



▶ Polycom Unified Communications
Deployment Guide for Cisco
Environments

Trademark Information

Polycom®, the Polycom “Triangles” logo, and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

© 2010 - 2012 Polycom, Inc. All rights reserved.

Polycom, Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Contents

About This Guide	1
Related Documentation	1
Required Skills	1
Polycom Solution Support Services	2
1 Polycom Unified Communications with Cisco Interoperability	3
Supported Deployment Models	3
Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager	4
Direct Registration of Polycom Telepresence Endpoints with the Cisco Unified Communications Manager	4
Neighbored Gatekeepers	4
Standalone Polycom CMA System as a Gatekeeper	4
Standalone Cisco IOS Gatekeeper	5
2 Direct Registration of Polycom Systems with the Cisco Unified Communications Manager	7
Deployment Model Advantages	7
Supported Products	8
Deployment Architecture	9
Device Licensing	9
Registering a Polycom HDX system with Cisco Unified Communications Manager	11
Configuring the Cisco Unified Communications Manager	11
Cisco Unified Communications Manager Considerations	11
Configure Security Settings	12
Add an HDX System User	14
Add a Device Entry	15
Register Polycom HDX System with the Cisco Unified Communications Manager	17
Registering a Polycom VVX with Cisco Unified Communications Manager	19

Register a Spectralink Phone with Cisco Unified Communications Manager
19

- Configure the Cisco Unified Communications Manager 19
 - Configure Security Settings 20
 - Add an Spectralink Phone User 22
 - Add a Device Entry 23
 - Associate the Phone with the User You Created 26
- Configure Your Spectralink Phone 26
- Registering a KIRK Wireless Server 26
- Configuring the Polycom RMX System to Route Calls to the Cisco Unified
Communications Manager 27
 - Call Routing with the Polycom RMX System 27
 - Call Routing with the Polycom DMA System 27
 - Configuring RMX to statically route outbound SIP calls to the Cisco
Unified Communications Manager 27
 - Configuring an RMX Ad Hoc Entry Queue or Meeting Rooms (if
DMA system is not used) 28
- Supporting Telepresence Calls with the RMX System 28

3 Direct Registration of Polycom Telepresence Systems with the Cisco Unified Communications Manager 29

- Deployment Model Advantages 29
- Supported Products 30
- Deployment Architecture 31
- Telepresence Deployment Design Considerations 32
 - Polycom Telepresence Systems Considerations 32
 - Content Sharing in Telepresence Environments 33
 - Polycom Endpoints Registered to the Cisco Unified
Communications Manager 33
 - Device Licensing 34
- Registering a Polycom Telepresence or HDX system with a Cisco Unified
Communications Manager 35
 - Configuring the Cisco Unified Communications Manager for an HDX or
ITP System 35
 - Create a Security Profile 35
 - Add a System User 37
 - Add a Device Entry 40
- Define your Polycom ITP Endpoints in the Cisco TelePresence Server .. 42
 - Configuring the Polycom Endpoint 44
 - Register the Polycom System with the Cisco Unified
Communications Manager 44
 - Ensure the TIP Protocol is Enabled 46
- Configuring the Polycom RMX System to Support TIP Calls 47

Contents

About This Guide	1
Related Documentation	1
Required Skills	1
Polycom Solution Support Services	2
1 Polycom Unified Communications with Cisco Interoperability	3
Supported Deployment Models	3
Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager	4
Direct Registration of Polycom Telepresence Endpoints with the Cisco Unified Communications Manager	4
Neighbored Gatekeepers	4
Standalone Polycom CMA System as a Gatekeeper	4
Standalone Cisco IOS Gatekeeper	5
2 Direct Registration of Polycom Systems with the Cisco Unified Communications Manager	7
Deployment Model Advantages	7
Supported Products	8
Deployment Architecture	9
Device Licensing	9
Registering a Polycom HDX system with Cisco Unified Communications Manager	11
Configuring the Cisco Unified Communications Manager	11
Cisco Unified Communications Manager Considerations	11
Configure Security Settings	12
Add an HDX System User	14
Add a Device Entry	15
Register Polycom HDX System with the Cisco Unified Communications Manager	17
Registering a Polycom VVX with Cisco Unified Communications Manager	19

Configure Call Routing with the Polycom RMX System	47
Configure Call Routing with the Polycom DMA System	47
Configuring the RMX System for a Cisco Telepresence Environment	47
Configure the RMX System for Telepresence Conferencing	48
Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag .	48
Configure a TIP Enabled Profile on the RMX system	48
Configure an Ad Hoc Entry Queue on the RMX (if DMA system is not used)	49
Configure a Meeting Room on the RMX	49
Configure Participant Properties for dial out calls	49
Configure the RMX system for your H.323 gatekeeper	49
Operations During Ongoing Conferences	50
4 Using a Polycom DMA System in a Cisco Environment	51
Supported Products	52
Architecture Diagram	53
Content Sharing with Polycom Endpoints Registered to a DMA System	54
Polycom Endpoints Registered to a Polycom DMA System	54
Task Overview	55
Configuring a DMA SIP Trunk on Cisco Unified Communications Manager	55
Add a SIP Trunk on the Cisco Unified Communications Manager .	55
Configuring route groups, route lists and patterns	56
Configuring the DMA System for Cisco Unified Communications Manager	60
Configure a SIP Peer for the Cisco Unified Communications Manager	60
Set up a Dial Rule for the Cisco Unified Communications Manager	61
Create a TIP-Enabled Conference Template	62
5 Neighbored Cisco IOS and Polycom CMA Gatekeepers ...	65
Deployment Model Advantages	66
End User Advantages	66
System Administrator Advantages	66
Supported Products	67
Design Considerations	68
Architecture Diagram	69
Task Overview	69
Configure the Cisco IOS Gatekeeper for use with a CMA System ...	70
Basic Cisco IOS Gatekeeper Monitoring	72

Configuring CMA for use with Cisco IOS Gatekeeper	75
Add a new site (if applicable)	75
Add a site link	76
Define a Neighboring Gatekeeper	77
Add a Dial Rule	78
Configuring Cisco Unified Communications Manager for H.323 ...	80
Define a gatekeeper	81
Create a trunk	82
Configuring Route groups, Route lists and Route Patterns	82
6 Using a Polycom CMA System as a Gatekeeper	87
Deployment Model Advantages	87
Supported Products	88
Architecture Diagram	89
Task Overview	90
Configuring Cisco Unified Communications Manager for H.323 ...	90
Define a gatekeeper	90
Create a trunk	91
Configuring route groups, route lists and patterns	91
Configuring CMA for Cisco Unified Communications Manager	95
7 Using a Standalone Cisco IOS Gatekeeper	97
Supported Products	98
Architecture Diagram	99
Design Considerations	99
Task Overview	100
Configuring the Cisco IOS Gatekeeper	100
Configuring Cisco Unified Communications Manager for H.323 ...	103
Define a gatekeeper	103
Create a trunk	104
Configuring route groups, route lists and patterns	104
Integrating Polycom H.323 Endpoints with an IOS Gatekeeper	108

About This Guide

This guide provides design considerations and guidelines for deploying Polycom Unified Communications for Cisco Unified Communications Manager.

This guide is intended to assist administrators with integration of Polycom H.323, SIP-based, or telepresence devices with Cisco Unified Communications Manager, previously called Call Manager.

Related Documentation

Please refer to the product documentation for the appropriate Polycom product for detailed documentation. You can find Polycom product documentation online at <http://www.support.polycom.com>.

Refer to the *Cisco Unified Communications Manager Documentation Guide* which is found on <http://www.cisco.com>.

Required Skills

Integrating Polycom infrastructure and endpoints with the Cisco Unified Communications Manager requires planning and elementary knowledge of Polycom video conferencing and video conferencing administration.

Polycom assumes the readers of this guide have a basic understanding of H.323, SIP, TIP, Cisco Unified Communications Manager and Polycom device concepts. Users should also be comfortable with navigating and configuring Cisco Unified Communications Manager as well as Cisco IOS (Internetwork Operating System)-based devices.

Users should have knowledge of the following third-party products:

- Cisco video and voice endpoints
- Cisco IOS Gatekeeper
- Cisco Unified Communications Manager

Polycom Solution Support Services

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services, and its certified partners, to help customers successfully design, deploy, optimize and manage Polycom unified communication within their third-party environments.

Please see

http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.

Polycom Unified Communications with Cisco Interoperability

Polycom's integrated suite of hardware devices and software applications allows you to integrate high-quality video and audio communications across Cisco® platforms.

Specifically, the Polycom video infrastructure allows you to integrate with Cisco Unified Communications Manager infrastructure to enable common dial plans between Polycom and Cisco Unified IP phones or video endpoints, as well as take advantage of the Cisco Unified Communications Manager monitoring capabilities.

The Polycom HDX system is the first HD video device to carry a "Cisco Compatible" logo and ensures that Polycom customers can natively deploy Polycom HDX systems within a Cisco environment, taking advantage of Cisco Unified Communications Manager's bandwidth management, call processing, and provisioning capabilities.

Supported Deployment Models

Polycom supports the following deployment models when integrating Polycom Unified Communications with the Cisco Unified Communications Manager.

- ["Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager"](#) on page 4
- ["Direct Registration of Polycom Telepresence Endpoints with the Cisco Unified Communications Manager"](#) on page 4
- ["Neighbored Gatekeepers"](#) on page 4
- ["Standalone Polycom CMA System as a Gatekeeper"](#) on page 4
- ["Standalone Cisco IOS Gatekeeper"](#) on page 5

Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager

When you register your Polycom endpoints directly with Cisco Unified Communications Manager, you have a single source for call admission control and bandwidth management. Cisco endpoints can also use telephone functions like hold, transfer and so on when on calls with Polycom endpoints.

This deployment model can also be used in conjunction with other deployment models in this guide.

For deployment details, see [“Direct Registration of Polycom Systems with the Cisco Unified Communications Manager”](#) on page 7.

Direct Registration of Polycom Telepresence Endpoints with the Cisco Unified Communications Manager

When you register your Polycom telepresence endpoints directly with Cisco Unified Communications Manager, you have a single source for call admission control and bandwidth management. Cisco endpoints can also use telephone functions like hold, transfer and so on when on calls with Polycom endpoints.

When Polycom telepresence and video endpoints have the TIP option key installed, they can participate in calls with Cisco CTS endpoints.

For deployment details, see [“Direct Registration of Polycom Telepresence Systems with the Cisco Unified Communications Manager”](#) on page 29.

Neighbored Gatekeepers

Consider neighboring gatekeepers if you are integrating an existing Cisco environment with an existing Polycom network. Neighbored gatekeepers make it easier to create a common dial plan. With neighbored gatekeepers, you can do number translation and maintain your existing environments.

For deployment details, see [“Neighbored Cisco IOS and Polycom CMA Gatekeepers”](#) on page 65.

Standalone Polycom CMA System as a Gatekeeper

When you register your Polycom components with Polycom CMA system, bandwidth and call admission control is split between the CMA system and Cisco Unified Communications Manager. Polycom CMA system fully manages your Polycom components and you can take advantage of CMA provisioning with dynamic management.

For deployment details, see [“Using a Polycom CMA System as a Gatekeeper”](#) on page 87.

Standalone Cisco IOS Gatekeeper

You can use the Cisco IOS Gatekeeper as the only gatekeeper for your deployment if you do not need the management capabilities of the Polycom CMA system.

In this deployment model, the Cisco Unified Videoconferencing MCU is supported along with Polycom H.323 devices, such as the Polycom RMX system.

For deployment details, see [“Using a Standalone Cisco IOS Gatekeeper”](#) on page 97.

Direct Registration of Polycom Systems with the Cisco Unified Communications Manager

When you register your Polycom endpoints directly with Cisco Unified Communications Manager, you have a single source for call admission control and bandwidth management. You can also take advantage of telephone functions like hold, transfer and so on.

This deployment model can also be used in conjunction with other deployment models in this guide.

Polycom endpoints can be registered with the Cisco Unified Communications Manager and the Polycom CMA system simultaneously. See [“Neighbored Cisco IOS and Polycom CMA Gatekeepers”](#) on page 65 or [“Using a Polycom CMA System as a Gatekeeper”](#) on page 87 for more information on using a CMA system.

Deployment Model Advantages

Registering Polycom video and voice endpoints with the Cisco Unified Communications Manager allows you to easily integrate Polycom products within a Cisco deployment without additional network management overhead.

Polycom voice and video endpoints can take advantage of telephone functions like hold, transfer and so on when SIP-enabled and registered with the Cisco Unified Communications Manager.

Supported Products

Polycom has tested its most recent product versions with the following Cisco products.

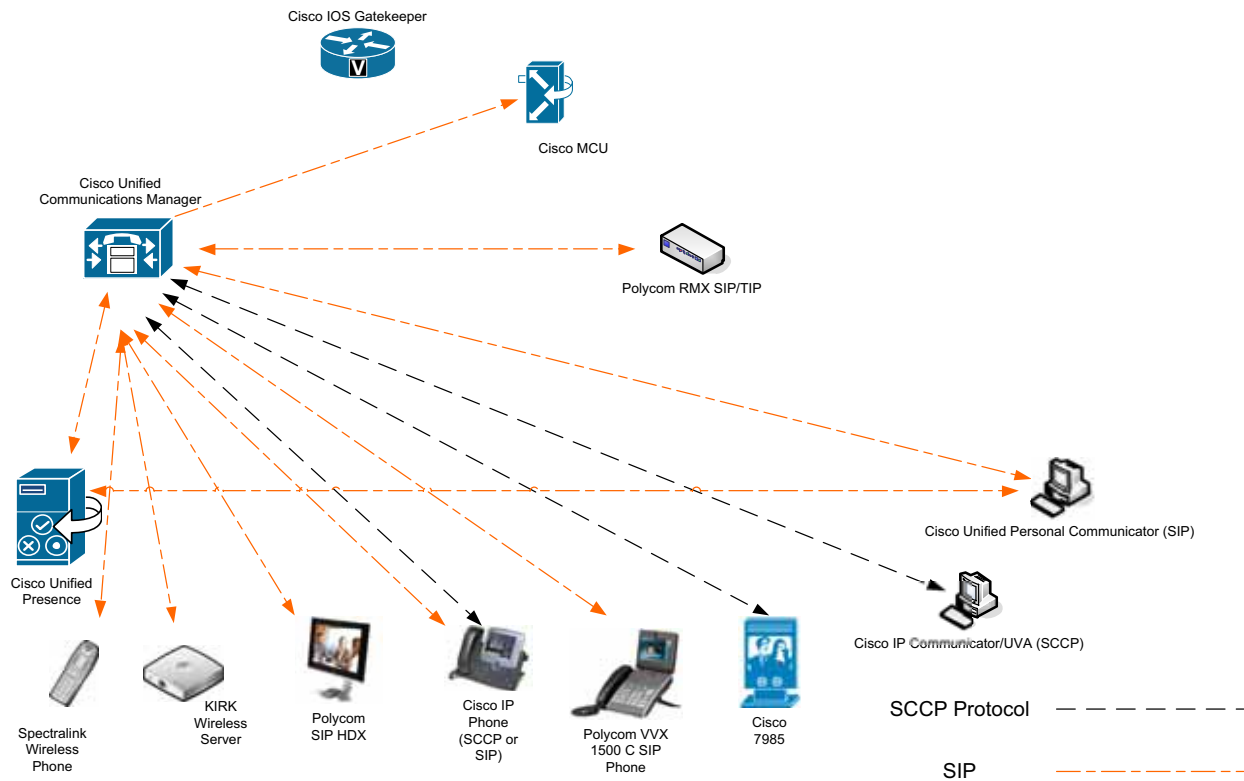
Table 2-1 Matrix for supported current Polycom products with Cisco components.

Cisco	Version(s)
Cisco Unified Communications Manager	8.0, 8.5
Cisco Unified Videoconferencing 5230	7.x
Cisco Unified Presence	8.x
Unified Contact Center Express	8.x
Cisco IP Communicator	7.x
Cisco Unified Personal Communicator	8.x
Cisco Unified Video Advantage	2.2(x)
Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971	
Polycom	Version(s)
RMX 1500/2000/4000 systems	v7.6 MPMx card required for TIP support.
HDX system (all models)	v3.0.4
Polycom Touch Control	1.4.0
Spectralink wireless phones 8020/8030	
Polycom VVX 1500	v4.0
Polycom VVX 1500 C	v3.3.1
KIRK Wireless Server 300/6000/2500/8000	

Deployment Architecture

Figure 2-1 shows the reference architecture for this deployment model.

Figure 2-1 Architecture when Polycom devices are directly registered to Cisco Unified Communications Manager



Device Licensing

Device license units are assigned to each device connected to Cisco Unified Communications Manager. Each device is assigned a unit number based on the type and capabilities of the device. Devices with more complex and high-end capabilities are assigned a higher number of units compared to devices with basic capabilities. For more information, see your Cisco documentation.

Table 2-2 *Required Device License Units.*

Polycom Device	Required Device License Units
Polycom HDX System	Six(6)
Polycom VVX System	Six(6)
Spectralink 8020/8030 wireless telephones	Three(3)
KIRK Wireless Server 300/6000/2500/8000	Three(3)

Registering a Polycom HDX system with Cisco Unified Communications Manager

To register the Polycom HDX system with the Cisco Unified Communication Manager, you need to perform steps in both the Cisco Unified Communications Manager and the Polycom HDX system.

For more information about the Cisco Unified Communications Manager, see the Cisco Unified Communications Manager Documentation Guide (http://www.cisco.com/en/US/docs/viscerotome/cucm/docguide/8_5_1/dg851.html)

For more information about Polycom HDX systems, see the *Administrator's Guide for HDX Systems*.

Configuring the Cisco Unified Communications Manager

Use the Cisco Unified Communications web administrator to perform the following tasks:

- “Configure Security Settings” on page 12
- “Add an HDX System User” on page 14
- “Add a Device Entry” on page 15

Cisco Unified Communications Manager Considerations

- Location settings should allow for video bandwidth when integrating Polycom video endpoints and infrastructure.
- Region settings should allow for a minimum of 256k video bandwidth (region settings should match the Polycom HDX system maximum call rate).
- Region settings should allow for a G.722 audio protocol for the best audio experience.
- Each Polycom HDX system requires six Device License Units.
- The Polycom HDX system should be added to a device pool in which the Media Resource Group List does not contain MTP resources.

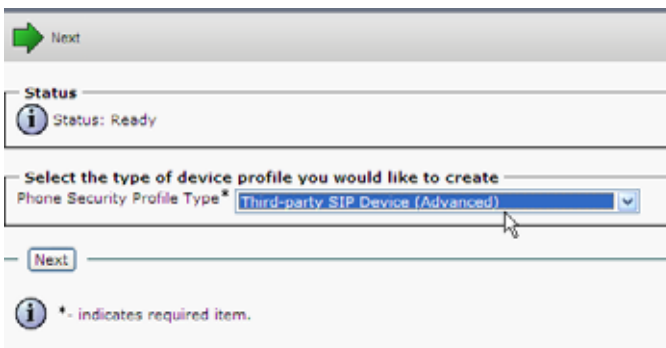
Note Due to the nature of out-of-band DTMF signalling, Cisco Unified Communications Manager will sometimes insert Media Termination Point Resources (MTP) in a call. This will prevent video on the Polycom HDX system from operating correctly. This is most common on H.323 and SIP trunk calls. To prevent this from occurring, the MTP resources should be removed from any Media Resource Groups and Media Resource Group Lists that would be used in the trunked calls.

Task 1: Configure Security Settings

You need to create a Phone Security Profile for your HDX systems to use. If you want to create a secure profile, you can choose to enable digest authentication to secure the Polycom HDX system's connection to Cisco Unified Communications Manager.

To configure security settings:

- 1 Log into the Cisco Unified Communications Manager console.
- 2 Select **System > Security Profile > Phone Security Profile**.
- 3 Select **Add New**.
- 4 Select a Phone Security Profile Type. Select **Third-party SIP Device (Advanced)** and click **Next**.



- 5 On **Phone Security Profile Information** page, complete the following fields:
 - a In the **Name** text box, enter a profile name for the system.
 - b In the **Description** field, enter a description for the security profile.
 - c If you want to use digest authentication (recommended), mark the **Enabled Digest Authentication** check box. When you use digest authentication, a valid login password is required.

- d Select the default values for all other fields. This example uses digest authentication.

Phone Security Profile Configuration

Save

— Status —

Status: Ready

— Phone Security Profile Information —

Product Type: Third-party SIP Device (Advanced)

Device Protocol: SIP

Name* Polycom Security Profile

Description security profile for Polycom devices

Nonce Validity Time* 600

Transport Type* TCP+UDP

Enable Digest Authentication

— Parameters used in Phone —

SIP Phone Port* 5060

Save

*- indicates required item.

- 6 Click the Save button.

In the status bar near the top of the page, **Update Successful** appears.

Task 2: Add an HDX System User

If you cannot add a user here, your system may be LDAP integrated. If that is the case, you can use an existing user ID (essentially associating the endpoint to an existing user) or have your LDAP administrator create a new user ID for the Polycom endpoint.

To add an HDX system user:

- 1 Select **User Management > End User**.
- 2 Click **Add New**.

The following screen appears.

- 3 Complete the required fields.
 - a If you are not using digest authentication, leave the **Digest Credentials** fields blank.
 - b If you are using digest authentication, enter the **Digest Credentials** (password) for the Polycom system.

This is the same password that will be used by the system to access the web interface.

- 4 Click the **Save** button.

In the status bar near the top of the page, **Update Successful** appears.

Task 3: Add a Device Entry

To add a device entry

- 1 Select **Device > Phone**.
- 2 Click **Add New**.
- 3 Select **Third-party SIP Device (Advanced)**, then click **Next**.

The following screen appears. The data shown in this section is shown as an example.

Device Information	
MAC Address *	<input type="text" value="00E0DB0A1AE8"/>
Description	<input type="text" value="SEP00E0DB0A1AE8"/>
Device Pool *	<input type="text" value="DP-Westminster"/> View Details
Common Device Configuration	<input type="text" value="< None >"/> View Details
Phone Button Template *	<input type="text" value="Third-party SIP Device (Advanced)"/>
Common Phone Profile *	<input type="text" value="Standard Common Phone Profile"/>
Calling Search Space	<input type="text" value="< None >"/>
AAR Calling Search Space	<input type="text" value="< None >"/>
Media Resource Group List	<input type="text" value="< None >"/>
Location *	<input type="text" value="Loc-Westminster"/>
AAR Group	<input type="text" value="< None >"/>
Device Mobility Mode *	<input type="text" value="Default"/> View Current Device Mobility Settings
Owner User ID	<input type="text" value="< None >"/>
Use Trusted Relay Point *	<input type="text" value="Default"/>
Always Use Prime Line *	<input type="text" value="Default"/>
Always Use Prime Line for Voice Message *	<input type="text" value="Default"/>
Calling Party Transformation CSS	<input type="text" value="< None >"/>
Geolocation	<input type="text" value="< None >"/>
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS <input checked="" type="checkbox"/> Retry Video Call as Audio <input type="checkbox"/> Ignore Presentation Indicators (internal calls only) <input checked="" type="checkbox"/> Logged Into Hunt Group <input type="checkbox"/> Remote Device	

- a In the **MAC Address** text box, enter the MAC Address of the HDX system.
- b (Optional) In the **Description** text box, enter a description.
- c From the **Device Pool** list, select the device pool appropriate for your Cisco Unified Communications Manager system video devices.
- d From the **Phone Button Template** list, select **Third-party SIP Device (Advanced)**.
- e (Optional) From the **Calling Search Space** list, select an appropriate calling search space for the HDX system.
- f From the **Location** list, select an appropriate location for the HDX system. This location should contain video bandwidth. See “[Cisco Unified Communications Manager Considerations](#)” on page 11.

4 Scroll to the **Protocol Specific Information** section.

- a** From the **Device Security Profile** list, select the profile created in “**Configure Security Settings**” on page 12.
- b** In the **SIP Profile** field, select **Standard SIP Profile**.
- c** In the **Digest User** field, select the user created in “**Add an HDX System User**” on page 14.

5 Click **Save**.

In the status bar near the top of the page, an **Update Successful** message appears.

After you have saved the new device, the **Association Information** section is displayed.

6 In the **Association Information** section, click **Line [1] - Add a new DN**.

- 7 Complete the following required fields:
 - a In the **Directory Number** field, enter the phone's extension number.
 - b In the **Route Partition** field, choose the appropriate value.

- 8 Click **Save**.
In the status bar near the top of the page, an **Update Successful** message appears.
- 9 Reset the Polycom HDX system in Cisco Unified Communications Manager.

Register Polycom HDX System with the Cisco Unified Communications Manager

When an Polycom endpoint is registered with a Cisco Unified Communications Manager, the endpoint can make calls to Cisco endpoints that are also registered to the Cisco Unified Communications Manager.

To register an HDX or ITP system with the Cisco Unified Communications Manager

- 1 Open a browser window and in the **Address** field enter the Polycom HDX system IP address or host name.
- 2 Go to **Admin Settings > Network > IP Network** and select **SIP**.

3 Configure the settings in the **SIP Settings** section of the **IP Network** screen. For guidance, see [Table 2-3](#).

Table 2-3 SIP Settings fields and their descriptions.

Settings	Description
Enable SIP	Mark this check box to enable the HDX system to receive and make SIP calls.
Registrar Server	Specify the IP address of the Cisco Unified Communications Manager. If you leave this field blank, the Proxy Server is used.
Proxy Server	Specify the IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you leave both fields blank, no Proxy Server is used. By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. The syntax used for this field is the same as for the SIP Registrar Server field.
Transport Protocol	The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required. For Cisco environments, select either Auto or TCP.
Domain Name	For Cisco environments, leave this field blank.

Settings	Description
User Name	Specify the system's SIP name. This is the SIP URI. Set this to the directory number you assigned to the HDX system.
Password	When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Registrar Server. If using Digest Authentication, mark the Password check box and set the password to the Digest Credentials password you set for the Cisco Unified Communications user you created for this HDX system.
Directory: Microsoft Lync Server	Specifies whether the SIP Registrar Server is a Lync Server. For Cisco environments, leave this check box unmarked.

4 Click **Update**.

Registering a Polycom VVX with Cisco Unified Communications Manager

For detailed instructions on registering a Polycom VVX with Cisco Unified Communications Manager, see the *Deployment Guide for the Polycom® VVX™ C Business Media Phone for Cisco® Unified Communications Manager (SIP)* available on <http://support.polycom.com>.

Register a Spectralink Phone with Cisco Unified Communications Manager

To register a Spectralink phone with the Cisco Unified Communication Manager, you need to perform steps in both the Cisco Unified Communications Manager and the Spectralink phone.

Configure the Cisco Unified Communications Manager

Use the Cisco Unified Communications web administrator to perform the following tasks.

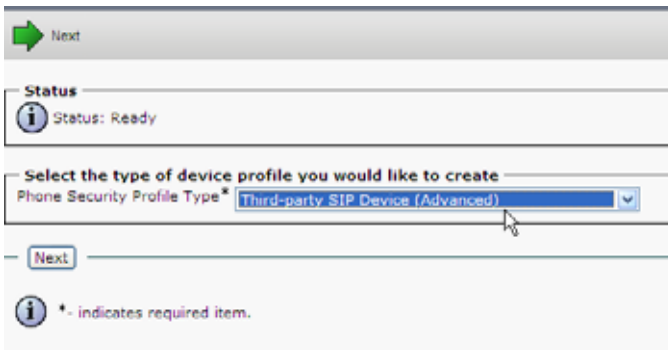
- “[Configure Security Settings](#)” on page 20
- “[Add an Spectralink Phone User](#)” on page 22

- “Add a Device Entry” on page 23

Task 1: Configure Security Settings

To configure security settings:

- 1 Log into the Cisco Unified Communications Manager console.
- 2 Select **System > Security Profile > Phone Security Profile**.
- 3 Select **Add New**.
- 4 Select a Phone Security Profile Type. Select **Third-party SIP Device (Advanced)** and click **Next**.



The screenshot shows a web interface for configuring a security profile. At the top, there is a green arrow labeled 'Next'. Below that, a 'Status' section shows 'Status: Ready' with an information icon. The main section is titled 'Select the type of device profile you would like to create'. It contains a dropdown menu labeled 'Phone Security Profile Type*' with the selected option 'Third-party SIP Device (Advanced)'. A 'Next' button is located below the dropdown. At the bottom, an information icon is followed by the text '* - indicates required item.'

- 5 On **Phone Security Profile Information** page, complete the following fields:
 - a In the **Name** text box, enter a profile name for the system.
 - b In the **Description** field, enter a description for the security profile.
 - c If you want to use digest authentication (recommended), mark the **Enabled Digest Authentication** check box. When you use digest authentication, a valid login password is required.

- d Select the default values for all other fields. This example uses digest authentication.

Phone Security Profile Configuration

Save

— Status —
Status: Ready

— Phone Security Profile Information —
Product Type: Third-party SIP Device (Advanced)
Device Protocol: SIP
Name*: Polycom Security Profile
Description: security profile for Polycom devices
Nonce Validity Time*: 600
Transport Type*: TCP+UDP
 Enable Digest Authentication

— Parameters used in Phone —
SIP Phone Port*: 5060

Save

i *- indicates required item.

- 6 Click the Save button.

In the status bar near the top of the page, **Update Successful** appears.

Task 2: Add an Spectralink Phone User

If you cannot add a user here, your system may be LDAP integrated. If that is the case, you can use an existing user ID (essentially associating the endpoint to an existing user) or have your LDAP administrator create a new user ID for the Polycom endpoint.

To add an Spectralink phone user:

- 1 Select **User Management > End User**.
- 2 Click **Add New**.

The following screen appears.

User Information	
User ID*	<input type="text" value="8015551212"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Last name*	<input type="text" value="Smith"/>
Middle name	<input type="text"/>
First name	<input type="text"/>
Telephone Number	<input type="text"/>
Mail ID	<input type="text"/>
Manager User ID	<input type="text"/>
Department	<input type="text"/>
User Locale	<input type="text" value=" < None >"/>
Associated PC	<input type="text"/>
Digest Credentials	<input type="password" value="*****"/>
Confirm Digest Credentials	<input type="password" value="*****"/>

- a In the **User ID** field, use the phone number for the phone.
 - b For the **Password** field, the password must be five digits.
 - c In the **Last Name** text box, enter a last name.
 - d In the **Digest Credentials** text box, use the phone's extension number.
 - e In the **Confirm Digest Credentials** text box, enter the same value that you entered in the previous step.
- 3 Click the **Save** button.

In the status bar near the top of the page, **Update Successful** appears.

Task 3: Add a Device Entry

To add a device entry

- 1 Select **Device > Phone**.
- 2 Click **Add New**.
- 3 Select **Third-party SIP Device (Basic)**, then click **Next**.

The following screen appears.

Device Information

⚠ Device is not trusted

MAC Address*

Description

Device Pool* -- Not Selected -- [View Details](#)

Common Device Configuration < None > [View Details](#)

Phone Button Template* -- Not Selected --

Common Phone Profile* Standard Common Phone Profile

Calling Search Space < None >

AAR Calling Search Space < None >

Media Resource Group List < None >

Location* Hub_None

AAR Group < None >

Device Mobility Mode* Default [View Current Device Mobility Settings](#)

Owner User ID < None >

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

Ignore Presentation Indicators (internal calls only)

Logged Into Hunt Group

Remote Device

- a In the **MAC Address** text box, enter the MAC Address of the phone.
- b (Optional) In the **Description** text box, enter a description.
- c From the **Device Pool** list, select the device pool appropriate for your Cisco Unified Communications Manager system video devices.
- d From the **Phone Button Template** list, select **Third-party SIP Device (Advanced)**.
- e (Optional) From the **Calling Search Space** list, select an appropriate calling search space for the phone.
- f From the **Location** list, select an appropriate location for the phone system. This location should contain audio bandwidth, “[Cisco Unified Communications Manager Considerations](#)” on page 11.

4 Scroll to the **Protocol Specific Information** section.

- a** From the **Device Security Profile** list, select the profile created in “[Configure Security Settings](#)” on page 12.
- b** In the **SIP Profile** field, select **Standard SIP Profile**.
- c** In the **Digest User** field, select the user created in “[Add an Spectralink Phone User](#)” on page 22.

5 Click **Save**.

6 In the **Association Information** section, click **Line [1] - Add a new DN**.

7 Complete the following required fields:

- a** In the **Directory Number** field, enter the phone’s extension number.

- b** In the **Route Partition** field, choose the appropriate value.

Directory Number Configuration

Save

Status

Status: Ready

Directory Number Information

Directory Number* 2011

Route Partition Internal

Description Polycom HDX001

Alerting Name Polycom HDX001

ASCII Alerting Name Polycom HDX001

Active

- 8** Click **Save**.

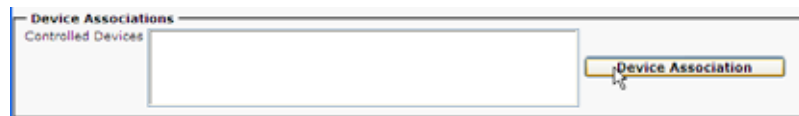
In the status bar near the top of the page, an **Update Successful** message appears.

Task 4: Associate the Phone with the User You Created

You need to associate the phone (device entry) with the user you created.

To associate the phone with a user:

- 1 Select **User Management > End User**.
- 2 Navigate to the user you created (the user name is the phone number).
- 3 In the **Device Associations** area, click **Device Association**.



- 4 Navigate to the directory number you created by selecting Directory Number as a filter and typing the phone extension in the text box.
- 5 In the User Device Association list, mark the check box next to the phone you created.
- 6 Click **Save/Selected Changes**.

Configure Your Spectralink Phone

You need to add a SIP configuration file to the TFTP server that specifies the Cisco Unified Communications Manager is the proxy server for this phone.

For complete instructions, see the Spectralink documentation.

Registering a KIRK Wireless Server

For detailed instructions on registering a KIRK Wireless Server with Cisco Unified Communications Manager, see the *Using Polycom® KIRK® Wireless Server 300 or 600 with Cisco® Unified Communications Manager* available on <http://www.polycom.com>.

Configuring the Polycom RMX System to Route Calls to the Cisco Unified Communications Manager

You can configure your Polycom RMX system to route calls to the Cisco Unified Communications Manager.

Call Routing with the Polycom RMX System

If your deployment does not include a DMA system, you need to configure the RMX system to route calls to the Cisco Unified Communications Manager in order to support outgoing calls to Cisco endpoints.

Call Routing with the Polycom DMA System

If your deployment includes a Polycom DMA system, you can configure the DMA system as a SIP peer to the Cisco Unified Communications Manager to ensure that incoming SIP/TIP calls can be routed to the RMX system. See [“Configuring a DMA SIP Trunk on Cisco Unified Communications Manager”](#) on page 55.

When you use a DMA system, you can also configure the DMA system to route calls to the Cisco Unified Communications Manager.

Task 1: Configuring RMX to statically route outbound SIP calls to the Cisco Unified Communications Manager

- 1 In the **IP Network Services Properties** dialog box, click the **SIP Servers** tab.
- 2 In the **SIP Server** field, select **Specify**.
- 3 In the **SIP Server Type** field, select **Generic**.
- 4 Set **Refresh Registration every 3600 seconds**.
- 5 If not selected by default, change the **Transport Type** to **TCP**.
- 6 In the **SIP Servers** table:
 - a Enter the IP address of the Cisco Unified Communications Manager in both the **Server IP Address or Name** and **Server Domain Name** fields.
 - b The **Port** field must be set to its default value: 5060. The Cisco Unified Communications Manager uses this port number by default.
- 7 In the **Outbound Proxy Servers** table:
 - a Enter the IP address in the **Server IP Address or Name** field. (The same value as entered in Step 6a.)
 - b The **Port** field must be set to its default value: 5060. (By default, the Outbound Proxy Server is the same as the SIP Server.)

- 8 If your RMX system also supports H.323 calls, you need to configure the RMX system's H.323 Service to register with a gatekeeper.

For more information see the *RMX Administrator's Guide*.

- 9 Assign the New Profile to the Meeting Room. For more information see the *RMX Administrator's Guide*, "Creating a New Meeting Room"?

Task 2: Configuring an RMX Ad Hoc Entry Queue or Meeting Rooms (if DMA system is not used)

If your deployment does not include a DMA system, you need to configure an Ad Hoc Entry Queue or meeting rooms on the RMX system. Be sure to use a conference profile that is TIP enabled.

To create an Ad Hoc Entry Queue

- 1 Create or select the **Entry Queue** as described in the *RMX Administrator's Guide*, "Entry Queues".
- 2 In the **New Entry Queue or Entry Queue Properties** dialog box, ensure that **Ad Hoc** is selected.
- 3 Ensure that the **Entry Queue** is designated as the **Transit Entry Queue** as described in the *RMX Administrator's Guide*, "Setting a Transit Entry Queue".

To create a meeting room

For more information see the *RMX Administrator's Guide*, "Creating a New Meeting Room".

Supporting Telepresence Calls with the RMX System

If your deployment requires the RMX to host telepresence calls that include Cisco endpoints, you need to configure your RMX system for TIP.

See "[Configuring the Polycom RMX System to Support TIP Calls](#)" on page 45.

Direct Registration of Polycom Telepresence Systems with the Cisco Unified Communications Manager

When you register your Polycom systems directly with Cisco Unified Communications Manager, you have a single source for call admission control and bandwidth management. You can also take advantage of telephone functions like hold, transfer and so on.

When Polycom telepresence and video endpoints have the TIP option key installed, they can participate in direct, point-to-point calls with Cisco CTS endpoints.

You can also configure your Polycom RMX system to host multipoint conference calls that include Cisco telepresence endpoints.

Polycom telepresence endpoints can also participate in multipoint calls hosted by the Cisco Telepresence Server

Deployment Model Advantages

Within an enterprise with a mixture of telepresence equipment, Polycom HDX and ITP systems are able make and receive calls to and from Cisco CTS endpoints.

Registering Polycom video and telepresence endpoints with the Cisco Unified Communications Manager allows you to easily integrate Polycom telepresence endpoints within a Cisco deployment without additional network management overhead.

Polycom endpoints can also participate in multipoint calls hosted by either an RMX system or a Cisco TelePresence Server.

Supported Products

Polycom supports the following telepresence devices for direct registration with Cisco Unified Communications Manager.

Polycom has tested its most recent product versions with the following Cisco products.

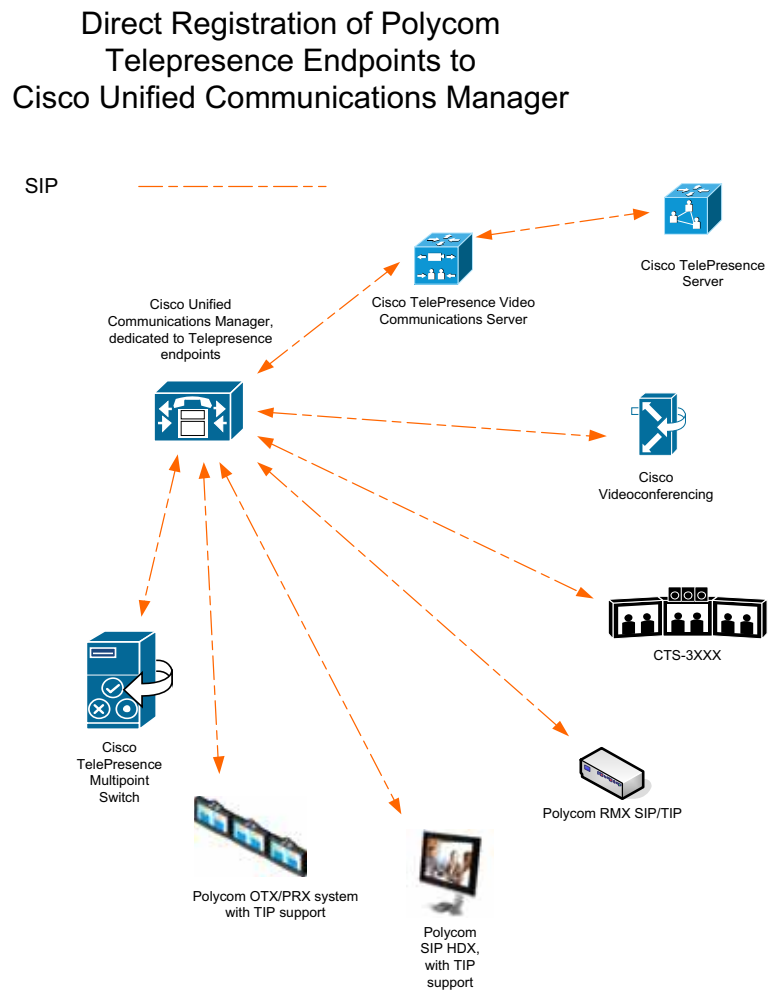
Table 3-1 Matrix for supported current Polycom products with Cisco components.

Cisco	Version(s)
Cisco Unified Communications Manager	8.5
Cisco Unified Videoconferencing	7.2
Cisco TelePresence Server	2.2
Cisco TelePresence Video Communications Server	x6.1
Cisco TelePresence System	1.7
Cisco TelePresence Multipoint Switch	1.7.2
Cisco Unified Border Element	15.1T
Polycom	Version(s)
Polycom RMX systems	v7.6 MPMx card required for TIP support.
The following Polycom Immersive Telepresence Systems: <ul style="list-style-type: none"> • RPX 200 and 400 systems • OTX 300 system • TPX HD 306 system • ATX HD 300 system 	v3.0.4 Requires TIP option key. Requires Polycom Touch Control.
Polycom DMA system	v4.0
Polycom Multipoint Layout Application	v3.0.3
The following Polycom HDX system models: <ul style="list-style-type: none"> • 7000 HD Rev C • 8000 HD Rev B • 9006 • 4500 	v3.0.4 Requires TIP option key.
The following Polycom peripheral: <ul style="list-style-type: none"> • Polycom Touch Control 	1.4.0

Deployment Architecture

Figure 3-1 shows the reference architecture for this deployment model.

Figure 3-1 Architecture when Polycom devices are directly registered to Cisco Unified Communications Manager.



Telepresence Deployment Design Considerations

Before you register any Polycom HDX systems or telepresence systems to the Cisco Unified Communications Manager, consider the following information about interoperability between Cisco Unified Communications Manager and Polycom systems.

- Location settings should allow for video bandwidth when integrating Polycom video endpoints and infrastructure.
- When supporting telepresence systems, region settings should allow for a minimum of 1024k video bandwidth (region settings should match the Polycom HDX system maximum call rate).
- Region settings should allow for an G.722 audio protocol for the best audio experience.
- The Polycom HDX system or Polycom ITP system should be added to a device pool in which the Media Resource Group List does not contain MTP resources.

Note With out-of-band DTMF signalling, Cisco Unified Communications Manager sometimes inserts Media Termination Point Resources (MTP) in a call. This prevents video on the Polycom HDX system from operating correctly on H.323 and SIP trunk calls. You should remove MTP resources from any Media Resource Groups and Media Resource Group Lists that are used in trunked calls.

Polycom Telepresence Systems Considerations

- The TIP option key is required in order to support TIP calls. Polycom telepresence endpoints support TIP version 7.
- If you have a Polycom ITP system, the TIP option key must be installed on each HDX system.
- In order for Polycom ITP endpoints to participate in calls hosted by the Cisco TelePresence Server, you must predefine them on the Cisco TelePresence Server.

Content Sharing in Telepresence Environments

Within a Cisco telepresence environment, Polycom and Cisco endpoints can share content. However the content sharing experience depends on where the Polycom endpoints are registered.

Polycom endpoints can be registered to the Polycom DMA system or the Cisco Unified Communications Manager.

In addition, the following guidelines apply:

- Content sharing within a Polycom/Cisco environment is limited to XGA at 5 fps.
- Content sharing on Polycom ITP or HDX systems is only supported via VGA cable. USB content sharing is not supported.
- Polycom People + Content IP tool is not supported in Cisco telepresence environments.

Polycom Endpoints Registered to the Cisco Unified Communications Manager

The following considerations apply to content sharing when Polycom endpoints are registered to the Cisco Unified Communications Manager.

- In point to point calls with other Polycom endpoints, Polycom endpoints registered to the Cisco Unified Communications Manager can only receive and send content on the video (people) channel.
- In multipoint calls hosted by the Polycom RMX system, Polycom endpoints registered to the Cisco Unified Communications Manager cannot send content to or receive content from a Cisco TelePresence System (CTS).

Device Licensing

Device license units are assigned to each device connected to Cisco Unified Communications Manager. For more information, see your Cisco documentation.

Table 3-2 *Required Device License Units.*

Polycom Device	Required Device License Units
Polycom HDX System	Six(6)
Polycom ITP system Each codec requires device license units when registered to the Cisco Unified Communications Manager.	Six(6) per codec

Registering a Polycom Telepresence or HDX system with a Cisco Unified Communications Manager

When incorporating Polycom telepresence endpoints into your Cisco environment, please note the following:

- The TIP option key is required in order to support TIP calls. Polycom telepresence endpoints support TIP version 7.
- If you have a Polycom ITP system, the TIP option key must be installed on each codec.
- You need to register each codec in the Polycom ITP system with the Cisco Unified Communications Manager.

To register the Polycom HDX system or Polycom ITP system with the Cisco Unified Communication Manager, you need to perform steps in both the Cisco Unified Communications Manager and the Polycom system.

- [“Configuring the Cisco Unified Communications Manager for an HDX or ITP System”](#) on page 35
- [“Define your Polycom ITP Endpoints in the Cisco TelePresence Server”](#) on page 42
- [“Configuring the Polycom Endpoint”](#) on page 44

See the *Polycom Immersive Telepresence (ITP) Administrator's Guide* for detailed documentation on Polycom ITP systems.

Configuring the Cisco Unified Communications Manager for an HDX or ITP System

Use the Cisco Unified Communications web administrator to perform the following tasks:

- [“Create a Security Profile”](#) on page 35
- [“Add a System User”](#) on page 37
- [“Add a Device Entry”](#) on page 40

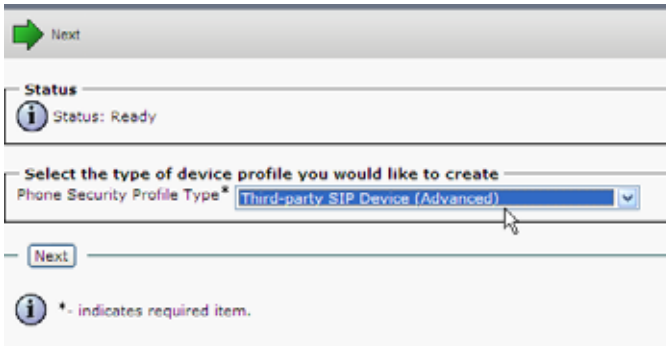
Task 1: Create a Security Profile

You need to create a security profile to use with your Polycom ITP system. Each codec uses the same security profile. You only need to create one security profile.

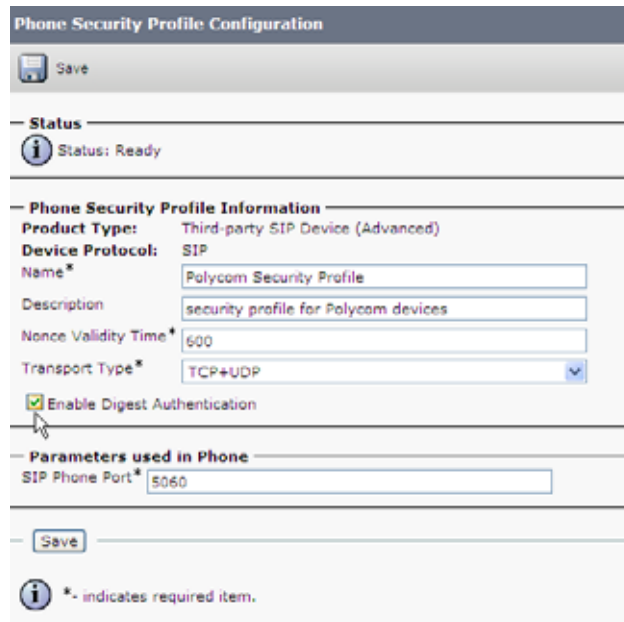
To configure security settings

- 1 Log into the Cisco Unified Communications Manager console.

- 2 Select **System > Security Profile > Phone Security Profile**.
- 3 Select **Add New**.
- 4 Select a Phone Security Profile Type. Select **Third-party SIP Device (Advanced)** and click **Next**.



- 5 On **Phone Security Profile Information** page, complete the following fields:
 - a In the **Name** text box, enter a profile name for the system.
 - b In the **Description** field, enter a description for the security profile.
 - c If you want to use digest authentication (recommended), mark the **Enabled Digest Authentication** check box. When you use digest authentication, a valid login password is required.
 - d Select the default values for all other fields. This example uses digest authentication.



6 Click the **Save** button.

In the status bar near the top of the page, **Update Successful** appears.

Task 2: Add a System User

You need to create a Cisco Unified Communications Manager system user for each codec in your Polycom ITP system. For example, if you are registering a Polycom OTX system that has three codecs, you need to create a unique system user for each codec.

If you cannot add a user here, your system may be LDAP integrated. If that is the case, you can use an existing user ID (essentially associating the endpoint to an existing user) or have your LDAP administrator create a new user ID for each codec.

To add a system user

- 1** Select **User Management > End User**.
- 2** Click **Add New**.

The following screen appears.

The screenshot shows the 'End User Configuration' form. At the top left is a 'Save' button. Below it is a 'Status' section with an information icon and the text 'Status: Ready'. The main section is titled 'User Information' and contains the following fields:

- User ID*: HDX1
- Password: [Redacted]
- Confirm Password: [Redacted]
- PIN: [Empty]
- Confirm PIN: [Empty]
- Last name*: HDX1
- Middle name: [Empty]
- First name: [Empty]
- Telephone Number: [Empty]
- Mail ID: [Empty]
- Manager User ID: [Empty]
- Department: [Empty]
- User Locale: < None >
- Associated PC: [Empty]
- Digest Credentials: [Redacted]
- Confirm Digest Credentials: [Redacted]

- 3** Complete the required fields.
 - a** If you are not using digest authentication, leave the **Digest Credentials** fields blank.

- b** If you are using digest authentication, enter the **Digest Credentials** (password) for the Polycom system.

This is the same password that will be used by the system to access the web interface.

- 4** Click the **Save** button.

In the status bar near the top of the page, **Update Successful** appears.

This is the same password that will be used by the HDX system to access the web interface.

- a** In the **Confirm Digest Credentials** text box, enter the same value that you entered in the previous step.

- 5** Click **Save**.

In the status bar near the top of the page, an **Update Successful** message appears.

After you have saved the new device, the **Association Information** section is displayed.

- 6** In the **Association Information** section, click **Line [1] - Add a new DN**.



- 7 Complete the following required fields. Each unique system user needs a unique directory number.
 - a In the **Directory Number** field, enter the phone's extension number.
 - b In the **Route Partition** field, choose the appropriate value.

The screenshot displays the 'Directory Number Configuration' interface. At the top, there is a 'Save' button. Below it, the 'Status' section shows 'Status: Ready'. The main section is 'Directory Number Information', which contains the following fields:

Directory Number*	2011
Route Partition	Internal
Description	Polycom HDX001
Alerting Name	Polycom HDX001
ASCII Alerting Name	Polycom HDX001

At the bottom of the form, there is a checked checkbox labeled 'Active'.

- 8 Click **Save**.

In the status bar near the top of the page, an **Update Successful** message appears.
- 9 Repeat these steps for each codec in your Polycom ITP system. You need a unique system user (and directory number) for each codec.

Task 3: Add a Device Entry

You need to create a Cisco Unified Communications Manager device entry for each codec in your Polycom ITP system. For example, if you are registering a Polycom OTX system that has three codecs, you need to create a unique device entry for each codec.

To add a device entry

- 1 Select **Device > Phone**.
- 2 Click **Add New**.
- 3 Select **Third-party SIP Device (Advanced)**, then click **Next**.

The following screen appears. The data shown in this section is shown as an example.

The screenshot shows the 'Device Information' configuration page for a 'Third-party SIP Device (Advanced)'. The fields are as follows:

Field	Value	Link
MAC Address *	00E0DB0A1AE8	
Description	SEPO0E0DB0A1AE8	
Device Pool *	DP-Westminster	View Details
Common Device Configuration	< None >	View Details
Phone Button Template *	Third-party SIP Device (Advanced)	
Common Phone Profile *	Standard Common Phone Profile	
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Media Resource Group List	< None >	
Location *	Loc-Westminster	
AAR Group	< None >	
Device Mobility Mode *	Default	View Current Device Mobility Settings
Owner User ID	< None >	
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 >	

Checkboxes at the bottom:

- Use Device Pool Calling Party Transformation CSS
- Retry Video Call as Audio
- Ignore Presentation Indicators (internal calls only)
- Logged Into Hunt Group
- Remote Device

- a In the **MAC Address** text box, enter a unique MAC Address for the HDX system.
This can be any valid, unique MAC address. The Cisco Unified Communications Manager actually uses the HDX user name to identify the HDX system.
- b (Optional) In the **Description** text box, enter a description.
- c From the **Device Pool** list, select the device pool appropriate for your Cisco Unified Communications Manager system video devices.

- d From the **Phone Button Template** list, select **Third-party SIP Device (Advanced)**.
 - e (Optional) From the **Calling Search Space** list, select an appropriate calling search space for the HDX system.
 - f From the **Location** list, select an appropriate location for the HDX system. This location should contain video bandwidth. See [“Location settings should allow for video bandwidth when integrating Polycom video endpoints and infrastructure.”](#) on page 32.
- 4 Scroll to the **Protocol Specific Information** section.

- a From the **Device Security Profile** list, select the profile created in [“Create a Security Profile”](#) on page 35.
 - b In the **Digest User** field, select the user created in [“Add a System User”](#) on page 37.
- 5 Click the **Save** button.

In the status bar near the top of the page, an **Update Successful** message appears.

After you have saved the new device, the **Association Information** section is displayed.

- 6 In the **Association Information** section, click **Line [1] - Add a new DN**.

- 7 Complete the following required fields:
 - a In the **Directory Number** field, enter the phone's extension number.
 - b In the **Route Partition** field, choose the appropriate value.

- 8 Click **Save**.
In the status bar near the top of the page, an **Update Successful** message appears.
- 9 Reset the Polycom system in Cisco Unified Communications Manager.

Define your Polycom ITP Endpoints in the Cisco TelePresence Server

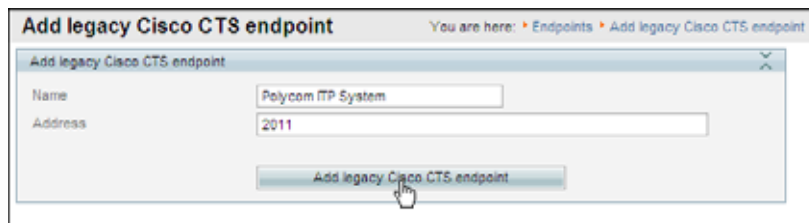
If your Cisco environment includes a Cisco TelePresence Server as well as Polycom ITP endpoints, you need to predefine your Polycom ITP endpoints on the Cisco TelePresence Server in order for them to participate in calls hosted by Cisco TelePresence Server.

You'll need to define the Primary codec of your ITP system as a Legacy CTS endpoint.

To define your Polycom ITP endpoint

- 1 Log onto the Cisco TelePresence Server.
- 2 Select **Endpoints > Add legacy Cisco CTS endpoint**.
- 3 In the **Add legacy Cisco CTS endpoint** dialog box, complete the following fields:
 - a In the **Name** field, enter a name for your Polycom ITP system.

- b** In the **Address** field, enter the Directory Number you created for the Primary codec of your Polycom ITP system.



The screenshot shows a web interface for adding a legacy Cisco CTS endpoint. The title is "Add legacy Cisco CTS endpoint" and the breadcrumb trail is "You are here: Endpoints > Add legacy Cisco CTS endpoint". The form contains two input fields: "Name" with the value "Polycom ITP System" and "Address" with the value "2011". A button labeled "Add legacy Cisco CTS endpoint" is located at the bottom of the form, and a mouse cursor is hovering over it.

- 4** Click **Add legacy Cisco CTS endpoint**.

Configuring the Polycom Endpoint

Complete the following tasks on the Polycom endpoint:

- “Register the Polycom System with the Cisco Unified Communications Manager” on page 44
- “Ensure the TIP Protocol is Enabled” on page 46

Task 1: Register the Polycom System with the Cisco Unified Communications Manager

When an Polycom endpoint is registered with a Cisco Unified Communications Manager, the endpoint can make calls to Cisco endpoints that are also registered to the Cisco Unified Communications Manager.

To register an HDX or ITP system with the Cisco Unified Communications Manager

- 1 Open a browser window and in the **Address** field enter the Polycom HDX system IP address or host name.
- 2 Go to **Admin Settings > Network > IP Network** and select **SIP**.
- 3 Configure the settings in the **SIP Settings** section of the **IP Network** screen. For guidance, see [Table 3-3](#).

<ul style="list-style-type: none"> General Settings Network <ul style="list-style-type: none"> IP Network Call Preference Network Dialing Call Speeds Monitors Cameras Audio Settings Polycom Touch Control LAN Properties Global Services Tools 	<p>IP Network Update</p> <p>Enable SIP: <input checked="" type="checkbox"/></p> <p>SIP Server Configuration: Specify</p> <p>Registrar Server: 10.223.11.4</p> <p>Proxy Server: 10.223.11.4</p> <p>Transport Protocol: TCP</p> <p>Domain Name: </p> <p>User Name: 2011</p> <p>Domain User Name: HDX1</p> <p>Password: <input type="checkbox"/></p> <p>Directory: <input type="checkbox"/></p> <p>Microsoft Lync Server 2010: <input type="checkbox"/></p>
---	--

Table 3-3 SIP Settings fields and their descriptions.

Settings	Description
Enable SIP	Mark this check box to enable the HDX system to receive and make SIP calls.
Registrar Server	Specify the IP address of the Cisco Unified Communications Manager. If you leave this field blank, the Proxy Server is used.
Proxy Server	Specify the IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you leave both fields blank, no Proxy Server is used. By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. The syntax used for this field is the same as for the SIP Registrar Server field.
Transport Protocol	The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required. For Cisco environments, select either Auto or TCP.
Domain Name	For Cisco environments, leave this field blank.
User Name	Specify the system's SIP name. This is the SIP URI. Set this to the directory number you assigned to the HDX system.
Password	When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Registrar Server. If using Digest Authentication, mark the Password check box and set the password to the Digest Credentials password you set for the Cisco Unified Communications user you created for this HDX system.
Directory: Microsoft Lync Server	Specifies whether the SIP Registrar Server is a Lync Server. For Cisco environments, leave this check box unmarked.

4 Click Update.

Task 2: Ensure the TIP Protocol is Enabled

Verify that TIP option key has been installed and that TIP has been enabled by verifying these settings:

- A TIP check box is displayed and enabled on the HDX Call Preferences screen.
- The SIP (TIP) Calls settings appear on the HDX Call Preference screen.

The screenshot displays the 'Call Preference' configuration page. On the left is a navigation menu with 'Call Preference' selected. The main content area is titled 'Call Preference' and includes an 'Update' button. Under the 'Call Preference' heading, there are several settings with checkboxes: 'SIP' (checked), 'TIP' (checked), 'Analog Phone' (unchecked), 'Diagnostic Mode' (unchecked), 'Transcoding' (unchecked), 'ISDN Gateway' (unchecked), and 'IP Gateway' (unchecked). Below this is the 'Preferred Speeds' section, which contains two sub-sections. The first, 'Select the preferred speeds for placing calls', has 'IP Calls' and 'SIP(TIP) Calls' both set to '6144'. The second, 'Select the maximum speeds for receiving calls', also has 'IP Calls' and 'SIP(TIP) Calls' both set to '6144'.

- The 1024 setting is enabled on the HDX Call Speeds screen.

Configuring the Polycom RMX System to Support TIP Calls

If your environment includes a Polycom RMX system, you can configure it to support telepresence calls that include Cisco telepresence endpoints.

Depending on your environment, you can choose to route calls differently. Specifically, if your deployment includes a Polycom DMA system, you do not need to configure your RMX system to route calls to the Cisco Unified Communications Manager.

Configure Call Routing with the Polycom RMX System

If your deployment does not include a DMA system, you need to configure the RMX system to route calls to the Cisco Unified Communications Manager in order to support outgoing calls to Cisco endpoints.

See [“Configuring the Polycom RMX System to Route Calls to the Cisco Unified Communications Manager”](#) on page 27.

Configure Call Routing with the Polycom DMA System

If your deployment includes a Polycom DMA system, you can configure the DMA system as a SIP peer to the Cisco Unified Communications Manager to ensure that incoming SIP/TIP calls can be routed to the RMX system.

When you use a DMA system, you can also configure the DMA system to route calls to the Cisco Unified Communications Manager.

See [“Using a Polycom DMA System in a Cisco Environment”](#) on page 51.

Configuring the RMX System for a Cisco Telepresence Environment

You need to configure your RMX system to support telepresence calls that include Cisco telepresence endpoints.

Perform the following tasks:

- [“Configure the RMX System for Telepresence Conferencing”](#) on page 48
- [“Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag ”](#) on page 48
- [“Configure a TIP Enabled Profile on the RMX system”](#) on page 48
- [“Configure an Ad Hoc Entry Queue on the RMX \(if DMA system is not used\) ”](#) on page 49
- [“Configure a Meeting Room on the RMX”](#) on page 49
- [“Configure Participant Properties for dial out calls ”](#) on page 49
- [“Configure the RMX system for your H.323 gatekeeper”](#) on page 49

Task 1: Configure the RMX System for Telepresence Conferencing

Be sure you have configured your RMX system to support telepresence conferencing.

Please see the *RMX System Administrator's Guide* for detailed instructions on setting up your RMX system for telepresence conferencing.

Task 2: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag

The `MIN_TIP_COMPATIBILITY_LINE_RATE` *System Flag* determines the minimum line rate at which an *Entry Queue* or *Meeting Room* can be *TIP* enabled.

Polycom systems support TIP version 7 which requires a minimum line rate of 1024 kbps and will reject calls at lower line rates, therefore the **System Flag** value must be **1024** or higher.

For more information see the *RMX Administrator's Guide, "System Configuration"*.

Task 3: Configure a TIP Enabled Profile on the RMX system

When you need to support TIP calls, you must ensure that the conference profiles for the RMX Entry Queues and Meeting Rooms are enabled for TIP support. (Different profiles can be assigned to Entry Queues and Meeting Rooms, however they must be TIP enabled.

When you enable TIP, content sharing capabilities are affected for TIP calls. See "[Content Sharing in Telepresence Environments](#)" on page 33.

- 1 Create a New Profile for the Meeting Room. For more information see the *RMX Administrator's Guide, "Defining Profiles"*.
- 2 In the **New Profile - General** tab, set the **Line Rate** to a value of at least that specified for the `MIN_TIP_COMPATIBILITY_LINE_RATE` System Flag.
- 3 Click the **Advanced** tab.
- 4 Select the **TIP Compatibility** mode. The TIP Compatibility mode affects in the user Video and Content experience as described in Table 1-4.
- 5 Click the **Video Quality** tab. The Content Settings check box is disabled if **TIP Compatibility** is set to **Video and Content** in the **Advanced** tab.
- 6 Click the **Video Settings** tab. If the **TIP Compatibility Mode** was set to **Video and Content**, the **Send Content to Legacy Endpoints** is disabled. This setting cannot be changed.
- 7 Set the **Telepresence Mode** to **Auto**.
- 8 Assign the New Profile to the Meeting Room. For more information see the *RMX Administrator's Guide, "Creating a New Meeting Room"*.

Task 4: Configure an Ad Hoc Entry Queue on the RMX (if DMA system is not used)

If your deployment does not include a DMA system, you must configure an Ad Hoc Entry Queue for the RMX system. Be sure to use a conference profile that is TIP enabled.

- 1 Create or select the **Entry Queue** as described in the *RMX Administrator's Guide*, "Entry Queues".
- 2 In the **New Entry Queue or Entry Queue Properties** dialog box, ensure that **Ad Hoc** is selected.
- 3 Ensure that the **Entry Queue** is designated as the **Transit Entry Queue** as described in the *RMX Administrator's Guide*, "Setting a Transit Entry Queue".

Task 5: Configure a Meeting Room on the RMX

For more information see the *RMX Administrator's Guide*, "Creating a New Meeting Room".

Task 6: Configure Participant Properties for dial out calls

You need to configure the **Participant Properties** to ensure that defined participants inherit their TIP settings from the Profile assigned to the Meeting Room.

- 1 Define the **New Participant's General** settings. For more information see the *RMX Administrator's Guide*, "Adding a Participant to the Address Book".
- 2 Click the **Advanced** tab.
- 3 Ensure that:
 - **Video Bit Rate** is set to **Automatic** or at least equal to or greater than the value specified by the `MIN_TIP_COMPATIBILITY_LINE_RATE` System Flag.
 - **Resolution** is set to **Auto** or at least **HD 720**.
 - **Video Protocol** is set to **Auto** or at least **H.264**.

Task 7: Configure the RMX system for your H.323 gatekeeper

If your RMX system also supports H.323 calls, you can to configure the RMX system's H.323 Service to register with a gatekeeper.

For more information see the *RMX Administrator's Guide*.

Operations During Ongoing Conferences

Moving participants between TIP enabled meetings and non TIP enabled meetings is not possible.

Displaying Participants Properties:

- 1** In the **Participant List** pane double-click the participant entry.
The **Participant Properties - General** dialog box opens.
- 2** Click the **SDP** tab. The following are indicated in the Remote Capabilities, Remote Communication Mode and Local Communication Mode panes:
 - AAC_LD
 - Audio Protocol
 - Main Profile
 - Video protocol

Using a Polycom DMA System in a Cisco Environment

You can configure the Polycom DMA system as a SIP peer and registrar for your environment.

When you incorporate a Polycom DMA system within your Cisco environment, you can do the following:

- Use the Polycom DMA system to manage conferences on your Polycom RMX systems.
- Route outgoing calls from the DMA system to the Cisco Unified Communications Manager.
- Route incoming calls from your Cisco Unified Communications Manager to endpoints and systems registered to the DMA system.

See the *Polycom DMA 7000 System Operations Guide* for more information about using the Polycom DMA system.

This chapter includes the following sections:

- [“Supported Products”](#) on page 52
- [“Architecture Diagram”](#) on page 53
- [“Task Overview”](#) on page 55

Supported Products

Polycom has tested its most recent product versions with the following Cisco products.

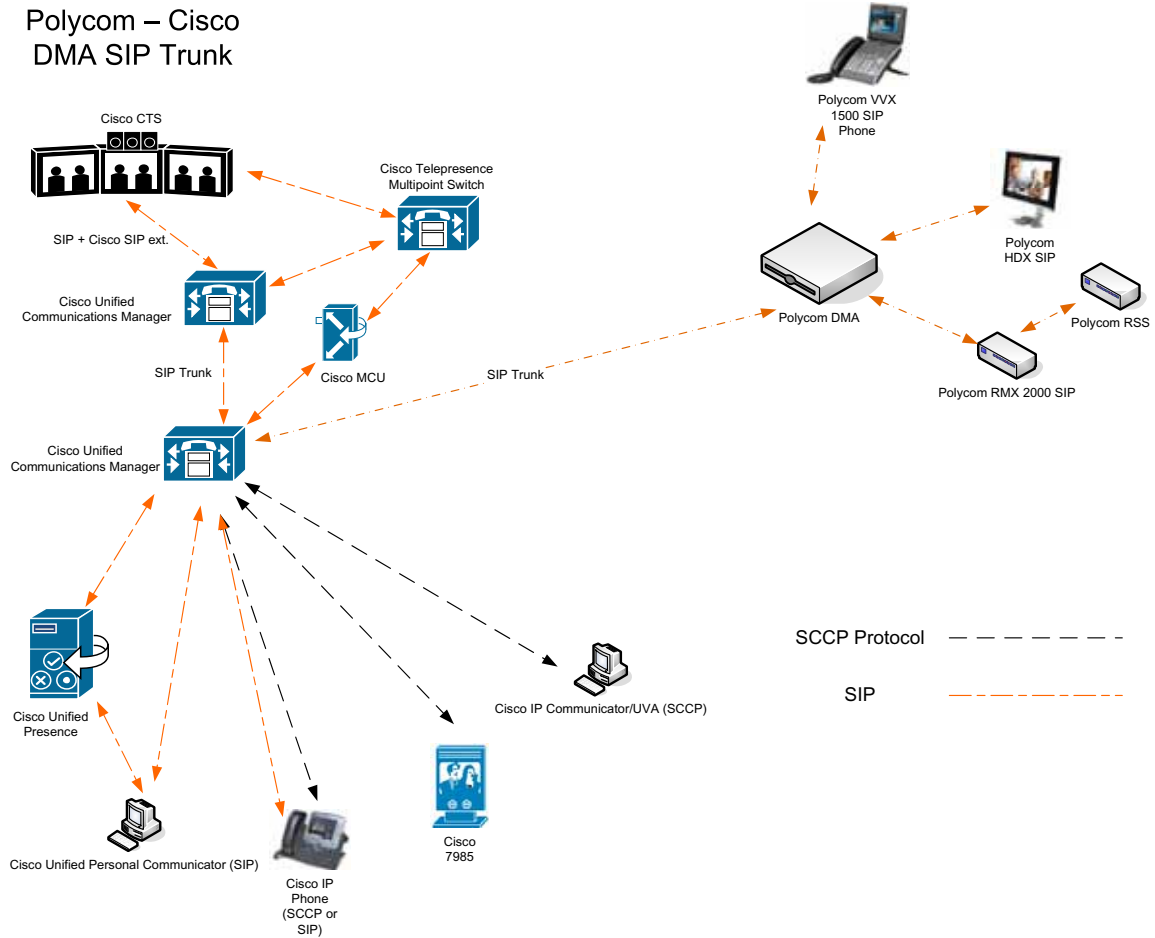
Table 4-1 Matrix for supported current Polycom products with Cisco components.

Cisco	Version(s)
Cisco Unified Communications Manager	8.5
Cisco Unified Videoconferencing 5230	7.x
Cisco TelePresence Multipoint Switch	1.7.2
Cisco IP Communicator	7.x
Cisco Unified Personal Communicator	8.0
Cisco Unified Video Advantage	2.2(x)
Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971	
Polycom	Version(s)
Polycom HDX system(all models)	v3.0.4
Polycom RMX 1500/2000/4000 systems	v7.6 MPMx card required for TIP support.
Polycom CMA system	v6.0
Polycom DMA system	v4.0
Spectralink wireless phones 8020/8030	
KIRK Wireless Server 300/6000/2500/8000	
Polycom RSS system	v6.4

Architecture Diagram

Figure 4-1 shows the reference architecture for this deployment model.

Figure 4-1 Architecture when using the Polycom DMA system as a SIP peer.



Content Sharing with Polycom Endpoints Registered to a DMA System

Table 4-2 lists content sharing scenarios when Polycom endpoints are registered to a Polycom DMA system that has been configured as a SIP peer.

Polycom Endpoints Registered to a Polycom DMA System

The following considerations apply to content sharing when Polycom endpoints are registered to a Polycom DMA system that has been configured as a SIP peer.

Table 4-2 lists content sharing scenarios when Polycom endpoints are registered to a Polycom DMA system that has been configured as a SIP peer.

Table 4-2 Content sharing when Polycom endpoints are registered to a Polycom DMA system that has been configured as a SIP peer.

Call Types	People + Content Sharing (dual-stream channels with one for video and one for content)
Point to Point Calls	
HDX/ITP system to HDX/ITP system	Yes
HDX/ITP system to Cisco CTS	Yes
Cisco CTS to HDX/ITP system	Yes
Multipoint calls on a Polycom RMX	
HDX/ITP system to HDX/ITP system	Yes
HDX/ITP system to Cisco CTS	Yes
Cisco CTS to HDX/ITP system	Yes

Task Overview

The tasks for configuring a SIP trunk connection between the Polycom DMA system and the Cisco Unified Communications Manager include:

- “Configuring a DMA SIP Trunk on Cisco Unified Communications Manager” on page 55
- “Configuring the DMA System for Cisco Unified Communications Manager” on page 60

Configuring a DMA SIP Trunk on Cisco Unified Communications Manager

You need to configure Cisco Unified Communications Manager so that it route calls to the DMA system.

For more information, see the Cisco documentation, http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

Perform the following steps to create a SIP trunk to the DMA system and establish the call routing infrastructure.

- “Add a SIP Trunk on the Cisco Unified Communications Manager” on page 55
- “Configuring route groups, route lists and patterns” on page 56

Task 1: Add a SIP Trunk on the Cisco Unified Communications Manager

When you configure a SIP Trunk for the DMA system, the Cisco Unified Communications Manager can route calls to the DMA system, including any endpoints registered to the DMA system or associated RMX systems.

To add a SIP trunk

- 1 Navigate to **Device > Trunk**.
- 2 Click **Add New** in the upper left.
- 3 For **Trunk Type**, select **SIP Trunk**.
- 4 For **Device Protocol**, the default is **SIP** and cannot be changed.
- 5 For **Trunk Service Type**, select **None (Default)**.
- 6 Then click **Next**.
- 7 Enter a **Device Name** for this trunk, and a description.
- 8 Fill out most fields as appropriate for your system and location.
- 9 For **Call Classification**, select **OnNet**.

10 In the **SIP Information** section, use the IP address for the DMA SIP signalling domain for the **Destination Address**.

11 Click **Save**.

12 Click **Apply Config** to apply your changes.

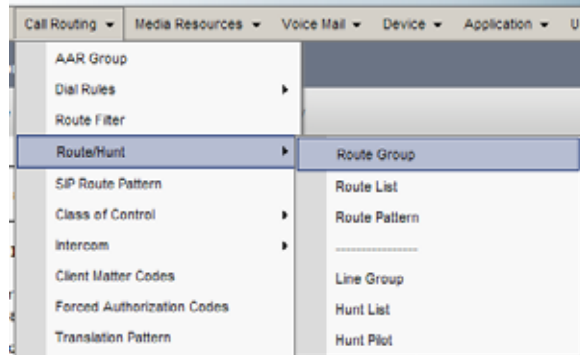
Task 2: Configuring route groups, route lists and patterns

In this task, you create everything the Cisco Unified Communications Manager needs to route calls to the DMA system, as well as receive them. Video calls are an automatic negotiation as part of the call setup.

- A *route group* in Cisco Unified Communications Manager is a collection of gateways and trunks.
- A *route list* is a collection of route groups that Cisco Unified Communications Manager can route calls through.
- The *route pattern* defines what specific dial pattern or patterns may be sent to a route list.

To configure Route groups, Route lists and Patterns:

1 Navigate to **Call Routing > Route/Hunt > Route Group**.



2 Click **Add New**.

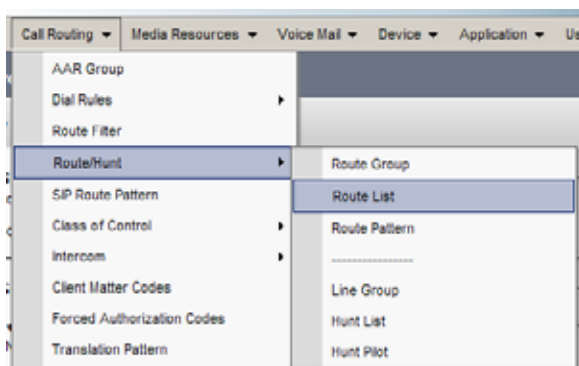
3 Enter a name for the **Route Group**.

4 In the **Find Devices to Add to Route Group** section, select the trunk you created and click **Add to Route Group**.

a Click Add to Route Group.

5 Once the trunk appears in the **Route Group Members** list, click **Save**.

6 Navigate to **Route Plan > Route/Hunt > Route List**.



7 Click **Add**.

8 Type a **Route List Name** and description.

9 Assign the route list to an appropriate **Cisco Unified Communications Manager Group** for your Cisco Unified Communications Manager cluster.

10 Click **Save**.

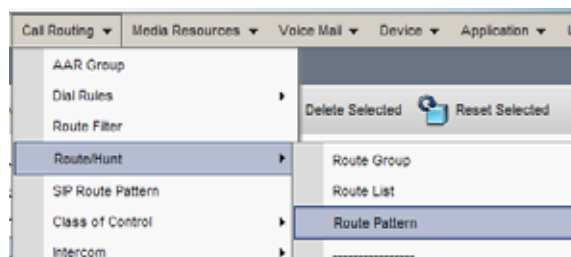
11 Once the route list has been created, click the **Add Route Group** button.

In the **Route List Member Information** section, use the **Route Group** drop-down list to select the route group you created.

12 Click **Save**.

13 After the route group has been inserted, click **Reset**, to make the route list become active.

14 Next go to **Route Plan > Route/Hunt > Route Pattern**.



15 Click **Add New**.

16 Add a route pattern representing a single E.164 extension or range of extensions available on the H.323/CMA network.

- a In the **Route Pattern** field, enter a name for the pattern. This example uses 3XXX.
- b Select the **Route List** you created.
- c Fill in all other pertinent information for your network, such as partition.
- d In the **Call Classification** field, select **OnNet**.

e Once complete, click **Save**.

Pattern Definition

Route Pattern* 3XXX

Route Partition < None >

Description

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Resource Priority Namespace Network Domain < None >

Route Class* Default

Gateway/Route List* DMA-SIP-Trunk-List (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

Note If a route pattern is pointed directly at a trunk, any subsequent route patterns that get added will reset and drop ALL calls on the trunk. The use of route groups and route lists allows calls to stay active while adding route patterns.

Once you complete the above steps, any Cisco endpoint attached to your Cisco Unified Communications Manager should be able to call any DMA system registered extension.

Configuring the DMA System for Cisco Unified Communications Manager

On the DMA system, you need to configure an external SIP peer for the Cisco Unified Communications Manager. This allows the DMA system to route SIP calls to devices registered to the Cisco Unified Communications Manager.

Perform the following tasks:

- [“Configure a SIP Peer for the Cisco Unified Communications Manager”](#) on page 60
- [“Set up a Dial Rule for the Cisco Unified Communications Manager”](#) on page 61
- [“Create a TIP-Enabled Conference Template”](#) on page 62

Task 1: Configure a SIP Peer for the Cisco Unified Communications Manager

To configure the DMA System as a SIP Peer for Cisco Unified Communications Manager calls

- 1 Log into the DMA System.
- 2 Navigate to **Network > External SIP Peer**.
- 3 In the Actions menu, click **Add**.
- 4 Type a name and description for the SIP Peer.
- 5 Ensure that the **Enabled** check box is marked.
- 6 In the **Address** field, type the IP address of the Cisco Unified Communications Manager.
- 7 In the Port field, enter the SIP port to use. The default port is 5060.
- 8 Optionally, in the **Prefix Range** field, enter the prefix associated with the Cisco Unified Communications Manager.

Associating a prefix with your Cisco Unified Communications Manager depends on how you have set up dial plans and rules within your DMA system. See the *Polycom DMA System Operations Guide* for detailed information.

- 9 In the **Type** drop-down list, select **Other**.

10 In the **Transport Type** drop-down list, select either **TCP** or **UDP**.

11 Ensure the **Register Externally** check box is unmarked.

Some external SIP peers (Acme SBC, for example) require peer proxies to register with them. The Microsoft Lync Server does not.

12 Click **OK**.

Task 2: Set up a Dial Rule for the Cisco Unified Communications Manager

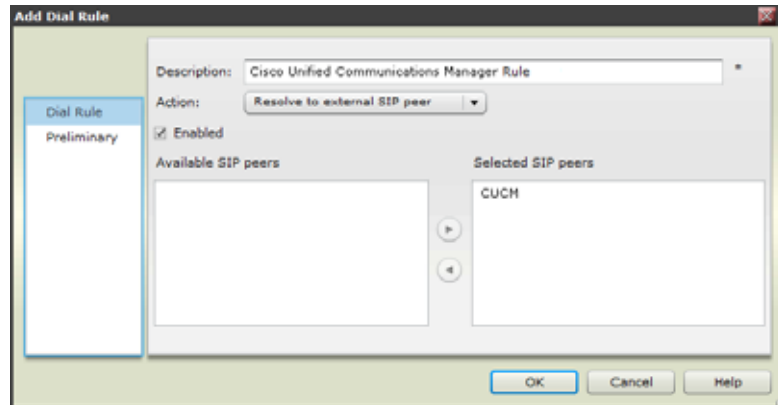
As a best practice, the dial rule you use for the Cisco Unified Communications Manager should be last in your logical list of dial rules.

Please see the DMA system documentation for detailed information about using dial rules.

To set up a dial rule for Cisco Unified Communications Manager calls

- 1** Select **Admin > Call Server > Dial Rules**.
- 2** Click **Add**.
- 3** In the **Add Dial Rule** dialog box, enter a description for your dial rule.
- 4** In the **Action** drop-down menu, select **Resolve to external SIP peer**.
- 5** In the **Available SIP Peers** area, select the SIP peer you created for Cisco Unified Communications Manager and move it to the **Selected Peers** area using the arrow.

Figure 4-2 Add a dial rule that resolves to the external SIP peer you created for Cisco Unified Communications Manager.



- 6 Ensure you mark the **Enabled** check box.
- 7 Click **OK**.

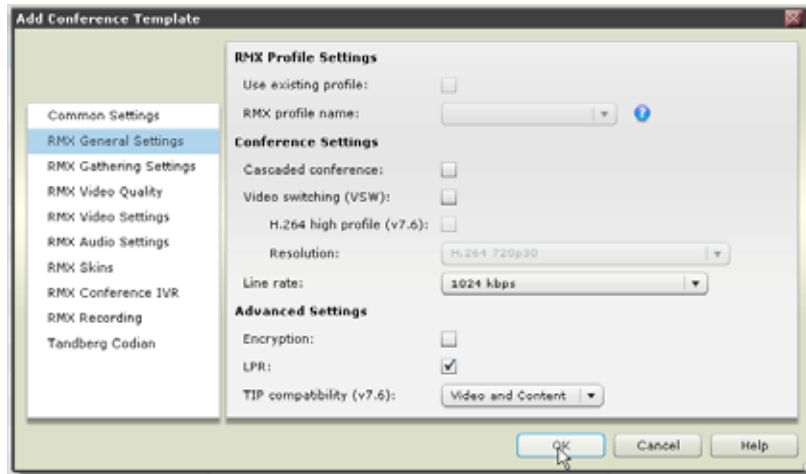
Task 3: Create a TIP-Enabled Conference Template

If you are using the Polycom DMA system to route or host telepresence conferences, you need to create a Conference Profile that is TIP-enabled and supports a minimum of 1024 kbps.

To create a TIP-enabled conference profile

- 1 Log onto your DMA system.
- 2 Select **Admin > Conference Manager > Conference Templates**.
- 3 Click **Add**.
- 4 On the **Common Settings** tab, enter a name and description for your template.
- 5 In the **Add Conference Template** dialog, click **RMX General Settings** to view this tab.
 - a In the **Line rate** field, select a line rate of **1024 kbps** or higher.

- b** In the **TIP compatibility** field, select **Video Only** or **Video and Content**, depending on what you want to support.



- 6** Click **OK**.

Neighbored Cisco IOS and Polycom CMA Gatekeepers

Consider neighboring gatekeepers if you are integrating an existing Cisco environment with an existing Polycom network. Neighbored gatekeepers make it easier to create a common dial plan. With neighbored gatekeepers, you can do number translation and maintain your existing environments.

In this scenario, Polycom devices use the Polycom CMA system as their gatekeeper. The Polycom CMA system will neighbor to the Cisco IOS gatekeeper and allow dialing between Cisco Unified Communications Manager and the CMA H.323 domain.

In order to have a common dial-plan for Cisco Unified Communications Manager and an H.323 network, you need to configure your gatekeeper topology. The gatekeepers can be thought of as the “phone books “ for the H.323 network. Any attempt to dial from any device (Cisco Unified Communications Manager or H.323) to an H.323 based platform will first consult with the gatekeepers on the network to establish proper addressing, bandwidth use and call admission control before attempting the actual call.

Improper gatekeeper configuration (as well as improper network QoS) can lead to poor video quality, and poor audio quality for already established Cisco Unified Communications Manager IP Phone calls, or the inability to complete calls.

Deployment Model Advantages

Neighbored gatekeepers make it easier to create a common dial plan. With neighbored gatekeepers, you can do number translation and maintain your existing environments.

Within this deployment model, you can also directly register Polycom SIP devices directly to Cisco Unified Communications Manager, see [“Direct Registration of Polycom Systems with the Cisco Unified Communications Manager”](#) on page 7.

End User Advantages

For endpoint users, this solution makes it simple to:

- Experience a common dial plan between video devices across the enterprise. This allows users to dial video numbers as they would any phone in the system.
- Experience a common directory when the CMA system is integrated with Active Directory. Users can dial by the names they already know from their corporate directory.

System Administrator Advantages

For system administrators, this solution makes it easier to:

- Provide logistical support for large scale deployment of Polycom HDX systems in a Cisco Unified Communications Manager environment.
- Simplify bandwidth management and call admission control (CAC).
- Use Polycom's SIP expertise to integrate Cisco Unified Communication Manager SIP clients with a Polycom video network and endpoints in a way that requires a minimum of network administration and maintenance.

Supported Products

This section lists the supported products for this deployment model.

Polycom has tested its most recent product versions with the following Cisco products.

Table 5-1 Matrix for supported current Polycom products with Cisco components.

Cisco	Version(s)
Cisco Unified Communications Manager	8.0, 8.5
Cisco Unified Videoconferencing 5230	7.x
Cisco Unified Presence	8.0, 8.5
Unified Contact Center Express	8.0
Cisco IP Communicator	7.x
Cisco Unified Personal Communicator	8.x
Cisco Unified Video Advantage	2.2(x)
Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971	
Polycom	Version(s)
Polycom HDX system (all models)	v3.0.4
Polycom RMX system 1500/2000/4000	v7.6 MPM+ card required for TIP support.
Polycom CMA system	v6.0
Polycom DMA system	v4.0
Spectralink wireless phones 8020/8030	
KIRK Wireless Server 300/6000/2500/8000	
Polycom RSS system	v6.4
Polycom VBP-E	v9.1.5.3

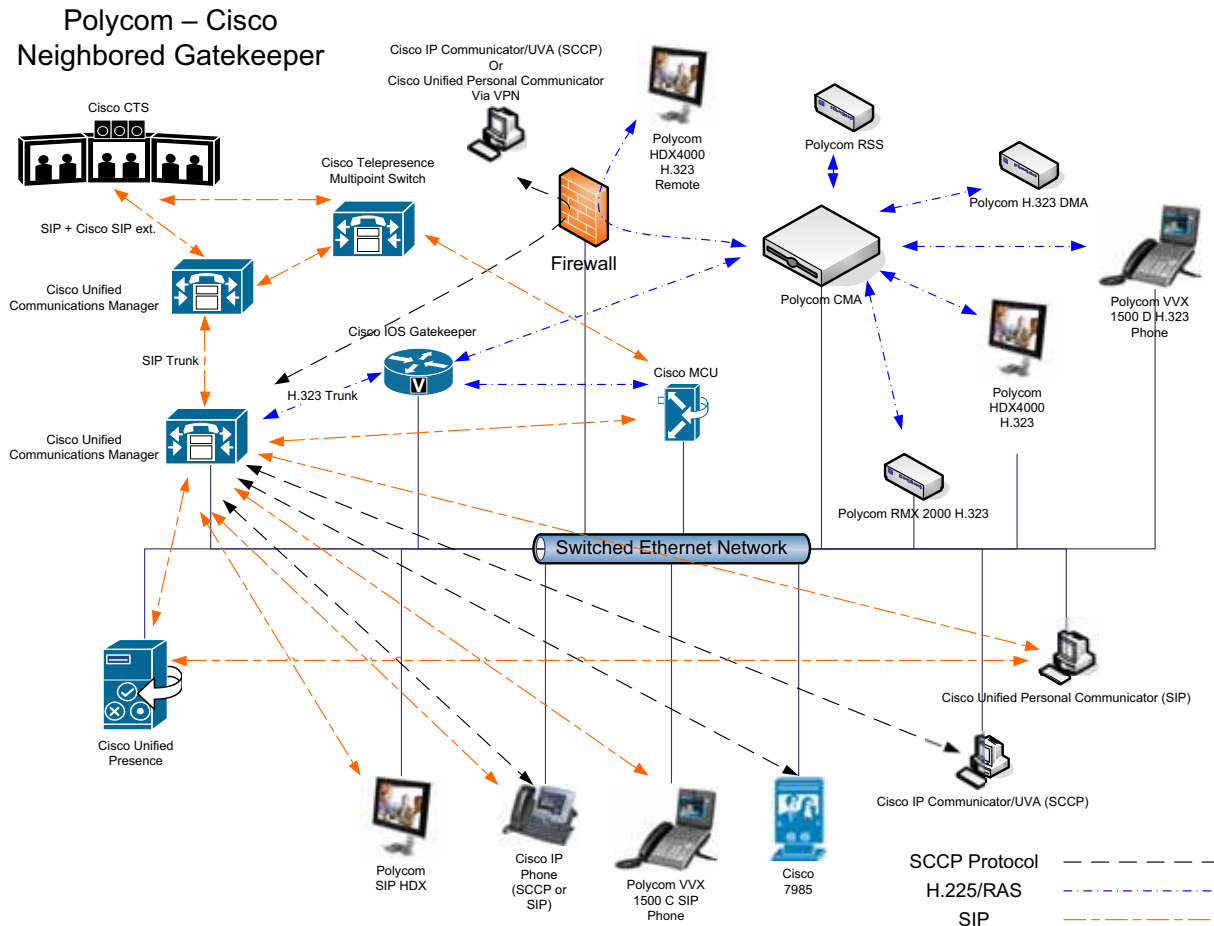
Design Considerations

- You must use an IOS gatekeeper when a Cisco Unified Videoconferencing MCU is present in the environment.
- Gatekeeper load-balancing including the Cisco Gatekeeper Update protocol is beyond the scope of this document. Additionally, complex gatekeeper network design should also be reviewed if deploying into a large enterprise network. For more information, please consult <http://www.cisco.com>.

Architecture Diagram

Figure 5-1 shows a reference architecture for this deployment model.

Figure 5-1 Reference architecture for neighboring gatekeepers.



Task Overview

Use the following steps to configure neighbored gatekeepers:

- “Configure the Cisco IOS Gatekeeper for use with a CMA System” on page 70
- “Configuring CMA for use with Cisco IOS Gatekeeper” on page 75
- “Configuring Cisco Unified Communications Manager for H.323” on page 80

Configure the Cisco IOS Gatekeeper for use with a CMA System

You need to configure the Cisco IOS gatekeeper for two separate zones. Designate one zone for your Cisco Unified Communications Manager cluster and another remote zone that defines how to reach the Polycom CMA.

You also need to configure basic bandwidth settings, including overall session limits.

[Figure 5-2](#) provides a sample configuration with inline comments that describe each set of IOS commands:

Figure 5-2 *Sample Cisco IOS Gatekeeper configuration with comments.*

```

!
! - One network interface (Ethernet or Loopback) must be designated as the source interface.
! - This ensures that all H.323 gatekeeper traffic originates from the same address
! - for each call.
!
interface FastEthernet0/1
 ip address 10.232.253.253 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 10.232.253.253
!
!
! - The command "gatekeeper" puts the router into GK configuration mode
!
gatekeeper
!
! - The first local zone created must contain the IP address of the network interface on the
! - IOS device to which H.323 has been bound. This establishes the address of the gatekeeper.
! - The zone name and domain name are requirements for each zone to help the GK manage
! - endpoint registrations properly. The "enabled-intrazone" is required to allow devices in
! - each zone to call each other. The remote zone must use the IP Address of the CMA as
! - that is the point to which all Polycom devices attach.
!
zone local cucm company.com enable-intrazone
zone remote video company.com 192.168.51.1 1719
!
! - Zone prefixes are required to properly route calls into CUCM as CUCM does not register
! - E.164 prefixes or extensions. Therefore, by adding a zone prefix, we are telling the GK that
! - any Call Admission Request (ARQ) looking for an extension starting with 1, and is x digits
! - long, gets routed to the CUCM zone, and eventually the CUCM itself. A "*" represents a
! - multiple digit wildcard match (i.e. 123456). The use of the "*" is required
! - as the IOS GK uses this to route all cucm zone calls to the registered CUCM cluster.
!
zone prefix cucm 1*
zone prefix video 2*
!
! - The remote and zone session bandwidth should be set (even in small environments)
! - to prevent potential overloading of the CUCM H.323 interface or other network segments.
!
bandwidth remote 5000
bandwidth session zone cucm 5000
!
!

```

Figure 5-3 (Cont.) Sample Cisco IOS Gatekeeper configuration with comments.

```

! - The GW-type-prefix command allows routing into the Call Manager
! - zone. This is a required statement.
!
Gw-type-prefix 1#* default technology
!
! - turn off proxy so calls can go directly to destinations, by default
! - the proxy of calls to mcu and gateway type devices is off.
!
no use-proxy cucm default inbound-to terminal
no use-proxy cucm default outbound-from terminal
!
! - The "no shutdown" is required to turn the gatekeeper on.
!
no shutdown
!

```

Basic Cisco IOS Gatekeeper Monitoring

The Cisco IOS gatekeeper has several commands that help you verify that it is running properly, and has devices registered. For more information about managing your Cisco IOS gatekeeper, see your Cisco documentation.

- show gatekeeper status, see [Figure 5-4](#)
- show gatekeeper endpoints, see [Figure 5-5](#)
- show gatekeeper zone status, see [Figure 5-6](#)
- show gatekeeper zone prefix, see [Figure 5-7](#)

Figure 5-4 The show gatekeeper status command for Cisco IOS gatekeeper.

```

! - This command shows the operational state of all the gatekeeper components on this router,
! - including remote bandwidth.

router#sh gatekeeper status
  Gatekeeper State: UP
  Load Balancing:  DI SABLED
  Flow Control:    DI SABLED
  License Status:  AVAI LABLE
  Zone Name:       cucm
  Accounting:      DI SABLED
  Endpoint Throttling:  DI SABLED
  Security:        DI SABLED
  Maximum Remote Bandwidth:      5000 kbps
  Current Remote Bandwidth:      0 kbps
  Current Remote Bandwidth (w/ Alt GKs): 0 kbps
  Hunt Scheme: Random

```

Figure 5-5 The show gatekeeper endpoints command for the IOS gatekeeper.

! - This command shows what devices are registered to the gatekeeper, their H.323 IDs
! - (if available) and their E.164 IDs as well.

```
router#sh gatekeeper endpoints
                GATEKEEPER ENDPOINT REGISTRATION
                =====
Call Signal Addr  Port  RASignal Addr  Port  Zone Name      Type  Flags
-----
10.232.253.239  53260 10.232.253.239  33234 cucm            VOIP-GW
    H323-ID: Local-IOS-GK_1
    Voice Capacity Max.= Avail.= Current.= 0
Total number of active registrations = 1
```

Figure 5-6 The show gatekeeper zone status command for the IOS gatekeeper.

! - This command lists each zone, the zones status, and all the configured aspects of the zone,
! - including subnets and bandwidth.

```
router#sh gatekeeper zone status
                GATEKEEPER ZONES
                =====
GK name          Domain Name    RAS Address    PORT  FLAGS
-----
cucm             pwnhome.com    10.232.253.253  1719  LS
BANDWIDTH INFORMATION (kbps) :
  Maximum total bandwidth : unlimited
  Current total bandwidth : 0.0
  Maximum interzone bandwidth : unlimited
  Current interzone bandwidth : 0.0
  Maximum session bandwidth : unlimited
SUBNET ATTRIBUTES :
  All Other Subnets : (Enabled)
PROXY USAGE CONFIGURATION :
  Inbound Calls from all other zones :
    to terminals in local zone cucm : do not use proxy
    to gateways in local zone cucm : do not use proxy
    to MCUs in local zone cucm : do not use proxy
  Outbound Calls to all other zones :
    from terminals in local zone cucm : do not use proxy
    from gateways in local zone cucm : do not use proxy
    from MCUs in local zone cucm : do not use proxy
vi deo          pwnhome.com    10.232.253.251  1719  RS
```


Figure 5-7 The show gatekeeper zone prefix command for the IOS gatekeeper.

```
! - This command lists all the known routing prefixes for all the zones.

router#sh gatekeeper zone prefix
      ZONE PREFIX TABLE
      =====
GK-NAME          E164-PREFIX
-----          -
cucm             1*
vi deo          2*
```

"show gatekeeper calls" - shows any active calls in the system including some call statistics.

"show gatekeeper gw-type-prefix" - shows systems for call routing (in this case CUCM)

```
router#show gatekeeper gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=====
Prefix: 1#*      (Default gateway-technology)
Zone cucm master gateway list:
  10.232.253.239:53260 Local-10S-GK_1
```

Configuring CMA for use with Cisco IOS Gatekeeper

You need to configure your Polycom CMA system for use with Cisco Unified Communications Manager. Once completed, calls will work bi-directionally. The steps listed here may be repeated as many times as is necessary to complete your particular dial plan.

Task 1: Add a new site (if applicable)

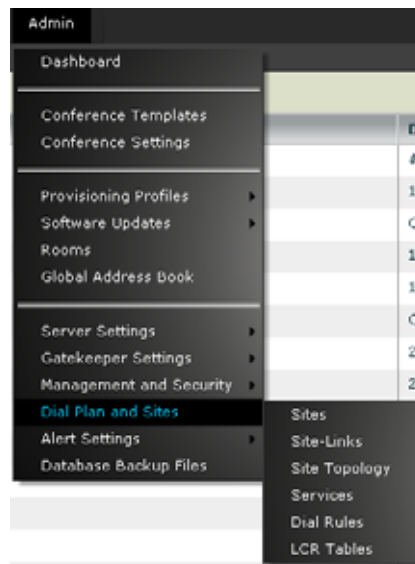
You need to add a new site that represents the Cisco Unified Communications Manager if the Cisco Unified Communications Manager IP addresses are not already part of an existing site.

Sites are a group of devices that usually represent a remote location or central hub. A site contains one or more network subnets, so a device's IP address identifies the site to which it belongs.

Note The addition of a new site, subnet, and site-link is only necessary if the IOS gatekeeper and Cisco Unified Communications System are not in the same subnet as the CMA platform. Subnets may be added to the existing default site.

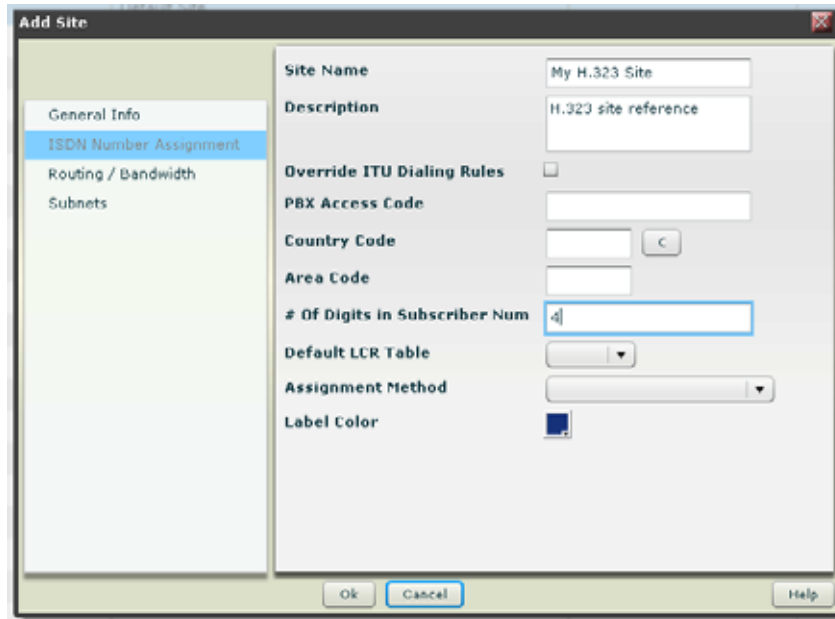
To add a new site:

- 1 Log onto the Polycom CMA system.
- 2 Navigate to **Admin > Dial Plan and Sites > Sites**.



- 3 Click **Sites** on the left navigation bar.

- 4 Enter a site name that represents the Cisco Unified Communications Manager environment, description and the number of digits for the Cisco Unified Communications Manager dial plan (in this example it is four).



- 5 Click **Site Subnet**, then enter the IP address and subnet mask that represent the Cisco IOS Gatekeeper, and the Cisco Unified Communications Manager servers (unless the IP addresses of those devices exist in an already defined site) then click **Add** - once per IP Address/Subnet mask pair.
- 6 When complete, click **OK**.

Task 2: Add a site link

A site link is network connection between two sites or between a site and an MPLS network cloud. Site links tell the Polycom CMA system which sites and subnets can communicate with each other.

To add a site link:

- 1 Click **Site-Links** on the left navigation bar then click **Add**.
- 2 In the **Add Site** dialog,
 - a Give the site-link an appropriate name and description
 - b Select the site you created for the **From Site**
 - c Select the default region for the **To Site** select the default region.
 - d The **Link Type** should be direct.

- e Set the bandwidth values as appropriate for your network.
- f Click **Save** when finished.

You will need to perform this step for each site defined in your Polycom CMA system.

Task 3: Define a Neighboring Gatekeeper

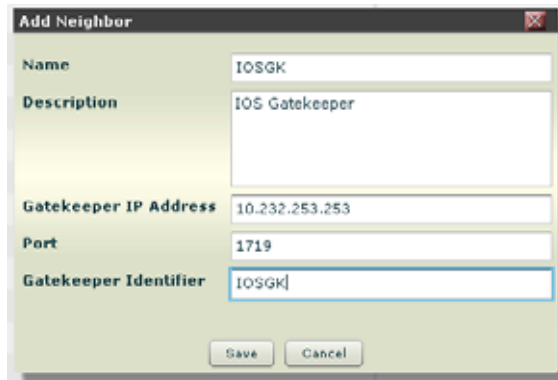
You need to define the Cisco IOS gatekeeper as a neighbored gatekeeper for the Polycom CMA system.

Neighboring gatekeepers are gatekeepers that manage other H.323 regions within an enterprise. When a call originates within one gatekeeper region but that region's gatekeeper is unable to resolve the dialed address, it is forwarded to the neighbored gatekeepers for resolution.

To define a neighboring gatekeeper:

- 1 Navigate to **Admin > Gatekeeper Settings > Neighboring Gatekeepers**.

2 Click Add.



Name	IOSGK
Description	IOS Gatekeeper
Gatekeeper IP Address	10.232.253.253
Port	1719
Gatekeeper Identifier	IOSGK

- a** Enter a name and description for the gatekeeper.
- b** The **Gatekeeper IP Address** to be entered should be the IP Address of the Cisco IOS gatekeeper created in [“Configure the Cisco IOS Gatekeeper for use with a CMA System”](#) on page 70.
- c** **Port** should be 1719.
- d** For the identifier enter a short, meaningful name.

3 Click Save.

Task 4: Add a Dial Rule

Within the Polycom CMA system, you need to configure dial rules that will route calls with designated prefixes to designated neighboring gatekeepers, such as the Cisco IOS gatekeeper.

To add a dial rule:

- 1** Navigate to **Admin > Dial Plan and Sites > Dial Rules**.

- 2 Click **Add** to add a dial rule. Enter a name and description for the dial rule. Check the **Enabled** box. Set the pattern type to **Prefix** or **Prefix Range** and select the site you created in “[Add a site link](#)” on page 76. **All** will also work.

The screenshot shows the 'Add Dialing Rule' dialog box with the 'General Information' tab selected. The fields are filled as follows:

- Name: CUCM Dialing
- Description: Dialing to extensions on CUCM
- Priority: 0
- Enabled:
- Pattern Type: Prefix
- Applicable Site: All

Buttons at the bottom: Ok, Cancel, Help.

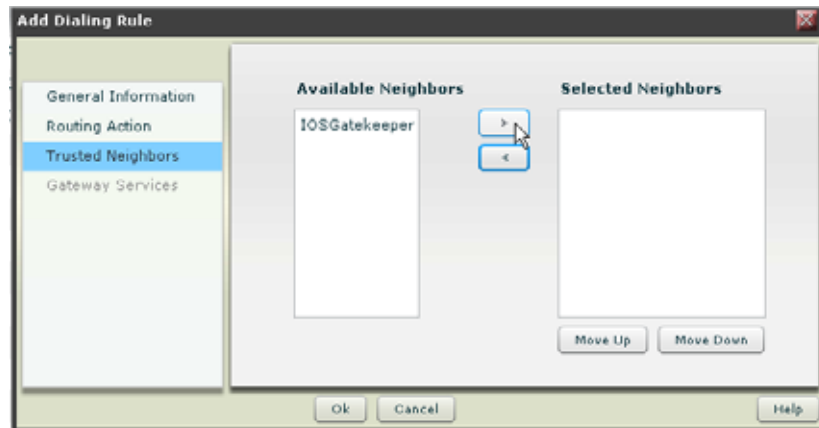
- 3 Click **Routing Action** to view the Routing Action panel.
 - a In the **IP Address Pattern Data** field, type the prefix for call routing (if **Prefix Range** was selected in the prior step).
 - b In the **Start Value** and **End Value** fields, enter the prefix range.
 - c Set the **Action** field to **Route to a trusted neighbor**.

The screenshot shows the 'Add Dialing Rule' dialog box with the 'Routing Action' tab selected. The fields are filled as follows:

- IP Address Pattern Data: [Empty]
- Start Value: [Empty] End Value: [Empty]
- # Characters to Remove: 0
- Prefix to Add: [Empty]
- Action: Route to a trusted neighbor

Buttons at the bottom: Ok, Cancel, Help.

4 Click **Trusted Neighbors** on the left side of the screen.



- a** Select the gatekeeper you created in “[Define a Neighboring Gatekeeper](#)” on page 77.
- b** Click the > to move it to the **Selected Neighbors** pane.

5 Click **OK**.

This completes the setup of the Polycom CMA system.

Note When you add devices to the Polycom CMA system, it can take up to five minutes for added devices to function and work with call routing between neighboring gatekeepers.

Configuring Cisco Unified Communications Manager for H.323

You need to configure Cisco Unified Communications Manager so that it can send and receive calls from the H.323 network.

You need to define a gatekeeper, create an H.323 trunk and establish the call routing infrastructure.

Note This section assumes you are familiar with several critical Cisco Unified Communications Manager concepts such as Calling Search Space, Location, and Device pool. Be sure that in your environment, you know the proper settings for these fields as they will determine how your devices (in particular the UVA devices) connect to the H.323 network.

For more information, see the Cisco documentation, http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

Task 1: Define a gatekeeper

You need to define a gatekeeper for Cisco Unified Communications Manager in order to integrate with H.323 endpoints.

These steps assume you are using Cisco Unified Communications Manager 6. Other versions of Cisco Unified Communications Manager require roughly the same steps.

To define a gatekeeper:

- 1 Navigate to **Device > Gatekeeper**.
- 2 Click **Add New**.
- 3 Enter the IP Address of the gatekeeper that this Cisco Unified Communications Manager needs to use and its description then click **Save**.
- 4 Once entered, click **Reset Gatekeeper**, then **Reset**.

Task 2: Create a trunk

You need to add an H.225 trunk.

To add a trunk:

- 1 Navigate to **Device > Trunk**.
- 2 Click **Add New** in the upper left.
- 3 Select **H.225 Trunk (Gatekeeper Controlled)**. Then click **Next**.
- 4 Enter a **Device Name** for this trunk, and a description.
Fill out all other fields as appropriate for your system and location.

Note Do not check the **Media Termination Point Required** check box.

- 5 In the **Gatekeeper Information** area, select the gatekeeper created earlier.
- 6 Select **Gateway** for the **Terminal Type**.
- 7 Fill in the appropriate **Technology Prefix** (for example, 1#).
- 8 Fill in the appropriate **Zone** name.

Note Zone names are case-sensitive.

- 9 Once all the fields are filled in correctly, click **Save**.
- 10 After saving, click **Reset**, then **Reset** to force the Cisco Unified Communications Manager to register to the gatekeeper.

To verify that your Cisco Unified Communications Manager is registered to the gatekeeper, check to see that your Cisco Unified Communications Manager is an active endpoint on the gatekeeper. See [“Basic Cisco IOS Gatekeeper Monitoring”](#) on page 72 for more information.

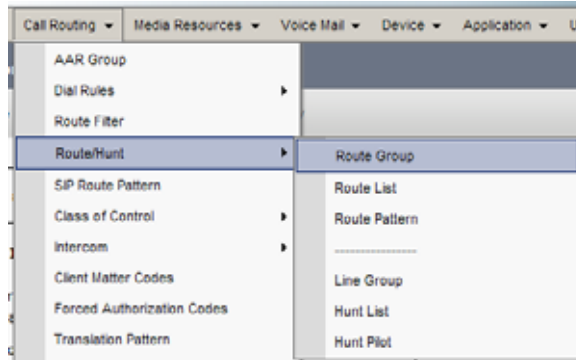
Task 3: Configuring Route groups, Route lists and Route Patterns

In this task, you create everything the Cisco Unified Communications Manager needs to route calls to the H.323 network, as well as receive them. Video calls are an automatic negotiation as part of the call setup.

- A *route group* in Cisco Unified Communications Manager is a collection of gateways and trunks.
- A *route list* is a collection of route groups that Cisco Unified Communications Manager can route calls through.
- The *route pattern* defines what specific dial pattern or patterns may be sent to a route list.

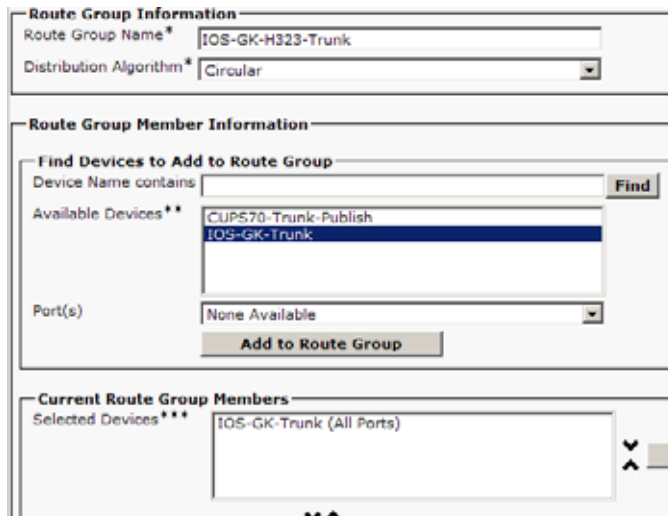
To configure Route Groups, Route lists and Patterns:

1 Navigate to **Call Routing > Route/Hunt > Route Group**.



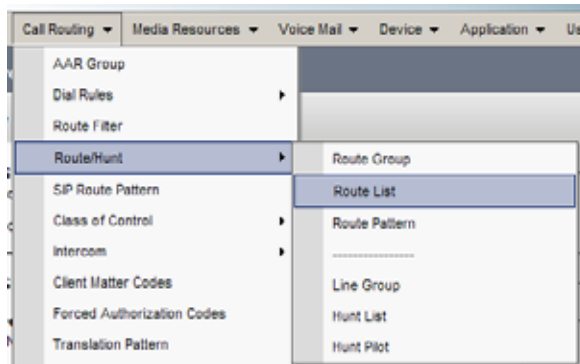
2 Click **Add New**.

- a** Type in a name for the **Route Group**.
- b** Select the trunk you created.
- c** Click **Add to Route Group**.



3 Once the trunk appears in the **Route Group Members** list, click **Save**.

4 Navigate to **Call Routing > Route/Hunt > Route List**.



5 Click **Add New**.

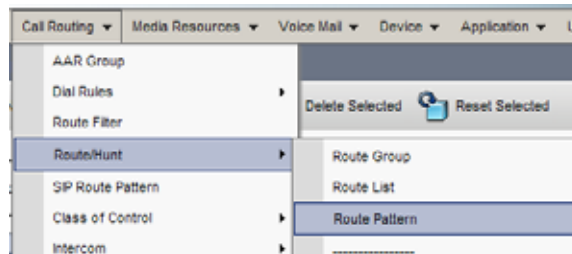
- a** Type a **Name** and description.
- b** Assign the route list to an appropriate **Cisco Unified Communications Manager Group** for your Cisco Unified Communications Manager cluster.

A screenshot of the 'Route List Information' form in the Cisco Unified Communications Manager web interface. The form has three input fields: 'Name*' with the value 'H323-Route-List', 'Description' with the value 'H323 Call Routing', and 'Cisco Unified Communications Manager Group*' with a dropdown menu showing 'Default'. A 'Save' button is located at the bottom left of the form.

6 Click **Save**.

- 7 Once the route list has been created, click the **Add Route Group** button.
In the **Route List Member Information** section, use the **Route Group** drop-down list to select the route group you created.

- 8 Click **Save**.
- 9 After the route group has been inserted, click **Reset**, to make the route list become active.
- 10 Next go to **Call Routing > Route/Hunt > Route Pattern**.



- 11 Click **Add New**.
- 12 Add a route pattern representing a single E.164 extension or range of extensions available on the H.323/CMA network.
 - a In the **Route Pattern** field, enter a name for the pattern. This example uses 2XXX.
 - b Select the **Gateway/Route List** you created.
 - c Fill in all other pertinent information for your network, such as partition.

d Once complete, click **Save**.

Pattern Definition

Route Pattern*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence*

Resource Priority Namespace Network Domain

Gateway/Route List* [\(Edit\)](#)

Route Option
 Route this pattern
 Block this pattern

Call Classification*

Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority

Require Forced Authorization Code

Authorization Level*

Require Client Matter Code

13 Repeat this step for each prefix range in the H.323 network.

Note If a route pattern is pointed directly at a trunk, any subsequent route patterns that get added will reset and drop ALL calls on the trunk. The use of route groups and route lists allows calls to stay active while adding route patterns.

Once you complete the above steps, any Cisco IP phone attached to your Cisco Unified Communications Manager should be able to call any gatekeeper registered extension.

Using a Polycom CMA System as a Gatekeeper

You can use the Polycom CMA system as the only gatekeeper for the network. When you register your components with Polycom CMA system, bandwidth and call admission control is split between the CMA system and Cisco Unified Communications Manager. Polycom CMA system fully manages your Polycom components and you can take advantage of CMA provisioning with dynamic management.

Within this deployment model, you can also directly register Polycom SIP devices to the Cisco Unified Communications Manager, see [“Direct Registration of Polycom Systems with the Cisco Unified Communications Manager”](#) on page 7.

Deployment Model Advantages

- Supports Polycom RSS systems and remote H.323 access with the Polycom VBP.
- Administrators can easily manage Polycom endpoints with provisioning capabilities and dynamic management of endpoints.

Supported Products

This section lists the supported products for this deployment model.

Polycom has tested its most recent product versions with the following Cisco products.

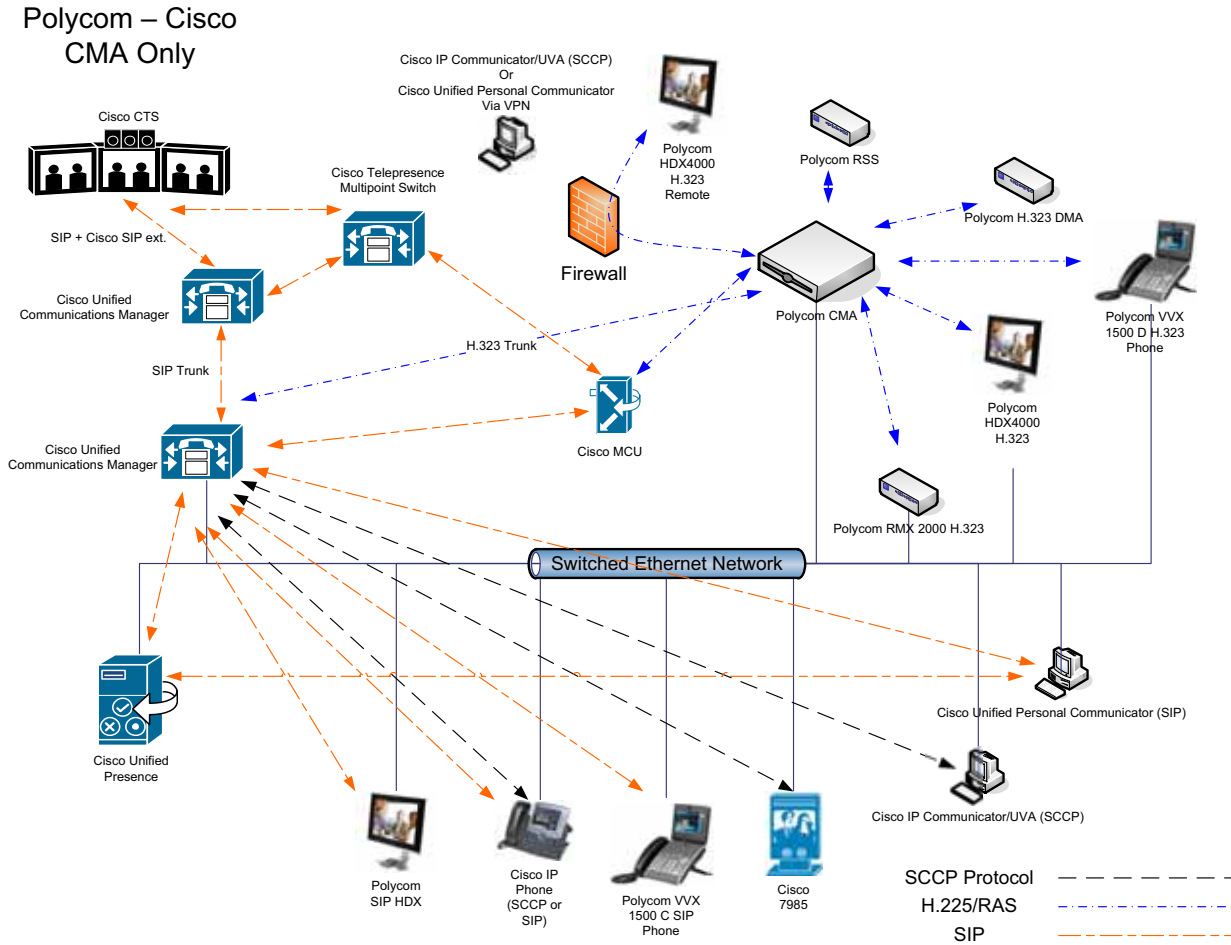
Table 6-1 Matrix for supported current Polycom products with Cisco components.

Cisco	Version(s)
Cisco Unified Communications Manager	8.0, 8.5
Cisco Unified Videoconferencing 5230	7.x
Cisco IP Communicator	7.x
Cisco Unified Personal Communicator	8.0, 8.5
Cisco Unified Video Advantage	2.2(x)
Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971	
Polycom	Version(s)
Polycom HDX system(all models)	v3.0.4
Polycom RMX system 1500/2000/4000	v7.6 MPMx card required for TIP support.
Polycom CMA system	v6.0
Polycom DMA system	v4.0
Spectralink wireless phones 8020/8030	
KIRK Wireless Server 300/6000/2500/8000	
Polycom RSS system	v7.0
Polycom VBP-E	v9.1.5.3

Architecture Diagram

Figure 6-1 shows the reference architecture for this deployment model.

Figure 6-1 Architecture when using a Polycom CMA system as the only gatekeeper.



Task Overview

The tasks for configuring a standalone Polycom CMA gatekeeper include:

- “[Configuring Cisco Unified Communications Manager for H.323](#)” on page 90
- “[Configuring CMA for Cisco Unified Communications Manager](#)” on page 95

Configuring Cisco Unified Communications Manager for H.323

You need to configure Cisco Unified Communications Manager so that it can send to and receive calls from the H.323 network.

You need to define a gatekeeper, create an H.323 trunk and establish the call routing infrastructure.

Note This section assumes you are familiar with several critical Cisco Unified Communications Manager concepts such as Calling Search Space, Location, and Device pool. Be sure that in your environment, you know the proper settings for these fields as they will determine how your devices (in particular the UVA devices) connect to the H.323 network.

For more information, see the Cisco documentation, http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

Task 1: Define a gatekeeper

You need to define a gatekeeper for Cisco Unified Communications Manager in order to integrate with H.323 endpoints.

These steps assume you are using Cisco Unified Communications Manager 8.x. Most versions of Cisco Unified Communications Manager require roughly the same steps.

To define a gatekeeper:

- 1 Navigate to **Device > Gatekeeper**.
- 2 Click **Add New**.
- 3 Enter the IP Address of the gatekeeper that this Cisco Unified Communications Manager needs to use and its description then click **Save**.
- 4 Once entered, click **Reset Gatekeeper**, then **Reset**.

Task 2: Create a trunk

You need to add an H.225 trunk.

To add a trunk:

- 1 Navigate to **Device > Trunk**.
- 2 Click **Add New** in the upper left.
- 3 Select **H.225 Trunk (Gatekeeper Controlled)**. Then click **Next**.
- 4 Enter a **Device Name** for this trunk, and a description.
Fill out all other fields as appropriate for your system and location.

Note Do not check the **Media Termination Point Required** check box.

- 5 In the **Gatekeeper Information** area, select the gatekeeper created earlier.
- 6 Select **Gateway** for the **Terminal Type**.
- 7 Fill in the appropriate **Technology Prefix** (for example, 1#).
- 8 Fill in the appropriate **Zone** name.

Note Zone names are case-sensitive.

- 9 Once all the fields are filled in correctly, click **Save**.
- 10 After saving, click **Reset**, then **Reset** to force the Cisco Unified Communications Manager to register to the gatekeeper.

To verify that your Cisco Unified Communications Manager is registered to the gatekeeper, check to see that your Cisco Unified Communications Manager is an active endpoint on the gatekeeper. See [“Basic Cisco IOS Gatekeeper Monitoring”](#) on page 72 for more information.

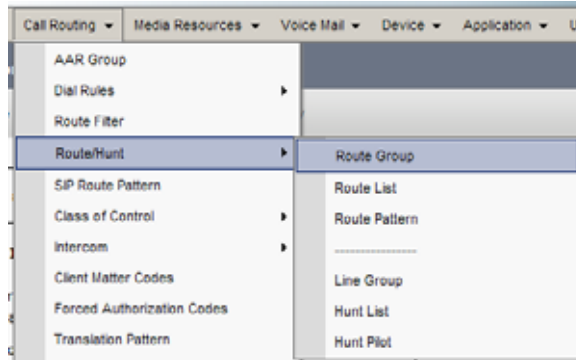
Task 3: Configuring route groups, route lists and patterns

In this task, you create everything the Cisco Unified Communications Manager needs to route calls to the H.323 network, as well as receive them. Video calls are an automatic negotiation as part of the call setup.

- A *route group* in Cisco Unified Communications Manager is a collection of gateways and trunks.
- A *route list* is a collection of route groups that Cisco Unified Communications Manager can route calls through.
- The *route pattern* defines what specific dial pattern or patterns may be sent to a route list.

To configure route groups, route lists and patterns:

- 1 Navigate to **Call Routing > Route/Hunt > Route Group**.

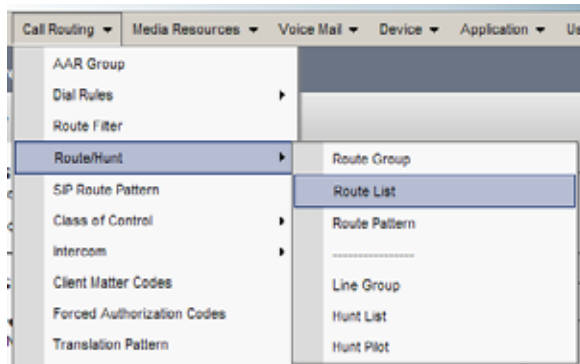


- 2 Click **Add New**.
 - a Type in a name for the **Route Group**.
 - b Select the trunk you created.
 - c Click **Add to Route Group**.

A screenshot of the 'Route Group Information' configuration form. The form is divided into three sections: 'Route Group Information', 'Route Group Member Information', and 'Current Route Group Members'. In the 'Route Group Information' section, the 'Route Group Name' field contains 'IOS-GK-H323-Trunk' and the 'Distribution Algorithm' is set to 'Circular'. The 'Route Group Member Information' section includes a 'Find Devices to Add to Route Group' area with a 'Device Name contains' search box and a 'Find' button. Below this is a list of 'Available Devices' with 'IOS-GK-Trunk' selected. A 'Part(s)' dropdown is set to 'None Available'. An 'Add to Route Group' button is located below the available devices list. The 'Current Route Group Members' section shows a list of 'Selected Devices' containing 'IOS-GK-Trunk (All Ports)'. Navigation arrows are visible at the bottom of the list.

- 3 Once the trunk appears in the **Route Group Members** list, click **Save**.

4 Navigate to **Call Routing > Route/Hunt > Route List**.



5 Click **Add New**.

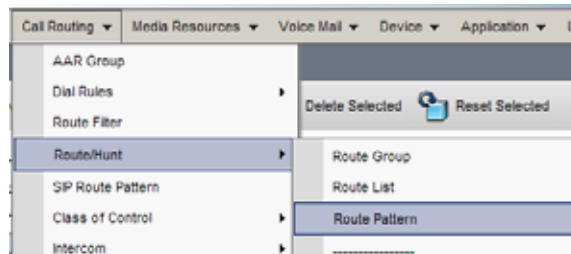
- a Type a **Name** and description.
- b Assign the route list to an appropriate **Cisco Unified Communications Manager Group** for your Cisco Unified Communications Manager cluster.

A screenshot of the 'Route List Information' form in the Cisco Unified Communications Manager administration console. The form has three input fields: 'Name*' with the value 'H323-Route-List', 'Description' with the value 'H323 Call Routing', and 'Cisco Unified Communications Manager Group*' with a dropdown menu showing 'Default'. A 'Save' button is located at the bottom left of the form.

6 Click **Save**.

- 7 Once the route list has been created, click the **Add Route Group** button.
In the **Route List Member Information** section, use the **Route Group** drop-down list to select the route group you created.

- 8 Click **Save**.
- 9 After the route group has been inserted, click **Reset**, to make the route list become active.
- 10 Next go to **Call Routing > Route/Hunt > Route Pattern**.



- 11 Click **Add New**.
- 12 Add a route pattern representing a single E.164 extension or range of extensions available on the H.323/CMA network.
 - a In the **Route Pattern** field, enter a name for the pattern. This example uses 2XXX.
 - b Select the **Gateway/Route List** you created.
 - c Fill in all other pertinent information for your network, such as partition.

d Once complete, click **Save**.

13 Repeat this step for each prefix range in the H.323 network.

Note If a route pattern is pointed directly at a trunk, any subsequent route patterns that get added will reset and drop ALL calls on the trunk. The use of route groups and route lists allows calls to stay active while adding route patterns.

Once you complete the above steps, any Cisco IP phone attached to your Cisco Unified Communications Manager is able to call any gatekeeper registered extension.

Configuring CMA for Cisco Unified Communications Manager

The Polycom CMA system must be configured with routing information similar to that found in Cisco Unified Communications Manager. This allows calls from the H.323 network to reach devices inside Cisco Unified Communications Manager.

To configure CMA for Cisco Unified Communications Manager calls:

- 1** Log into the CMA system.
- 2** Navigate to **Network Device > Monitor View**.
- 3** Verify that your Cisco Unified Communications Manager is in the device list. If it does not appear, reset the trunk in Cisco Unified Communications Manager.
- 4** Navigate to **Admin > Dial Plan and Sites > Dial Rules**.
- 5** Click **Add** to add a dial rule.

- a** Type a name and description for the dial rule.
 - b** Check the **Enabled** box.
 - c** Set the **Prefix Type** to **Prefix** or **Prefix Range**.
- 6** Click **Routing Action** on the left side of the screen.
 - a** In the **Start Value** and **End Value** fields, enter the prefix range.
 - b** In the **Action** field, select **Route to a GW Service**.
- 7** Select **Gateway Services** on the left-hand side. For example, **1#** and then click the **>**.

Use the gateway prefix you defined in Cisco Unified Communications Manager.
- 8** Click **OK**.

Repeat these steps for each prefix range that needs to be routed to Cisco Unified Communications Manager.

Once these steps have been completed calls will successfully route between Cisco Unified Communications Manager and the CMA system.

Using a Standalone Cisco IOS Gatekeeper

You can use the Cisco IOS Gatekeeper as the only gatekeeper for your deployment if you do not need the management capabilities of the Polycom CMA system.

In this deployment, the Cisco Unified Video Conferencing MCU is supported along with Polycom H.323 devices.

Within this deployment model, you can also directly register Polycom SIP devices directly to Cisco Unified Communications Manager, see [“Direct Registration of Polycom Systems with the Cisco Unified Communications Manager”](#) on page 7.

Supported Products

This section lists the supported products for this deployment model.

Polycom has tested its most recent product versions with the following Cisco products.

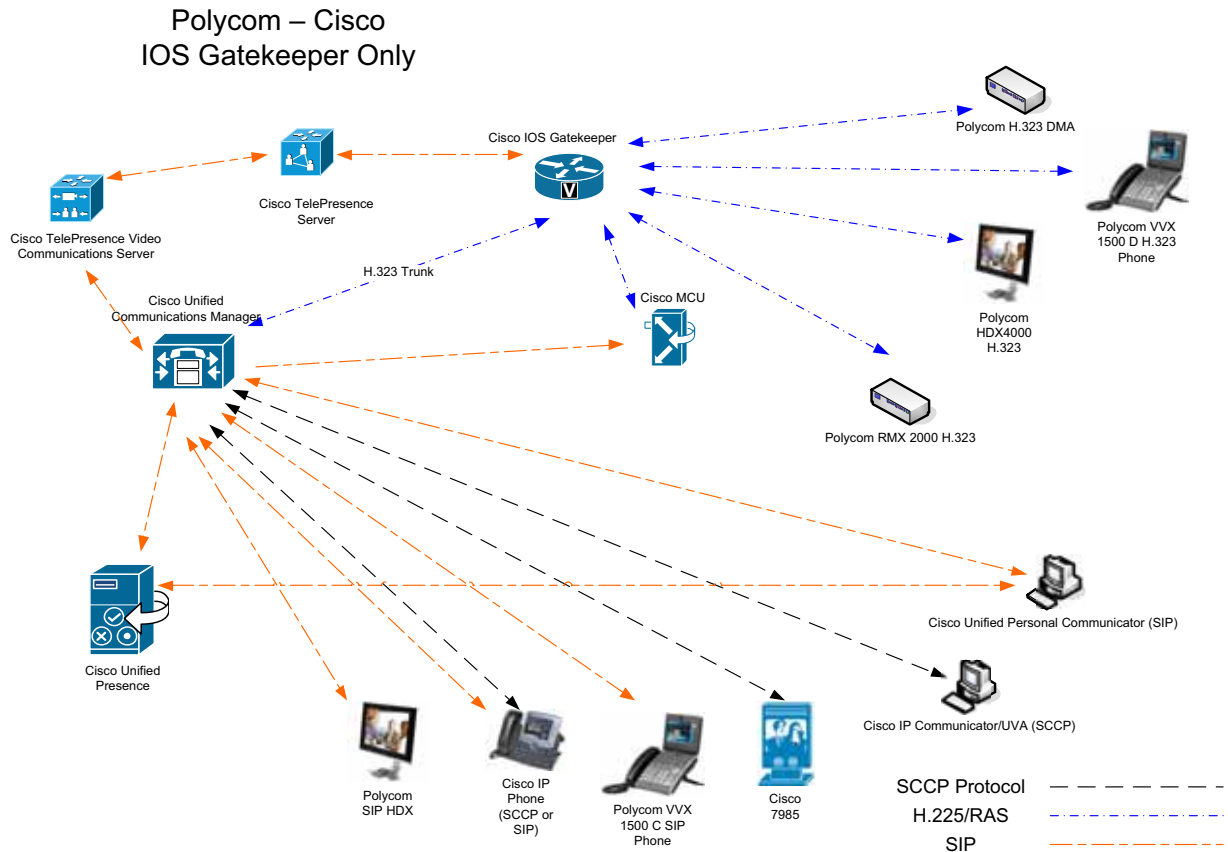
Table 7-1 Matrix for supported current Polycom products with Cisco components.

Cisco	Version(s)
Cisco Unified Communications Manager	8.0, 8.5
Cisco Unified Videoconferencing 5230	7.x
Cisco IOS Gatekeeper	15.x
Cisco TelePresence Server	2.2
Cisco TelePresence Video Communications Server	x6.1
Cisco IP Communicator	7.x
Cisco Unified Personal Communicator	8.0, 8.5
Cisco Unified Video Advantage	2.2(2)
Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971	
Polycom	Version(s)
Polycom HDX system (all models)	v3.0.4
Polycom RMX system 1500/2000/4000	v7.6 MPMx card required for TIP support.
Polycom CMA system	v6.0
Polycom DMA system	v4.0
Spectralink wireless phones 8020/8030	
KIRK Wireless Server 300/6000/2500/8000	
Polycom RSS system	v7.0
Polycom VBP-E	v9.1.5.3

Architecture Diagram

Figure 7-1 shows a reference architecture for this deployment.

Figure 7-1 Architecture when Using a Cisco IOS Gatekeeper only.



Design Considerations

- Polycom DMA and Polycom RMX systems must be configured as gatekeepers when registering to the Cisco gatekeeper.
- Polycom VSX and Polycom HDX system endpoints are configured as they would be normally.

Task Overview

In order to support this deployment model, you must complete the following tasks:

- [“Configuring the Cisco IOS Gatekeeper”](#) on page 100
- [“Configuring Cisco Unified Communications Manager for H.323”](#) on page 103
- [“Integrating Polycom H.323 Endpoints with an IOS Gatekeeper”](#) on page 108

Configuring the Cisco IOS Gatekeeper

When you use the Cisco IOS gatekeeper as a standalone gatekeeper, you need to set up several zones as well as some gateway type prefixes to allow dialing to the DMA and RMX systems.

[Figure 7-2](#) shows a sample configuration. Adjust prefixes according to the your dial plan.

Figure 7-2 Example configuration for standalone IOS gatekeeper.

```

!
! - One network interface (Ethernet or Loopback) must be designated as the source interface.
! - This ensures that all H.323 gatekeeper traffic originates from the same address for each call.
!
interface FastEthernet0/1
 ip address 10.232.253.253 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 10.232.253.253
!
!
! - The command "gatekeeper" puts the router into GK configuration mode
!
gatekeeper
!
! - The first local zone created must contain the IP address of the network interface on the
! - IOS device to which H.323 has been bound. This establishes the address of the gatekeeper.
! - The zone name and domain name are requirements for each zone to help the GK manage
! - endpoint registrations properly. The "enabled-intrazone" is required to allow devices
! - in each zone to call each other. The zone use for Polycom devices must be listed
! - first as Polycom devices do not understand zone names.
!
zone local video company.com enable-intrazone
zone local cucm company.com
!
! - Zone prefixes are required to properly route calls into CUCM as CUCM does not register
! - E.164 prefixes or extensions. Therefore, by adding a zone prefix, we are telling the GK that
! - any Call Admission Request (ARQ) looking for an extension starting with 1, and is x digits
! - long, gets routed to the CUCM zone, and eventually the CUCM itself. A "*" represents a
! - multiple digit wildcard match (i.e. 123456). The use of the "*" is required as the IOS GK
! - uses this to route all cucm zone calls to the registered CUCM cluster.
!
zone prefix cucm 1*

```

```
!  
! - It is recommended to set the remote and zone session bandwidth (even in small environments)  
! - to prevent potential overloading of the CUCM H.323 interface or other network segments.  
!  
!  
!  
bandwidth remote 5000  
bandwidth session zone cucm 5000  
!  
! - The GW-type-prefix command allows routing into the CallManager zone.  
! - This is a required statement. A gw-type-prefix statement is required for every DMA and RMX  
! - registering to the IOS GK. The prefix MUST match the dialing prefixes in the DMA or RMX  
! - In the example shown below, the DMA uses a prefix of 53 and the RMX uses a prefix of 196.  
!  
Gw-type-prefix 1#* default-technology  
Gw-type-prefix 53*  
Gw-type-prefix 196*  
!  
!  
! - turn off proxy so calls can go directly to destinations, by default  
! - the proxy of calls to mcu and gateway type devices is off  
!  
no use-proxy cucm default inbound-to terminal  
no use-proxy cucm default outbound-from terminal  
no use-proxy video default inbound-to terminal  
no use-proxy video default outbound-from terminal  
!  
! - the RRQ statement below allows the RMX and DMA to properly register  
!  
rrq dynamic-prefixes-accept  
!  
! - The "no shutdown" is required to turn the gatekeeper on.  
no shutdown
```

Configuring Cisco Unified Communications Manager for H.323

You need to configure Cisco Unified Communications Manager so that it can send to and receive calls from the H.323 network.

You need to define a gatekeeper, create an H.323 trunk and establish the call routing infrastructure.

Note This section assumes you are familiar with several critical Cisco Unified Communications Manager concepts such as Calling Search Space, Location, and Device pool. Be sure that in your environment, you know the proper settings for these fields as they will determine how your devices (in particular the UVA devices) connect to the H.323 network.

For more information, see the Cisco documentation, http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

Task 1: Define a gatekeeper

You need to define a gatekeeper for Cisco Unified Communications Manager in order to integrate with H.323 endpoints.

These steps assume you are using Cisco Unified Communications Manager 8.x. Most versions of Cisco Unified Communications Manager require roughly the same steps.

To define a gatekeeper:

- 1 Navigate to **Device > Gatekeeper**.
- 2 Click **Add New**.
- 3 Enter the IP Address of the gatekeeper that this Cisco Unified Communications Manager needs to use and its description then click **Save**.
- 4 Once entered, click **Reset Gatekeeper**, then **Reset**.

Task 2: Create a trunk

You need to add an H.225 trunk.

To add a trunk:

- 1 Navigate to **Device > Trunk**.
- 2 Click **Add** in the upper left.
- 3 Select **H.225 Trunk (Gatekeeper Controlled)**. Then click **Next**.
- 4 Enter a **Device Name** for this trunk, and a description.
Fill out all other fields as appropriate for your system and location.

Note Do not check the **Media Termination Point Required** check box.

- 5 At the bottom of the page, select the gatekeeper created in step 3.
- 6 Fill in the appropriate Zone name.
- 7 Add **Select Gateway** for the terminal type.
- 8 Once all the fields are filled in correctly, click **Save**.

Note Zone names are case-sensitive.

- 9 Click **Reset**, then **Reset** to force the Cisco Unified Communications Manager to register to the gatekeeper.

To verify that your Cisco Unified Communications Manager is registered to the gatekeeper, check to see that your Cisco Unified Communications Manager is an active endpoint on the gatekeeper, see [“Basic Cisco IOS Gatekeeper Monitoring”](#) on page 72 for more information.

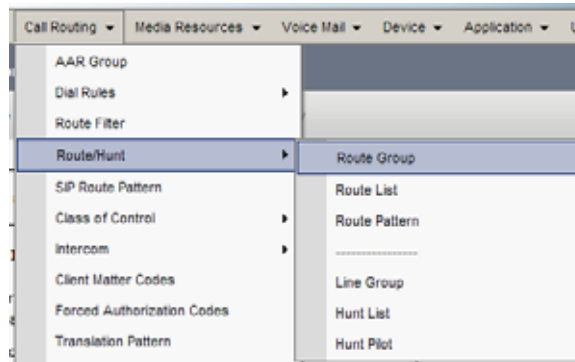
Task 3: Configuring route groups, route lists and patterns

In this task, you create everything the Cisco Unified Communications Manager needs to route calls out to the H.323 network, as well as receive them. Video calls are an automatic negotiation as part of the call-setup.

- A *route group* in Cisco Unified Communications Manager is a collection of gateways servicing a common system, such as ISDN or H.323.
- A *route list* is a collection of route groups that Cisco Unified Communications Manager can route calls through.
- The *route pattern* defines what specific dial pattern or patterns may be routed with a route list.

To configure route groups, route lists and patterns:

- 1** Navigate to **Call Routing > Route/Hunt > Route Group**.



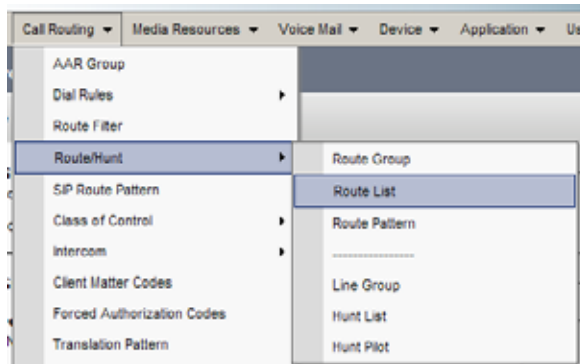
- 2** Click **Add New**.
 - a** Type in a name for the **Route Group**.
 - b** Select the trunk you created.
 - c** Click **Add to Route Group**.

 A screenshot of the 'Route Group Information' configuration page. The page is divided into three main sections:

- Route Group Information:** Contains a text field for 'Route Group Name*' with the value 'IOS-GK-H323-Trunk' and a dropdown menu for 'Distribution Algorithm*' set to 'Circular'.
- Route Group Member Information:** Contains a 'Find Devices to Add to Route Group' section with a 'Device Name contains' search box and a 'Find' button. Below this is a list of 'Available Devices**' with 'IOS-GK-Trunk' selected. A 'Part(s)' dropdown is set to 'None Available', and an 'Add to Route Group' button is present.
- Current Route Group Members:** Contains a 'Selected Devices***' list with 'IOS-GK-Trunk (All Ports)' listed.

- 3** Once the trunk appears in the **Route Group Members** list, click **Save**.

4 Navigate to **Call Routing > Route/Hunt > Route List**.



5 Click **Add New**.

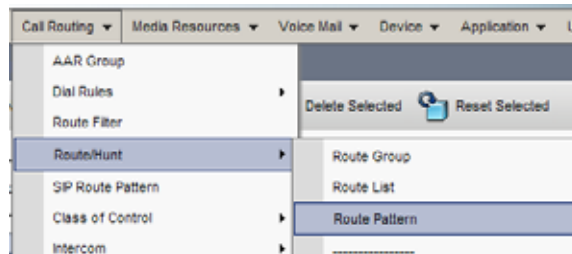
- a** Type a **Name** and description.
- b** Assign the route list to an appropriate **Cisco Unified Communications Manager Group** for your Cisco Unified Communications Manager cluster.

A screenshot of the 'Route List Information' form in the Cisco Unified Communications Manager web interface. The form contains three input fields: 'Name*' with the value 'H323-Route-List', 'Description' with the value 'H323 Call Routing', and 'Cisco Unified Communications Manager Group*' with a dropdown menu set to 'Default'. A 'Save' button is located at the bottom left of the form.

6 Click **Save**.

- 7 Once the route list has been created, click the **Add Route Group** button. In the **Route List Member Information** section, use the **Route Group** drop-down list to select the route group you created.

- 8 Click **Save**.
- 9 After the route group has been inserted, click **Reset**, to make the route list become active.
- 10 Next go to **Call Routing > Route/Hunt > Route Pattern**.



- 11 Click **Add New**.
- 12 Add a route pattern representing a single E.164 extension or range of extensions available on the H.323/CMA network.
- In the **Route Pattern** field, enter a name for the pattern. This example uses 2XXX.
 - Select the **Gateway/Route List** you created.
 - Fill in all other pertinent information for your network, such as partition.

d Once complete, click **Save**.

Pattern Definition

Route Pattern*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence*

Resource Priority Namespace Network Domain

Gateway/Route List* [\(Edit\)](#)

Route Option
 Route this pattern
 Block this pattern

Call Classification*

Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority

Require Forced Authorization Code

Authorization Level*

Require Client Matter Code

13 Repeat this step for each prefix range in the H.323 network.

Note If a route pattern is pointed directly at a trunk, any subsequent route patterns that get added will reset and drop ALL calls on the trunk. The use of route groups and route lists allows calls to stay active while adding route patterns.

Once you complete the above steps, any Cisco IP phone attached to your Cisco Unified Communications Manager should be able to call any gatekeeper registered extension.

Integrating Polycom H.323 Endpoints with an IOS Gatekeeper

You need to ensure your Polycom HDX endpoints are configured for H.323 and for your Cisco IOS gatekeeper.

To configure using the HDX system onscreen setup:

- 1** Navigate to **System**.
- 2** Navigate to **Admin settings**.
- 3** Navigate to **Network**.
- 4** Navigate to **IP**.
- 5** Navigate to **H.323**.
- 6** Navigate to page 2
- 7** Change the **Gatekeeper** setting to **Specify**.
- 8** Enter a valid E.164 for your dial-plan in the **H.323 Extension (E.164)** field.

- 9 Enter the IP Address of the gatekeeper.
- 10 Exit the screen.

To configure using the HDX system web interface:

- 1 Browse to the IP address of the Polycom HDX system.
- 2 Click **Admin settings**.
- 3 Click **Network**.
- 4 Click **IP Network**.
Enter a valid E.164 for your dial-plan in the **H.323 Extension (E.164)** field.
- 5 Change the **Use Gatekeeper** setting to **Specify**.
- 6 Enter the IP address of the gatekeeper in the **Gatekeeper IP Address** field.
- 7 Click **Update** at the top of the page.

Once the gatekeeper address has been set, the unit will attempt to register to the gatekeeper. You can verify successful registration with the `show gatekeeper endpoints` command on the IOS Gatekeeper, see [“Basic Cisco IOS Gatekeeper Monitoring”](#) on page 72. You should see your endpoint registered with its E.164 ID, and an H.323 ID.

