Avaya Aura® Communication Manager Release 6.2 and Radvision SCOPIA Release 7.7 Interoperability

Day 90 Solution Quick Setup

Issue 1
September 2012

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

1.0 Introduction

This quick start document provides information about basic administration tasks required for interoperability between Avaya Aura® Communication Manager Release 6.2 and the Radvision SCOPIA solution Release 7.7.

For more information about basic administration tasks, see *Avaya Video Conferencing Solution Networking Guide Release 6.0* at the Avaya Support website: http://support.avaya.com.

1.1 Intended audience

This document is intended for system administrators who install video equipment for Avaya Aura® and Radvision SCOPIA.

1.2 Components

The following table lists the components of Avaya Aura® and Radvision SCOPIA:

Type of component	**Avaya Aura®**	**Radvision SCOPIA**
Infrastructure	Communication Manager Release 6.2 Avaya Aura® Session Manager Release 6.2 Avaya Aura® System Manager Release 6.2	SCOPIA iVIEW Management Suite Release 7.7 SCOPIA Enhanced Communication Server (ECS) Gatekeeper SCOPIA Elite MCU Release 7.7 SCOPIA Desktop Server Release 7.7 SCOPIA PathFinder Release 7.7
Endpoints	Avaya 1000 series video endpoints Avaya Desktop Video Device Avaya Flare® Communicator for iPad Avaya one-X® Communicator Avaya 96xx series Avaya 96x1 series	SCOPIA XT1200 SCOPIA XT4200 SCOPIA XT5000 SCOPIA VC240 SCOPIA Desktop SCOPIA Mobile

Note:

- Radvision endpoints involved in this interoperability solution are based on the H.323 protocol.
- Users of analog and DCP endpoints must dial in to SCOPIA Elite MCU conference rooms through external numbers. For example, users must dial *9* to access an external PSTN trunk, and then, dial the external SCOPIA Elite MCU conference room number.
- Installation of SCOPIA PathFinder is optional.
- Installation of SCOPIA Desktop Server is optional. This server is required only if you install SCOPIA Desktop or SCOPIA Mobile.
- Installation of the optional components of Radvision SCOPIA depends on the configuration of the solution.
- The following Radvision SCOPIA components can either co-exist on the same server or as separate instances on multiple servers for increased capacity and as a distributed configuration.
    - SCOPIA iVIEW Management Suite
    - SCOPIA ECS Gatekeeper

  For more information about these Radvision SCOPIA components, see the Radvision SCOPIA documents listed in Related documents.
- The following users cannot create virtual meeting rooms through SCOPIA Desktop Server:
    - Guest user on Radvision SCOPIA Desktop

    - Avaya one-X® Communicator user
    - Avaya 1000 series endpoint user
- For more information about compatible versions of the Avaya Aura® Release 6.2 components and the Radvision SCOPIA Release 7.7 components, see the product support notice *Avaya Aura® Core 6.2 Interoperability Compatibility with the Radvision SCOPIA 7.7 Solution* at the Avaya Support website: http://downloads.avaya.com/css/P8/documents/100162905.
- For more information about how to apply service packs and how to install hot fixes to update the software of the Radvision SCOPIA Release 7.7 components, see Release Notes at the Radvision support website; http://support.radvision.com.

1.3 Prerequisites

Before you perform basic administration tasks for interoperability between Avaya Aura® and Radvision SCOPIA:

Ensure that you install the following components:

- Communication Manager Release 6.2 SP 13
- System Manager Release 6.2
- Session Manager Release 6.2
- SCOPIA iVIEW Management Suite Release 7.7
- SCOPIA Elite MCU Release 7.7
- SCOPIA Desktop Release 7.7
- SCOPIA PathFinder Release 7.7
- Avaya endpoints and endpoint interfaces
- Radvision endpoints and endpoint interfaces

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

Ensure that you are familiar with the following administration tasks:

- Session Manager administration through System Manager including administration of the following components:
    - SIP domains
    - SIP entities
    - SIP entity links
    - Locations
    - Routing
    - Dial patterns
- Communication Manager administration tasks including administration of the following:
    - Signaling groups
    - Trunk groups
    - Dial plans
    - AAR/ARS routing

1.4 Related documents

For more information about basic administration tasks, see the following documents:

- *Administering Avaya Video Conferencing Solution – Advanced Topics Release 6.1* at the Avaya support website: http://support.avaya.com.
- Radvision SCOPIA Solution Guide
- Radvision SCOPIA iVIEW Management Suite

- Radvision SCOPIA ECS
- Radvision SCOPIA Desktop Server
- Radvision SCOPIA XT1000 Series
- Radvision SCOPIA XT4200/XT5000
- Radvision SCOPIA VC240
- Radvision SCOPIA Elite MCU
- Radvision SCOPIA PathFinder

2.0 Overview

Interoperability between Avaya Aura® and Radvision SCOPIA includes the following two trunks:

- H.323 trunk between Communication Manager and SCOPIA ECS Gatekeeper

  Point-to-point calls between Avaya endpoints and Radvision endpoints connect through the H.323 trunk. Conference calls hosted on the SCOPIA Elite MCU that involve Avaya endpoints based on the H.323 protocol connect through the H.323 trunk.

- SIP entity link between Session Manager and SCOPIA ECS Gatekeeper

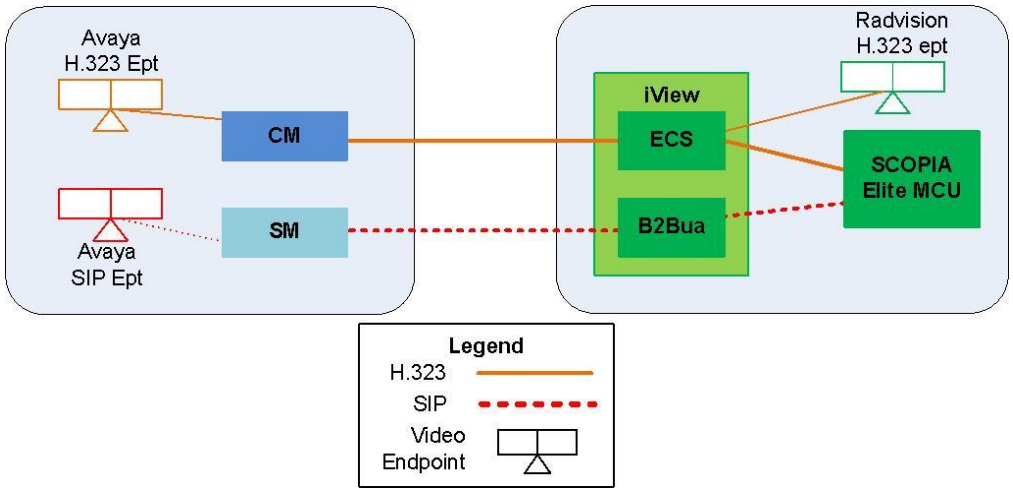
  Conference calls hosted on the SCOPIA Elite MCU that involve Avaya endpoints based on the SIP protocol connect through the SIP entity link.

Create route partitions to ensure that SIP-based calls establish through the SIP entity link and H.323-based calls establish 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, such as a SCOPIA Elite MCU meeting room, see Partition Routing.

Figure 1 Interconnectivity between Avaya Aura® and Radvision SCOPIA illustrates how Avaya Aura® connects with Radvision SCOPIA.

Figure 1 Interconnectivity between Avaya Aura® and Radvision SCOPIA



2.1 Interoperability recommendations

Administer the following setup for interoperability between Avaya Aura® and Radvision SCOPIA.

The routing administration tasks in this document refer to identifying extension ranges as part of the prerequisites. The minimum number of required group of extensions is categorized as:

- Radvision H.323 endpoints
- Radvision meeting room IDs or extensions
- Avaya Aura® endpoints

Session Manager routing

- Create a dial plan to set up SIP-based video calls to the SCOPIA Elite MCU through the SIP entity link to the B2BUA component of SCOPIA iVIEW Management Suite.

- Create a dial plan to set up SIP-based video calls to Radvision SCOPIA endpoints based on the H.323 protocol through the SIP entity link to Communication Manager.

Communication Manager routing

- Create a dial plan to set up calls to Radvision H.323 video endpoints through the H.323 trunk to SCOPIA ECS Gatekeeper.

- Create a dial plan to set up 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 7 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 that is not contiguous with other extensions to the SCOPIA Elite MCU. Assigning extensions that are not contiguous with other extensions ensures that you can administer specific routing for virtual meeting rooms.

3.0 Administering Communication Manager to communicate with SCOPIA ECS Gatekeeper using the H.323 protocol

The following procedures describe the administration steps 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 must be configured. Retain the default values for other fields.

3.1 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>

3.2 Adding a node name for SCOPIA ECS Gatekeeper

1. Click **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.

3.3 Adding an H.323 signaling group for SCOPIA ECS Gatekeeper

1. Click **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

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.

3.4 Adding an H.323 trunk group for SCOPIA ECS Gatekeeper

1. Click **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:
   These values on Page 1 are specific to the Radvision SCOPIA 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 a signaling group to the H.323 trunk group for SCOPIA ECS Gatekeeper

1. Click **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*>

Configuring a text string to replace the incoming numbers of restricted calls and unavailable calls to the H.323 trunk group of SCOPIA ECS Gatekeeper

1. Click **Communication Manager > Parameters > System Parameters – Features**.

2. On Page 9, enter values for the following fields:
   - **CPN/ANI/ICLID Replacement for Restricted Calls**: <*Text string*>
   - **CPN/ANI/ICLID Replacement for Unavailable Calls**: <*Text string*>

3. 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.

3.5 Adding a route pattern for SCOPIA ECS Gatekeeper

1. Click **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.

3.6 Creating and editing dial plans for SCOPIA ECS Gatekeeper

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

1. Click **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 that has rows available, 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 on **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 that has rows available, 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 **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 that has rows available, 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.

4.0 Administering Session Manager to communicate with the B2BUA component of SCOPIA iVIEW Management Suite using the SIP protocol

The following procedures describe the administration steps 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.

4.1 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>

4.2 Adding a SIP entity for the B2BUA component of SCOPIA iVIEW Management Suite

1. Click **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 B2BUA component of SCOPIA iVIEW Management Suite>*
   - **TYPE**: SIP Trunk
   - **Adaptation**: *<Depending on the dial plan of the system, create and select an adaptation>*
   - **Location**: *<Location of the B2BUA component of SCOPIA iVIEW Management Suite>*
   - **Time Zone**: *<Time zone of the location of the B2BUA component of SCOPIA iVIEW Management Suite>*

4. To submit, click **Commit**.

4.3 Adding a SIP entity link for the B2BUA component of SCOPIA iVIEW Management Suite

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 B2BUA component of SCOPIA iVIEW Management Suite>*
   - **Port**: 5060

4. To submit, click **Commit**.

4.4 Adding routing policies for the B2BUA component of SCOPIA iVIEW Management Suite

1. Click **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 B2BUA component of SCOPIA iVIEW Management Suite, and click **Select**.

6. To submit, click **Commit**.

4.5 Adding dial patterns for the B2BUA component of SCOPIA iVIEW Management Suite

1. Click **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**.

5.0 Administering SCOPIA iVIEW Management Suite to communicate with Avaya Aura®

The following procedures describe the administration steps to add the following trunks:

- H.323 trunk between SCOPIA ECS Gatekeeper and Communication Manager
- SIP entity link between the B2BUA component of SCOPIA iVIEW Management Suite and Session Manager.

5.1 Logging in to SCOPIA iVIEW Management Suite

To log in to SCOPIA iVIEW Management Suite, in the browser address bar, enter the SCOPIA iVIEW Management Suite FQDN in the following format:

http://<FQDN_or_IP_of_iVIEW>:<port>/icm

Note:
Unless specified in the SCOPIA iVIEW Management Suite installation, the default port is 8080.

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

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>*
   - **Management IP Address**: *<IP address of the procr or CLAN of Communication Manager>*
   - **Model**: Other Model
   - **Protocol**: H.323
     Note:
     Do not add the zone prefix in this step. Add the prefix in the subsequent steps.

4. To submit, click **OK** at the bottom of the screen.
   SCOPIA iVIEW Management Suite 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.

5.3 Adding a SIP entity link from the B2BUA component of SCOPIA iVIEW Management Suite to Session Manager

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>*
   - **Management IP Address**: *<IP address of the SIP entity of Session Manager>*
   - **Model**: Other Model
   - **Protocol**: SIP
   - **Port**: 5060

- **Transport type**: TCP
- **SIP Domain**: <*SIP domain configured in System Manager*>

4. To submit, click **OK**.

6.0 Advanced administration

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

6.1 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.

6.2 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>*.

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 H.323 trunk number to Partition Group Number 1 (PGN 1) and assign the SIP entity link number to Partition Group Number 2 (PGN 2). PGN 1 represents the H.323 trunk, and PGN 2 represents the SIP entity link.

5. To distinguish stations that establish calls through the H.323 trunk and the SIP entity link, 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 or the SIP entity link of SCOPIA iVIEW Management Suite, 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 B2BUA component of SCOPIA iVIEW Management Suite through the SIP entity link, 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: http://www.avaya.com/support.

7.0 Troubleshooting

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

Issue	Symptom	Details	Resolution
DNS FQDN name vs. SIP domain in SCOPIA iVIEW Management Suite	An outgoing SIP call from the SCOPIA Elite MCU logged in to the B2BUA component of SCOPIA iVIEW Management Suite connects to the Avaya SIP endpoint but disconnects after a short duration of approximately 30 seconds.	If the B2BUA component of SCOPIA iVIEW Management Suite 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 B2BUA component of SCOPIA iVIEW Management Suite that is registered in DNS.
Outgoing calls from the H.323 trunk or the SIP entity link of SCOPIA Management iVIEW Suite to Avaya Aura® do not connect	Outgoing calls from the H.323 trunk or the SIP entity link of SCOPIA iVIEW Management Suite 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. Review the following procedures: • Administering Communication Manager to communicate with SCOPIA ECS Gatekeeper using the H.323 protocol • Stripping the prefix of the dialed number for an H.323 call to Communication Manager For more information about the resolution of this issue, see *How to access the gatekeeper to check the values* in the SCOPIA ECS Gatekeeper document. For the SIP protocol,

			ensure that the SIP protocol configuration is entered in SCOPIA iVIEW Management Suite. Review the following procedures: • Administering Session Manager to communicate with the B2BUA component of SCOPIA iVIEW Management Suite using the SIP protocol • Adding a SIP entity link from the B2BUA component of SCOPIA iVIEW Management Suite to Session Manager
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 *Out-of-band*.

			• For the SIP entity link between Session Manager and Communication Manager, the DTMF over IP field is configured to *rtp-payload*.
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 *system-parameters customer-options* on the Communication Manager SAT interface.