



Administering Avaya Aura[®] Video Quick Setup

**Release 6.3.6
16-300310
Issue 1
June 2014**

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Open Source Attribution

The Product utilizes open source and third-party software. For copyright notifications and license text of third-party open source components, please see the file named Avaya/Gateway/LegalNotices.txt in the directory in which you have installed the software.

Trademarks

Avaya and Avaya Aura® are registered trademarks or trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

Contents

Chapter 1: Introduction	8
Purpose	8
Intended audience.....	8
Related resources.....	8
Documentation	8
Training	8
Avaya Mentor videos.....	9
Product compatibility	9
Support.....	9
Warranty	9
Send us your comments	9
Chapter 2: Overview	10
Avaya Aura® Conferencing without external gatekeepers or MCUs.....	10
Avaya Aura® and Scopia 8.3 interoperability	11
Avaya Aura® and Scopia 8.3 interoperability with third-party endpoints.....	13
Avaya Aura® with the external Polycom MCU and H.323-based endpoints.....	14
Avaya Aura® with the external Polycom MCU and SIP-based endpoints.....	14
Avaya Aura® and Polycom interoperability	15
Prerequisites.....	16
Chapter 3: Administering Communication Manager for video endpoints	18
Enabling video on Communication Manager through SMGR	18
1. Enabling Multimedia IP SIP Trunking feature.	18
2. Enabling video for the SIP signaling group.	18
3. Identifying the IP-codec-set.....	18
4. Adding video to IP-codec-set.	19
Enabling video on Communication Manager through SAT.....	19
Administering SIP-based video endpoints on System Manager.....	20
Creating a custom template for Avaya SIP video endpoints using System Manager	20
Adding users to Avaya SIP video endpoints using System Manager	21
Chapter 4: Administering SIP-based video endpoints.....	22
Administering Avaya one-X® Communicator	22
Administering Scopia XT series endpoints	22
Chapter 5: Administering Communication Manager for interoperability with the H.323- based Scopia ECS Gatekeeper	24
Logging in to System Manager.....	24
Adding a node name for Scopia ECS Gatekeeper	24
Adding an H.323 signaling group for Scopia ECS Gatekeeper	24
Adding an H.323 trunk group for Scopia ECS Gatekeeper.....	25

Adding the H.323 trunk group for channel selection to the signaling group of Scopia ECS Gatekeeper	25
Adding a route pattern for Scopia ECS Gatekeeper	26
Creating and editing dial plans for Scopia ECS Gatekeeper	26
Creating a uniform dial plan for Scopia ECS Gatekeeper	26
Creating an alternate route for the uniform dial plan of Scopia ECS Gatekeeper	27
Chapter 6: Administering Session Manager for interoperability with the SIP-based Scopia B2BUA component.....	28
Logging in to System Manager	28
Adding a SIP entity for the Scopia B2BUA component.....	28
Adding a SIP entity link/SIP trunk for the Scopia B2BUA component.....	28
Adding routing policies for the Scopia B2BUA component	28
Adding dial patterns for the Scopia B2BUA component.....	29
Chapter 7: Administering Scopia Management for interoperability with Avaya Aura®	30
Logging in to Scopia Management.....	30
Adding an H.323 trunk from Scopia ECS Gatekeeper to Communication Manager	30
Adding an H.323 trunk in Scopia iView Management Suite	30
Adding an H.323 trunk in Scopia Management	30
Adding a SIP trunk from the Scopia B2BUA component to Session Manager	31
Adding a SIP trunk in Scopia iView Management Suite	31
Adding a SIP trunk in Scopia Management	31
Changing the default SIP domain on Scopia Management	31
Chapter 8: Administering third-party components	33
Registering Polycom HDX endpoints on Communications Manager or Session Manager.	33
Prerequisites.....	33
Procedure	33
Registering Polycom VVX1500 as a SIP-based endpoint on Avaya Aura®	34
Prerequisites.....	34
Procedure	34
Administering Communication Manager for H.323-based Polycom HDX series video endpoints	35
Prerequisites.....	35
Procedure	35
Administering the Polycom RMX video conferencing bridge	35
Administering Adhoc video conferencing for the Polycom video conferencing bridge	36
Displaying capacity of Communication Manager for Adhoc video conferencing	37
Administering an H.323 trunk between Communication Manager and Polycom DMA	37
Adding Communication Manager as an external gatekeeper	37
Administering the call settings for Communication Manager	38
Administering a direct routing gatekeeper	38
Prerequisites.....	38
Adding an entry for the direct routing gatekeeper in the IP Node Names screen.....	38
Adding signaling groups to the direct routing gatekeeper	39

Adding trunk groups to the direct routing gatekeeper	39
Modifying signaling groups to the direct routing gatekeeper.....	39
Creating a route pattern for the direct routing gatekeeper	39
Adding an H.323 video signaling group	40
Modifying the inbound trunk group to the direct routing gatekeeper	40
Appendix A Interoperability recommendations.....	42
Session Manager routing	42
Communication Manager routing	42
Avaya Aura® endpoints and Radvision endpoints routing	42
Scopia Elite MCU routing	42
Appendix B Advanced administration.....	43
Stripping the prefix of the dialed number for an H.323 call to Communication Manager	43
Partition routing	43
Appendix C Troubleshooting	45

Chapter 1: Introduction

Purpose

This quick setup document provides information about the basic administration tasks required to set up SIP-based and H.323-based video endpoints along with information about the administration tasks required to administer interoperability between:

- Avaya Aura® and Scopia 8.3
- Avaya Aura® and Polycom

Intended audience

This document is intended for system administrators who install video equipment for Avaya Aura®, Scopia 8.3, and Polycom.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Administration		
Administering Avaya Aura® Video Quick Setup – Advanced Topics Release 6.1	Describes the basic administration tasks required to set up SIP-based and H.323-based video endpoints.	System Administrators, Sales Engineers, Solution Architects, Support Personnel
Administering Avaya Aura® Conferencing and Scopia 8.3 Interoperability guide	Describes the interoperability features of Avaya Aura® and Scopia 8.3.	System Administrators, Sales Engineers, Solution Architects, Support Personnel
Scopia Management Administrator Guide Version 8.2 for Solution 8.2	Describes configuring the dial plan on Scopia Management Release 8.2.	System Administrators, Sales Engineers, Solution Architects, Support Personnel
Avaya Video Telephony Solution Release 5.2 Networking Guide	Enables Avaya Communication Manager 5.2 to merge a set of enterprise features with videoconferencing adjuncts.	System Administrators, Sales Engineers, Solution Architects, Support Personnel

Training

The following courses are available on <https://www.avaya-learning.com> To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
ATC02071WEN	Video Conferencing Technical Fundamentals
ATC02071AEN	Video Conferencing Technical Fundamentals- Assessment
ATC02070IEN	Avaya Video Solutions and ADVD Flare Implementation, Administration and Maintenance

ATC02070AEN	Avaya Video Solutions and ADVD Flare - Implementation, Administration and Maintenance – Assessment
-------------	--

Avaya Mentor videos

Avaya Mentor videos are available to provide technical content on how to install, configure, and troubleshoot Avaya products.

Videos are available on the Avaya support site, listed under the video document type, and on the Avaya-run channel on YouTube.

To find videos on the Avaya support site, select the product name, and check the videos checkbox to see a list of available videos.

Note:

Videos are not available for all products.

To find the Avaya Mentor videos on YouTube, go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:

- Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Product compatibility

For the latest and most accurate compatibility information, go to <http://support.avaya.com/CompatibilityMatrix/Index.aspx>.

Support

Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Detailed terms and conditions are contained in the sales agreement or other applicable documentation and establish the terms of the limited warranty. In addition, the Avaya standard warranty description and details for support under warranty are available at Avaya Support under More Resources for Maintenance and Warranty Information, see <https://support.avaya.com/>.

Send us your comments

Avaya appreciates any comments or suggestions that you might have about this product documentation. Send your comments to infodev@avaya.com.

Chapter 2: Overview

Avaya Aura[®] Video Quick Setup can be administered in different configurations. This document briefly describes the configurations and provides information about the general administration of the configurations.

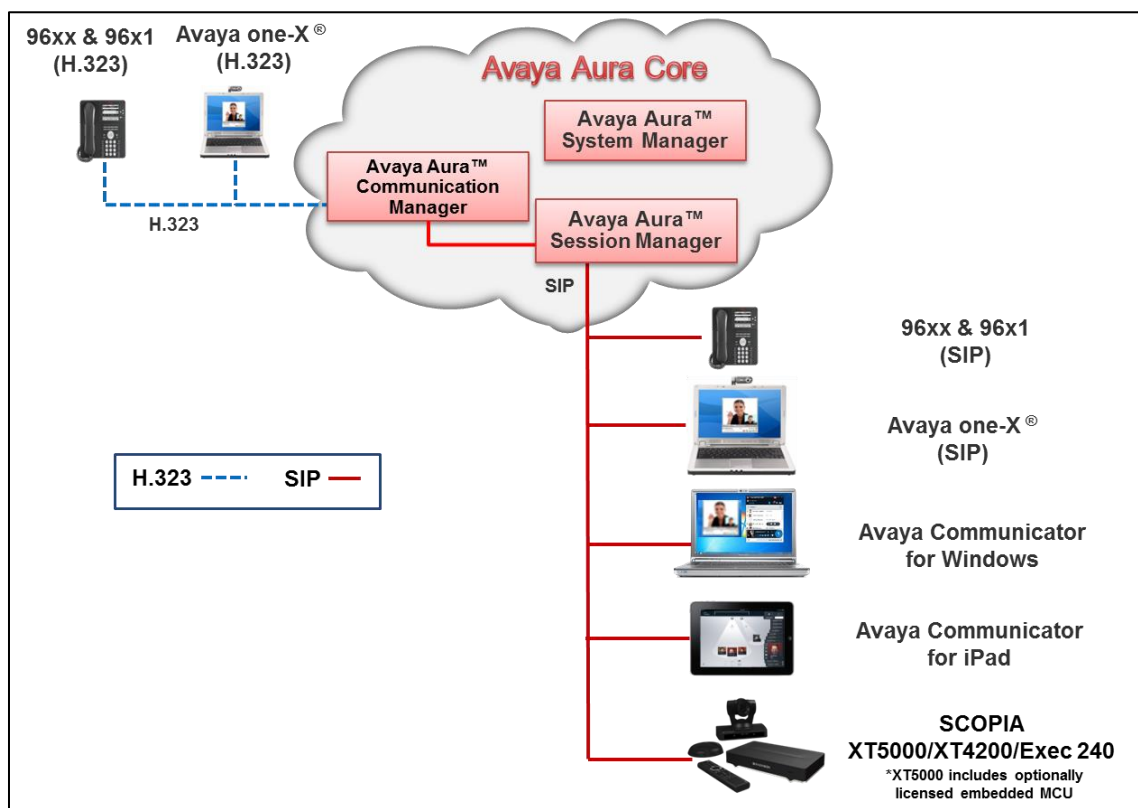
Note:

Combination of the deployments described in this document is not supported.

Avaya Aura[®] Conferencing without external gatekeepers or MCUs

This configuration does not involve external MCUs or external gatekeepers. All endpoints are H.323-based and registered to Communication Manager or SIP-based and registered to Avaya Aura[®] Session Manager. Scopia XT5000 includes an optional embedded MCU. Figure 1 Avaya Aura[®] Conferencing illustrates Avaya Aura[®] Conferencing without external gatekeepers or MCUs configuration.

Figure 1 Avaya Aura[®] Conferencing



Note:

If configuration includes XT endpoints, do not mix SIP and H.323 Scopia XT endpoints.

The following table lists the components of Avaya Aura[®] Conferencing:

Component	Avaya Aura [®] Conferencing
Infrastructure	Communication Manager Session Manager Avaya Aura [®] System Manager
Endpoints	Avaya Communicator

Component	Avaya Aura [®] Conferencing
	Avaya one-X [®] Communicator – SIP and H.323 Scopia XT Executive 240 – SIP Scopia XT 4200 Room System – SIP Scopia XT 5000 Room System with an optional embedded MCU – SIP

Avaya Aura[®] and Scopia 8.3 interoperability

This configuration describes the interoperability between Avaya Aura[®] and Scopia 8.3 through:

- An H.323 trunk between Communication Manager and Scopia ECS Gatekeeper.
Point-to-point calls between H.323-based and SIP-based Avaya video endpoints and H.323-based Radvision endpoints connect through the H.323 trunk. Conference calls that are hosted on the Scopia Elite MCU and involve H.323-based Avaya video endpoints connect through the H.323 trunk.
- A SIP trunk between Session Manager and the B2BUA component of Scopia Management.
Conference calls that are hosted on Scopia Elite MCU and involve SIP-based Avaya video endpoints connect through the SIP trunk.

Create route partitions to ensure that SIP-based calls to the Scopia Elite MCU are established through the SIP trunk and H.323-based calls to the Scopia Elite MCU are established through the H.323 trunk.

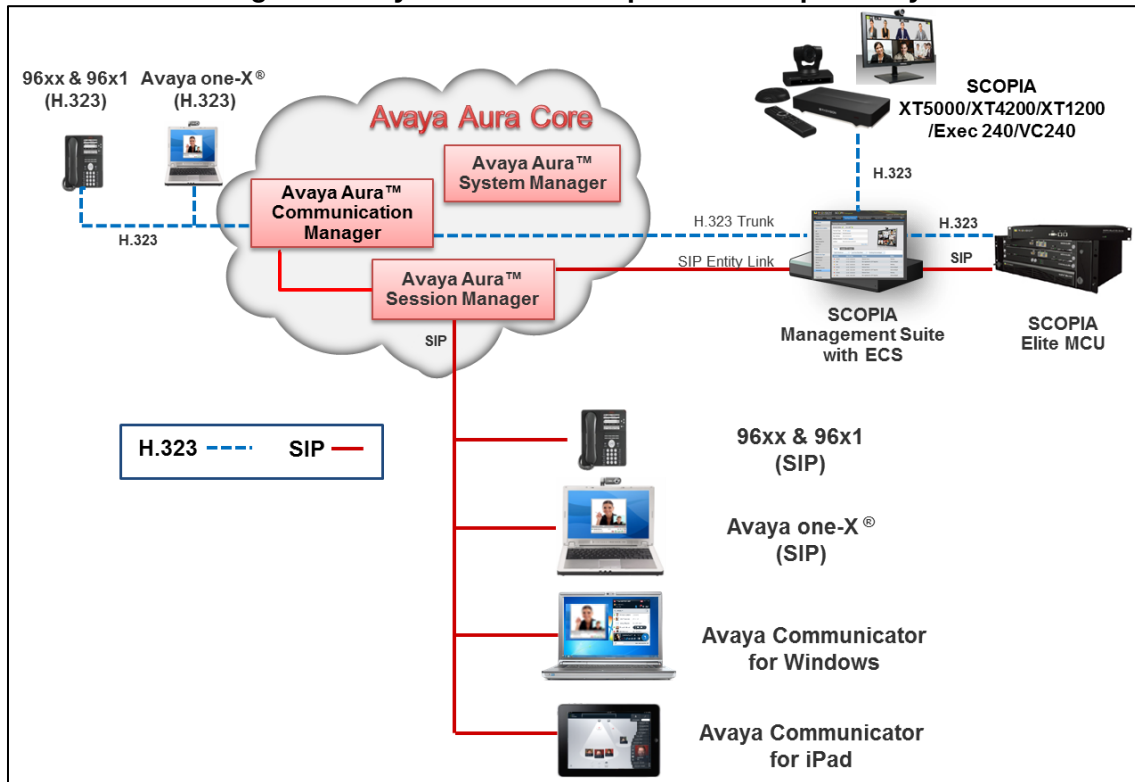
Note:

Avaya audio endpoints can connect to Scopia Elite MCU through the H.323 trunk or through the SIP trunk.

For information about how to create separate routes for a single, targeted extension based on the protocol of the endpoint at the originating location of a call, such as a Scopia Elite MCU meeting room, see [Partition Routing](#) on page 48.

Figure 2 Avaya Aura[®] and Scopia 8.3 interoperability illustrates how Avaya Aura[®] connects with Scopia 8.3.

Figure 2 Avaya Aura® and Scopia 8.3 interoperability



Note:

Avaya Aura® Communication Manager is the only component that supports interoperability between SIP and the H.323 protocols. Other components might support both these protocols, but do not perform any tasks for interoperability between SIP and the H.323 protocols. See the configuration description at the beginning of this section. Adhere to the required call routing for Scopia Elite MCU dial-in calls. Video calls to Scopia Elite MCU should be routed over the appropriate trunk type. The trunk type should match the originator's protocol type, SIP or H.323.

Note:

If configuration includes XT endpoints, do not mix SIP and H.323 Scopia XT endpoints.

The following table lists the components of Avaya Aura® and Scopia 8.3:

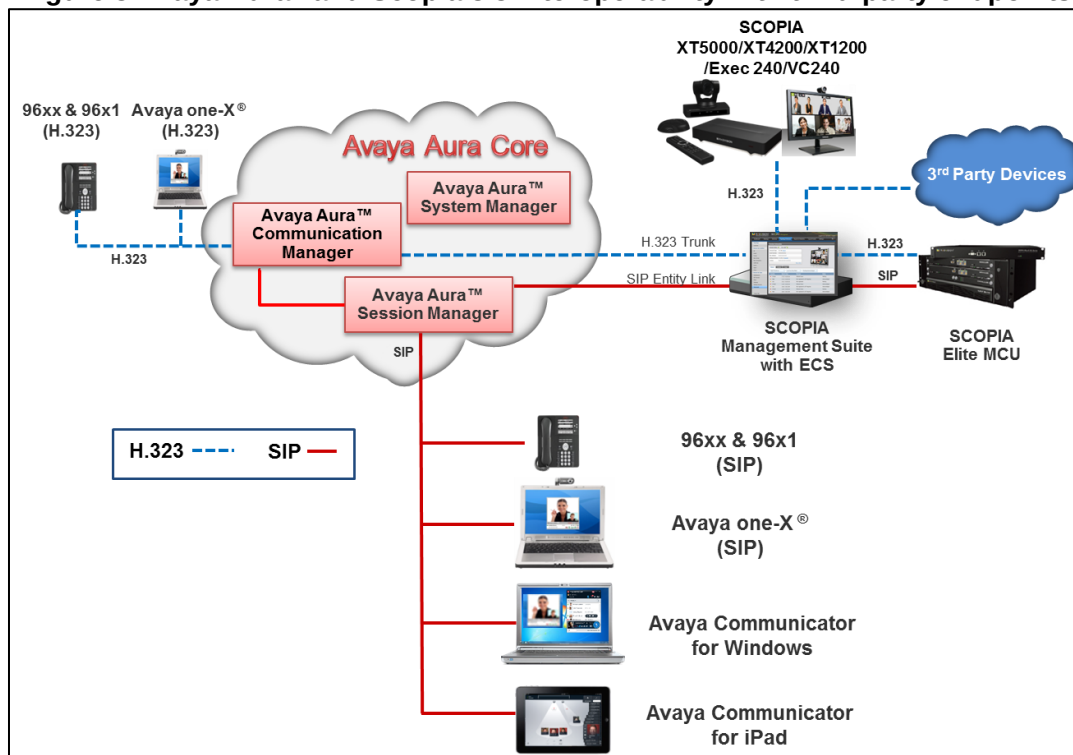
Component	Avaya Aura®	Scopia 8.3
Infrastructure	Communication Manager Session Manager Avaya Aura® System Manager	Scopia Management Scopia Enhanced Communication Server (ECS) Gatekeeper Scopia Elite MCU Scopia Desktop Server Scopia PathFinder
Endpoints	Avaya Communicator Avaya one-X® Communicator – SIP and H.323 Avaya Flare on desktop – SIP Avaya Flare on iPad – SIP Avaya Desktop Video Device – SIP	Scopia XT1200 Room System – H.323 Scopia XT4200 Room System – H.323 Scopia XT5000 Room System – H.323 Scopia XT Executive 240 – H.323 Scopia VC240 – H.323 Scopia Desktop Scopia Mobile

- Radvision endpoints involved in this interoperability solution use the H.323 protocol.
- Installation of the following Scopia 8.3 components is optional:
 - Scopia PathFinder.
 - Scopia Desktop Server. This server is required only if you install Scopia Desktop or Scopia Mobile as a part of the solution.
- Installation of the optional components of Scopia 8.3 depends on the configuration of the solution.
- For more information about how to apply service packs and how to install hot fixes to update the software of the Scopia 8.3 components, see *Administrator Guide for Scopia iView Management Suite Version 7.7* and *Scopia Management Administrator Guide Version 8.2 for Solution 8.2* at Radvision Knowledge Base: <http://docs.radvision.com/bundle>.

This configuration involves third-party endpoints that register to Scopia ECS Gatekeeper in the interoperability between Avaya Aura® and Scopia 8.3.

<https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

Figure 3 Avaya Aura® and Scopia 8.3 interoperability with third-party endpoints



Point-to-point video calls between Avaya Aura® video endpoints and third-party endpoints connected to Scopia Management are not supported. These calls must connect through the Radvision Elite MCU.

Avaya Aura® with the external Polycom MCU and H.323-based endpoints

This configuration describes how Polycom is integrated into Avaya Aura® Video.

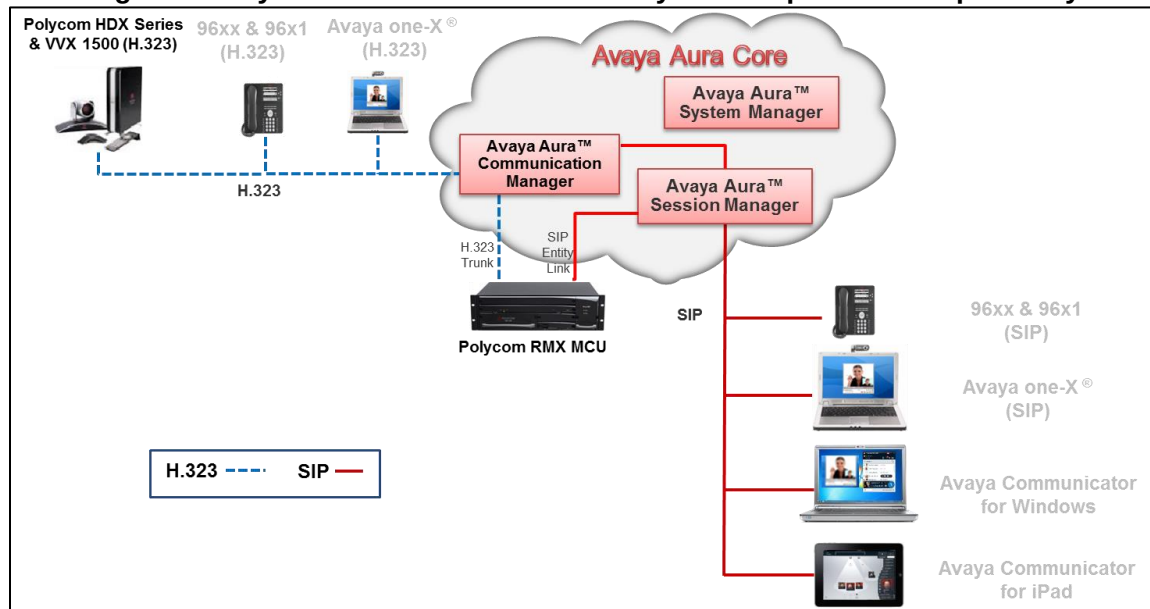
Polycom HDX series endpoints are registered directly to Communication Manager. The Polycom RMX MCU is administered for dual connectivity as:

- An H.323 trunk to Communication Manager.
- A SIP trunk to Session Manager.

Call routing is administered to ensure that call routes are established between these two trunks based on the protocol of the endpoint. For example, a SIP-based call route is established through the SIP trunk between Polycom RMX and Session Manager, while an H.323-based call route is established through the H.323 trunk between Polycom RMX and Communication Manager.

Figure 4 Avaya Aura® and H.323-based Polycom endpoints interoperability illustrates how Avaya Aura® connects with H.323-based Polycom endpoints through Communication Manager and Polycom RMX.

Figure 4 Avaya Aura® and H.323-based Polycom endpoints interoperability



Avaya Aura® with the external Polycom MCU and SIP-based endpoints

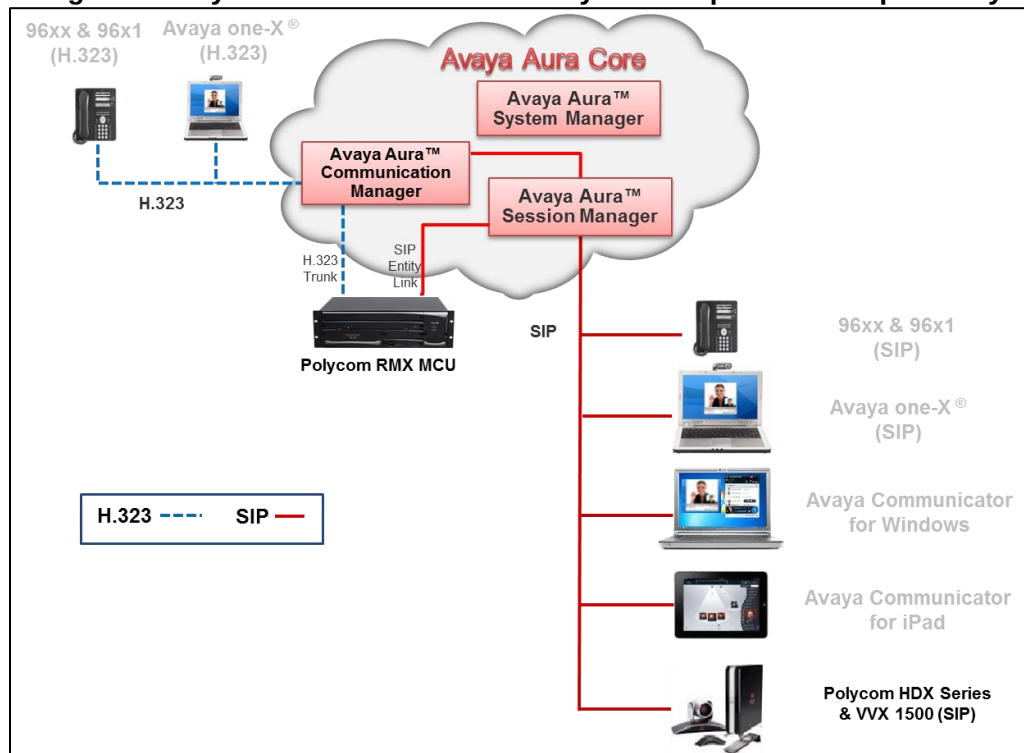
This configuration integrates an external Polycom MCU and SIP-based endpoints with Avaya Aura Video.

Polycom HDX series and Polycom VVX 1500 endpoints are SIP-based in this interoperability solution.

Call routing is administered to ensure that call routes are established between these two trunks based on the protocol of the endpoint. For example, a SIP-based call route is established through the SIP trunk between Polycom RMX and Session Manager, while an H.323-based call route is established through the H.323 trunk between Polycom RMX and Communication Manager.

Figure 5 Avaya Aura® and SIP-based Polycom endpoints interoperability illustrates how Avaya Aura® connects with SIP-based Polycom endpoints through Communication Manager and Polycom RMX.

Figure 5 Avaya Aura® and SIP-based Polycom endpoints interoperability



Avaya Aura® and Polycom interoperability

This configuration describes the interoperability between Avaya Aura® and Polycom through:

- Polycom RMX MCU administered for dual connectivity: An H.323 trunk to Communication Manager and a SIP trunk to Session Manager.
- Polycom DMA Gatekeeper or Polycom CMA Gatekeeper: An H.323 trunk to Communication Manager.

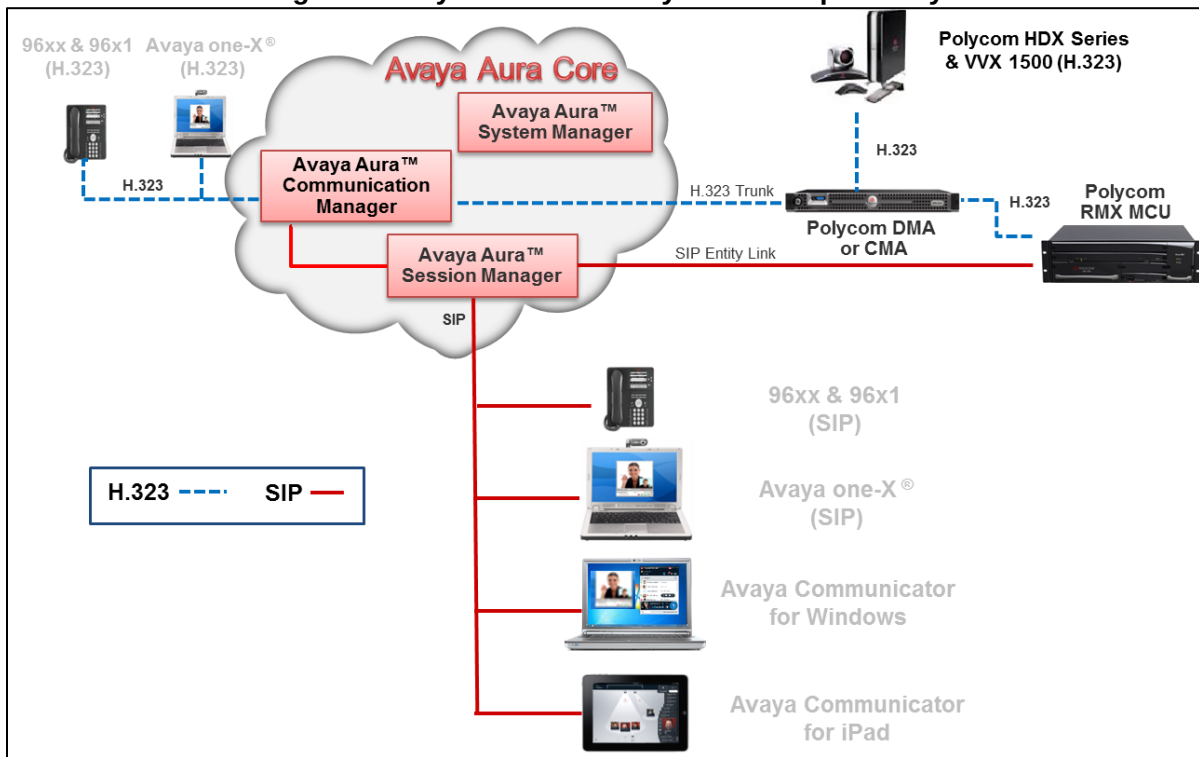
Point-to-point calls between H.323-based and SIP-based Avaya video endpoints and H.323-based Polycom endpoints connect through the H.323 trunk. Conference calls that are hosted on the Polycom RMX MCU and involve H.323-based Avaya video endpoints connect through the H.323 trunk, while conference calls that involve SIP-based Avaya video endpoints connect through the SIP trunk.

Call routing is administered to ensure that call routes are established between these two trunks based on the protocol of the endpoint. For example, a SIP-based call route is established through the SIP trunk between Polycom RMX and Session Manager, while an H.323 based call route is established through the H.323 trunk between Polycom CMA or DMA and Communication Manager. Create route partitions to ensure that SIP-based calls to the Polycom RMX MCU are established through the SIP trunk and H.323-based calls to the Polycom RMX MCU are established through the H.323 trunk.

For information about how to create separate routes for a single, targeted extension based on the protocol of the endpoint at the originating location of a call, see [Partition Routing](#) on page 48.

Figure 6 Avaya Aura® and Polycom interoperability illustrates how Avaya Aura® connects with the Polycom video conferencing solution.

Figure 6 Avaya Aura® and Polycom interoperability



Prerequisites

Before administering the Avaya Aura® Video Quick Setup, Scopia 8.3, and Polycom components ensure that you install compatible versions of the following components:

- Communication Manager
- System Manager
- Session Manager
- Polycom RMX with the MPM card
- Scopia iVIEW Management Suite or Scopia Management
- Scopia Elite MCU
- Scopia Desktop
- Scopia PathFinder
- Avaya endpoints and endpoint interfaces
- Radvision endpoints and endpoint interfaces
- Polycom endpoints and endpoint interfaces

For more information about compatible versions of the Avaya Aura® components and the Scopia 8.3 components, see the compatibility matrix on the Tools page of the Avaya Support website:

<https://support.avaya.com/>.

Ensure that you are familiar with the following tasks:

- Session Manager administration through System Manager, including administration of:
 - SIP domains
 - SIP entities
 - SIP entity links
 - Locations
 - Routing

- Dial patterns
- Communication Manager administration tasks, including administration of:
 - Signaling groups
 - Trunk groups
 - Dial plans
 - AAR/ARS routing

Perform a network assessment to ensure that the network supports bandwidth demands of video over IP. Implement QoS across the network.

Ensure that you have a well-defined routing plan.

For more information about administration tasks, see *Avaya Video Telephony Solution Networking Guide Release 5.2* at the Avaya Support website: <http://support.avaya.com>.

Chapter 3: Administering Communication Manager for video endpoints

This chapter provides information about administering Communication Manager for video endpoints, including enabling the video function and administering Communication Manager for SIP-based video endpoints through System Manager.

The administration can either be done through SMGR or the Communications Manager SAT.

These procedures contain steps only for the fields that you must change. For the remaining fields, retain the default value.

Enabling video on Communication Manager through SMGR

1. [Enable Multimedia IP SIP Trunking feature](#)
2. [Enable video for the SIP signaling group](#)
3. [Identify IP-codec-set](#)
4. [Add video to IP-codec-set](#)

1. Enabling Multimedia IP SIP Trunking feature.

1. On the System Manager interface, in the **Elements** column, click **Communication Manager > Parameters > System Parameters – Customer Options**.
2. Click the arrow icon next to the **Select Device(s)** from Communication Manager list.
3. Select the appropriate Communication Manager, and click **Show List**.
4. Select the radio button in the first column and click **View**.
5. Click **Next Page** until you navigate to Page 4. Ensure the feature **Multimedia IP SIP Trunking** is set to **y**.

2. Enabling video for the SIP signaling group.

1. On the System Manager interface, in the **Elements** column, click **Communication Manager > Network > Signaling Groups**.
2. On the Signaling Groups page, click the arrow icon next to Select Device(s) from Communication Manager list.
3. From the Communication Manager list, select the appropriate Communication Manager instance, and click **Show List**.
4. Select the appropriate **Signaling Group Number** and click **edit** to set parameters as mentioned below:
 - **IP Video:** **y**
 - **Direct IP-IP Audio connections:** **y**
 - **Initial IP-IP Direct Media:** **y**

3. Identifying the IP-codec-set.

1. On the System Manager interface, in the **Elements** column, click **Communication Manager > Network > Signaling groups** page.
2. Note the values of the **Near-end Node Name** and **Far-end Network Region** fields.
3. If the **Near-end Node Name** field is set to **PROCR**, use the listed value. If the **Near-end Node Name** field is set to **CLAN**, on Communication Manager SAT screen, enter `list ip-interface clan` to find the correct CLAN and note the slot value. These values are used to determine the IP-Codec-set.
4. On the Communication Manager SAT screen, enter `display ip-interface procr/slot`.

5. Note the value of the **Network Region** field.
6. On the System Manager interface, click **Elements > Communication Manager > Network > IP network Regions**.
7. On the IP Network Regions page, click the arrow icon next to Select Device(s) from Communication Manager list.
8. From the Communication Manager list, select the appropriate **Communication Manager**, and click **Show List**.
9. Select the appropriate Network Region and click **edit**. Navigate to the Inter Network Region Connection Management pages.
10. Ensure the **dst rgn** number aligns with the **Far-end Network Region**. Make note of the **codec set** number.

4. Adding video to IP-codec-set.

1. On the SAT screen, enter `change ip-codec-set n`, where **n** is the codec set number used by SIP signaling group.
2. Add or change the appropriate audio codecs as required. Set the following Multimedia parameters on page 2:

- **Allow Direct-IP Multimedia:** `y`

- **Maximum Call Rate for Direct-IP Multimedia:** `1024 Kbits`

Note:

These values are examples only. 1024 allows for 720p High Definition. Higher resolutions require more bandwidth. See *Avaya Video Telephony Solution Release 5.2 Networking Guide* for further details.

- **Maximum Call Rate for Priority Direct-IP Multimedia:** `2048 Kbits`

Note:

This applies to priority video users and is not required for minimal administration. See *Avaya Video Telephony Solution Release 5.2 Networking Guide* for further details.

Note:

Verify that the list of audio codecs on the first page includes at least one of the audio codecs supported by the video endpoint, such as G.722 or G.711.

Enabling video on Communication Manager through SAT

1. On the SAT screen, type `change system-parameters customer-options`.
2. On page 4, set **Multimedia IP SIP Trunking** field to `y`.
3. To enable video for the SIP signaling group, on the Communication Manager SAT screen, type `change signaling-group <group name>`, and set the following parameters:
 - **IP Video:** `y`
 - **Direct IP-IP Audio Connections:** `y`
 - **Initial IP-IP Direct Media:** `y`

Note:

 - Note the value of the **Far-end Network Region** field of the **Signaling Group**. Use this information in the following steps.
 - You do not need to modify Priority video options. For more details on Priority video options, see *Avaya Video Telephony Solution Release 5.2 Networking Guide* on the Avaya Support website at <http://support.avaya.com>.
4. To identify the codec set, on the Communication Manager SAT screen, type `display ip-network-region n`, where **n** is the ip-network-region shown in the SIP signaling group, and navigate to the Inter Network Region Connection Management pages. Ensure that the destination region number is identical to the far-end network region of the signaling group. Note the codec set number of the network region.

5. To add **video to ip-codec-set**, on the SAT screen, type `change ip-codec-set <codec set number used by the SIP signaling group>`.
6. Add or change the required audio codecs, and set the following parameters on page 2:
 - **Allow Direct-IP Multimedia:** y
 - **Maximum Call Rate for Direct-IP Multimedia:** 1024 Kbps
With a maximum call rate of 1024 Kbps, you can stream 720p high-definition video. For higher resolution video streaming, you need to allocate more bandwidth. For more details on allocating bandwidth for multimedia calls, see *Avaya Video Telephony Solution Release 5.2 Networking Guide* on the Avaya Support website at <http://www.avaya.com/support>.
 - **Maximum Call Rate for Priority Direct-IP Multimedia:** 2048 Kbps
Maximum Call Rate for Priority Direct-IP Multimedia applies only to priority video users. For more details on allocating bandwidth for multimedia calls, see *Avaya Aura® Video Quick Setup Networking Guide* on the Avaya Support website at <http://www.avaya.com/support>.

Note:

Verify that the list of audio codecs includes a minimum of one audio codec that the video endpoints support, for example, G.722 or G.711.

Repeat Steps 2 to 4 for each signaling group for which you want to enable video.

Administering SIP-based video endpoints on System Manager

Use System Manager to create an endpoint template and add users using these templates.

1. [Create a custom template for Avaya SIP video endpoints using System Manager](#)
2. [Add users to Avaya SIP video endpoints using System Manager](#)

Creating a custom template for Avaya SIP video endpoints using System Manager

1. Log in to the System Manager Web console.
2. In the **Services** column, click **Templates > CM Endpoint**.
3. Select **CM 6.3** on the Endpoint Templates page, and click **New**.
4. Set the following parameters:
 - **Set Type:** 9630SIP

Note:
9630 SIP is an alias for the Scopia XT series endpoints.

 - **Template Name:** Name the template according to the type of the Scopia XT series endpoint and Communication Manager release. For example, XT5000_CM_6_3.
 - **COR:** 1
 - **COS:** 1, or an appropriate COS group for priority video calling and bit-rate management
 - **SIP trunk:** AAR, or a specific SIP trunk used between System Manager and Communication Manager
5. On the **Feature Options** tab:
 - Select the **IP video** check box.
 - Select the **IP SoftPhone** check box for Avaya one- X® Communicator or Avaya Communicator for Windows.

Note:
When you select this check box, the title of the check box changes to **IP Video SoftPhone**.
6. To enable the **Call Appearance** feature, click the **Button Assignment** tab, and set the main buttons for each endpoint to `call appr` according to the following list:
 - **Scopia XT Executive 240:** 1

- **Scopia XT 4200:** 1
- **Scopia XT 5000 without the embedded MCU:** 1
- **Scopia XT 5000 with an embedded MCU for five participants:** 5
- **Scopia XT 5000 with an embedded MCU for nine participants:** 9
- **Avaya one-X® Communicator:** 3

Note:

- Set the call appearances to the maximum limit permitted for each endpoint.
- Ensure that the **Restrict Last Appearance** field on the Feature Options tab is set to *n*.

Repeat this procedure for each Avaya SIP endpoint for which you want to create a custom template by using System Manager.

Note: You can name the template according to the type of the Avaya Communication Manager release. For example, one-X Communicator _CM_6_3.

Adding users to Avaya SIP video endpoints using System Manager

1. Log in to the System Manager Web console.
2. To create a new user profile, in the **Users** column, click **User Management > Manage Users**.
3. Click **New** and set the following parameters

On the **Identity** tab:

- **Last Name**
- **First Name**
- **Login Name.** For example, ext@sip domain
- **Authentication Type:** *Basic*
- **System Manager Login Password**

On the **Communication Profile** tab:

Communication Profile Password: Corresponds to the authorization password of the endpoints.

4. In the **Address** section, click **New**, set the **FQDN**, and click **Add**.
5. To enable Session Manager Profile, select the check box corresponding to Session Manager profile, and set the following parameters:
 - **Primary Session Manager:** The appropriate Session Manager instance.
 - **Secondary Session Manager:** None.
 - **Survivability Server:** None.
 - **Origination Application Sequence:** The name of the Communication Manager server.
 - **Terminating Application Sequence:** The name of the Communication Manager server.
 - **Home Location:** The appropriate option.
6. To create an endpoint profile, select the check box corresponding to the CM Endpoint Profile.
7. Select the appropriate Communication Manager system, and set the following parameters:
 - **Extension**
 - **Template**
 - **Port:** *IP*
8. Click **Commit**.

For information about configuring Scopia XT series video endpoints, see the Scopia XT series documentation at: <http://www.avaya.com/support>.

Chapter 4: Administering SIP-based video endpoints

This chapter provides information about administering SIP-based video endpoints.

Administering Avaya one-X® Communicator

You can configure Avaya one-X® Communicator to use SIP or the H.323 protocol. Ensure that the Enable Video check box on one-X® Communicator is selected.

For more information about how to configure one-X® Communicator to use SIP or the H.323 protocol, see *Avaya one-X® Communicator Getting Started* Guide at the Avaya Support website:

<http://support.avaya.com>.

Administering Scopia XT series endpoints

Administer the Scopia XT series endpoint through the infrared remote control unit. You can also use the Scopia XT series endpoint GUI through a Web browser to configure the Scopia XT series endpoint.

1. To open the main menu of the Scopia XT series video endpoint, on the infrared remote control unit, click the **OK** button.
2. To set the system name, click **Configure > General**.
3. Enter the name of the system in the **System Name** field, and enter values for the other fields according to your requirement.

The video endpoint displays the system name on the screen.

4. To administer the IP address of the video endpoint, click **Configure > Network > GLAN 1 > Addresses** and set the following parameters:

The video endpoint management interface prompts you to enter your credentials when you click **Advanced**. The default credentials are:

Login: Admin

Password: 1234

- **Automatic IP Address:** No

Note:

If DHCP is used, ensure that the DHCP server is functional and set this parameter to **Yes**.

- **IP Address**
- **Subnet Mask**
- **Gateway IP Address**
- **DNS Server IP Address**

5. To configure the Advanced settings through the remote control, click **Configure > General** and set the following parameter:

Show Advanced Settings: Yes

6. To administer the SIP parameters, click **Configure > Advanced > Protocols > SIP**, and set the following parameters:

The video endpoint management interface prompts you to enter your credentials when you click **Advanced**. The default credentials are:

Login: Admin

Password: 1234

- **User:** <user name>
- **Authentication Name:** <extension>
- **Authentication Password:** <shared Communication Profile password>

- **UDP/TCP Listening Port:** 5060
 - **Transport Outbound Call:** TCP
 - **Use SIP Register:** Yes
 - **Register DNS Name:** <Session Manager FQDN or IP address>
 - **Use SIP Proxy:** Yes
 - **Proxy DNS Name:** <Session Manager FQDN or IP address>
 - **Use TLS:** No
 - **TLS Listening Port**
 - **Verify Certificate**
7. In order to use G.722 on XT, the XT DTMF setting should be:
Advanced > Calls > Preferences > IP > DTMF RFC2833 (H.323) > Yes.
8. To verify if the user is administered, click **Configure > System Status.**

Chapter 5: Administering Communication Manager for interoperability with the H.323- based Scopia ECS Gatekeeper

This chapter describes the procedures through System Manager. You can perform these procedures on the Communication Manager SAT interface too.

These procedures are guidelines on how to administer the system. Depending on the configuration of your system, values of the parameters might differ.

Note:

These procedures contain only fields that you must configure. Retain the default values for other fields.

Logging in to System Manager

To log in to System Manager, in the browser address bar, enter the System Manager FQDN in the following format:

http://<FQDN_of_SystemManager>

Adding a node name for Scopia ECS Gatekeeper

1. Click **Elements > Communication Manager > Network > Node Names**.
2. In the Select device(s) from Communication Manager list drop-down menu, select the relevant Communication Manager, and click **Show List**.
3. In the **Node Names** List section, click **New**.
4. In the **Enter Quantifier** input box, enter *ip*, and click **Add**.
5. In the **Name** column, enter a name for Scopia ECS Gatekeeper.
6. In the **IP Address** column, enter the IP address of Scopia ECS Gatekeeper.
7. Click **Enter** on the top of the screen.

Note:

Some browsers might indicate that you are about to leave the page. Click the appropriate option to continue.

Adding an H.323 signaling group for Scopia ECS Gatekeeper

1. Click **Elements > Communication Manager > Network > Signaling Groups**.
2. In the Select device(s) from Communication Manager list drop-down menu, select the relevant Communication Manager, and click **Show List**.
3. In the **Signaling Group List** section, click **New**.
4. In the **Enter Qualifier** input box, enter a signaling group number, and click **Add**.
5. On Page 1, enter values for the following fields:
 - **Group Type:** *h.323*
 - **IP Video:** *y*
 - **Priority Video:** *y*
 - **Near-end Node Name:** *procr* or *CLAN*
 - **Near-end Listen Port:** *1719*
 - **Far-end Node Name:** *<Name of Scopia ECS Gatekeeper entered in Step 5 of [Adding a node name for Scopia ECS Gatekeeper](#)>*
 - **Far-end Listen Port:** *1719*
 - **Far-end Network Region:** *<Network region based on the system administration>*

- **LRQ Required:** *y*
 - **DTMF over IP:** *out-of-band*
 - **direct ip audio connections –** *y*
6. Click **Enter** on the top of the screen.

Note:

Some browsers might indicate that you are about to leave the page. Click the appropriate option to continue.

Adding an H.323 trunk group for Scopia ECS Gatekeeper

1. Click **Elements > Communication Manager > Network > Trunk Group**.
2. In the Select device(s) from Communication Manager *List* drop-down menu, select the relevant Communication Manager, and click **Show List**.
3. In the **Trunk Group List** section, click **New**.
4. In the **Enter Qualifier** input box, enter a trunk group number, and click **Add**.
5. On Page 1, enter values for the following fields:
 - **Group Type:** *isdn*
 - **Group Name:** *<Name for the trunk group>*
 - **COR:** *<COR based on the system administration>*
 - **TAC:** *<TAC based on the dial plan of the system>*
 - **Outgoing Display:** *n*
 - **Carrier Medium:** *H.323*
 - **Service Type:** *tie*
 - **Member Assignment Method:** *auto*
 - **Signaling Group:** *<Number of the signaling group entered in Step 4 of [Adding an H.323 signaling group for Scopia ECS Gatekeeper](#)>*
 - **Number of Members:** *<Number of trunk group members>*

Note:

The values on Page 1 are specific to the Scopia 8.3 configuration.

6. Click **Next Page** on the top of the screen, and navigate to Page 3.
7. On Page 3, enter values for the following fields:
 - **Send Name:** *y*
 - **Send Calling Number:** *y*
 - **Format:** *<Value based on the dial plan of the system>*
 - **Replace Restricted Numbers?:** *y*
 - **Replace Unavailable Numbers?:** *y*
 - **Send connected number:** *y*
8. Click **Enter** on the top of the screen.

Note:

Some browsers might indicate that you are about to leave the page. Click the appropriate option to continue.

Adding the H.323 trunk group for channel selection to the signaling group of Scopia ECS Gatekeeper

1. Click **Elements > Communication Manager > Network > Signaling Groups**.

2. In the Select device(s) from Communication Manager list drop-down menu, select the relevant Communication Manager, and click **Show List**.
3. In the **Signaling Group List** section, select the signaling group added in [Adding an H.323 signaling group for Scopia ECS Gatekeeper](#), and click **Edit**.
4. On Page 1, enter a value for the following field:
Trunk Group for Channel Selection: <Trunk number entered in Step 4 of [Adding an H.323 trunk group for Scopia ECS Gatekeeper](#)>

Adding a route pattern for Scopia ECS Gatekeeper

1. Click **Elements > Communication Manager > Network > Route Pattern**.
2. In the Select device(s) from Communication Manager list drop-down menu, select the relevant Communication Manager, and click **Show List**.
3. In the **Route Pattern List** section, click **New**.
4. In the **Enter Qualifier** input box, enter a route pattern number, and click **Add**.
5. On Page 1, enter values for the following fields:
 - **Pattern Name:** <Name for the route pattern>
 - **Grp No:** <Number of the trunk group entered in Step 4 of [Adding an H.323 trunk group for Scopia ECS Gatekeeper](#)>
 - **FRL:** <FRL based on the system administration for trunk access policies>
6. Click **Enter** on the top of the screen.

Note:

Some browsers might indicate that you are about to leave the page. Click the appropriate option to continue.

Creating and editing dial plans for Scopia ECS Gatekeeper

The administration steps in this section depend on the administration of the network. These steps describe a typical dial plan usage leveraging UDP and AAR.

1. Click **Elements > Communication Manager > System > Dialplan Analysis**.
2. In the Select device(s) from Communication Manager list drop-down menu, select the relevant Communication Manager, and click **Show List**.
3. In the **Dialplan Analysis List** section, click **New**.
4. In the **Enter Qualifier** input box, enter *all*, and click **Add**.
5. Navigate to a page with empty rows, and add an entry for Scopia ECS Gatekeeper based on the dial plan of the system.
6. Enter a value for the following field:
Call Type: udp
7. Click **Enter** on the top of the screen.

Note:

Some browsers might indicate that you are about to leave the page. Click the appropriate option to continue.

Creating a uniform dial plan for Scopia ECS Gatekeeper

1. Click **Elements > Communication Manager > System > Uniform Dial Plan**.
2. In the Select device(s) from Communication Manager list drop-down menu, select the relevant Communication Manager, and click **Show List**.

3. In the **Uniform Dial Plan List** section, click **New**.
4. In the **Enter Qualifier** input box, enter digits based on the dial plan of the system, and click **Add**.
5. Navigate to a page with empty rows, and add an entry for Scopia ECS Gatekeeper based on the dial plan of the system.
6. Enter the appropriate network type. For example, **AAR**.
7. Click **Enter** on the top of the screen.

Note:

Some browsers might indicate that you are about to leave the page. Click the appropriate option to continue.

Creating an alternate route for the uniform dial plan of Scopia ECS Gatekeeper

1. Click **Elements > Communication Manager > Network > Automatic Alternate Routing Analysis**.
- Note:**
You might be using ARS instead of AAR.
2. In the Select device(s) from Communication Manager list drop-down menu, select the relevant Communication Manager, and click **Show List**.
3. In the **Automatic Alternate Routing Analysis List** section, click **New**.
4. In the **Enter Qualifier** input box, enter digits based on the dial plan of the system, and click **Add**.
5. Navigate to a page with empty rows, and add an entry for Scopia ECS Gatekeeper based on the dial plan of the system.
6. Select the appropriate route pattern and enter a value for the following field:
Call Type: unku
7. Click **Enter** on the top of the screen.

Note:

Some browsers might indicate that you are about to leave the page. Click the appropriate option to continue.

Chapter 6: Administering Session Manager for interoperability with the SIP-based Scopia B2BUA component

These procedures are guidelines on how to administer the system. Depending on the configuration of your system, values of the parameters might differ.

Logging in to System Manager

To log in to System Manager, in the browser address bar, enter the System Manager FQDN in the following format:

http://<FQDN_of_SystemManager>

Adding a SIP entity for the Scopia B2BUA component

1. Click **Elements > Routing > SIP Entities**.
2. Click **New**.
3. Enter values for the following fields:
 - **Name:** *<Name for the SIP entity>*
 - **FQDN or IP Address:** *<FQDN or IP address of the Scopia B2BUA component>*
 - **TYPE:** *SIP Trunk*
 - **Adaptation:** *<Depending on the dial plan of the system, create and select an adaptation>*
 - **Location:** *<Location of the Scopia B2BUA component>*
 - **Time Zone:** *<Time zone of the location of the Scopia B2BUA component>*
4. To submit, click **Commit**.

Adding a SIP entity link/SIP trunk for the Scopia B2BUA component

1. Click **Routing > Entity Links**.
2. Click **New**.
3. Enter values for the following fields:
 - **Name:** *<Name for the SIP entity link>*
 - **SIP Entity 1:** Select the relevant Session Manager
 - **Protocol:** *TCP*
 - **Port:** *5060*
 - **SIP Entity 2:** *<Select the Scopia B2BUA component>*
 - **Port:** *5060*
4. To submit, click **Commit**.

Adding routing policies for the Scopia B2BUA component

1. Click **Elements > Routing > Routing Policies**.
2. Click **New**.
3. Enter a value for the following field:
Name: *<Name for the routing policy>*
4. In the **SIP Entity as Destination** section, click **Select**.
5. Select the radio button for the Scopia B2BUA component, and click **Select**.
6. To submit, click **Commit**.

Adding dial patterns for the Scopia B2BUA component

1. Click **Elements > Routing > Dial Patterns**.
2. Click **New**.
3. Enter a value for the following fields:
 - **Pattern:** *<Value based on the dial plan of the system>*
 - **Min:** *<Value based on the dial plan of the system>*
 - **Max:** *<Value based on the dial plan of the system>*
4. In the **Originating Locations and Routing Policies** section, click **Add**.
5. Select the appropriate Originating Location and Routing Policy based on the dial plan of the system, and click **Select**.
6. To submit, click **Commit**.

Chapter 7: Administering Scopia Management for interoperability with Avaya Aura®

This chapter describes the procedures to add the following trunks:

- H.323 trunk between Scopia ECS Gatekeeper and Communication Manager.
- SIP trunk between the Scopia B2BUA component and Session Manager.

Note:

Scopia iVIEW Management Suite is renamed Scopia Management in Scopia Release 8.3.

Logging in to Scopia Management

To log in to Scopia Management, in the browser address bar, enter the Scopia Management FQDN in the following format:

http://<FQDN_or_IP_of_iVIEW>:<port>/iview

Note:

Unless specified in the Scopia Management installation guidelines, use the default port 8080.

Adding an H.323 trunk from Scopia ECS Gatekeeper to Communication Manager

Adding an H.323 trunk in Scopia iView Management Suite

1. In the **Admin** section, click **Resource Management**.
2. Select the **Gatekeeper/SIP Server/Presence Server** tab on the top of the screen, and click **Add** on the bottom-right corner of the screen.
3. Enter values for the following fields:
 - **Name:** <Name for Communication Manager>
 - **IP Address/FQDN:** <IP address of the procr or CLAN of Communication Manager>
 - **Model:** Avaya Aura®
 - **Location:** <Location of Communication Manager>

Note:

Do not add the zone prefix in this step. Add the prefix in the subsequent steps.

4. To submit, click **OK** on the bottom of the screen.
Scopia Management opens the initial page.
5. To edit the configuration of Communication Manager, click the relevant Communication Manager.
6. Click **Add Zone Prefix**, and add digits to route calls from Scopia ECS Gatekeeper to Communication Manager.
7. Click **OK** to submit.

Adding an H.323 trunk in Scopia Management

1. From the options on the top of the administrator portal, click **Devices**.
2. Click **Device by Type > Gatekeepers** and click **Add**.
3. Enter values for the following fields:
 - **Name:** <Name for Communication Manager>
 - **IP Address/FQDN:** <IP address of the procr or CLAN of Communication Manager>
 - **Model:** Avaya Aura®
 - **Location:** <choose appropriate location>

4. In the **Zone Prefix** field, add digits to route calls from Scopia ECS Gatekeeper to Communication Manager. Choose whether or not to strip local zone prefix for outgoing calls based on dial plan.
5. Click **OK** to submit.

Adding a SIP trunk from the Scopia B2BUA component to Session Manager

Adding a SIP trunk in Scopia iView Management Suite

1. In the **Admin** section, click **Resource Management**.
2. Select the **Gatekeeper/SIP Server/Presence Server** tab on the top of the screen, and click **Add** on the bottom-right corner of the screen.
3. Enter values for the following fields:
 - **Name:** *<Name for Session Manager>*
 - **IP Address/FQDN:** *<IP address of the SIP entity of Session Manager>*
 - **Model:** Avaya Aura®
 - **Location:** *<Location of Session Manager>*
 - **Port:** 5060
 - **Transport type:** TCP
 - **SIP Domain:** *<SIP domain configured in System Manager>*
4. To submit, click **OK**.

Adding a SIP trunk in Scopia Management

1. From the options on the top of the administrator portal, click **Devices**.
2. Click **Device by Type > SIP Servers** and click **Add**.
3. Enter values for the following fields:
 - **Name:** *<Name for Session Manager>*
 - **IP Address/FQDN:** *<IP address of the SIP entity of Session Manager>*
 - **Port:** 5060
 - **Transport type:** TCP
 - **Model:** Avaya Aura®
 - **SIP Domain:** *<SIP domain configured in System Manager>*
 - **Location:** *<choose appropriate location>*
4. To submit, click **OK**.

Changing the default SIP domain on Scopia Management

Change the default SIP domain on the FROM header of calls from Scopia Elite MCU to match the domain administered on Avaya Aura®.

1. From the options on the top of the Scopia Management Web interface, on the top-right corner, click the maintenance icon.
2. Click **Advanced Parameters** and enter values for the following fields:
 - **Property Name:** `vnex.vcms.core.conference.defaultDomain`
 - **Property Value:** *<SIP domain administered on Avaya Aura®>*
3. Click **Apply**.

To verify the new default SIP domain, type `defaultDomain` in the Search field.

Chapter 8: Administering third-party components

This chapter provides information about administering third-party components such as video endpoints, a video conferencing bridge, and a direct routing gatekeeper.

Registering Polycom HDX endpoints on Communications Manager or Session Manager.

Prerequisites

Before you administer the Polycom HDX endpoint, ensure that:

- The Polycom HDX endpoint has the latest supported version of the software.
- The Polycom HDX endpoint is connected to the network.
- Determine whether the HDX endpoint will be connected via H.323 to CM or via SIP to SM.

Procedure

1. In a Web browser, navigate to the home page of the Polycom HDX endpoint.
2. After logging in click **Admin Settings > Network > IP Network**, and set the following parameters:
 - **Enable IP H.323:** Select the check box if registering via H.323.
 - **Display H.323 Extension:** Select the check box
 - **H.323 Extension (E.164):** *<station number>*
Note:
The station number must be identical to the station number that you specified for the Polycom HDX endpoint on Communication Manager.
 - **Use Gatekeeper:** Select Specify with PIN.
Note:
For this option, to enable connection to Communication Manager, the endpoint might need a new license.
 - **Current Gatekeeper IP Address:** *<IP address of C-LAN or PC-LAN>*
Note:
 - If the “Current Gatekeeper IP Address” is incorrect it must be changed by entering the correct address in the “Primary Gatekeeper IP Address:” field.
 - To specify the port, append the IP address with the port number 1719.
 - Click **Change PIN**, enter **Authentication PIN:** *<security code>*, and click **Confirm PIN**.
Note:
The security code must be identical to the security code you entered in H.323 Extension (E.164).
 - **Number:** *<extension of the Polycom HDX endpoint>*
 - **Enable SIP:** Select the check box if registering via SIP.
 - **SIP Server Configuration:** Select Specify
 - **Registrar Server:** *<IP address of SM asset>*
 - **Proxy Server:** *<IP address of SM asset>*
 - **Transport Protocol:** Select TCP
 - **User Name:** *<SIP user name>*
 - **Domain User Name:** *<SIP user name>*
 - **Password:** Select the check box, enter password and confirmation.

- **Enabled PVEC:** Select the check box.
 - **Type of Service:** Select IP Precedence or Diffserv.
Note:
For more information on which type of service to select, contact the network administrator.
 - **Type of Service Value > Video:** QoS value of the IP Network Region setting to which the Polycom HDX endpoint belongs
 - **Type of Service Value > Audio:** QoS value of the IP Network Region setting to which the Polycom HDX endpoint belongs
 - **Type of Service Value > Control:** QoS value of the IP Network Region setting to which the Polycom HDX endpoint belongs
 - **Dynamic Bandwidth:** Select the check box.
 - **Maximum Transmit Bandwidth:** Select the setting that is identical to the Maximum Call Rate for Direct-IP Multimedia setting you specified for Communication Manager.
 - **Maximum Receive Bandwidth:** Select the setting that is identical to the Maximum Call Rate for Direct-IP Multimedia setting you specified for Communication Manager.
3. Configure values in the **Firewall** section.
 - Select the **Enable SIP Keep-Alive Messages** checkbox
 4. To enable application sharing, click **Network > Call Preference** and select the H.239 check box.
 5. Click **Update**.

Repeat Steps 1 to 4 for each Polycom HDX endpoint.

For information about how to administer Communication Manager for Polycom HDX series endpoint, see [Administering Communication Manager for H.323-based Polycom HDX series video endpoints](#).

Registering Polycom VVX1500 as a SIP-based endpoint on Avaya Aura®

Prerequisites

Before you administer the Polycom VVX1500 endpoint, ensure that:

- The Polycom VVX1500 endpoint has the latest supported version of the software.
- The Polycom VVX1500 endpoint is connected to the network.

Procedure

1. In a Web browser, navigate to the home page of the Polycom VVX1500 endpoint.
2. Click **Settings > Lines**, and choose a line number to administer the SIP settings. The endpoint interface opens the settings page of the line number that you select.
3. On the Line setting page, perform the following tasks:
 - In the **SIP Settings** section, select **Enable**.
 - In the **H.323 Settings** section, select **Disable**.
 - In the **Identification** section, enter values for
 - **Display Name**
 - **Address:** <extension number administered on System Manager>
 - **Label:** <line appearance label>
 - In the **Authentication** section, enter values for:
 - **User ID:** <extension number administered on System Manager>
 - **Password:** <password of the extension number>

Retain the default values for all the other fields.

- In the **SIP Server 1** section, enter values for:
 - **Address:** *<IP address of Session Manager>*
 - **Port:** 5060

Retain the default values for all the other fields.

Administering Communication Manager for H.323-based Polycom HDX series video endpoints

Prerequisites

Before you administer Polycom HDX series endpoints on Communication Manager, ensure that you have the following information:

- The maximum number of Polycom HDX series endpoints on the customer network
- The PIN for each Polycom HDX series endpoint.
- The key code that combines Avaya options with Polycom options.

Note:

To create a single key code, you must combine the Polycom Software License for this capability with the Avaya Option Polycom Software License.

- The IP address of the voice system.
- The IP codec sets that you want to use.
- The IP network regions that you want use.

Procedure

1. On the SAT screen, type `display system-parameters customer-options`, and verify the following parameter on page 2:
Maximum Video Capable Stations: This Polycom endpoint license file provides this number.
2. To configure COS, on the SAT screen, type `change cos`, and set the following parameter on page 2:
Priority IP Video: `COS levels`
3. To add a station, on the SAT screen, type `add station n`, and set the following parameters:
 - **Type:** `H.323`
 - **Security Code:** The PIN that you administer for the Polycom HDX series endpoint.
 - **IP Video:** `Y`

Note:
You can create an alias for the Polycom HDX series endpoints.

 - **Direct IP-IP Audio Connections:** `Y`

For information on how to configure the Polycom HDX series endpoint, see [Registering Polycom HDX](#).

Administering the Polycom RMX video conferencing bridge

1. Install Polycom RMX and connect it to your network. If required, upgrade the Polycom RMX software.
2. Log in to Polycom RMX Manager.
3. From the Setup menu, select the **System Configuration > System Configuration tab**. In `MCMS_PARAMETERS_USER`, set the following parameters:
 - **ENABLE_AUTO_EXTENSION:** `YES`

4. Click **Rarely Used** under RMX Management.
5. Click **IP Network Services > IP Network**.
6. On the **Gatekeeper** tab, create and configure an H.323 IP service with Communication Manager settings, such as the C-LAN IP address.
The MCU prefix and aliases must match the dial plan configured on Communication Manager. Ensure that the MCU Prefix is unique and that the prefix numbers are not identical to the starting digits of endpoints or aliases. Using a status signaling group, confirm that Polycom RMX has registered.
7. In the **Default Video Properties** dialog box, configure the conference profile with the line rate, codec settings, and the high definition video switching option. Multiple meeting rooms use this profile.
8. Create a meeting room to use a test direct dial conference ID.

Administering Adhoc video conferencing for the Polycom video conferencing bridge

1. Enter `display system-parameters customer-options` to verify the Maximum Administered Ad-hoc video Conferencing Ports (page 2 of screen). The maximum number of Ad-hoc video conferencing ports allowed is the sum of the ports on your RMX systems.
2. Enter `change cos` to set Ad-hoc video Conferencing (page 2 of screen) for the appropriate COS levels.
3. Use the `add video-bridge` command to configure a video bridge for the RMX system. Set the following parameters:
 - Name to the name for this video bridge, for example, Ad Hoc video Bridge - RMX.
 - Max Ports to the maximum number of Ad-hoc conferencing ports you want to assign to this bridge. (The minimum you can enter is 3.) This is equivalent to the number of ports for Ad-hoc use on the associated RMX. You can use Max Ports to limit the extent of Ad-hoc usage of an RMX and thereby reserve ports for scheduled usage.
 - Trunk Groups to the administered two-way ISDN H.323 trunk groups you added. All entries must be of the same carrier type (that is, all H.323 trunks).
 - **Far End Resource Info** :y
 - ID Range to the range of ports. The IDs you specify on this form must NOT be configured on the RMX. You must leave these IDs free for the factory to create its own conferences there. Note that AAR and UDP are not used to connect to these meeting room numbers. Conference IDs (and factory numbers) are completely independent of the dial plan.
 - Priority Factory Number. This number represents the Entry Queue created on the RMX and corresponds to a priority conference service level (for example, 784 Kbps). The Priority Factory Number must NEVER be in the conference ID range. If this field is left blank, all conferences can use the bridge. However, priority conferences will try to find a video bridge that has a priority factory (if there is one).
 - Standard Factory Number. This number represents the Entry Queue created on the RMX and corresponds to a standard conference service level (for example, 384 Kbps). The Standard Factory Number must NEVER be in the conference ID range. If this field is left blank, non-priority conferences cannot use this video bridge. A conference started by a priority user with non-priority users may be moved to a priority bridge, and the non-priority users will connect to it and receive video.

Note:

You must specify either a Priority Factory Number or a Standard Factory Number. Do not leave

- both fields blank.
4. Create conference profiles for Ad-hoc (and Meeting Room) style conferences.
Note:
 Ensure to choose Auto Layout under the video settings.
 5. Create the two entry queues (one for Ad-hoc conferences, and one for priority conferences).
 6. For the Conference IVR Service, perform the following steps:
 - Under the **Welcome** tab, disable the **Enable Welcome Messages** check box.
 - Under the **Conference Chairperson** tab, disable the **Chairperson messages** check box.
 - Under the **Conference Password** tab, disable the **Enable Password Messages** check box.
 7. Under the **General** tab, perform the following steps:
 - Deselect any .wav file for the first to Join announcement.
 - Disable roll call.
 - Disable click and view.
 - Under the **IVR Service** tab, click the music icon and set a silence .wav file as the IVR message. A silence .wav file will disable music from being played to the first party who joins the conference. To create a silence .wav file:
 - Open the Windows Sound Recorder application.
 - From the **File** menu, select **Save As**.
 - In the **Save As** dialog box, click **Change**.
 - In the **Name** box, enter `silence.wav`.
 - From the **Format** box, select **PCM**.
 - From the **Attributes** box, select 16.00 kHz, 16 Bit, Mono.
 - Click **OK**.

Displaying capacity of Communication Manager for Adhoc video conferencing

1. Use the `display capacity` command to access the System Capacity form.
2. Go to page 7. Ad-hoc video Conferencing Ports displays the following Ad-hoc video conferencing information:
 - **Used:** The number of video conferencing ports currently in use.
 - **Available:** The number of video conferencing ports currently available.
 - **System Limit:** The total number of video conference ports in your system. (This is the sum of Used ports and available ports)

Administering an H.323 trunk between Communication Manager and Polycom DMA

Adding Communication Manager as an external gatekeeper

1. In a Web browser, navigate to the home page of Polycom DMA.
2. Click **Network > External Gatekeeper**.
3. To add Communication Manager as an external gatekeeper, on the left pane, click **Add**.
4. The user interface opens the Add External Gatekeeper page.
5. On the Edit External Gatekeeper page, select **Enabled**, and enter values for:
 - **Name:** *<name of Communication Manager>*
 - **Address:** *<IP address of Communication Manager Procr or CLAN used for the H.323 trunk >*
 - **RAS port:** 1719
 - **Prefix range:** *<appropriate prefix to route Polycom sourced calls to Avaya endpoints>*

6. If you want Polycom DMA remove the prefix digits during the egress processing to Communication Manager, select **Strip Prefix**.
7. Select **Prefer Routed**.
Do not enable **Authentication mode**.
8. Click **OK**.

Administering the call settings for Communication Manager

1. Click **Admin > Call Server > Call Server Settings**.
The user interface opens the Call Server Settings page.
2. In the **H.323 Settings** section, enter values for:
Gatekeeper call mode: `Routed call mode`
3. Click **Update**.

Administering a direct routing gatekeeper

This section describes how to configure direct routing gatekeepers, such as SE200, PathNavigator, and Polycom CMA.

Prerequisites

Before administering a direct routing gatekeeper, note the following recommendations:

- Calls from Communication Manager to the direct routing gatekeeper must route through an outbound route pattern, ISDN tie trunk group, and H.323 LRQ signaling group.
- Calls from the direct routing gatekeeper to Communication Manager must route through a second incoming ISDN tie trunk group and either one incoming H.323 signaling group with an unspecified far-end or many incoming-per-cept H.323 signaling groups.
- Dial plan analysis, UDP, and AAR analysis must route the direct routing gatekeeper extension range to the outbound trunk group.
- Communication Manager must manage the direct routing gatekeeper inter-gatekeeper LRQ administration for extensions.
- Ensure that you have the following information:
 - The IP codec sets that you want to use
 - The IP network regions that you want to use
 - The IP address of the IP board of the gatekeeper

Adding an entry for the direct routing gatekeeper in the IP Node Names screen

1. On the SAT screen, type `change node-names ip` and set the following parameters:
 - **Name:** The name of the system.
 - **IP Address:** The IP address of the IP board of the system.
2. Go to IP Codec set screen and set the following parameters on page 2:
 - **Allow Direct-IP Multimedia:** `Y`
 - **Maximum Call Rate for Direct-IP Multimedia:** This parameter represents the combined audio and video transmission rate or receive rate for normal video calls. Use this setting to limit the amount of bandwidth used for normal video calls. For example, if you select 384 Kbps, the audio stream and video stream of normal video calls will not exceed a maximum bandwidth usage of 384 Kbps.
 - **Maximum Call Rate for Priority Direct-IP Multimedia:** This parameter represents the combined audio and video transmission rate or receive rate for priority video calls. Use this

setting to limit the amount of bandwidth used for priority video calls. For example, if you select 384 Kbps, the audio and video stream of priority video calls will not exceed a maximum bandwidth usage of 384 Kbps.

3. To administer the gatekeeper in its own network region, on the SAT screen, type `change ip-network-region <region number>` and set the following parameters:

- **Intra-region IP-IP Direct Audio:** Y
 - If the customer configuration uses only Polycom HDX endpoints registered to the Polycom CMA gatekeeper, set Intra-region IP-IP Direct Audio to Y.

Adding signaling groups to the direct routing gatekeeper

1. On the SAT screen, type `add signaling-group <signaling group>` and set the following parameters to add an outbound signaling group:

- **Group Type:** H.323
- **IP Video:** Y
- **Priority Video:** Y

Note:

If you set Priority Video to Y, all incoming calls receive priority video transmissions.

- **Near-end Listen Port:** 1719
- **LRQ Required:** Y
- **RRQ Required:** N
- **Far-end Node Name:** The name of the system
- **Far-end Listen Port:** 1719
- **Direct IP-IP Audio Connections:** Y
- **IP Audio Hairpinning:** N

Adding trunk groups to the direct routing gatekeeper

1. On the SAT screen, type `add trunk-group <trunk group>`, and set the following parameters to add an outbound trunk group:

- **Group Type:** ISDN
- **Carrier Medium:** IP

On page 1 of the Trunk Group screen, add members to the trunk group.

Modifying signaling groups to the direct routing gatekeeper

1. On the SAT screen, type `change signaling-group <chosen signaling group>`, and set the following parameter to modify an outbound signaling group:

Trunk Group for Channel Selection: The trunk group

Creating a route pattern for the direct routing gatekeeper

To create a route pattern that points to the trunk group, on the SAT screen, type `change route-pattern <route patten>` and set the following parameter:

Grp No: The number of the trunk group

Adding an H.323 video signaling group

1. On the SAT screen, enter `add signaling-group <chosen signaling group>` and set the following parameters:
 - **Group Type:** H.323
 - **LRQ Required:** Y
 - **RRQ Required:** N
2. For endpoints that do not support third-party pause, include the signaling group in an IP network region and set the following parameter:
direct-ip inter-region: Disabled

Modifying the inbound trunk group to the direct routing gatekeeper

Modify the inbound trunk group to include one trunk member for each endpoint that the direct routing gatekeeper manages.

The following table provides an example of a signaling trunk group

Group Number	51
Group Type	h.323
Remote Office	N
Max number of NCA TSC	0
SBS	N
Max number of CA TSC:	0
IP Video	Y
Priority Video	Y
Trunk Group for NCA TSC	—
Trunk Group for Channel Selection	51
TSC Supplementary Service Protocol	A
Network Call Transfer	N
T303 Timer(sec)	10
H.245 DTMF Signal Tone Duration(msec)	—
Near-end Node Name	Procr
Far-end Node Name	CMA4000
Near-end Listen Port	1719
Far-end Listen Port	1719
Far-end Network Region	2
LRQ Required	Y
Calls Share IP Signaling Connection	N
RRQ Required	N
Media Encryption	N
Bypass If IP Threshold Exceeded	N
H.235 Annex H Required	N
DTMF over IP	out-of-band
Direct IP-IP Audio Connections	Y
Link Loss Delay Timer(sec)	90

IP Audio Hairpinning	N
Enable Layer 3 Test	N
Interworking Message	PROGress
H.323 Station Outgoing Direct Media	N
DCP/Analog Bearer Capability	3.1kHz
Setp	—

Appendix A Interoperability recommendations

This section describes the setup required for interoperability between Avaya Aura® and Scopia. The routing administration tasks in this document refer to identifying extension ranges as a part of the prerequisites. The minimum number of required group of extensions is categorized as:

- Radvision meeting room IDs or extensions
- Avaya Aura® video endpoints
- Avaya Aura® audio endpoints

Session Manager routing

- Create a dial plan to set up SIP-based video endpoint calls to the Scopia Elite MCU through the SIP trunk to the Scopia B2BUA component.
- Create a dial plan to set up SIP-based video endpoint calls, which originate from Session Manager, to Radvision H.323 endpoints through the SIP trunk to Communication Manager. These calls connect to Scopia ECS Gatekeeper through the H.323 trunk of Communication Manager.

Communication Manager routing

- Create a dial plan to set up Avaya Aura® calls to Radvision H.323 video endpoints through the H.323 trunk to Scopia ECS Gatekeeper.
- Create a dial plan to set up Avaya H.323 video endpoint calls to the Scopia Elite MCU through the H.323 trunk to Scopia ECS Gatekeeper.

Avaya Aura® endpoints and Radvision endpoints routing

Assign stations with contiguous extensions to each group of endpoints. Contiguous extensions ensure that the starting digits of the extensions are common. You can specify routes using these common digits as a prefix.

For example, if extensions contain seven digits, and you assign extension 555-2222 and extension 555-2224 to endpoints in the same group, do not assign extension 555-2223 to an endpoint in a different group. This method of assigning contiguous extensions ensures that you can use 555-22xx as a prefix for a dial plan.

Scopia Elite MCU routing

Assign a range of meeting room extensions to the Scopia Elite MCU that is not contiguous with other endpoint extensions. Assigning contiguous extensions ensures that you can administer a generic routing prefix for Scopia Elite MCU meeting room extensions.

Appendix B Advanced administration

The procedures for advanced administration in this section might not be applicable to all configurations. You must perform these procedures in the Communication Manager SAT interface.

Stripping the prefix of the dialed number for an H.323 call to Communication Manager

1. Log in to the Communication Manager SAT interface as a user with craft level permissions.
2. On the SAT screen, type `change inc-call-handling-trmt trunk-group <Trunk group number of Scopia ECS Gatekeeper>`
3. Enter the following details of the number of the incoming call:
 - **Number length**
 - **Digits**
 - **Digits to delete**
 - **Digits to insert**
4. **Submit** the form.

Partition routing

1. Log in to the Communication Manager SAT interface as a user with craft level permissions.
2. To specify the route for the dialed string to a partition table in the ARS Digit Analysis table, on the SAT screen, type `change ars analysis <Digits entered in Step 5 of Creating and editing dial plans for Scopia ECS Gatekeeper>`.
Note: If your system uses AAR analysis routing, make the changes in the AAR analysis table by using `change aar analysis <Digits entered in Step 5 of Creating and editing dial plans for Scopia ECS Gatekeeper>`.
3. In the **Route Pattern** field, specify `p<partition-route-table number>`.
4. To specify the routing pattern for the corresponding partition group number in the partition routing table, on the SAT screen, type `change partition-route-table <route-pattern number>`.
For example, assign the number of the H.323 trunk to Scopia ECS Gatekeeper to Partition Group Number 1 (PGN 1) and assign the number of the SIP trunk to Session Manager to Partition Group Number 2 (PGN 2). PGN 1 represents the H.323 trunk to Scopia ECS Gatekeeper, and PGN 2 represents the SIP trunk to Session Manager.
5. To distinguish stations that establish calls through the H.323 trunk to Scopia ECS Gatekeeper and the SIP trunk to Session Manager, on the SAT screen, type `change cor <partition group number>`.
For example, assign COR 1 to PGN 1, and assign COR 2 to PGN 2.
6. To ensure that a call route is set up either through the H.323 trunk to Scopia ECS Gatekeeper or the SIP trunk through Session Manager to the Scopia B2BUA component, assign COR to a station.
For example, to ensure that all H.323 video endpoints connect to Scopia ECS Gatekeeper through the H.323 trunk, assign COR 1 to all H.323 video endpoints. To ensure that all SIP video endpoints connect to the Scopia B2BUA component through the SIP trunk to Session Manager, assign COR 2 to all SIP video endpoints.

For more information about partition routing, see *How to administer ARS partitions* in *Administering Avaya Aura® Communication Manager* on the Avaya support website at <http://www.avaya.com/support>.

Appendix C Troubleshooting

The following table lists the troubleshooting details of the issues that you might face due to incorrect configurations.

Issue	Symptom	Details	Resolution
DNS FQDN name vs. SIP domain in Scopia Management	An outgoing SIP call from the Scopia Elite MCU logged in to the Scopia B2BUA component connects to the Avaya SIP endpoint but disconnects after a short duration of approximately 30 seconds.	If the Scopia B2BUA component is configured with an FQDN that does not exist in DNS, and other components use the IP address to connect, the call initially connects, but the call disconnects after a short duration because of the mismatch in IP addresses.	Configure a valid FQDN for the Scopia B2BUA component that is registered in DNS.
Outgoing calls from the H.323 trunk or the SIP trunk of Scopia Management to Avaya Aura [®] do not connect	Outgoing calls from the H.323 trunk or the SIP trunk of Scopia Management to Avaya Aura [®] do not connect.	The call trace displays that call traffic does not transmit to Avaya Aura [®] .	For the H.323 protocol, ensure that the prefix is correctly configured in Scopia ECS Gatekeeper. For the SIP protocol, ensure that the SIP protocol configuration is entered in Scopia Management.
Only one-way calls based on the H.323 protocol connect	Calls from Scopia ECS Gatekeeper to Communication Manager do not connect.	The call trace displays that the call is set up on the route between Scopia ECS Gatekeeper and Communication Manager but the call does not connect.	Review the following configuration: • The signaling group contains the correct trunk number. • The total number of trunk members is not exhausted. • If required, the prefix in the number of the call is correctly stripped.
DTMF does not work in Avaya Aura [®]	Using DTMF from the approved video endpoints that are logged in to Avaya Aura [®] does not work.	For example, users cannot join a conference on the Scopia Elite MCU by entering a conference ID or PIN.	Review the following configuration: • For the H.323 trunk from Communication Manager to Scopia ECS Gatekeeper, the DTMF over IP field is configured to <i>Out-of-</i>

Issue	Symptom	Details	Resolution
			<i>band.</i> For the SIP trunk between Session Manager and Communication Manager, the DTMF over IP field is configured to <i>rtp-payload</i>.
No video among Avaya Aura [®] endpoints, Radvision endpoints, and the Scopia Elite MCU	When calling from a video endpoint registered to Avaya Aura [®] , video is not available.	Video is not available on Avaya endpoints.	Review the following configuration: - The IP Video field on the H.323 trunk between Communication Manager and Scopia ECS Gatekeeper. - The Direct-IP Multimedia field on the ip-codec-set used for the call. - System license for video. Verify the Multimedia entries on Page 4 of the <i>system-parameters customer-options</i> on the Communication Manager SAT interface.
No communication between Session Manager and Scopia Management	Calls from the SIP trunk of Scopia Management to Avaya Aura [®] do not connect.	The call trace displays that call traffic does not transmit between Session Manager and Scopia Management.	Review the following configuration: - Server that hosts Scopia Management - Firewall settings on server that hosts Scopia Management - SIP trunk between Session Manager and Scopia Management