the underlying complexity from the participants. Having two types of solutions is an operational issue for organizations when the technical intricacies are not taken into consideration.

Technology Overview

Cisco general-purpose and Cisco TelePresence System (CTS) immersive video solutions communicate directly on point-to-point calls without a video transcoder or multipoint control unit (MCU) in the middle. This level of interoperability allows the general-purpose room systems to communicate with the immersive systems without additional video infrastructure hardware and calling complexity. Remote-site workers who use the less expensive systems can participate in video calls with the executives at the main locations when needed.

The Cisco® TelePresence Video Communication Server (VCS) manages the general-purpose systems, and Cisco Unified Communications Manager (Unified CM) manages the CTS immersive solutions and the video telephony endpoints. Certain general-purpose endpoints can also register with Unified CM, but advanced H.323 features are only supported with VCS.

Cisco VCS is deployed as a single call-server to simplify the initial configuration. The VCS endpoints include multipurpose room systems, executive systems, and personal systems. The Unified CM configuration builds on the Cisco Smart Business Architecture (SBA) Collaboration Foundation using a two- or three-server cluster. The Unified CM endpoints consist of three-screen room systems, single-screen room systems, executive systems, personal video telephones, and video-enabled tablets. The connection between the call agents is accomplished with the Session Initiation Protocol (SIP).

When the two call agents are connected, organizations gain the following benefits:

- General-purpose endpoints register to VCS and maintain their advanced features, like duo-video, far end camera control (FECC), and multisite and multiway conferencing.
- CTS and video telephony endpoints register with Unified CM and maintain their centralized software updates, dynamic configuration settings, and simple, one-touch interfaces.
- General-purpose endpoints are given a unique phone number range to simplify the routing of calls between the two call agents.
- Quality of service (QoS) is configured differently for each solution, so the traffic is properly identified in the network infrastructure.

With general-purpose video endpoints, camera angles and aspect ratios are not considered critical as long as the remote sites can see, hear, and share data with each other. The most important aspect of the general-purpose systems is the short amount of time needed to set them up and the ease with which they are deployed in various conference room environments.

Advanced video conferencing features, like duo-video for sharing presentations, are only supported in VCS. Other features that are only supported in VCS are FECC to allow remote sites to manipulate their viewing angle and multisite/multiway conferences. Multisite conferencing allows an endpoint with built-in conference capabilities to add a third device into a call. Multiway conferencing allows endpoints to initiate ad-hoc multi-point calls using a standard MCU. Bandwidth management beyond a simple hub and spoke topology is modeled with the advanced call admission control features of Pipes and Links in VCS.

On the other hand, CTS immersive systems require very specific room dimensions to accommodate specific camera angles and audio speaker placement. The conference rooms are built with strict lighting and acoustical properties to provide the highest quality experience. Heating and A/C units are designed to run quietly, and small details like the color of the carpet and paint on the walls are taken into consideration. Matching furniture is purchased for the locations to further enhance the virtual room experience.

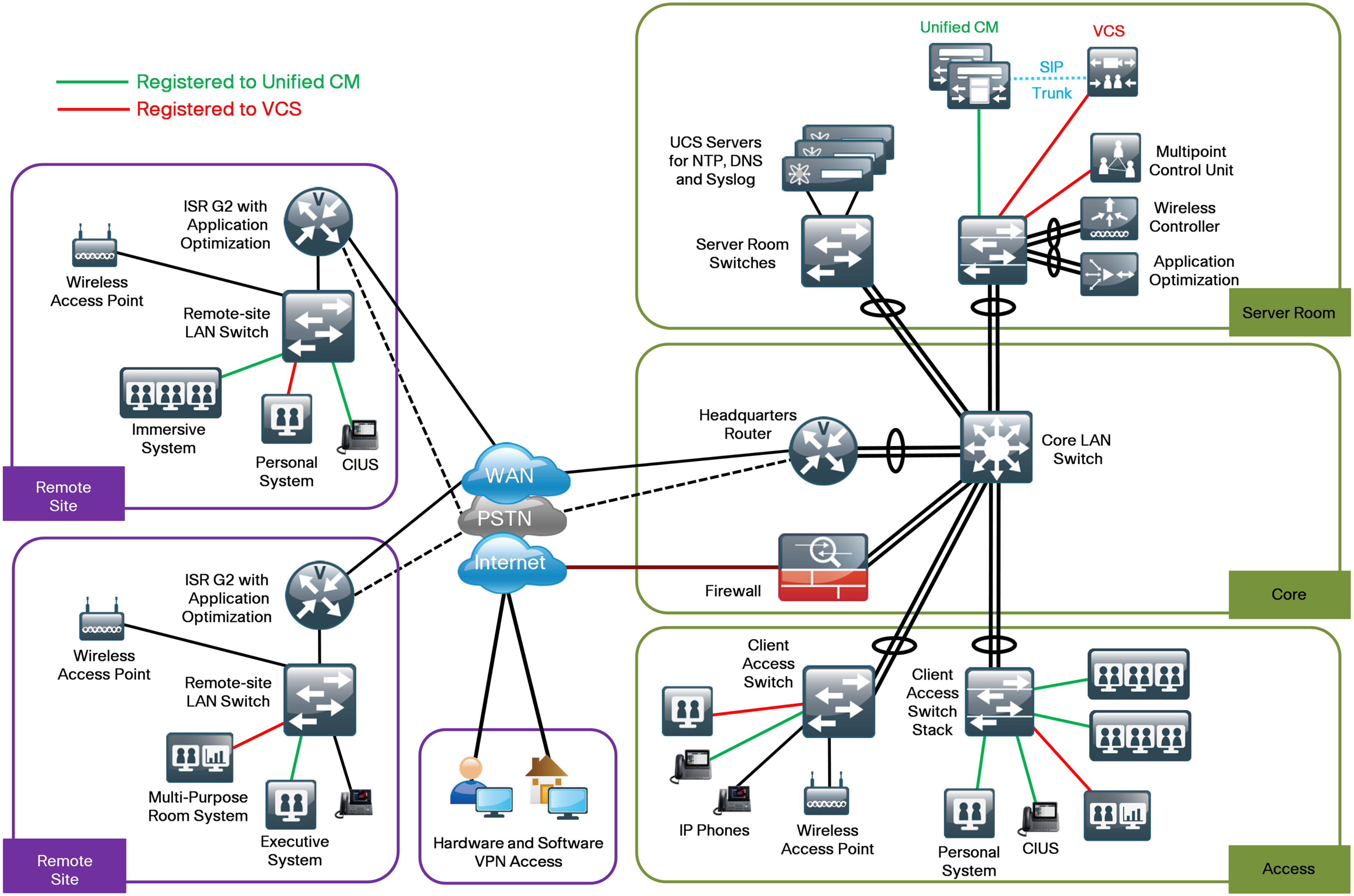
CTS endpoints register to Unified CM because it provides phone-like behavior for handling software updates and dynamic configuration settings. The user interaction on an immersive system comes from a simple telephone interface because the intended audience is different than a general-purpose video conference deployment. The ability to connect with non-Unified CM endpoints is solved by configuring the external call signaling to use a standards-based protocol that is supported by the two call agents.

Solution Details

The video integration solution includes the following components shown in the diagram below:

- VCS for general-purpose video conferencing systems
- Unified CM for CTS immersive and video telephony systems
- Personal, executive, and multi-purpose room systems
- Video telephones and video-enabled tablets
- Network Time Protocol (NTP) server for logging consistency
- Domain Name System (DNS) for name-to-IP resolution
- Syslog server for logging events (optional)

Figure 1 - VCS and Unified CM video in SBA midsize foundation architecture



The video endpoints on both systems use a numeric phone number for dialing, which preserves the capability for receiving calls from devices that only support number dialing. Both call agents convert the dialed digits and domain name attributes before sending the call, so the calls are properly formatted for the respective platforms.

The solution builds upon the Cisco SBA Midsize Organizations Borderless Networks Foundation network, which uses the medianet QoS and bandwidth control settings recommended by Cisco. General-purpose video conferencing traffic from VCS and video telephony traffic from Unified CM use assured forwarding 41 (AF41), and CTS traffic from Unified CM is marked as class selector 4 (CS4). The call-signaling traffic is marked as call selector 3 (CS3). The bandwidth for calls between locations is controlled by VCS for the general-purpose endpoints and by Unified CM for the CTS and video telephony endpoints. The two call agents work in parallel with each other for bandwidth control.

The priority bandwidth queues in the routers and switches are provisioned for the total amount required by both call agents. Because the call agents are working in parallel, the two types of video traffic are treated like "ships passing in the night" between the remote locations. This allows VCS and Unified CM to autonomously manage their bandwidth settings without interfering with each other at the queuing points in the network because the queues are configured to allow the combined bandwidth from both call agents. The bandwidth for calls within a location on a single call agent is handled by default call settings.

The Midsize Organization Borderless Networks Foundation is configured to allow 23 percent of the available WAN bandwidth for video calls. In this example, the remote sites have 15 Mbps of bandwidth into the Multiprotocol Label Switching (MPLS) cloud to accommodate two 1.5 Mbps calls at each location and the headquarters site has 30 Mbps to accommodate four calls. This means that each call control agent is limited to one call in and out of the remote site. If more calls are needed, you need additional WAN bandwidth at the remote sites and the headquarters location to accommodate the higher number.

The call control agents are centralized in the data center. The access, WAN, and campus networks are medianet-enabled, using highly available designs and localized services, like medianet call monitoring and media tracing. These services are configured in the remote sites whenever possible. The video monitoring capabilities are used to troubleshoot problems when they arise and media trace allows the administrator to view the health of all of the network components in the path. The advantage of bringing Cisco video technologies to the Cisco SBA reference design is that the initial foundation work remains intact because the architecture was originally designed with video communication in mind.

Notes

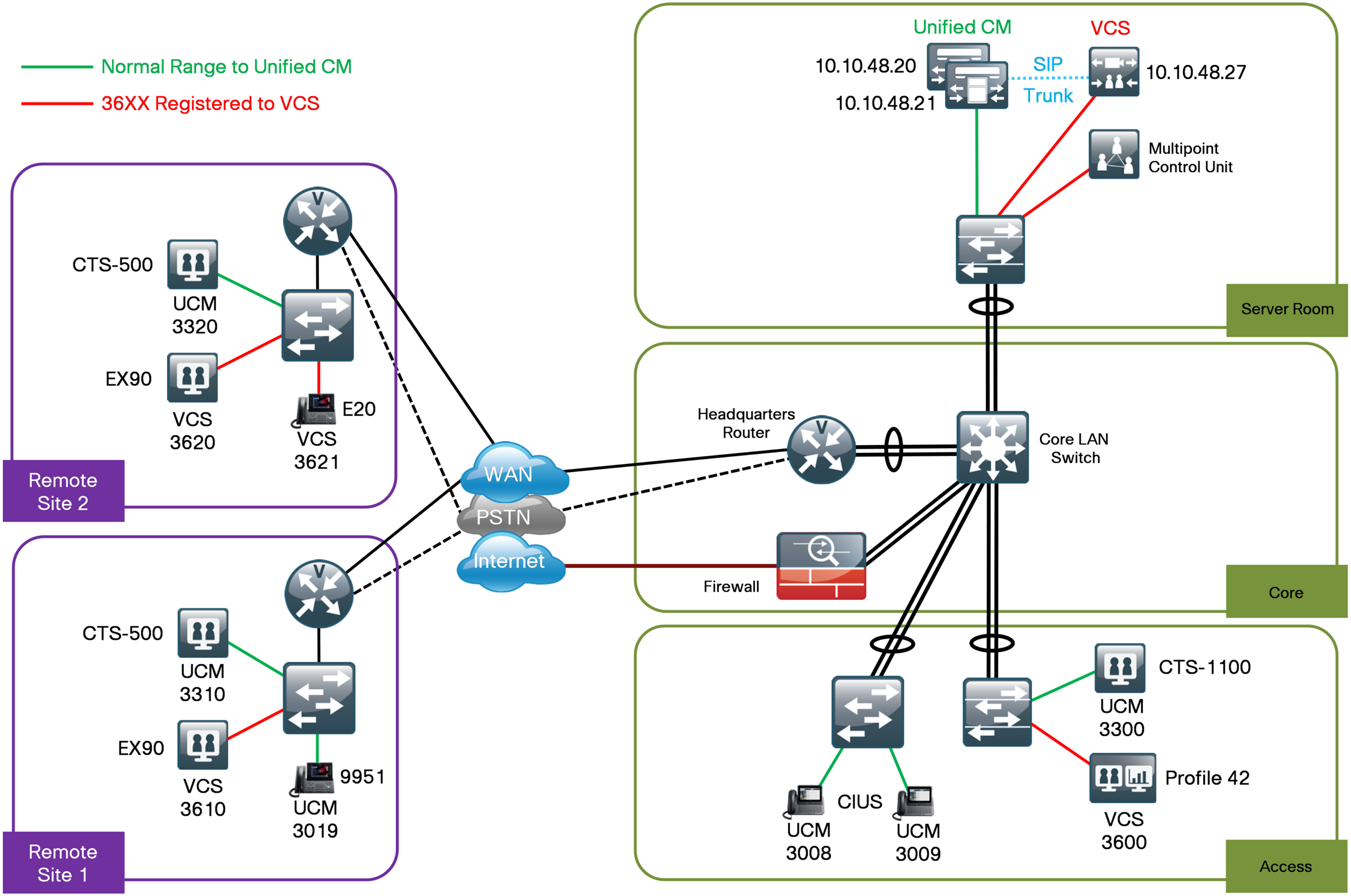
Deployment Details

This deployment guide focuses on calls between general-purpose video conferencing systems registered to a Cisco VCS and CTS immersive video endpoints registered to a Cisco Unified CM. The procedures for configuring and registering SIP and H.323 devices to VCS is documented in the *Room-System Video Foundation Deployment Guide* and the *H.323 Video Integration Deployment Guide*, so the concepts are not covered again in this guide.

The Unified CM endpoints use their full range of extensions and a domain name of [10.10.48.21]. The VCS endpoints use the 36XX range of extensions and a domain name of cisco.local. The distinct number range on VCS provides a non-overlapped dial plan that allows simple call routing on each call agent.

Notes

Figure 2 - Directory numbers for VCS and Unified CM video endpoints



Process

Configuring Cisco Unified CM

1. Configure CTS immersive endpoints
2. Configure CTS associated phones
3. Configure CTS phone application
4. Configure video telephony endpoints
5. Configure video-enabled tablets
6. Configure UCM call admission control
7. Unified CM to Unified CM calling
8. Configure Unified CM to VCS calling

The procedures for configuring a basic Unified CM cluster are documented in the *Unified Communications Manager Deployment Guide*, so the concepts are not covered again in this guide. The procedures for setting up the physical rooms and CTS endpoints are documented at http://www.cisco.com/go/telepresenceservices and they are not covered in this guide.

The steps in the following three procedures must be completed for each of the CTS endpoints and their associated phones.

Procedure 1 Configure CTS immersive endpoints

CTS endpoints and their associated IP phones are manually configured in Unified CM. Depending on the version of code on each device, the codec and phone might need to be upgraded to match the version in Unified CM. The upgrade process can take up to an hour to complete. .

Step 1: Connect the cables as specified in the endpoint installation guide, and turn on the main power switches for the codec and display. Wait several minutes for the system and associated Cisco IP phone to power up. As the system is powering up, the IP address and MAC address of the endpoint are displayed on the screen for several minutes. Make a note of this information, because you will need it in subsequent steps.

Step 2: Using your web browser, access the Unified CM Administration interface using the hostname or IP address.

Step 3: In the center of the page under **Installed Applications**, click the **Cisco Unified Communications Manager** link.

Tech Tip

If you receive a warning about the website's security certificate, ignore it and continue to the website page.

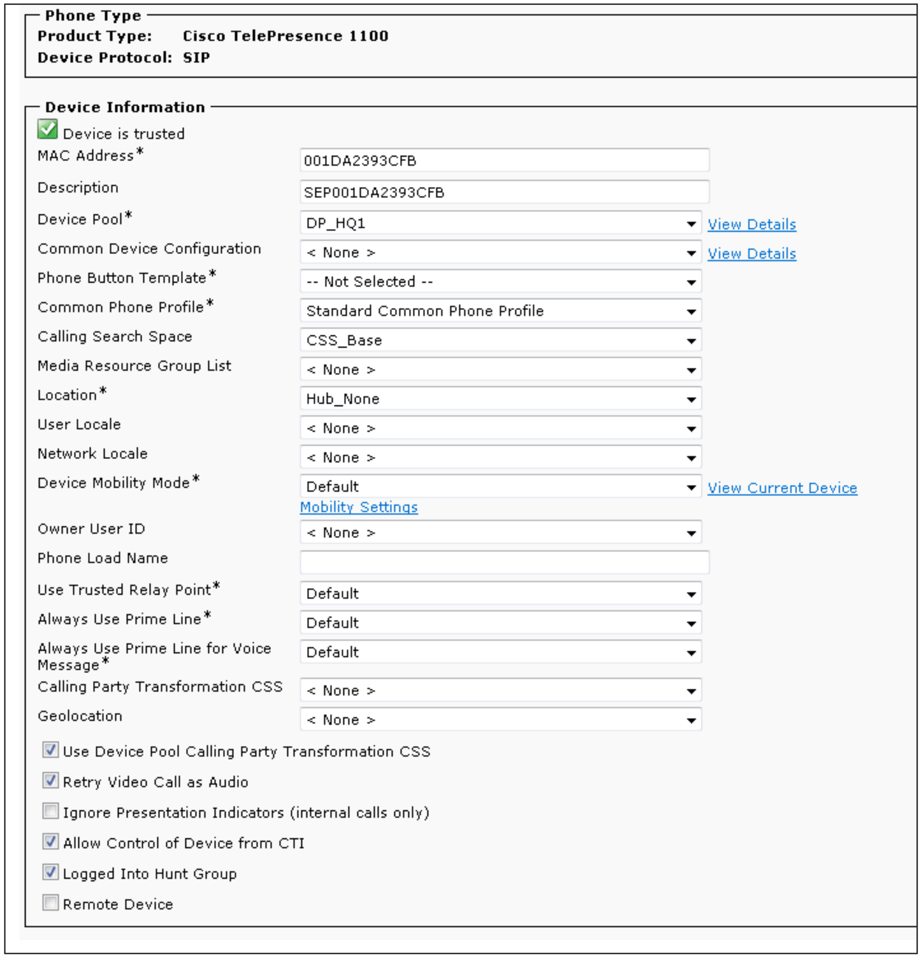
Step 4: Enter the **Username** and **Password** you entered for the Administrator User, and then click **Login**.

Step 5: Navigate to **Device > Phone**, and then click **Add New**.

Step 6: In the Product Phone list, choose: **Cisco TelePresence 1100**, and then click **Next.**

Step 7: On the Phone Configuration screen, enter the following values, and then click **Save:**

- MAC Address—[MAC Address]
- Description—HQ CTS-1100
- Device Pool—DP_HQ1
- Phone Button Template—Standard_Cisco_TelePresence_1100
- Calling Search Space—CSS_Base
- Device Security Profile—Cisco TelePresence 1100 - Standard SIP Non-Secure Profile
- SIP Profile—Standard SIP Profile
- SSH admin Password—[password]
- SSH admin Life—0 (does not expire)
- SSH helpdesk Password—[password]
- SSH helpdesk Life—0 (does not expire)
- Enable SNMP—Enabled (v2c)
- SNMP System Location—San Jose, CA (optional)
- SNMP System Contact—John Smith (optional)
- SNMP (v2c) Community Read Only—cisco
- SNMP (v2c) Community Read Write—cisco123



Phone Type

Product Type: Cisco TelePresence 1100

Device Protocol: SIP

Device Information

☑ Device is trusted

MAC Address*	001DA2393CFB
Description	SEP001DA2393CFB
Device Pool*	DP_HQ1 (View Details)
Common Device Configuration	< None > (View Details)
Phone Button Template*	-- Not Selected --
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	CSS_Base
Media Resource Group List	< None >
Location*	Hub_None
User Locale	< None >
Network Locale	< None >
Device Mobility Mode*	Default (View Current Device Mobility Settings)
Owner User ID	< None >
Phone Load Name	
Use Trusted Relay Point*	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
Calling Party Transformation CSS	< None >
Geolocation	< None >

☑ Use Device Pool Calling Party Transformation CSS

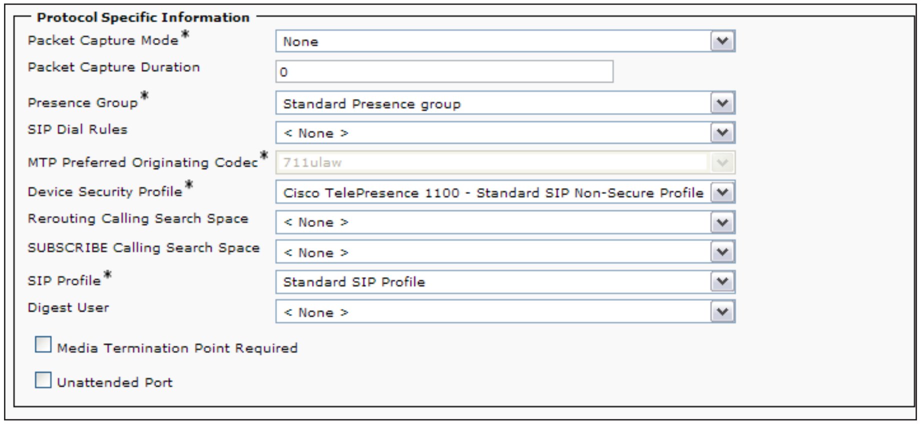
☑ Retry Video Call as Audio

☐ Ignore Presentation Indicators (internal calls only)

☑ Allow Control of Device from CTI

☑ Logged Into Hunt Group

☐ Remote Device

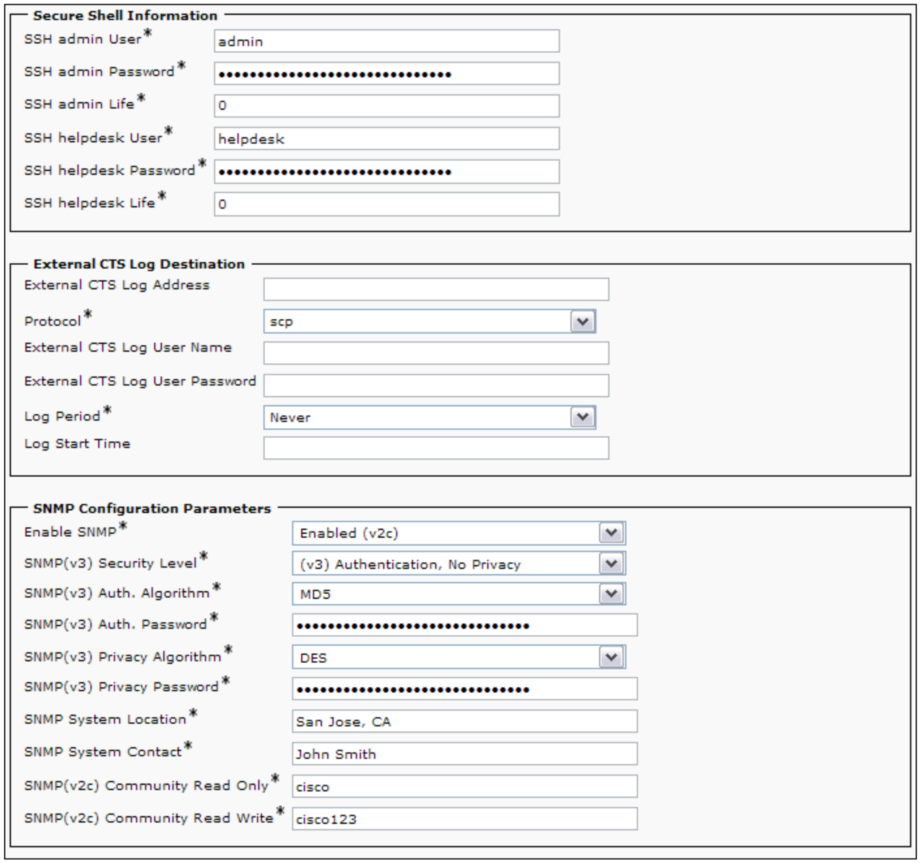


Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco TelePresence 1100 - Standard SIP Non-Secure Profile
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
Digest User	< None >

☐ Media Termination Point Required

☐ Unattended Port



Secure Shell Information

SSH admin User*	admin
SSH admin Password*	••••••••••••••••••••••••••••••
SSH admin Life*	0
SSH helpdesk User*	helpdesk
SSH helpdesk Password*	••••••••••••••••••••••••••••••
SSH helpdesk Life*	0

External CTS Log Destination

External CTS Log Address	
Protocol*	scp
External CTS Log User Name	
External CTS Log User Password	
Log Period*	Never
Log Start Time	

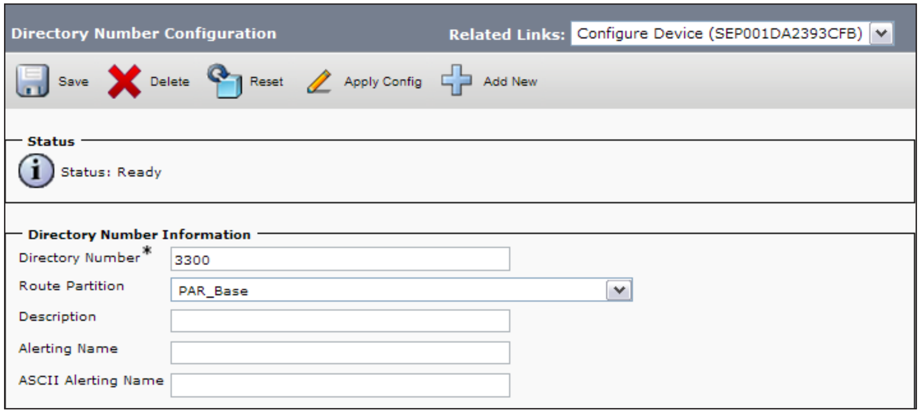
SNMP Configuration Parameters

Enable SNMP*	Enabled (v2c)
SNMP(v3) Security Level*	(v3) Authentication, No Privacy
SNMP(v3) Auth. Algorithm*	MD5
SNMP(v3) Auth. Password*	••••••••••••••••••••••••••••••
SNMP(v3) Privacy Algorithm*	DES
SNMP(v3) Privacy Password*	••••••••••••••••••••••••••••••
SNMP System Location*	San Jose, CA
SNMP System Contact*	John Smith
SNMP(v2c) Community Read Only*	cisco
SNMP(v2c) Community Read Write*	cisco123

Step 8: On the Phone Configuration screen, under Association Information, click **Line [1] - Add a new DN.**

Step 9: On the Directory Number Configuration screen, enter the following values, and then click **Save:**

- Directory Number—3300
- Route Partition—PAR_Base



Directory Number Configuration

Status

Status: Ready

Directory Number Information

Directory Number*	3300
Route Partition	PAR_Base
Description	
Alerting Name	
ASCII Alerting Name	

Procedure 2 Configure CTS associated phones

CTS endpoints use an associated IP phone to operate the day to day functions of the unit. The Unified CM Foundation design has auto-registration configured, so it is turned off temporarily to configure the associated phone as a SIP device. The directory number for the associated phone uses the 801XXXX range to distinguish it from phones that belong to individual users and phones that were auto-registered.

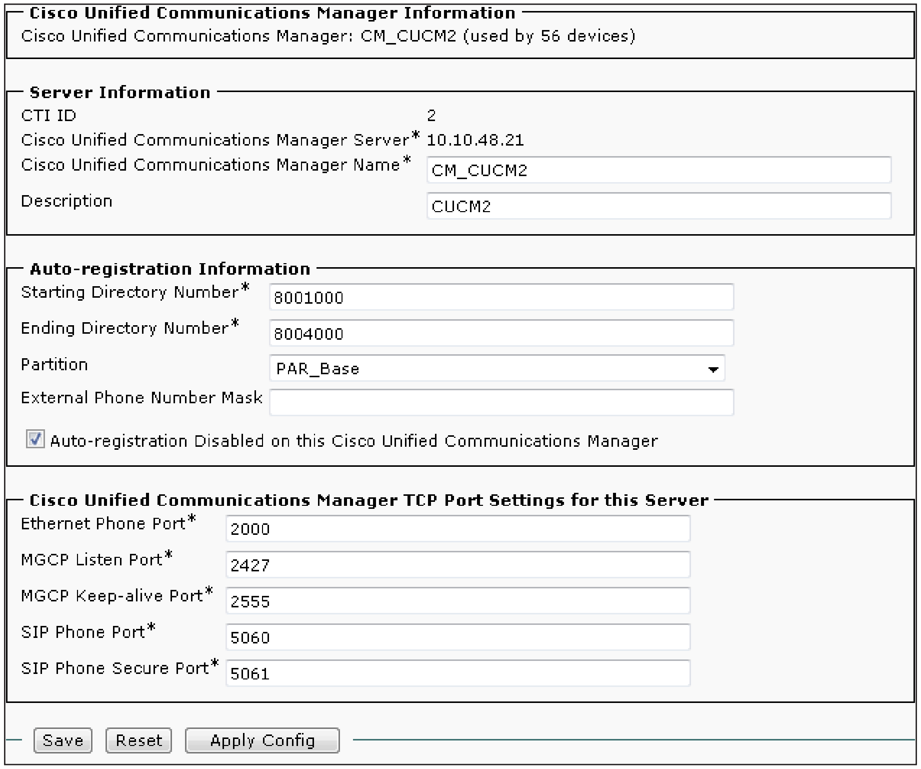
The easiest way to assign the directory number is to prepend 801 to the front of the four digit extension of the Cisco TelePresence System (CTS) endpoint. For example, if the CTS-1100 has an extension of 3300, assign 8013300 as the directory number of the associated CP-7975 phone.

Step 1: Navigate to **System > Cisco Unified CM**, click **Find**, and then choose the name of the Unified CM server.

Step 2: Select the **Auto-registration Disabled on the Cisco Unified Communications Manager** checkbox and click **Save**.

Tech Tip

After disabling auto-registration, the starting and ending directory number is changed to 1000. These values must be re-entered if auto-registration is enabled after adding the associated phones.



Cisco Unified Communications Manager Information

Cisco Unified Communications Manager: CM_CUCM2 (used by 56 devices)

Server Information

CTI ID	2
Cisco Unified Communications Manager Server*	10.10.48.21
Cisco Unified Communications Manager Name*	CM_CUCM2
Description	CUCM2

Auto-registration Information

Starting Directory Number*	8001000
Ending Directory Number*	8004000
Partition	PAR_Base
External Phone Number Mask	

☑ Auto-registration Disabled on this Cisco Unified Communications Manager

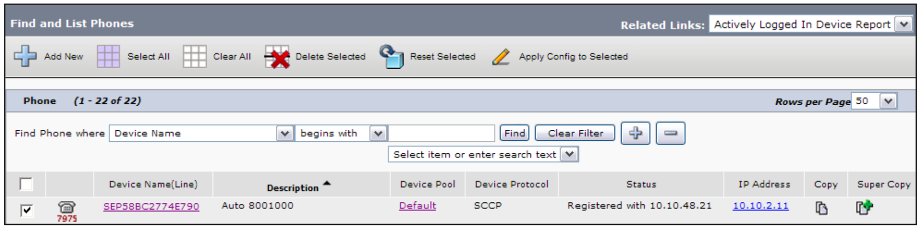
Cisco Unified Communications Manager TCP Port Settings for this Server

Ethernet Phone Port*	2000
MGCP Listen Port*	2427
MGCP Keep-alive Port*	2555
SIP Phone Port*	5060
SIP Phone Secure Port*	5061

Step 3: Repeat Step 1 and Step 2 for all of the servers that have auto-registration enabled.

Step 4: Use the touch interface of the phone to locate the MAC address under **Settings > Network Configuration > MAC Address**.

Step 5: On Unified CM, navigate to **Device > Phone**, click **Find**, and look for the MAC address from the previous step. Because the phone has auto-registered as a Skinny Call Control Protocol (SCCP) device, select the checkbox next to it, and then click **Delete Selected**.



Phone *(1 - 22 of 22)* *Rows per Page* 50

Find Phone where Device Name begins with

□		Device Name(Line)	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
☑	☎ 7975	SEP58BC2774E790	Auto 8001000	Default	SCCP	Registered with 10.10.48.21	10.10.2.11		

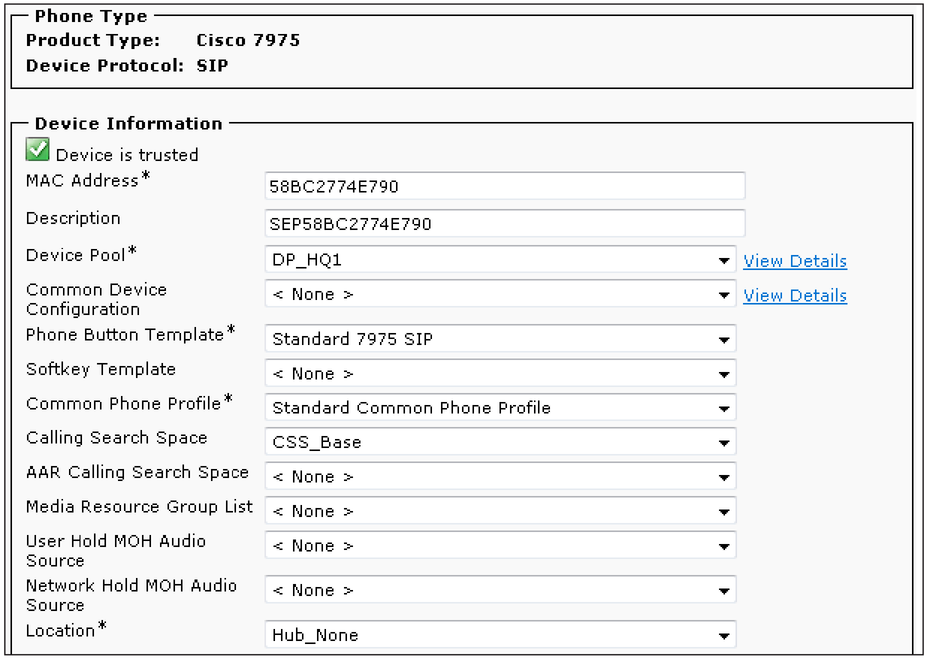
Step 6: On the Find and List Phones screen, click **Add New.**

Step 7: Enter the following values and after each entry, click **Next**:

- Product Type—Cisco 7975
- Select the device protocol—SIP

Step 8: On the Phone Configuration screen, enter the following values, and then click **Save**:

- MAC Address—**[MAC Address]**
- Description—**HQ CTS 7975**
- Device Pool—**DP_HQ1**
- Phone Button Template—**Standard 7975 SIP**
- Calling Search Space—**CSS_Base**
- Device Security Profile—**Cisco 7975 - Standard SIP Non-Secure Profile**
- SIP Profile—**Standard SIP Profile**
- Web Access—**Enabled**



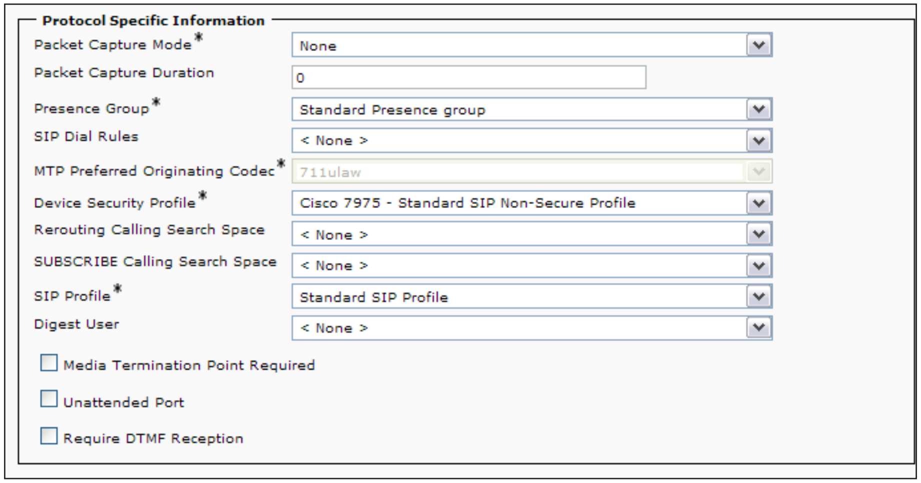
Phone Type

Product Type: Cisco 7975
Device Protocol: SIP

Device Information

☑ Device is trusted

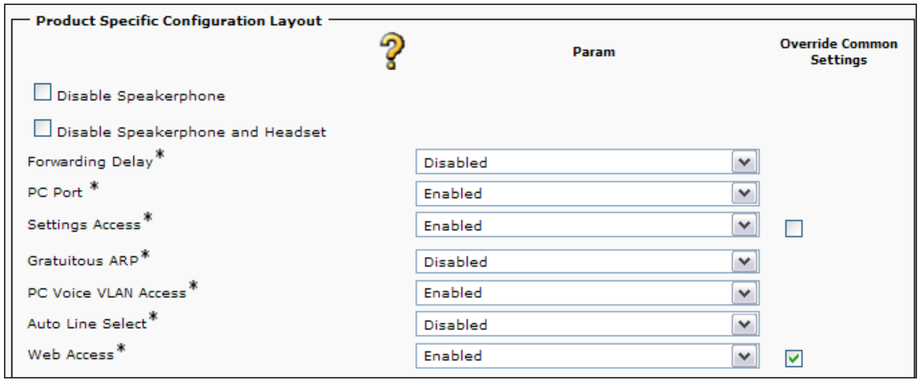
MAC Address*	58BC2774E790
Description	SEP58BC2774E790
Device Pool*	DP_HQ1 (View Details)
Common Device Configuration	< None > (View Details)
Phone Button Template*	Standard 7975 SIP
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	CSS_Base
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None



Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco 7975 - Standard SIP Non-Secure Profile
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
Digest User	< None >

□ Media Termination Point Required
□ Unattended Port
□ Require DTMF Reception



Product Specific Configuration Layout

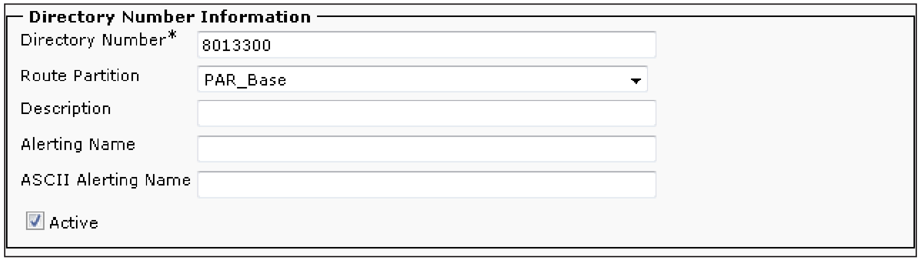
□ Disable Speakerphone
□ Disable Speakerphone and Headset

	Param	Override Common Settings
Forwarding Delay*	Disabled	
PC Port*	Enabled	
Settings Access*	Enabled	□
Gratuitous ARP*	Disabled	
PC Voice VLAN Access*	Enabled	
Auto Line Select*	Disabled	
Web Access*	Enabled	☑

Step 9: On the Phone Configuration screen, under Association Information, click **Line [1] - Add a new DN.**

Step 10: On the Directory Number Configuration screen, enter the following values, and then click **Save.**

- Directory Number—8013300 (801 prepended to 3300)
- Route Partition—PAR_Base



Directory Number Information

Directory Number*	8013300
Route Partition	PAR_Base
Description	
Alerting Name	
ASCII Alerting Name	

☑ Active

Repeat Procedure 1 and Procedure 2 for each CTS endpoint and associated phone that needs to be added to Unified CM.

Procedure 3 Configure CTS phone application

You need a valid cisco.com User ID and password to download the Cisco TelePresence MIDlet Phone Application from the cisco.com website.

Step 1: Using your web browser, access www.cisco.com, and navigate to **Support > All Downloads**.

Step 2: On the Select a Product screen, navigate to **Products > TelePresence > Telepresence Endpoints - Personal > TelePresence Office > Cisco TelePresence System** *Device* **> TelePresence Software > Latest Releases**

Step 3: Choose the latest .jad and .jar files for your version of CTS endpoint software, and then download the files to your PC. If you do not choose the correct version, you will get a version mismatch error when you try to use the phone application.

Step 4: Using your web browser, access the Unified CM Administration interface with the hostname or the IP address of each TFTP server in your cluster.

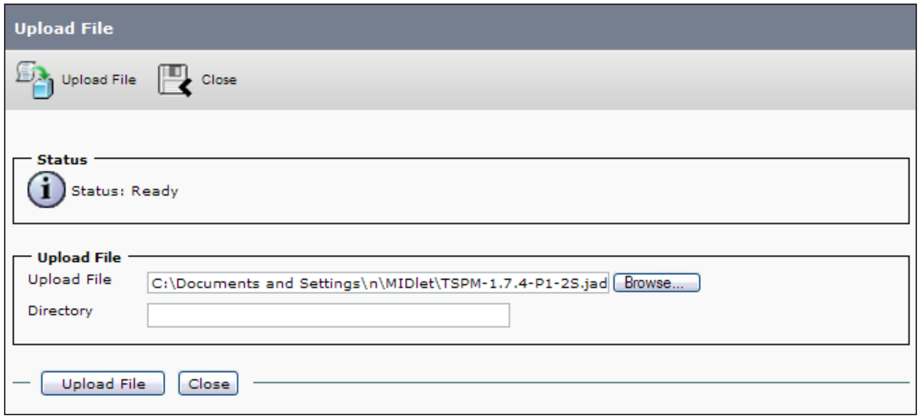
Step 5: In the center of the page under Installed Applications, click the **Cisco Unified Communications Manager** link.

Step 6: In the Navigation list at the top of the page, choose **Cisco Unified OS Administration**, and then click **Go**.

Step 7: Enter the **Username** and **Password** for the Platform Administrator User, and then click **Login**.

Step 8: Navigate to **Software Upgrades > TFTP File Management**, and then click **Upload File.**

Step 9: On the Upload File screen, click **Browse,** navigate to the location of the .jad and .jar files downloaded in Step 3, and then click **Upload File** for each one.



Status: Ready

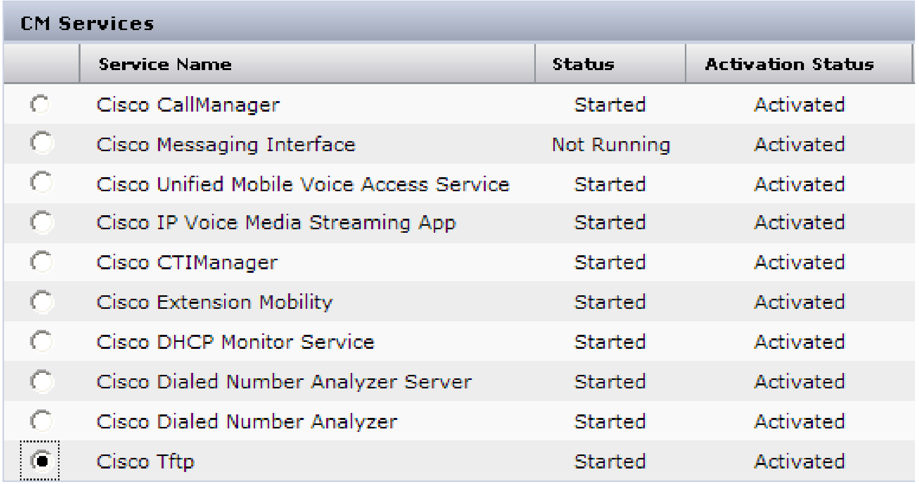
Upload File	C:\Documents and Settings\n\MIDlet\TSPM-1.7.4-P1-2S.jad
Directory	

Step 10: In the Navigation list at the top of the page, choose **Cisco Unified Serviceability**, and then click **Go**.

Step 11: Enter the **Username** and **Password** for the Application Administrator User, and then click **Login**.

Step 12: Navigate to **Tools > Control Center - Feature Services**, choose the server running TFTP from the list, and then click **Go**.

Step 13: Scroll down to the CM Services section, select the **Cisco Tftp** service radio button, and then click **Restart** at the bottom of the page.



CM Services

	Service Name	Status	Activation Status
○	Cisco CallManager	Started	Activated
○	Cisco Messaging Interface	Not Running	Activated
○	Cisco Unified Mobile Voice Access Service	Started	Activated
○	Cisco IP Voice Media Streaming App	Started	Activated
○	Cisco CTIManager	Started	Activated
○	Cisco Extension Mobility	Started	Activated
○	Cisco DHCP Monitor Service	Started	Activated
○	Cisco Dialed Number Analyzer Server	Started	Activated
○	Cisco Dialed Number Analyzer	Started	Activated
●	Cisco Tftp	Started	Activated

Step 14: Repeat Step 4 through Step 13 for all the TFTP servers in your cluster.

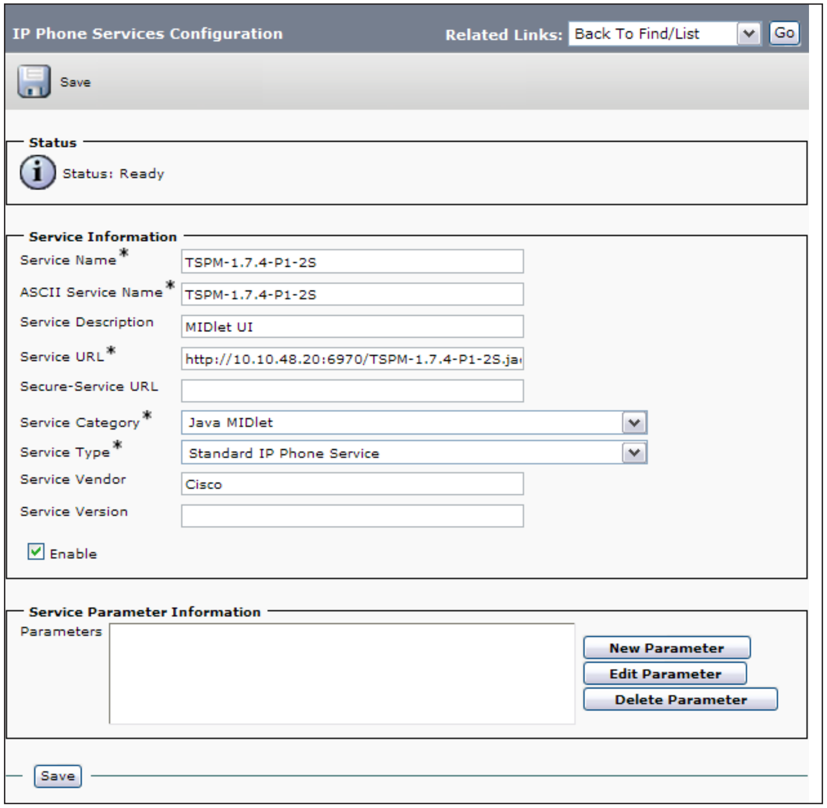
Step 15: From your web browser, access the Unified CM Administration interface of the publisher with the hostname or the IP address.

Step 16: In the Navigation list at the top of the page, choose **Cisco Unified CM Administration**, and then click **Go**.

Step 17: Navigate to **Device > Device Settings > Phone Services**, and then click **Add New**.

Step 18: On the IP Phone Services Configuration screen, enter the following values, and then click **Save**:

- Service Name—**TSPM-1.7.4-P1-2S**
- ASCII Service Name—**TSPM-1.7.4-P1-2S**
- Service Description—**MIDlet UI**
- Service URL—**http://10.10.48.20:6970/TSPM-1.7.4-P1-2S.jad**
- Service Category—**Java MIDlet**
- Service Type—**Standard IP Phone Service**
- Service Vendor—**Cisco**
- Enable Checkbox—**Yes**


IP Phone Services Configuration
Related Links: Back To Find/List
Go
Save

Status

Status: Ready

Service Information

Service Name*	TSPM-1.7.4-P1-2S
ASCII Service Name*	TSPM-1.7.4-P1-2S
Service Description	MIDlet UI
Service URL*	http://10.10.48.20:6970/TSPM-1.7.4-P1-2S.ja
Secure-Service URL	
Service Category*	Java MIDlet
Service Type*	Standard IP Phone Service
Service Vendor	Cisco
Service Version	

☑ Enable

Service Parameter Information

Parameters

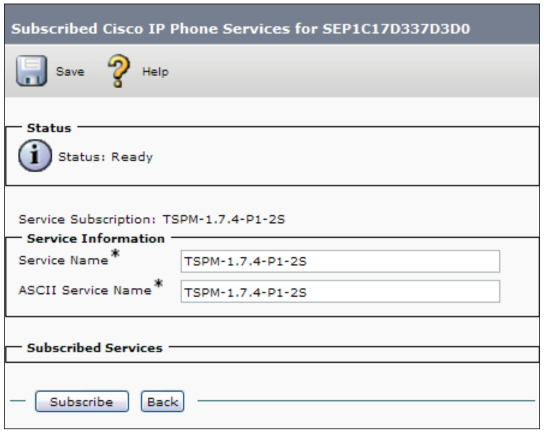
New Parameter
Edit Parameter
Delete Parameter
Save

Step 19: Navigate to **Device > Phone,** click **Find**, and then choose the MAC address of an associated phone.

Step 20: In the Related Links list, choose **Subscribe/Unsubscribe Services**, and then click **Go**.

Step 21: In the Select a Service list, choose the service you configured in Step 18, and then click **Next**.

Step 22: On the next screen, click **Subscribe**.



Subscribed Cisco IP Phone Services for SEP1C17D337D3D0

Status

Status: Ready

Service Subscription: TSPM-1.7.4-P1-2S

Service Information

Service Name* TSPM-1.7.4-P1-2S

ASCII Service Name* TSPM-1.7.4-P1-2S

Subscribed Services

After a minute or two, the application starts on the phone and it can be used to place calls.

Repeat Step 19 through Step 22 for the rest of the phones associated with CTS endpoints.

Procedure 4 Configure video telephony endpoints

Telephony endpoints use the auto-registration process from the Unified CM Foundation to register with the cluster. Extension mobility assigns user-specific information to the phones. Device mobility information places the phone in the correct device pool to use all of its associated settings. Video telephony and video-enabled tablets can use extension mobility, or they can be configured with a specific directory number.

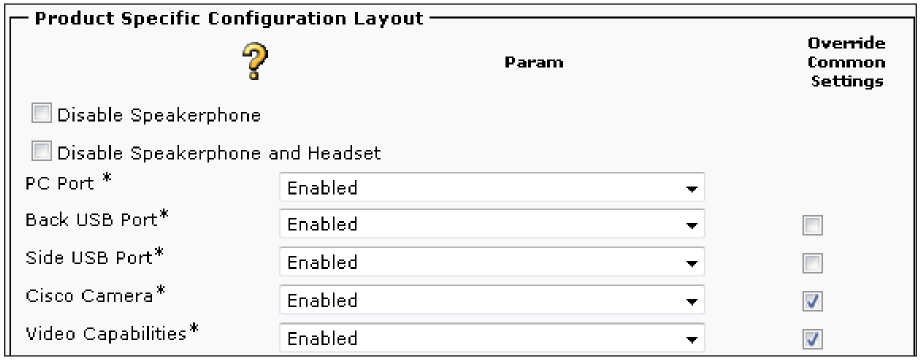
The following steps are required to prepare the phone for sending and receiving video calls.

Step 1: Use the touch interface of the phone to locate the MAC address under **Settings > Network Configuration > MAC Address**.

Step 2: On Unified CM, navigate to **Device > Phone**, click **Find,** look for the video telephone, and then click the MAC address from the previous step.

Step 3: On the Phone Configuration screen, enter the following values, and then click **Save**:

- Cisco Camera—Enabled
- Video Capabilities—Enabled



Product Specific Configuration Layout

Param		Override Common Settings
□ Disable Speakerphone		
□ Disable Speakerphone and Headset		
PC Port *	Enabled	
Back USB Port*	Enabled	□
Side USB Port*	Enabled	□
Cisco Camera*	Enabled	☑
Video Capabilities*	Enabled	☑

If the phone is not used with Extension Mobility, you must complete Step 4 and Step 5 to assign it a four-digit directory number within the proper range of the site. In this example, the phone's directory number is configured for the Site01 location.

Step 4: On the Phone Configuration screen, under Association Information, click **Line [1].**

Step 5: On the Directory Number Configuration screen, enter the following values, and then click **Save:**

- Directory Number—3019
- Route Partition—PAR_Base

Procedure 5 Configure video-enabled tablets

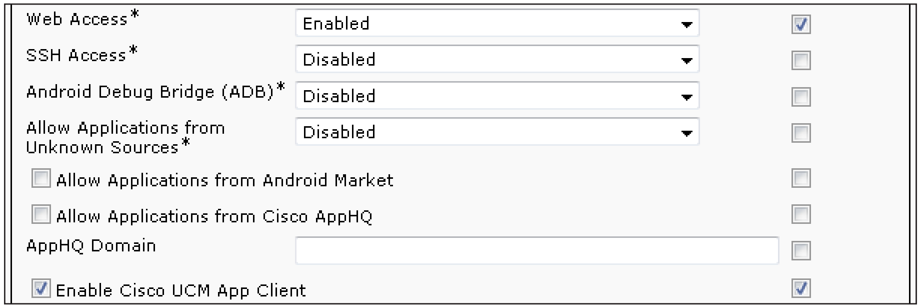
The following steps are required to prepare the Cisco video-enabled tablet (Cius) for sending and receiving calls.

Step 1: Use the touch interface of the Cius to locate the MAC address under **Home > Settings > Wireless & networks > Ethernet settings > MAC address**.

Step 2: Navigate to **Device > Phone**, click **Find,** and then click the MAC address from the previous step.

Step 3: On the Phone Configuration screen, enter the following values, and then click **Save**:

- Web Access—Enabled
- Enable Cisco UCM App Client—Yes



Web Access*	Enabled	☑
SSH Access*	Disabled	□
Android Debug Bridge (ADB)*	Disabled	□
Allow Applications from Unknown Sources*	Disabled	□
□ Allow Applications from Android Market		□
□ Allow Applications from Cisco AppHQ		□
AppHQ Domain		□
☑ Enable Cisco UCM App Client		☑

If the Cius is not used with Extension Mobility, you must complete Step 4 and Step 5 to assign it a four digit directory number within the proper range of the site. In this example, the Cius uses a directory number for the headquarters location.

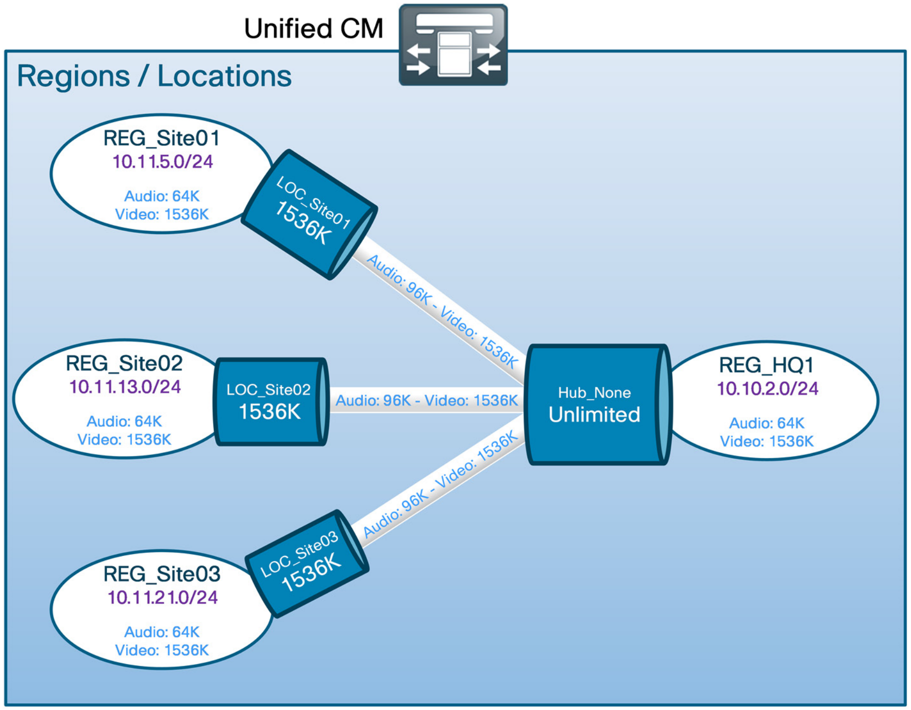
Step 4: On the Phone Configuration screen, under Association Information, click **Line [1].**

Step 5: On the Directory Number Configuration screen, enter the following values, and then click **Save:**

- Directory Number—3009
- Route Partition—PAR_Base

Procedure 6 Configure UCM call admission control

Video calls between different locations are limited to 1.5 Mbps for this configuration guide, and one call is allowed per site. For this example, the remote sites require at least 15 Mbps of total WAN bandwidth and the headquarters site requires 30 Mbps into the MPLS cloud. The additional WAN bandwidth permits higher-quality video and audio between the locations. If your location needs more than one call per remote site, you must upgrade the WAN bandwidth between the sites to accommodate the higher values.



The Region configuration max audio bit rate is set to 64 kbps because the initial call signal between the two CTS endpoints is an audio-only call, which requires G.722. The Location configuration audio bandwidth is set to at least 96 kbps because video calls from general-purpose endpoints to CTS endpoints are initially audio-only calls and they will be rejected if the bandwidth is less than 96 kbps.

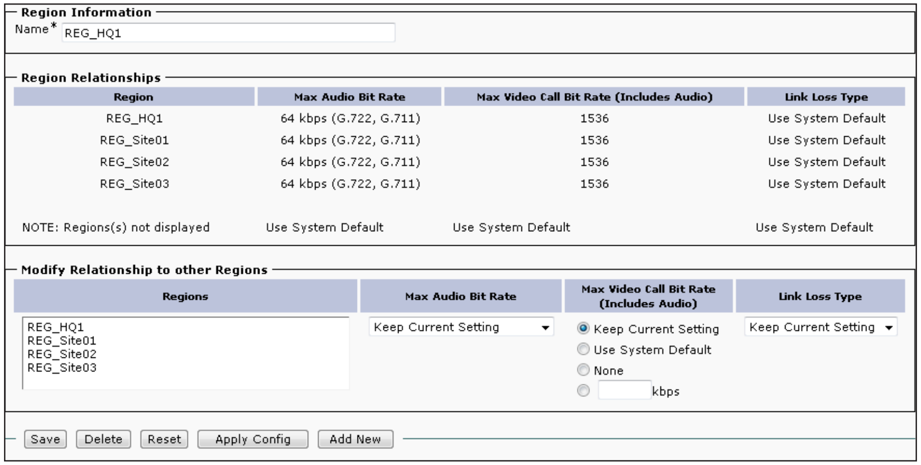
The following steps are configured for each region and location that has CTS endpoints.

Step 1: Navigate to **System > Region**, click **Find**, and then click the name of a region.

Step 2: Under Modify Relationship to other Regions, choose each region that has CTS video endpoints, change the following values, and then click **Save**:

- Max Audio Bit Rate—64 kbps (G.722, G.711)
- Max Video Call Bit Rate—1536

Step 3: After all of the regions in the Region list are modified, click **Apply Config**.



Region Information

Name* REG_HQ1

Region Relationships

Region	Max Audio Bit Rate	Max Video Call Bit Rate (Includes Audio)	Link Loss Type
REG_HQ1	64 kbps (G.722, G.711)	1536	Use System Default
REG_Site01	64 kbps (G.722, G.711)	1536	Use System Default
REG_Site02	64 kbps (G.722, G.711)	1536	Use System Default
REG_Site03	64 kbps (G.722, G.711)	1536	Use System Default
NOTE: Regions(s) not displayed	Use System Default	Use System Default	Use System Default

Modify Relationship to other Regions

Regions	Max Audio Bit Rate	Max Video Call Bit Rate (Includes Audio)	Link Loss Type
REG_HQ1 REG_Site01 REG_Site02 REG_Site03	Keep Current Setting	● Keep Current Setting ○ Use System Default ○ None ○ kbps	Keep Current Setting

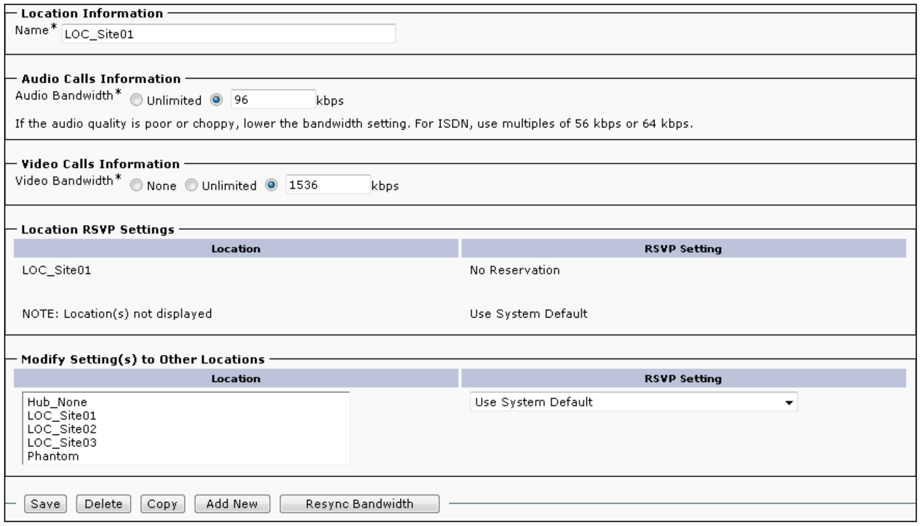
Step 4: Repeat Step 1, Step 2, and Step 3 for all regions with CTS endpoints.

Step 5: Navigate to **System > Location**, click **Find**, and then click the name of a remote-site location.

Step 6: Enter the following values, and then click **Save**:

- Audio Bandwidth radio button—Yes
- Audio kbps—96
- Video Bandwidth radio button—Yes
- Video kbps—1536

Step 7: Click **Resync Bandwidth**, and on the message that appears, click **OK**.



Location Information

Name* LOC_Site01

Audio Calls Information

Audio Bandwidth* ○ Unlimited ● 96 kbps

If the audio quality is poor or choppy, lower the bandwidth setting. For ISDN, use multiples of 56 kbps or 64 kbps.

Video Calls Information

Video Bandwidth* ○ None ○ Unlimited ● 1536 kbps

Location RSVP Settings

Location	RSVP Setting
LOC_Site01	No Reservation
NOTE: Location(s) not displayed	Use System Default

Modify Setting(s) to Other Locations

Location	RSVP Setting
Hub_None LOC_Site01 LOC_Site02 LOC_Site03 Phantom	Use System Default

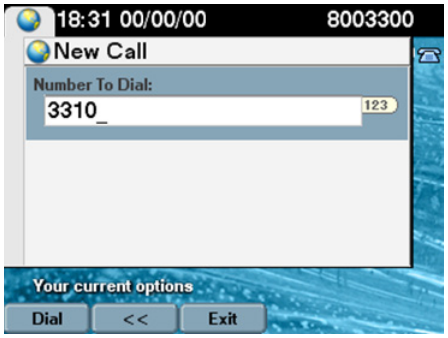
Step 8: Repeat Step 3, Step 5, and Step 6 for all remote-site locations with CTS endpoints.

Procedure 7 Unified CM to Unified CM calling

After the endpoints have been registered and call admission control has been configured, place test calls between the locations to confirm that everything is working as expected.

Step 1: On the associated phone, tap **New Call**.

Dial the four digit extension of another CTS endpoint—3310— and then tap **Dial**.



18:31 00/00/00 8003300

New Call

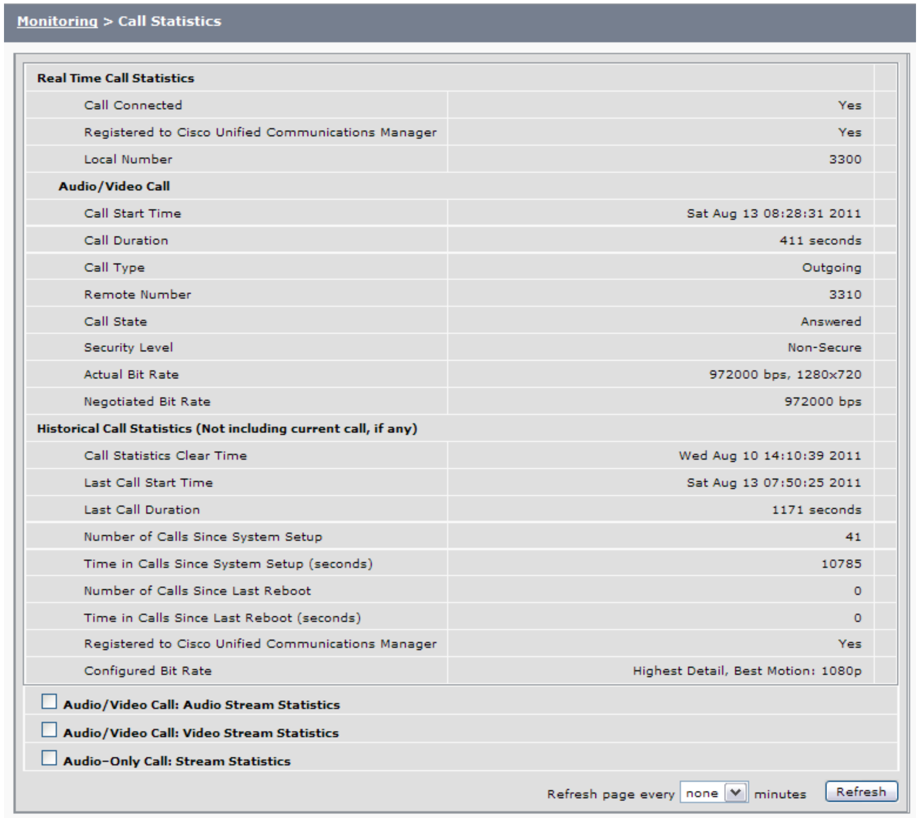
Number To Dial: 3310_

Step 2: Use your web browser to access the endpoints administrative interface—https://10.10.2.50/— and log in using the SSH admin username and password you configured in Procedure 1.

Step 3: On the Cisco TelePresence Systems Administration screen, enter the following values, and then click **Login**:

- Username—admin
- Password—[password]

Step 4: Navigate to **Monitoring > Call Statistics** and verify the bandwidth is what you expect. If the bandwidth is too high or too low, confirm the values you entered in Procedure 6 match the available bandwidth for the link.



Monitoring > Call Statistics

Real Time Call Statistics	
Call Connected	Yes
Registered to Cisco Unified Communications Manager	Yes
Local Number	3300
Audio/Video Call	
Call Start Time	Sat Aug 13 08:28:31 2011
Call Duration	411 seconds
Call Type	Outgoing
Remote Number	3310
Call State	Answered
Security Level	Non-Secure
Actual Bit Rate	972000 bps, 1280x720
Negotiated Bit Rate	972000 bps
Historical Call Statistics (Not including current call, if any)	
Call Statistics Clear Time	Wed Aug 10 14:10:39 2011
Last Call Start Time	Sat Aug 13 07:50:25 2011
Last Call Duration	1171 seconds
Number of Calls Since System Setup	41
Time in Calls Since System Setup (seconds)	10785
Number of Calls Since Last Reboot	0
Time in Calls Since Last Reboot (seconds)	0
Registered to Cisco Unified Communications Manager	Yes
Configured Bit Rate	Highest Detail, Best Motion: 1080p

□ **Audio/Video Call: Audio Stream Statistics**

□ **Audio/Video Call: Video Stream Statistics**

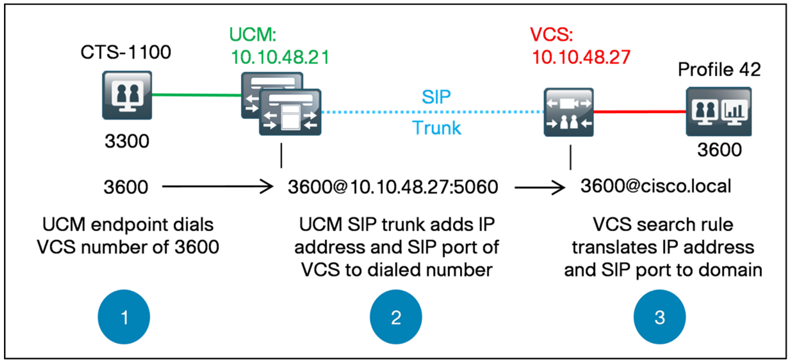
□ **Audio-Only Call: Stream Statistics**

Refresh page every none minutes

Step 5: To hang up the call from the phone, tap **End Call**.

Procedure 8 Configure Unified CM to VCS calling

Calls from Unified CM to VCS are routed using a SIP trunk. Sending calls for the 36XX range of numbers requires a single route pattern in Unified CM. The diagram below shows the call flow for simple numeric dialing from a Unified CM endpoint to a VCS endpoint.


CTS-1100
3300
UCM:
10.10.48.21
SIP
Trunk
VCS:
10.10.48.27
Profile 42
3600
3600
3600@10.10.48.27:5060
3600@cisco.local
UCM endpoint dials VCS number of 3600
UCM SIP trunk adds IP address and SIP port of VCS to dialed number
VCS search rule translates IP address and SIP port to domain
1
2
3

A SIP trunk, route group, route list and route pattern direct the calls to the IP address of the VCS. After you finalize the Unified CM dial plan, you perform additional steps in the following process to translate the called number format in the VCS.

Step 1: Using your web browser, access the Unified CM Administration interface using the hostname or IP address.

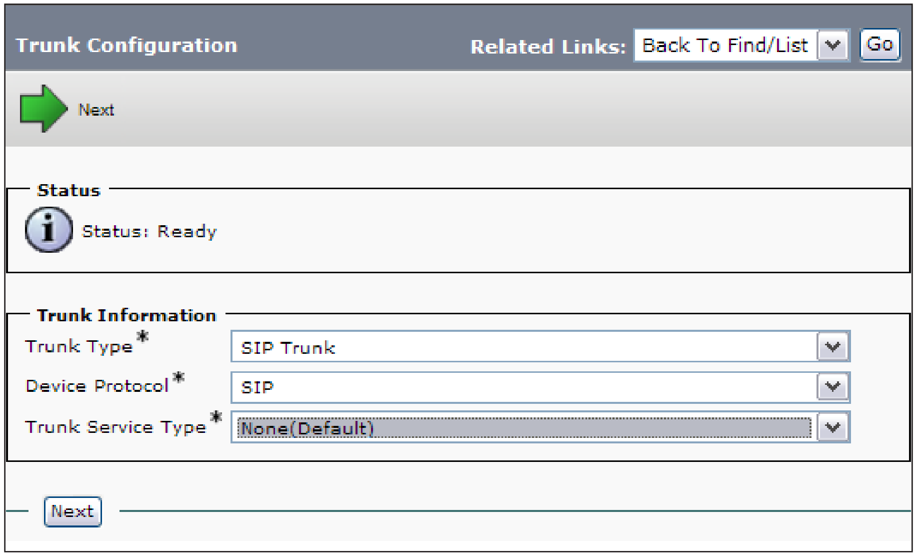
Step 2: In the center of the page under Installed Applications, click the **Cisco Unified Communications Manager** link.

Step 3: Enter the **Username** and **Password** you created for the Administrator User, and then click **Login**.

Step 4: Navigate to **Device > Trunk**, and then click **Add New**.

Step 5: On the Trunk Configuration screen, enter the following values, and then click **Next**:

- Trunk Type—SIP Trunk
- Device Protocol—SIP
- Trunk Service Type—None (Default)

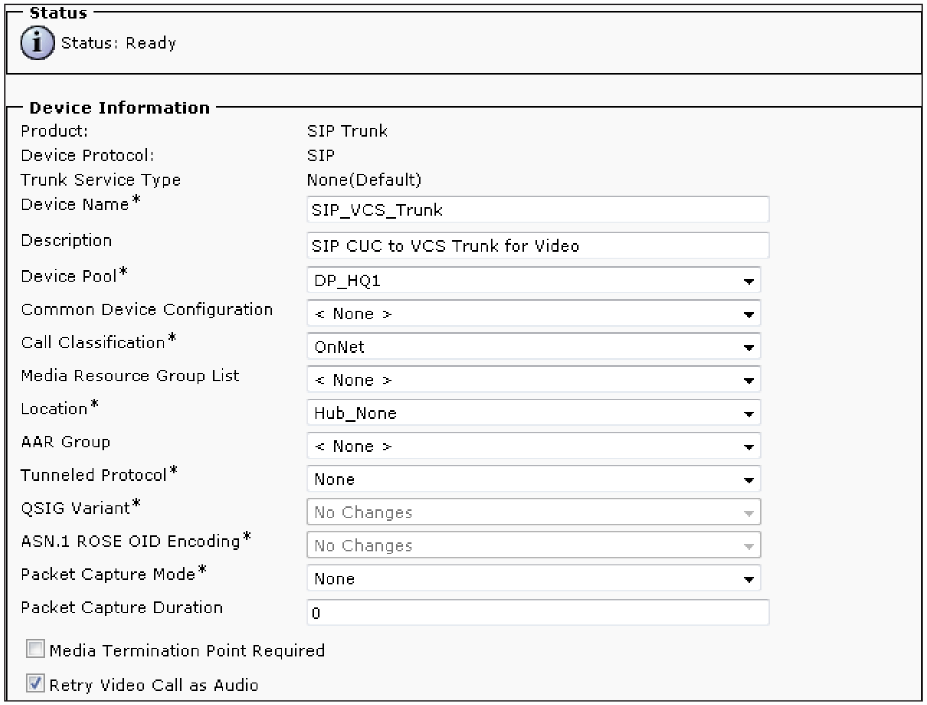


Status: Ready

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Step 6: On the next screen, enter the following values, and then click **Save.**

- Device Name—SIP_VCS_Trunk
- Description—SIP CUCM to VCS Trunk for Video
- Device Pool—DP_HQ1
- Call Classification—OnNet
- Location—Hub_None
- Retry Video Call as Audio—Yes
- Significant Digits—4
- Calling Search Space—CSS_Base
- Destination Address—10.10.48.27
- Destination Port—5060
- SIP Trunk Security Profile—Non Secure SIP Trunk Profile
- SIP Profile—Standard SIP Profile
- DTMF Signaling Method—RFC 2833



Status

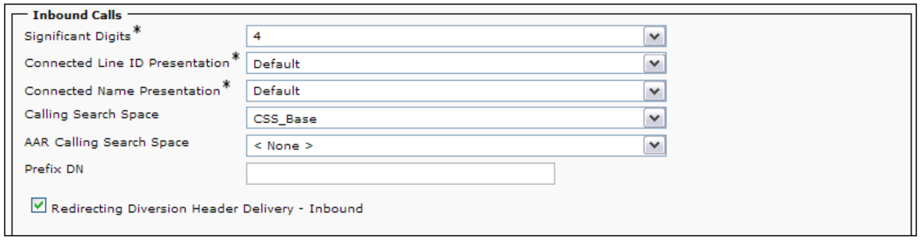
Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SIP_VCS_Trunk
Description	SIP CUC to VCS Trunk for Video
Device Pool*	DP_HQ1
Common Device Configuration	< None >
Call Classification*	OnNet
Media Resource Group List	< None >
Location*	Hub_None
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

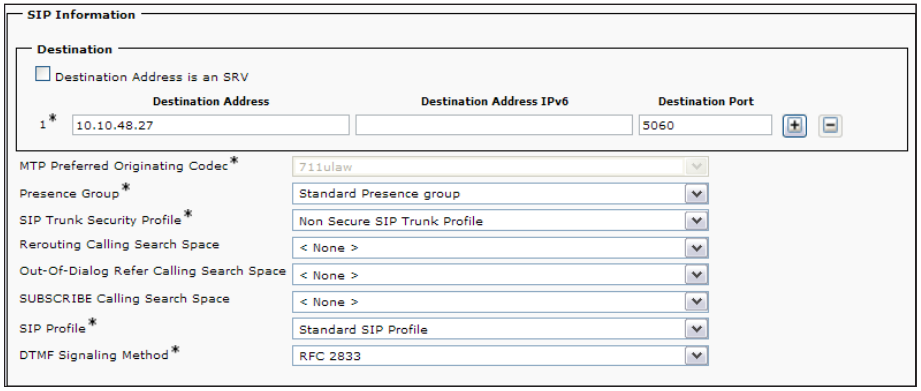
☑ Retry Video Call as Audio



Inbound Calls

Significant Digits*	4
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	CSS_Base
AAR Calling Search Space	< None >
Prefix DN	

☑ Redirecting Diversion Header Delivery - Inbound



SIP Information

Destination

□ Destination Address is an SRV

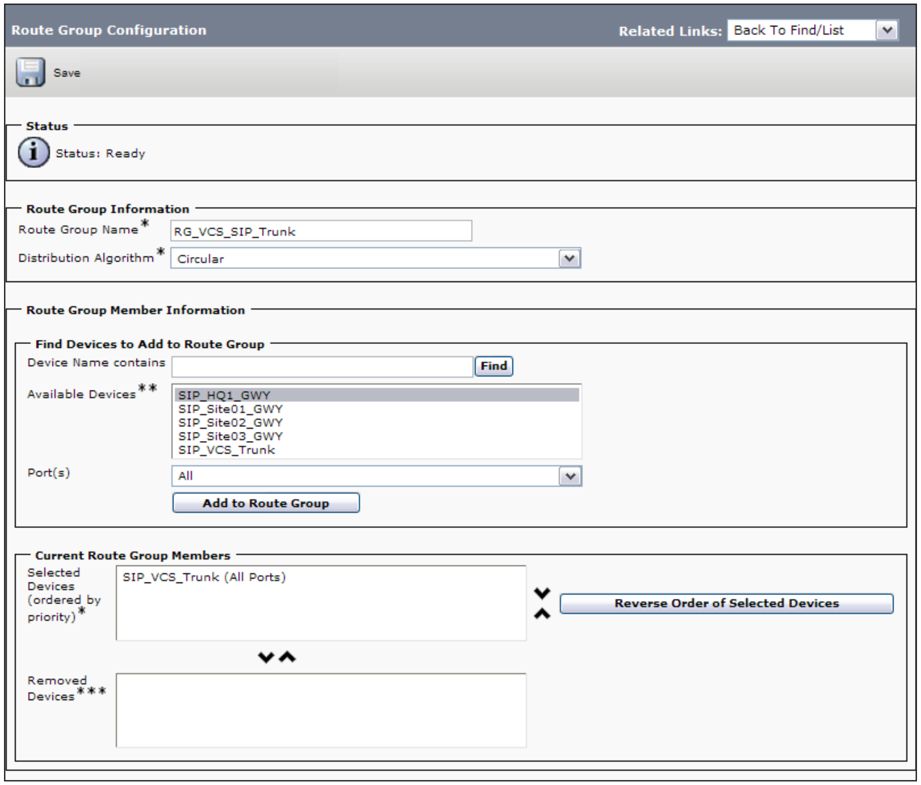
	Destination Address	Destination Address IPv6	Destination Port
1*	10.10.48.27		5060

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*	RFC 2833

Step 7: Navigate to **Call Routing > Route / Hunt > Route Group**, and then click **Add New.**

Step 8: On the Route Group Configuration screen, enter the Route Group Name—RG_VCS_SIP_Trunk.

Step 9: From the Available Devices, choose—SIP_VCS_Trunk (All Ports), click Add to Route Group, and then click Save.


Route Group Configuration

Related Links: Back To Find/List

Save

Status

Status: Ready

Route Group Information

Route Group Name* RG_VCS_SIP_Trunk

Distribution Algorithm* Circular

Route Group Member Information

Find Devices to Add to Route Group

Device Name contains [ ] Find

Available Devices** SIP_HQ1_GWY
SIP_Site01_GWY
SIP_Site02_GWY
SIP_Site03_GWY
SIP_VCS_Trunk

Port(s) All

Add to Route Group

Current Route Group Members

Selected Devices (ordered by priority)* SIP_VCS_Trunk (All Ports)

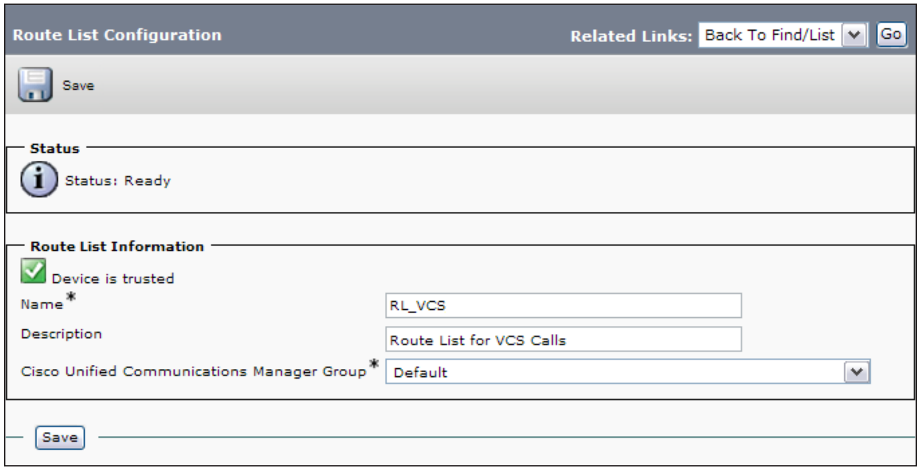
Reverse Order of Selected Devices

Removed Devices***

Step 10: Navigate to Call Routing > Route / Hunt > Route List, and then click Add New.

Step 11: On the Route Group Configuration screen, enter the following values, and then click Save:

- Name—RL_VCS
- Description—Route List for VCS Calls
- Cisco Unified Communications Manager Group—Default


Route List Configuration

Related Links: Back To Find/List Go

Save

Status

Status: Ready

Route List Information

✓ Device is trusted

Name* RL_VCS

Description Route List for VCS Calls

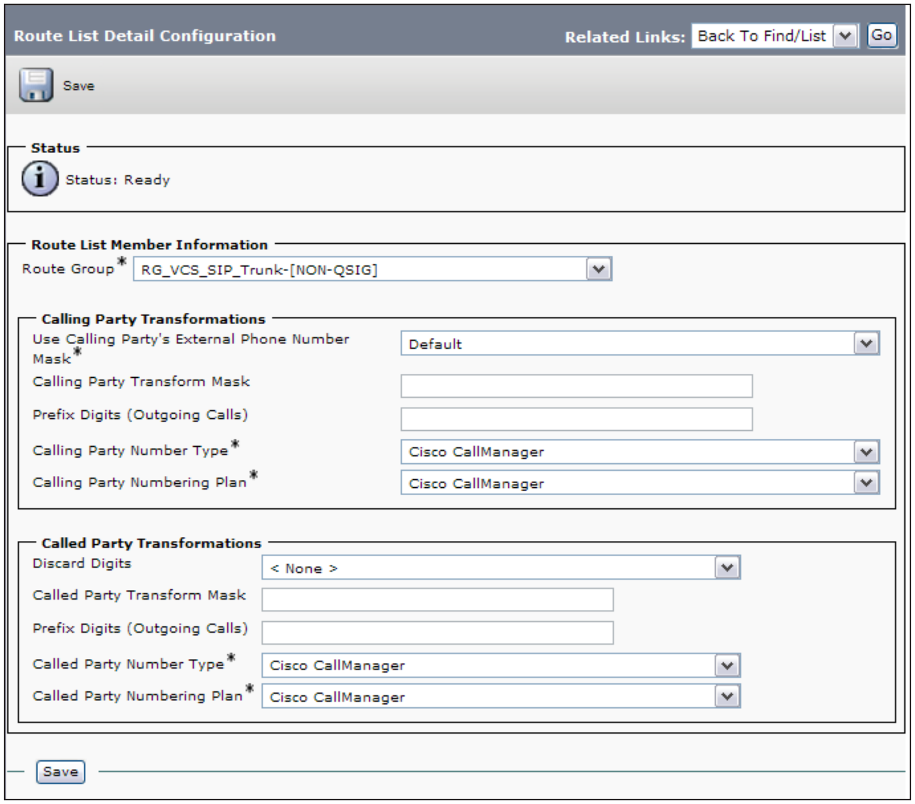
Cisco Unified Communications Manager Group* Default

Save

Step 12: On the Route List Configuration screen, click Add Route Group.

Step 13: On the Route List Detail Configuration screen, enter the following value, and then click **Save**:

- Route Group—RG_VCS_SIP_Trunk [NON-QSIG]



Route List Detail Configuration Related Links: Back To Find/List Go

Save

Status

Status: Ready

Route List Member Information

Route Group* RG_VCS_SIP_Trunk-[NON-QSIG]

Calling Party Transformations

Use Calling Party's External Phone Number Mask*	Default
Calling Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Calling Party Number Type*	Cisco CallManager
Calling Party Numbering Plan*	Cisco CallManager

Called Party Transformations

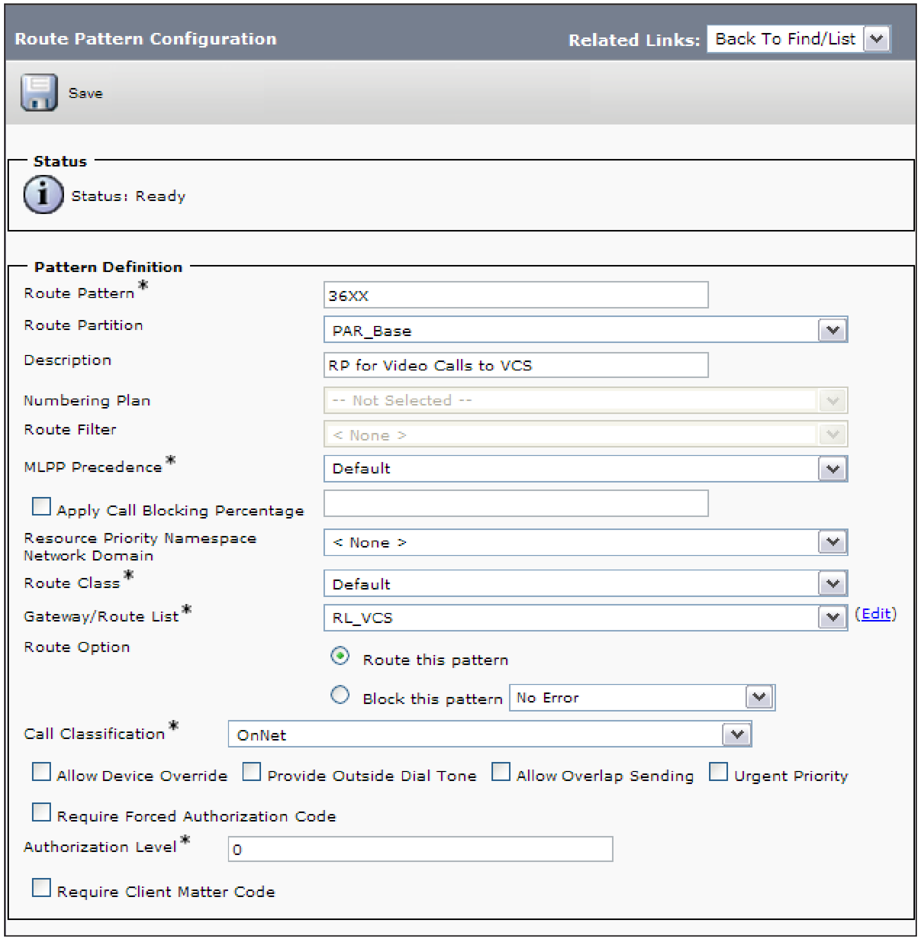
Discard Digits	< None >
Called Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Called Party Number Type*	Cisco CallManager
Called Party Numbering Plan*	Cisco CallManager

Save

Step 14: Navigate to **Call Routing > Route / Hunt > Route Pattern**, and then click **Add New.**

Step 15: On the Route Pattern Configuration screen, enter the following values, and then click **Save**:

- Route Pattern—36XX
- Route Partition—PAR_Base
- Description—RP for Video Calls to VCS
- Gateway/Route List—RL_VCS
- Call Classification—OnNet



Route Pattern Configuration Related Links: Back To Find/List

Save

Status

Status: Ready

Pattern Definition

Route Pattern*	36XX
Route Partition	PAR_Base
Description	RP for Video Calls to VCS
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	RL_VCS (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

Process

Configuring Cisco TelePresence VCS

1. Configure VCS inbound calls
2. Configure VCS outbound calls
3. Configure VCS call admission control
4. VCS to Unified CM dialing
5. Unified CM to VCS dialing

After registering the CTS endpoints with Unified CM, modifying call admission control, and creating the dial plan, you configure Cisco VCS to allow inbound and outbound calls to and from the neighboring call agent.

Procedure 1 Configure VCS inbound calls

When a call is received from Unified CM, the called number is in the format of [called number]@[VCS IP address]:5060. Cisco VCS uses a search rule to translate the called number to the format [called number]@[domain name].

For example, a call to a VCS endpoint at extension 3600 arrives as 3600@10.10.48.27:5060. The VCS translates the called number to 3600@cisco.local before searching for the device in the local zone.

When a call is received from Unified CM, the callback number is in the format of [calling number]@[IP address of Unified CM]. For the VCS to route the call back to Unified CM, VCS uses a transform to translate the calling number to the format [calling number]@[domain name].

For example, a Unified CM endpoint call from 3300 arrives as 3300@10.10.48.21. The VCS translates the calling number to 3300@cisco.local before it is sent to the endpoint so the recent calls list has the properly formatted callback number.

Notes

Step 1: Using your web browser, access the Cisco VCS Administration interface using the hostname or IP address.

Step 2: Click **Administrator login**.

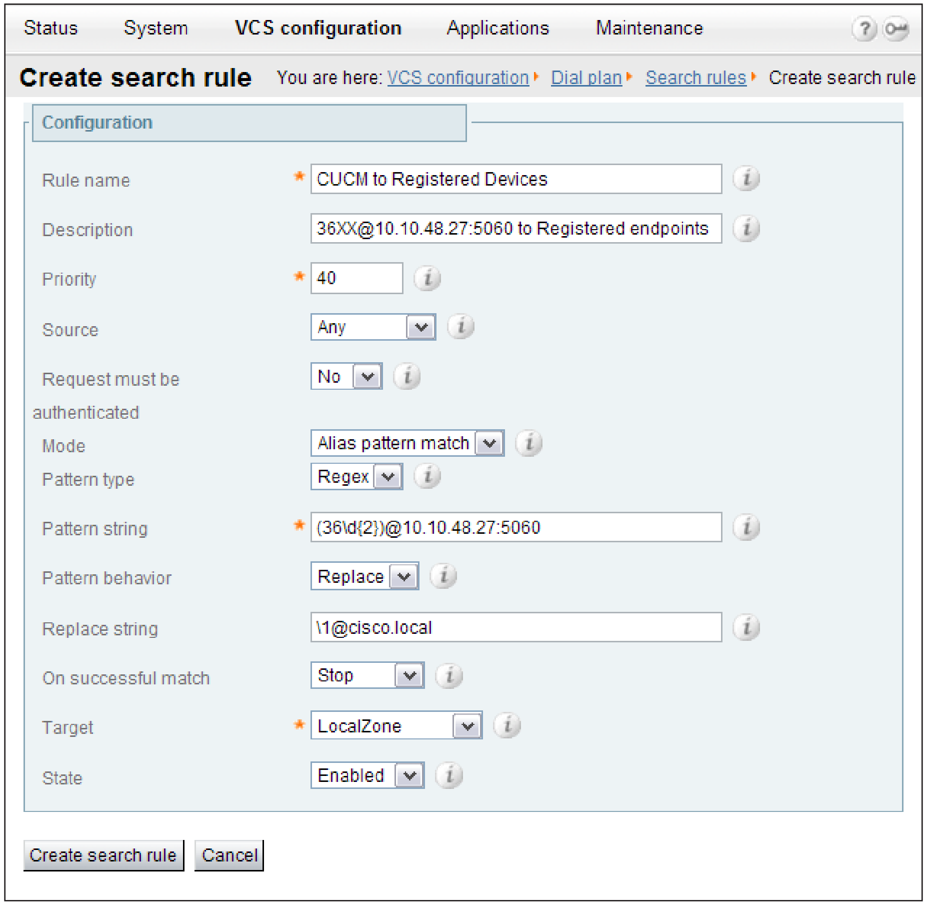
Step 3: Enter the following values, and then click **Login**:

- Username—**admin**
- Password—**[password]**

Step 4: Navigate to **VCS configuration > Dial Plans > Search rules**, and then click **New**.

Step 5: Enter the following values, and then click **Create search rule**:

- Rule name—**CUCM to Registered Devices**
- Description—**36XX@10.10.48.27:5060 to Registered endpoints**
- Priority—**40**
- Source—**Any**
- Request must be Authenticated—**No**
- Mode—**Alias Pattern Match**
- Pattern Type—**Regex**
- Pattern String—**(36\d{2})@10.10.48.27:5060**
- Pattern behavior—**Replace**
- Replace String—**\1@cisco.local**
- On successful match—**Stop**
- Target—**LocalZone**
- State—**Enabled**

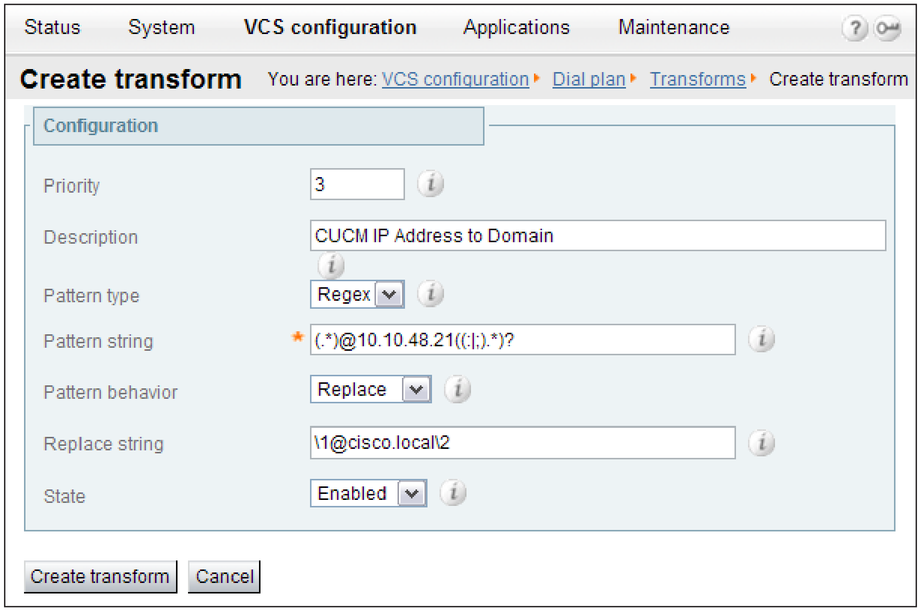


Rule name *	CUCM to Registered Devices
Description	36XX@10.10.48.27:5060 to Registered endpoints
Priority *	40
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string *	(36\d{2})@10.10.48.27:5060
Pattern behavior	Replace
Replace string	\1@cisco.local
On successful match	Stop
Target *	LocalZone
State	Enabled

Step 6: Navigate to **VCS configuration > Dial Plans > Transforms**, and then click **New**.

Step 7: Enter the following values, and then click **Create transform**:

- Priority—**3**
- Description—**CUCM IP Address to Domain**
- Pattern type—**Regex**
- Pattern string—**(.*)@10.10.48.21((:|;).*)?**
- Pattern behavior—**Replace**
- Pattern string—**\1@cisco.local\2**
- State—**Enabled**



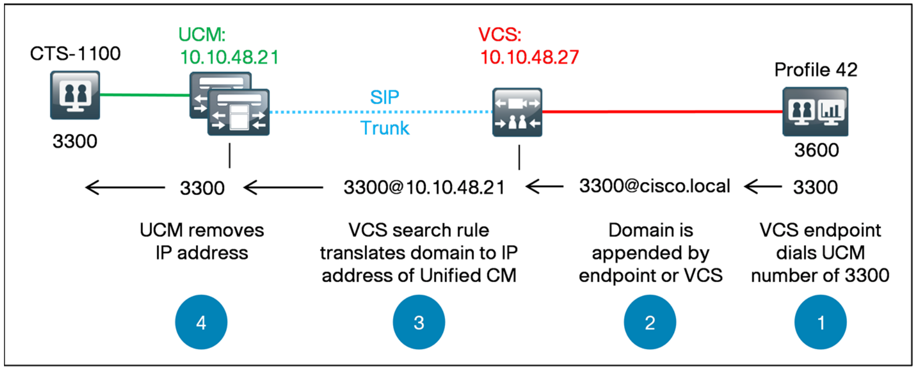
Create transform You are here: VCS configuration ▸ Dial plan ▸ Transforms ▸ Create transform

Configuration

Priority	3
Description	CUCM IP Address to Domain
Pattern type	Regex
Pattern string *	(.*)@10.10.48.21((:|;).*)?
Pattern behavior	Replace
Replace string	\1@cisco.local\2
State	Enabled

Procedure 2 Configure VCS outbound calls

Calls from general-purpose endpoints are routed from VCS to Unified CM using a SIP trunk. You create a neighbor zone and two search rules in VCS to allow dialing between the two systems. The diagram below shows the call flow for simple numeric dialing from a VCS endpoint to a Unified CM endpoint.

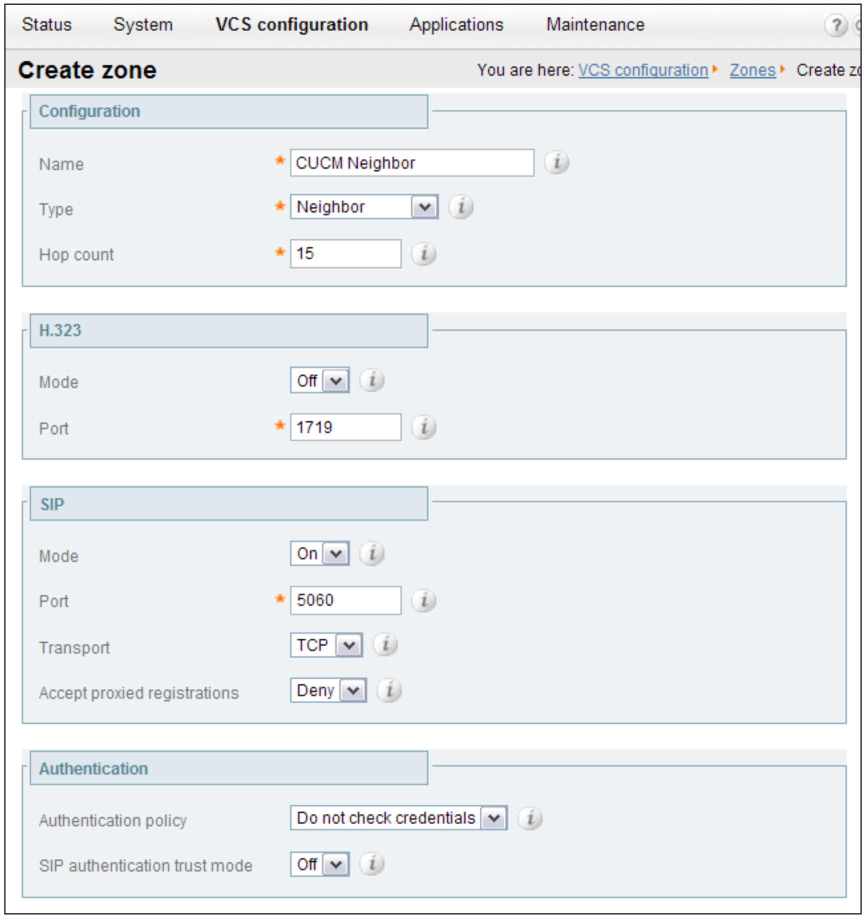

CTS-1100
3300
UCM:
10.10.48.21
SIP
Trunk
VCS:
10.10.48.27
Profile 42
3600
3300
3300@10.10.48.21
3300@cisco.local
3300
UCM removes IP address
VCS search rule translates domain to IP address of Unified CM
Domain is appended by endpoint or VCS
VCS endpoint dials UCM number of 3300
4
3
2
1

You configure a neighbor zone to connect to the subscriber and publisher of the Unified CM cluster to provide a level of redundancy. The two search rules send all four-digit calls except 36XX to the neighbor zone defined for the Unified CM cluster. The local domain name is replaced with the IP address of the Unified CM subscriber.

Step 1: Navigate to **VCS Configuration > Zones**, and then click **New**.

Step 2: On the Create Zone screen, enter the following values, and then click **Create zone**:

- Name—CUCM Neighbor
- Type—Neighbor
- H.323 Mode—Off
- SIP Mode—On
- SIP Port—5060
- SIP Transport—TCP
- Accept proxied registrations—Deny
- Peer 1 Address—10.10.48.21
- Peer 2 Address—10.10.48.20
- Zone Profile—Cisco Unified Communications Manager



Create zone

You are here: VCS configuration ▸ Zones ▸ Create zo

Configuration

Name * CUCM Neighbor

Type * Neighbor

Hop count * 15

H.323

Mode Off

Port * 1719

SIP

Mode On

Port * 5060

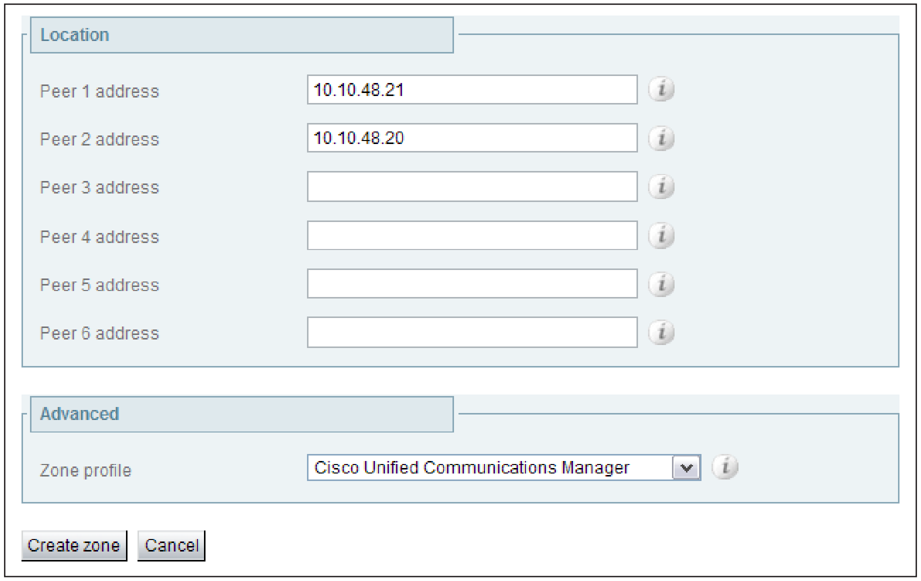
Transport TCP

Accept proxied registrations Deny

Authentication

Authentication policy Do not check credentials

SIP authentication trust mode Off



Location

Peer 1 address 10.10.48.21

Peer 2 address 10.10.48.20

Peer 3 address

Peer 4 address

Peer 5 address

Peer 6 address

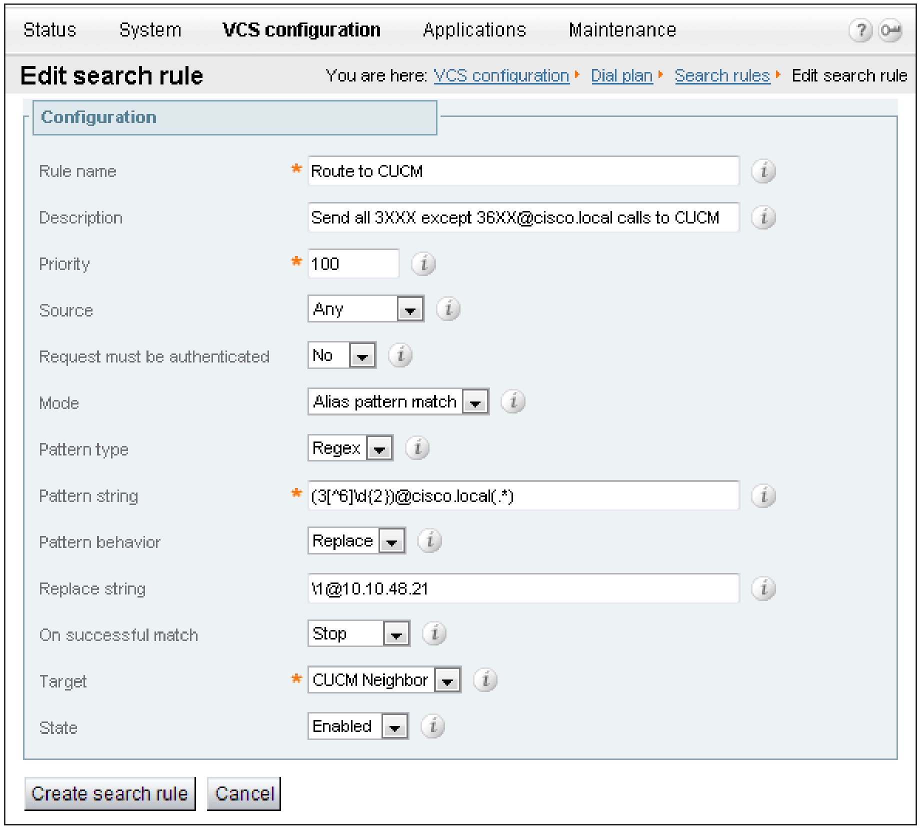
Advanced

Zone profile Cisco Unified Communications Manager

Step 3: Navigate to **VCS configuration > Dial Plans > Search rules**, and then click **New**.

Step 4: Enter the following values, and then click **Create search rule**:

- Rule name—Route to CUCM
- Description—Send all 3XXX except 36XX@cisco.local calls to CUCM
- Priority—100
- Source—Any
- Request must be Authenticated—No
- Mode—Alias Pattern Match
- Pattern Type—Regex
- Pattern String—(3[^6]\d{2})@cisco.local(.*)
- Pattern behavior—Replace
- Replace String—\1@10.10.48.21
- On successful match—Stop
- Target—CUCM Neighbor
- State—Enabled

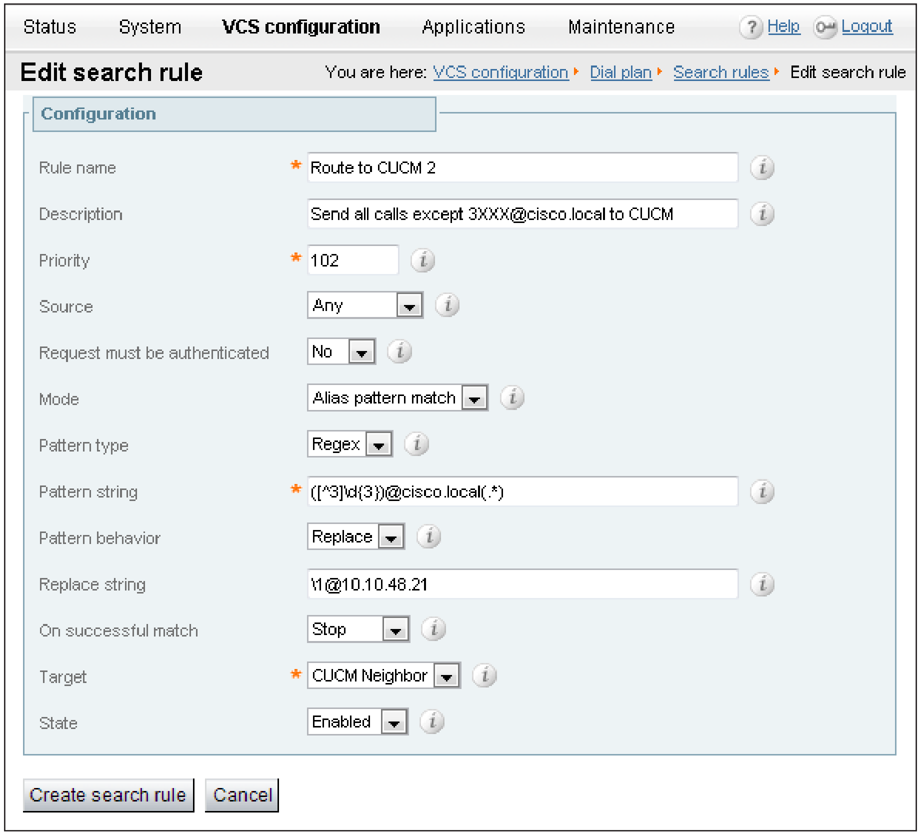


Rule name *	Route to CUCM
Description	Send all 3XXX except 36XX@cisco.local calls to CUCM
Priority *	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string *	(3[^6]\d{2})@cisco.local(.*)
Pattern behavior	Replace
Replace string	\1@10.10.48.21
On successful match	Stop
Target *	CUCM Neighbor
State	Enabled

Step 5: Navigate to **VCS configuration > Dial Plans > Search rules**, and then click **New**.

Step 6: Enter the following values, and then click **Create search rule**:

- Rule name—Route to CUCM 2
- Description—Send all calls except 3XXX@cisco.local to CUCM
- Priority—102
- Source—Any
- Request must be Authenticated—No
- Mode—Alias Pattern Match
- Pattern Type—Regex
- Pattern String—([^3]\d{3})@cisco.local(.*)
- Pattern behavior—Replace
- Replace String—\1@10.10.48.21
- On successful match—Stop
- Target—CUCM Neighbor
- State—Enabled



Edit search rule

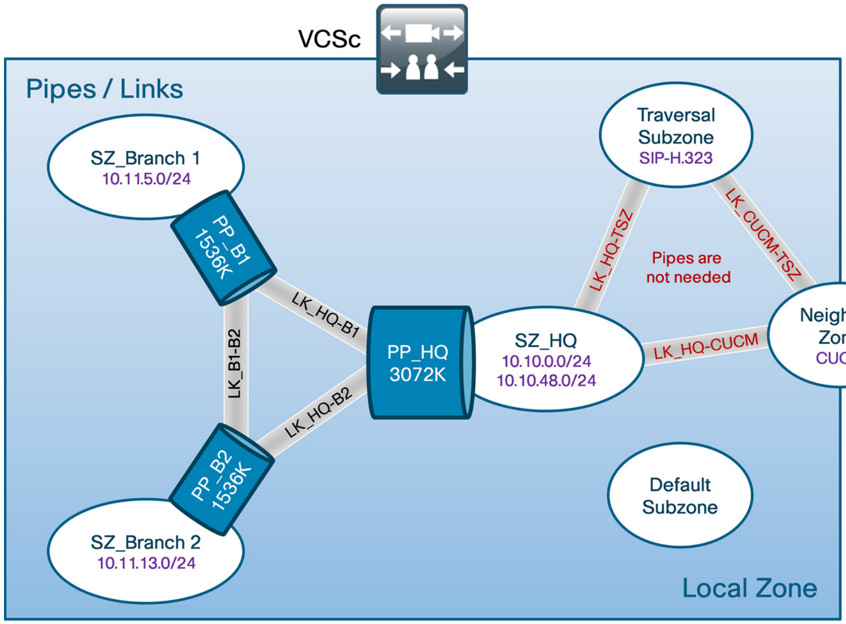
Configuration

Rule name	* Route to CUCM 2
Description	Send all calls except 3XXX@cisco.local to CUCM
Priority	* 102
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	* ([^3]\d{3})@cisco.local(.*)
Pattern behavior	Replace
Replace string	\1@10.10.48.21
On successful match	Stop
Target	* CUCM Neighbor
State	Enabled

Procedure 3 Configure VCS call admission control

You modify call admission control from the VCS base configuration to accommodate the higher bandwidth requirements of the CTS endpoints. The remote-site locations allow a single call at 1536 kbps and the head-quarters site allows two calls at 1536 kbps. The additional WAN bandwidth permits higher quality video and audio between the locations.

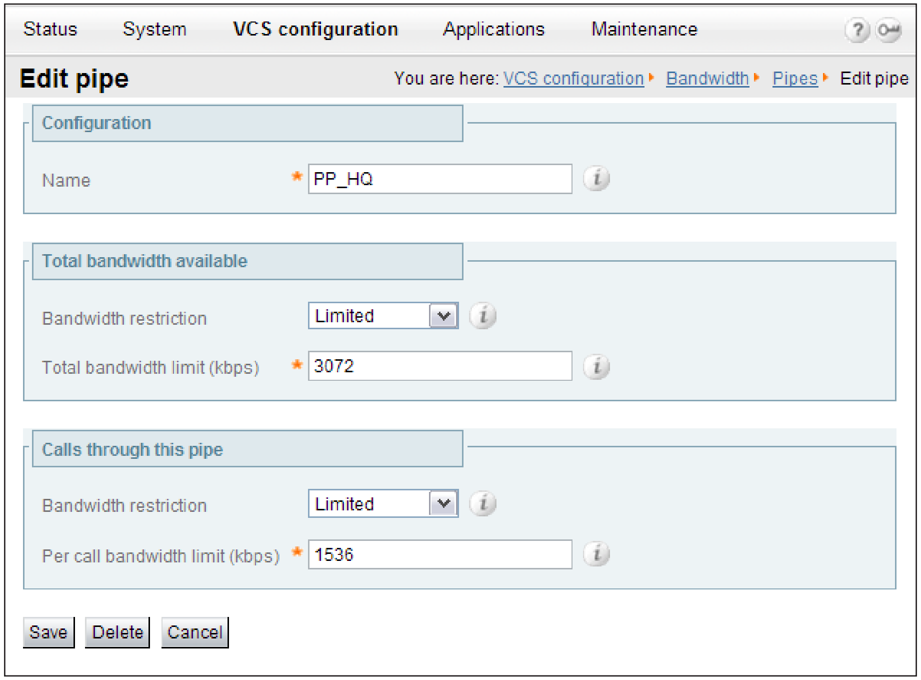
A link is automatically created between the traversal subzone and the Unified CM neighbor zone, which permits H.323 calls to CTS endpoints. However, a link is needed between the neighbor zone and the headquarters subzone to allow SIP calls between the two systems. The bandwidth is controlled by the remote-site settings in each call agent, so pipes are not needed on the links to the neighbor zone.



Step 1: Navigate to **VCS Configuration > Bandwidth > Pipes**, and then click the name of the main site location—**PP_HQ**.

Step 2: On the Edit pipe configuration screen, enter the following values, and then click **Save**:

- Total bandwidth limit (kbps)—**3072** (two 1.5 Mbps calls)
- Per call bandwidth limit (kbps)—**1536**



Edit pipe

You are here: VCS configuration ▸ Bandwidth ▸ Pipes ▸ Edit pipe

Configuration

Name * PP_HQ

Total bandwidth available

Bandwidth restriction: Limited

Total bandwidth limit (kbps) * 3072

Calls through this pipe

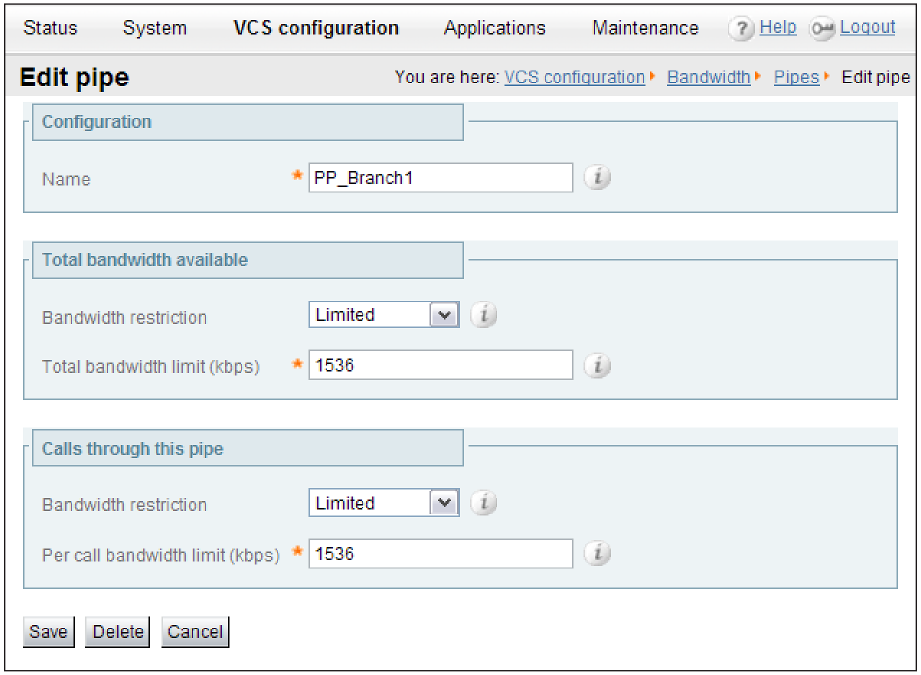
Bandwidth restriction: Limited

Per call bandwidth limit (kbps) * 1536

Step 3: On the Pipes screen, click the name of the remote site pipe—**PP_Branch1**

Step 4: On the Edit pipe configuration screen, enter the following values, and then click **Save**:

- Total bandwidth limit (kbps)—**1536** (one 1.5 Mbps call)
- Per call bandwidth limit (kbps)—**1536**



Edit pipe

You are here: VCS configuration ▸ Bandwidth ▸ Pipes ▸ Edit pipe

Configuration

Name * PP_Branch1

Total bandwidth available

Bandwidth restriction: Limited

Total bandwidth limit (kbps) * 1536

Calls through this pipe

Bandwidth restriction: Limited

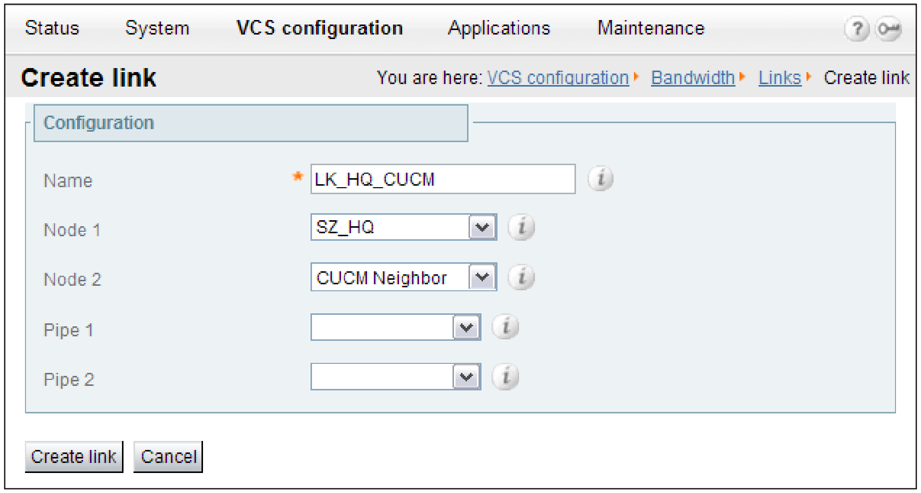
Per call bandwidth limit (kbps) * 1536

Step 5: Repeat the previous two steps for all remote-site locations.

Step 6: Navigate to **VCS Configuration > Bandwidth > Links**, and then click **New**.

Step 7: On the Create link screen, enter the following values, and then click **Create link**:

- Name—LK_HQ_CUCM
- Node 1—SZ_HQ
- Node 2—CUCM Neighbor



Create link

You are here: VCS configuration ▸ Bandwidth ▸ Links ▸ Create link

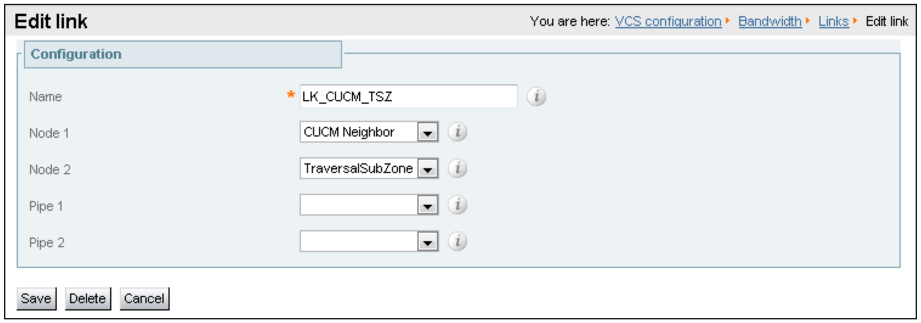
Configuration

Name *	LK_HQ_CUCM
Node 1	SZ_HQ
Node 2	CUCM Neighbor
Pipe 1	
Pipe 2	

VCS creates default links to the CUCM Neighbor Zone. Step 8 and Step 9 modify the name of the Traversal Subzone link to make it more readable. Step 10 deletes the link to the Default Zone because it is not needed.

Step 8: From the Links screen, click **Zone001toTraversalSZ**.

Step 9: From the Edit link screen, change the name of the link — LK_CUCM_TSZ, and then click **Save**.



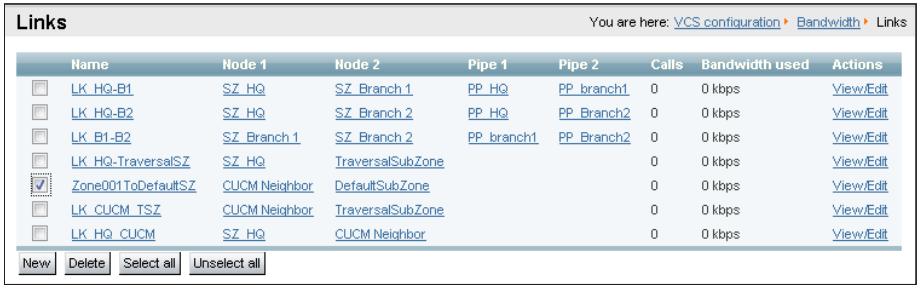
Edit link

You are here: VCS configuration ▸ Bandwidth ▸ Links ▸ Edit link

Configuration

Name *	LK_CUCM_TSZ
Node 1	CUCM Neighbor
Node 2	TraversalSubZone
Pipe 1	
Pipe 2	

Step 10: From the Links screen, select **Zone001toDefaultSZ,** and then click **Delete**.



Links

You are here: VCS configuration ▸ Bandwidth ▸ Links

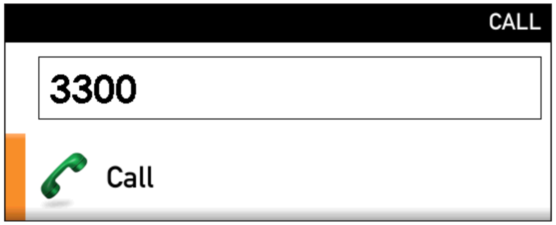
	Name	Node 1	Node 2	Pipe 1	Pipe 2	Calls	Bandwidth used	Actions
□	LK_HQ-B1	SZ_HQ	SZ_Branch 1	PP_HQ	PP_branch1	0	0 kbps	View/Edit
□	LK_HQ-B2	SZ_HQ	SZ_Branch 2	PP_HQ	PP_Branch2	0	0 kbps	View/Edit
□	LK_B1-B2	SZ_Branch 1	SZ_Branch 2	PP_branch1	PP_Branch2	0	0 kbps	View/Edit
□	LK_HQ-TraversalSZ	SZ_HQ	TraversalSubZone			0	0 kbps	View/Edit
☑	Zone001ToDefaultSZ	CUCM Neighbor	DefaultSubZone			0	0 kbps	View/Edit
□	LK_CUCM_TSZ	CUCM Neighbor	TraversalSubZone			0	0 kbps	View/Edit
□	LK_HQ_CUCM	SZ_HQ	CUCM Neighbor			0	0 kbps	View/Edit

Procedure 4 VCS to Unified CM dialing

After the configurations in both call agents are complete, place a numeric call from the VCS endpoint to the Unified CM endpoint to verify that everything is working as expected.

Step 1: If there is no menu on the screen, press the **Home** button on the remote.

Step 2: Enter the extension of a CTS endpoint—3300—and press the green **Call** button.



Step 3: Use the remote to navigate to **Home > Settings > System Information,** and on the Systems Information screen, verify the following settings:

- Video: Transmit: Channel Rate—1472 kbps (variable based on movement)
- Video: Receive: Channel Rate—1472 kbps (variable based on movement)
- Audio: Transmit: Channel Rate—64 kbps
- Audio: Receive: Channel Rate—64 kbps

Step 4: Press the red **End call** button to hang up the call.

Procedure 5 Unified CM to VCS dialing

Place a numeric call from a Unified CM endpoint to a VCS endpoint to verify everything is working as expected.

Step 1: On the associated phone, select **New Call**.

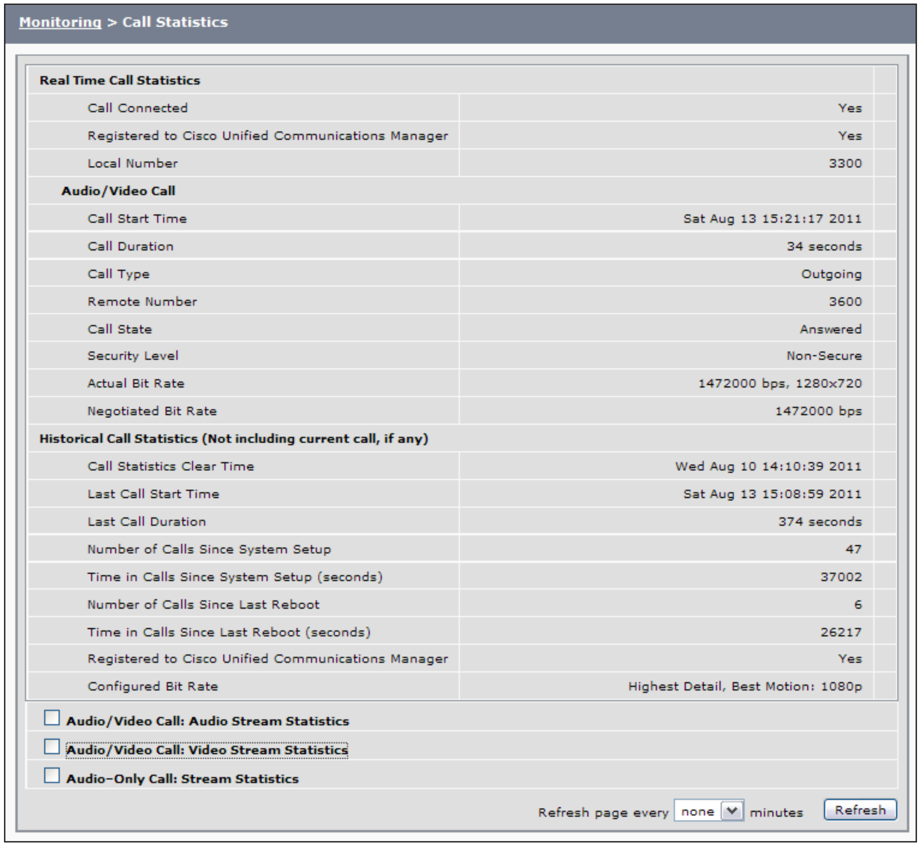
Step 2: Dial the four-digit extension of a general-purpose endpoint—3600—and then select **Dial**.

Step 3: Use your web browser to access the endpoints administrative interface—https://10.10.2.50/—and log in using the SSH admin username and password.

Step 4: On the Cisco TelePresence Systems Administration screen, enter the following values, and then click **Login**:

- Username—admin
- Password—[password]

Step 5: Navigate to **Monitoring > Call Statistics** to verify the bandwidth being used.



Monitoring > Call Statistics

Real Time Call Statistics	
Call Connected	Yes
Registered to Cisco Unified Communications Manager	Yes
Local Number	3300
Audio/Video Call	
Call Start Time	Sat Aug 13 15:21:17 2011
Call Duration	34 seconds
Call Type	Outgoing
Remote Number	3600
Call State	Answered
Security Level	Non-Secure
Actual Bit Rate	1472000 bps, 1280x720
Negotiated Bit Rate	1472000 bps
Historical Call Statistics (Not including current call, if any)	
Call Statistics Clear Time	Wed Aug 10 14:10:39 2011
Last Call Start Time	Sat Aug 13 15:08:59 2011
Last Call Duration	374 seconds
Number of Calls Since System Setup	47
Time in Calls Since System Setup (seconds)	37002
Number of Calls Since Last Reboot	6
Time in Calls Since Last Reboot (seconds)	26217
Registered to Cisco Unified Communications Manager	Yes
Configured Bit Rate	Highest Detail, Best Motion: 1080p

□ Audio/Video Call: Audio Stream Statistics

□ Audio/Video Call: Video Stream Statistics

□ Audio-Only Call: Stream Statistics

Step 6: To hang up the call from the phone, select **End Call**.

Appendix A: Product List

The following products and software versions were validated for Cisco SBA.

Functional Area	Product	Part Numbers	Software Version
CTS Immersive Call Control	Cisco Unified Communications Manager—MCS 7835	MCS7835I3-K9-CMD1 (2 required)	8.6.2
	Cisco Unity Connection - MCS 7835	MCS7835I3-K9-UCC1	8.6.2
	Cisco Unified Communications Manager Business Edition 6000 - UCS C200M2	UCS-C200M2-BE6K	8.6.2
	UCS Virtual Server	UCS-C200M2-VCD2	ESXi 4.1
CTS Immersive Endpoints	Cisco TelePresence 500	CTS-500 TelePresence 500 System	1.7.4 (270)
		CTS500-STRUC-TABL TelePresence 500 Structure - Tabletop	
		CTS-CODEC-PRI-G2 TelePresence Primary Codec	
		CP-7975G-CTS UC Phone CP-7975G to Control CTS	9-2-1S
	Cisco TelePresence 1100	CTS-1100 TelePresence 1100 System	1.7.4 (270)
		CTS-CODEC-PRI-G2 TelePresence Primary Codec	
		CP-7975G-CTS UC Phone CP-7975G to Control CTS	9-2-1S
Video Telephones	Cisco Video Telephones	CP-8945 Four Line Video Color Phone	9-1-2-SR-1
		CP-9951 Six Line Video Color Phone	9-2-1
		CIUS-7-K9-PR 7 inch Tablet - Wifi	9-2-1 SR2
		CIUS-MS-H= Media Station with Standard Handset	

Functional Area	Product	Part Numbers	Software Version
General Purpose Call Control	Cisco TelePresence Video Communications Server - Control	CTI-VCS-BASE-K9 PWR-CORD-US-A SW-VCS-BASE-K9 LIC-VCS-BASE-K9 LIC-VCS-DEVPROV LIC-VCS-GW LIC-VCSE-100	X6.1
Multipurpose Room System	Cisco TelePresence Profile Series 42”	CTS-P42C40-K9 PWR-CORD-US-A SW-S52000-TC4.XK9 CTS-P4252S-WBK LIC-P42SC40 LIC-PCXX-NPP LIC-S52000-TC4.XK9 CTS-C40CODEC-K9- CTS-CTRL-DVC8 CTS-DNAM-III- CTS-P42MONITOR CTS-PHD-1080P12XS+ CTS-RMT-TRC5	TC4.2.1
Executive Room System	Cisco TelePresence Executive 90	CTS-EX90-K9 PWR-CORD-US-A SW-S52000-TC4.XK9 CTS-CTRL-DV8 LIC-ECXX-NPP LIC-EX90 LIC-S52000-TC4.XK9	TC4.2.1

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**