Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Conferencing 7.2 and Radvision SCOPIA Elite MCU – Issue 1.0

Abstract

These Application Notes describe the configuration of Avaya Aura® Conferencing 7.2 and Radvision SCOPIA Management 8.0.

- Avaya Aura® Conferencing 7.2 communicates with Radvision SCOPIA Management via a SIP trunk and Avaya Aura® Session Manager.
- The administration of a SIP trunk between Session Manager and SCOPIA Management.
- The administration of Subscriber data between Avaya Aura® Conferencing and Radvision SCOPIA components.
- The administration of Radvision SCOPIA Management with Avaya Aura® Conferencing

These Application Notes provide information for the setup, configuration, and verification of the call flows on this solution.

Table of Contents

1. Introduction

These Application Notes describe the administration tasks required to implement interoperability between Avaya Aura® Conferencing and Radvision SCOPIA.

Additional subscriber provisioning is not required on SCOPIA Management. Optionally, you can provision Avaya Aura® Conferencing subscribers as users on SCOPIA Manager. You can provision each of these subscribers with a unique virtual room.

Integration of Avaya Aura® Conferencing is a feature of SCOPIA Management. To configure interoperability between Avaya Aura® Conferencing and Radvision SCOPIA, you must perform several tasks.

Note: This document assumes that Avaya Aura® Conferencing, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and all Radvsion servers are network configured, administered and online.

2. Interoperability Testing

Interoperability testing is out of scope for this Application Note. This Application Note describes how to configure the SIP Link between Avaya Aura® Conferencing and Radvsion Scopia Elite MCU. Verification of The actual Interoperability Testing is covered in the following Application Note:

> Application Notes for Radvision Scopia® XT 5000 Series Endpoint with Multi Avaya Aura® Communication Manager and Multi Avaya Aura® Session Manager Integration

2.1. Test Description and Coverage

- See **Section 11 Use Cases**

3. Reference Configuration

The diagram below **Figure 1** shows Interoperability between Avaya Aura® and Radvision SCOPIA and illustrates how Avaya Aura® Conferencing connects with Radvision SCOPIA. The endpoints are displayed in the figure for display purposes only.

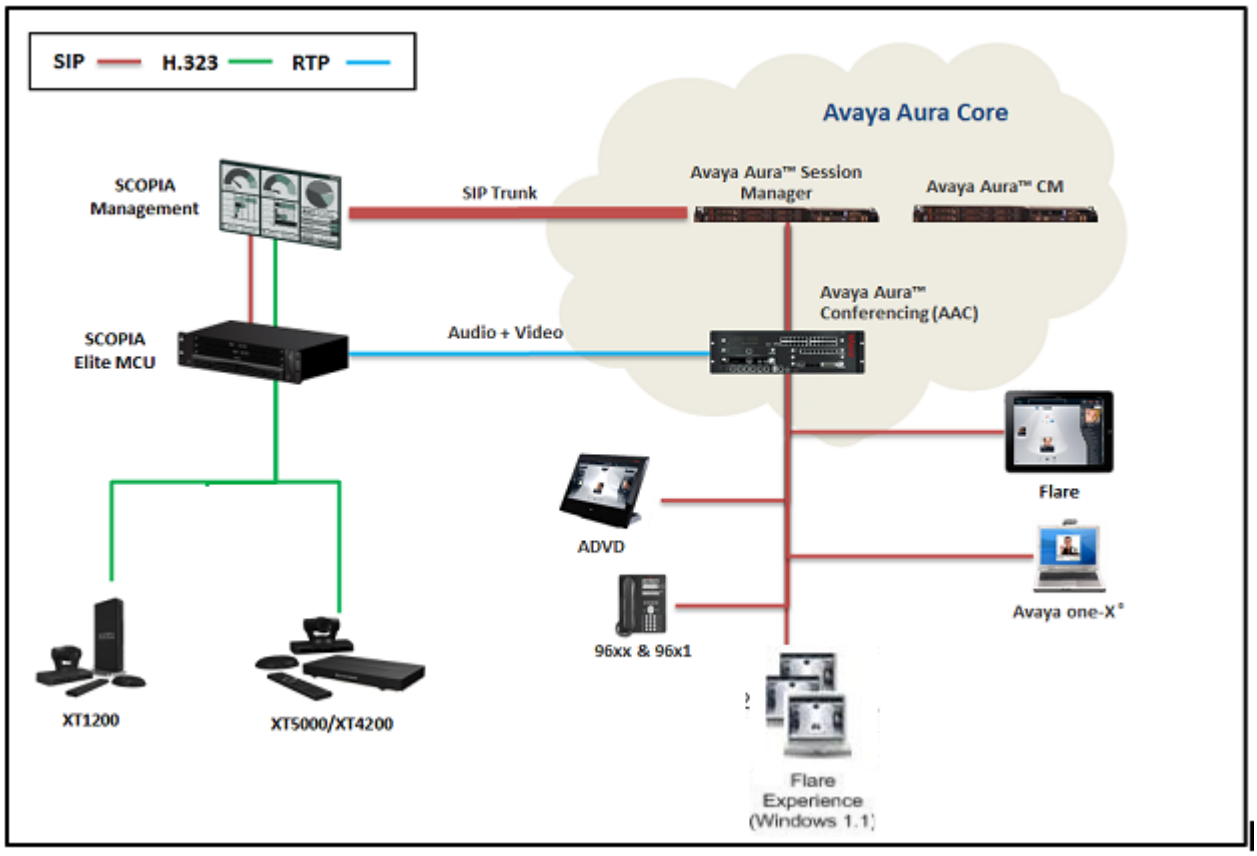


Figure 1: Interoperability between Avaya Aura® Conferencing and Radvision SCOPIA

4. Equipment and Software Validated

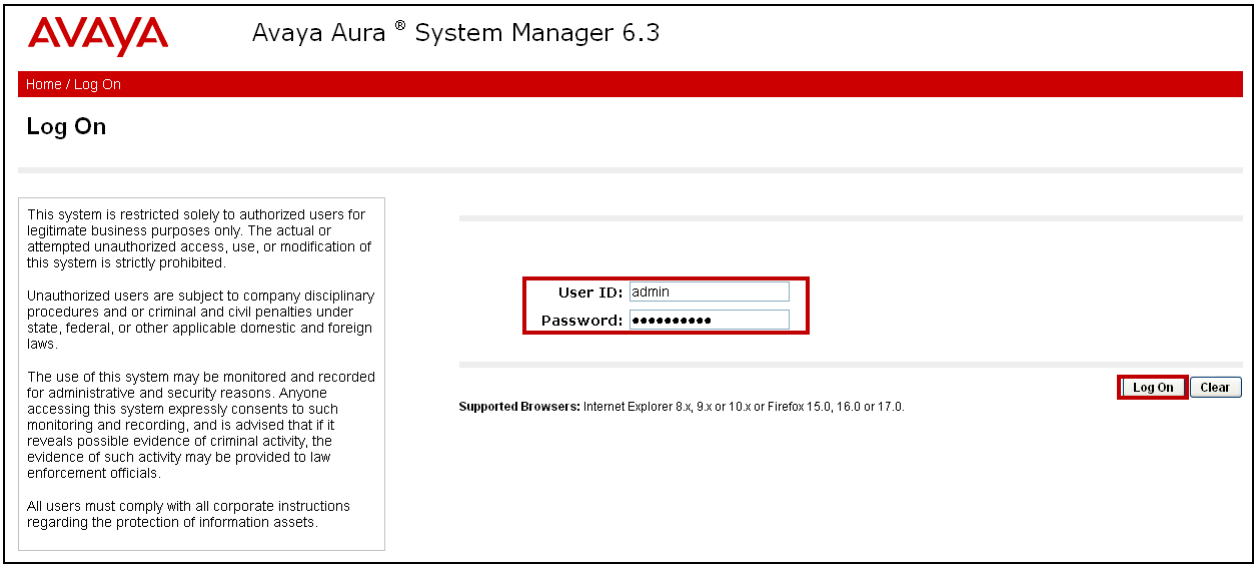
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Conferencing 7.2	MCP Platform Release Level : 17.0.6 (via patching) Linux Kernel Version: 2.6.18-308.24.1.el5 Version: MCP_17.0.4.00_2013-01-19-1429
Avaya Aura® Session Manager on Avaya S8800 server	Release 6.2 FP2 - 6.3.2.0.84005
Avaya Aura® System Manager on System Platform	Release 6.2 FP2 - 6.3.2.3.1275 System Platform – 6.3.0.0.17001
Avaya Aura® Communication Manager Evolution Server on System Platform	Release R016x.03.0.123.0 System Platform – 6.3.0.0.18002
SCOPIA Management/iView	Release 8.0.1.0.6.5
SCOPIA Elite MCU 5110	Release 7.7.3.9.0
Radvision XT4200 (H.323)	Release 3.01.01.0035
Radvision XT5000 (H.323)	Release 3.01.01.0035
Avaya Flare® Experience on iPad (SIP)	Release R1.1
Avaya Flare® Experience on Windows (SIP)	Release R1.1
Avaya Desktop Video Device	Release 1.1.2 Version: SIP_A175_1_1_2_020002
Avaya one-X® Communicator (SIP)	Release 6.1.7.04-SP7-39506
Avaya 96x1 (SIP)	6.3.0.54

5. Configure Avaya Aura® Session Manager

This section describes the procedures for configuring a SIP trunk between Avaya Aura® Session Manager and SCOPIA Management. These procedures describe the administration steps through System Manager. Depending on the configuration of your system, values of the parameters might differ.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL "**http://<ip-address>/SMGR**", where "**<ip-address>**" is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.



5.1. Adding a SIP Entity for Avaya Aura® Session Manager

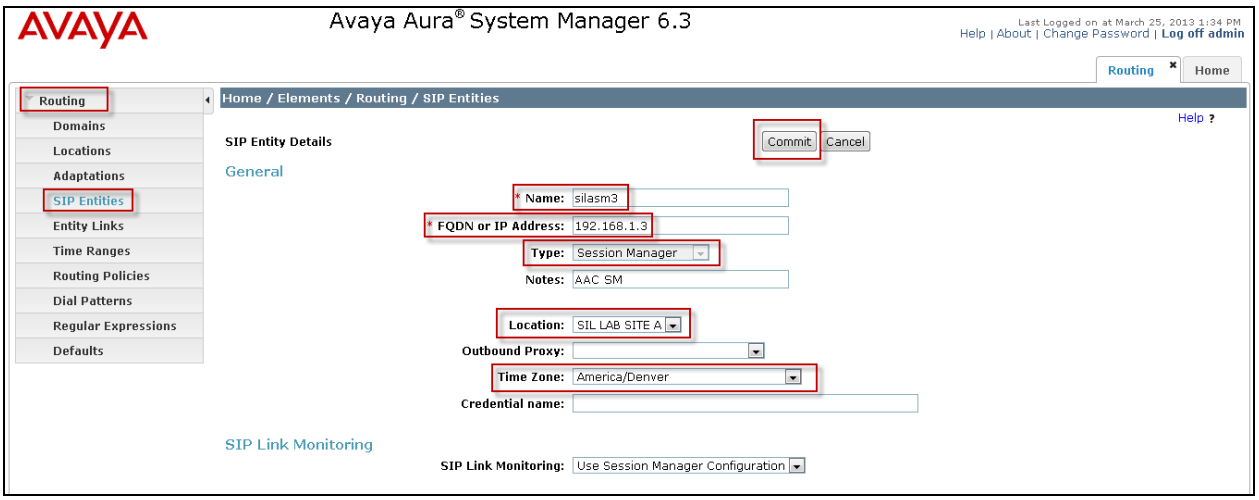
To add a SIP Entity, expand **Elements → Routing** and select **SIP Entities** from the left navigation menu (not shown).

Press **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for new SIP Entity. In the sample configuration "**silasm3**" was used.
- **FQDN or IP Address:** Enter FQDN or IP address of the signaling interface for Session Manager.
- **Type:** Select "**Session Manager**".
- **Location:** Select the applicable Location for Session Manager.
- **Time Zone:** Enter the Time Zone of the location of Session Manager.

Press **Commit** to save SIP Entity definition.

The following screen shows the SIP Entity defined for Session Manager.



5.2. Adding a SIP Entity for SCOPIA Management

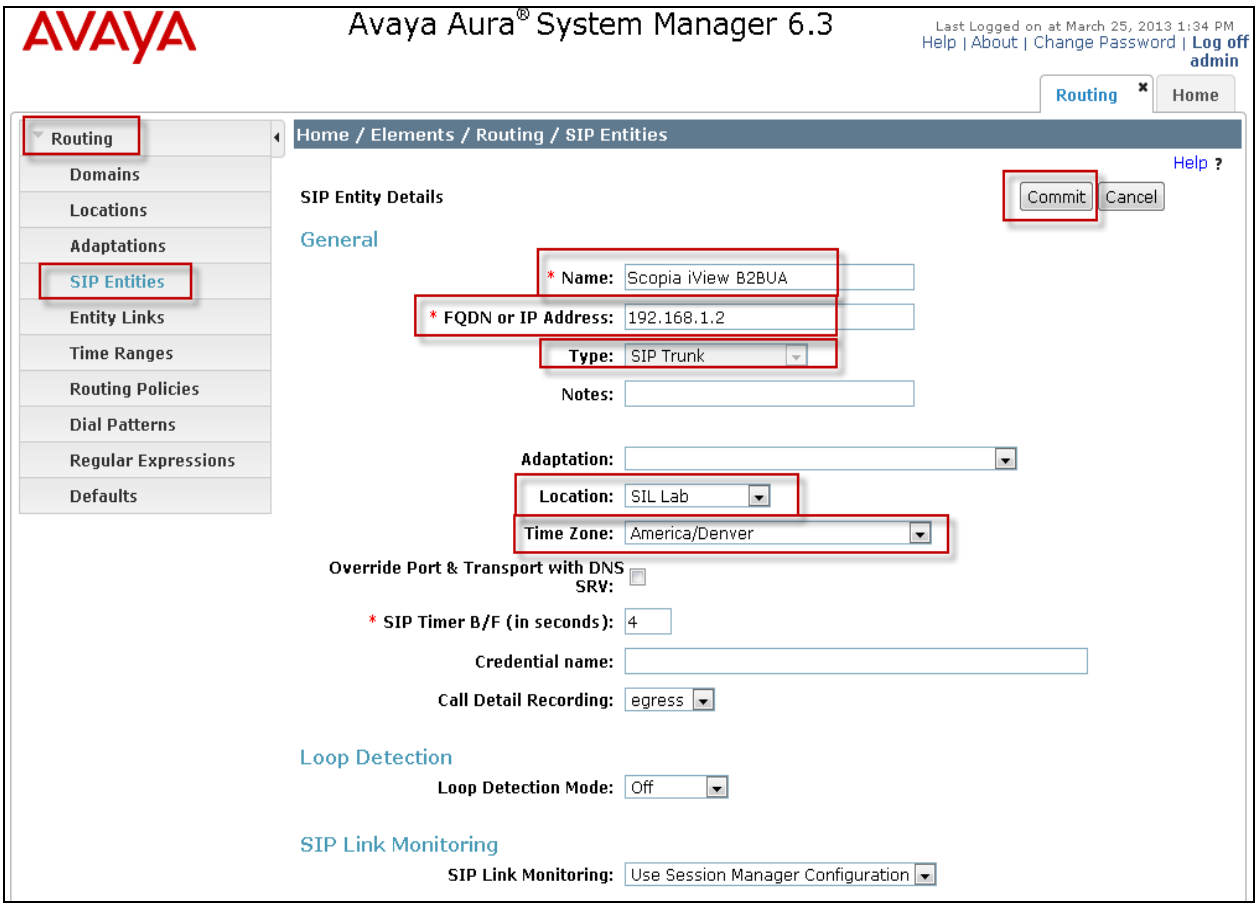
To add a SIP Entity, expand **Elements → Routing** and select **SIP Entities** from the left navigation menu (not shown).

Press **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for new SIP Entity. In the sample configuration "**Scopia iView B2BUA**" was used.
- **FQDN or IP Address:** Enter FQDN or IP address of the signaling interface for Scopia Management.
- **Type:** Select "**SIP Trunk**".
- **Location:** Select the applicable Location for Scopia Management.
- **Time Zone:** Enter the Time Zone of the location of Scopia Management.

Press **Commit** to save SIP Entity definition.

The following screen shows the SIP Entity defined for Scopia Management.



5.3. Adding a SIP Entity Link for SCOPIA Management

A SIP link between Session Manager and Scopia Management is described by an Entity Link. In the sample configuration, a SIP Entity Link was added between Avaya Aura® Session Manager server and Scopia Management server.

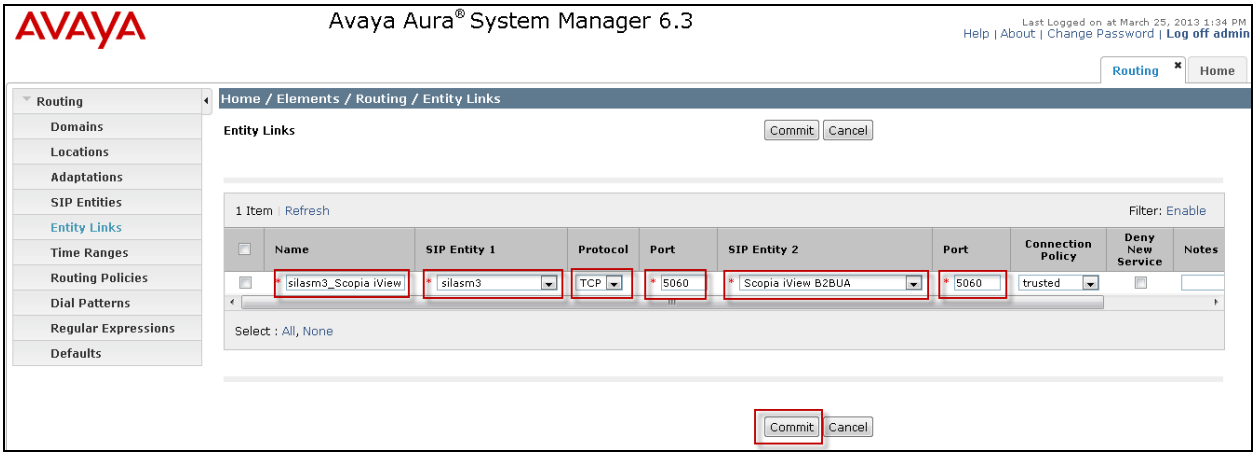
To add an Entity Link, expand **Elements → Routing** and select **Entity Links** from the left navigation menu.

Press **New** (not shown). Enter the following values**.**

- **Name** — Enter an identifier for the SIP entity link. In the sample configuration, "**silasm3_Scopia iView**" was used.
- **SIP Entity 1** — Select the SIP Entity for Session Manager defined in **Section 5.1** from the drop-down menu**.**
- **SIP Entity 2** — Select the SIP Entity for Scopia Management defined in **Section 5.2** from the drop-down menu.
- **Protocol** — After selecting both SIP Entities, verify "**TCP**" is selected as the required Protocol.
- **Port** — Verify **Port** for both SIP entities is "**5060**".
- **Policy** — Select "**Trusted"** from the drop-down menu.

Press **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Avaya Aura® Session Manager server and Scopia Management server.



6. Configure Radvision SCOPIA Management Release 8.0

This section provides the procedures for configuring the interoperability between Avaya Aura® Conferencing and Radvision Scopia Management. The procedures include the following areas:

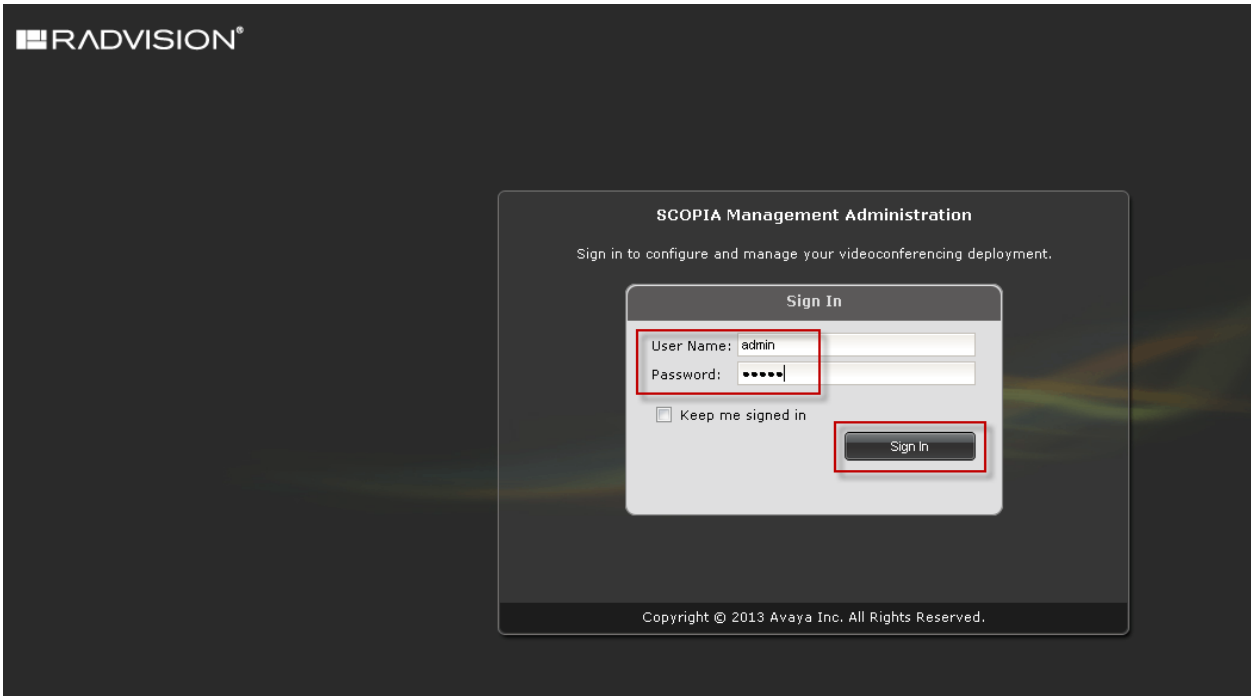
- Login to SCOPIA Management
- Configure the Avaya Aura® Conferencing integrations settings
- Configure the meeting types
- Configure the Session Manager SIP Entity Link on Scopia Management
- Configure the Subscriber Virtual Room
- Configure the Virtual Conference Room Prefix Translation
- Configure the Avaya Aura® Conferencing and Radvision Scopia Media Trunk Label
- Configure the Avaya Aura® Conferencing and Radvision Scopia Roster Label
- Configure the conference default domain
- Configure DNS on Radvision Elite MCU
- Enable the SIP P-Asserted-Identity header

6.1. Logging in to SCOPIA Management

To log in to SCOPIA Management, in the browser address bar, enter the SCOPIA Management Release 8.0 IP Address or FQDN in the following format:

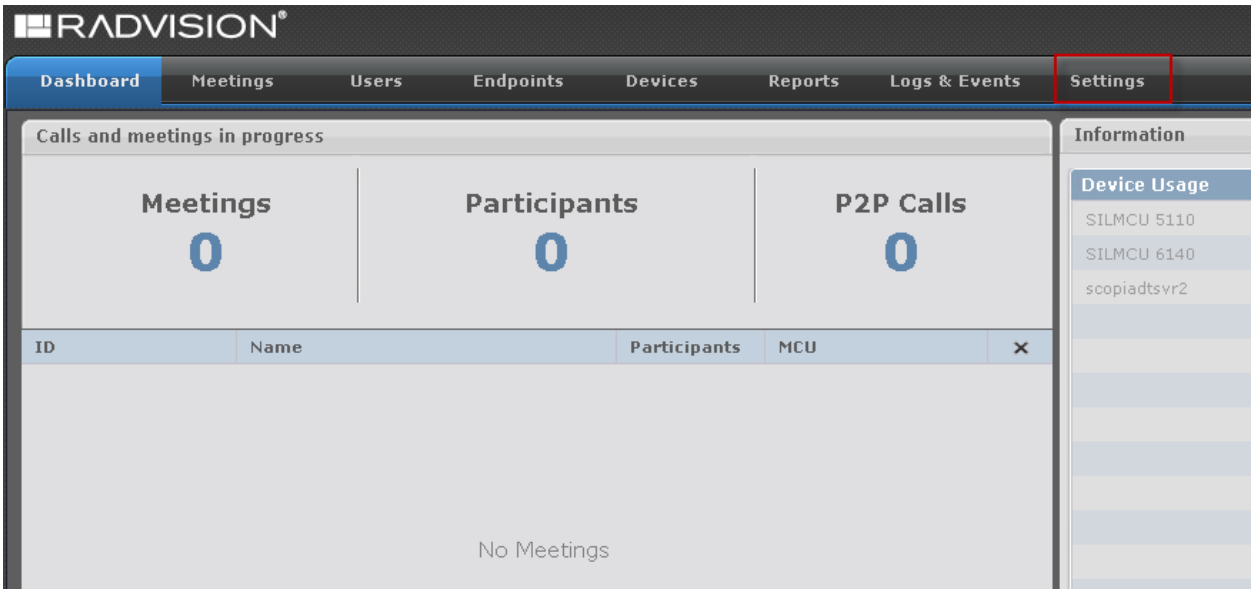
http://<IP_or_FQDN_of_iVIEW>:<port>/iview

Enter a valid **User Name** and **Password**. Press **Sign In**.



6.1.1. Configure the Avaya Aura® Conferencing Integration Settings

From the options on the top of the administrator console, select the **Settings** tab.



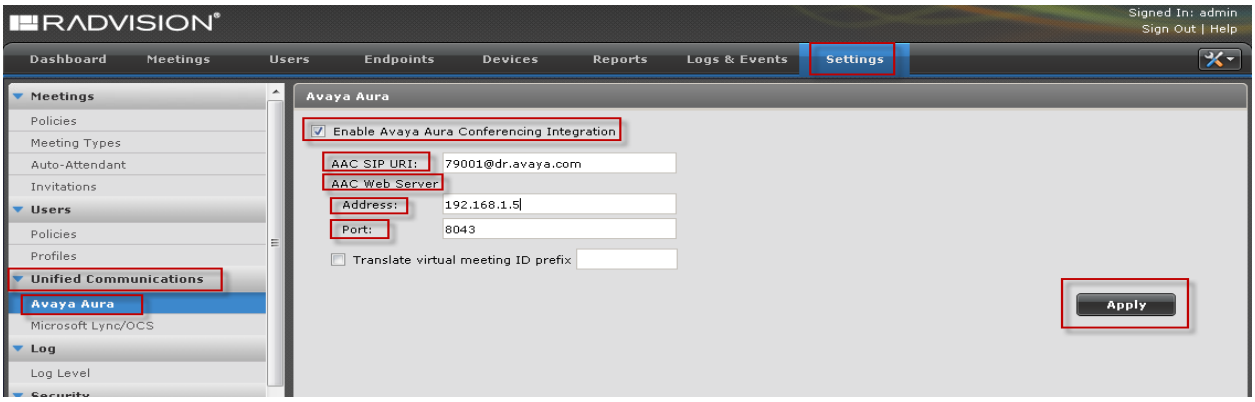
To add Avaya Aura® Conferencing details, click **Unified Communications → Avaya Aura** and select the **Enable Avaya Aura Conferencing Integration** check box.

Enter the following values**.**

- **AAC SIP URI:** Enter the SIP URI for Avaya Aura® Conferencing. In the sample configuration "**79001@dr.avaya.com**" was used.
- **Address:** Enter the IP address of the Avaya Aura® Conferencing Collaboration Agent server.
- **Port:** Enter the Port of the Avaya Aura® Conferencing Collaboration Agent server.

Press **Apply**.

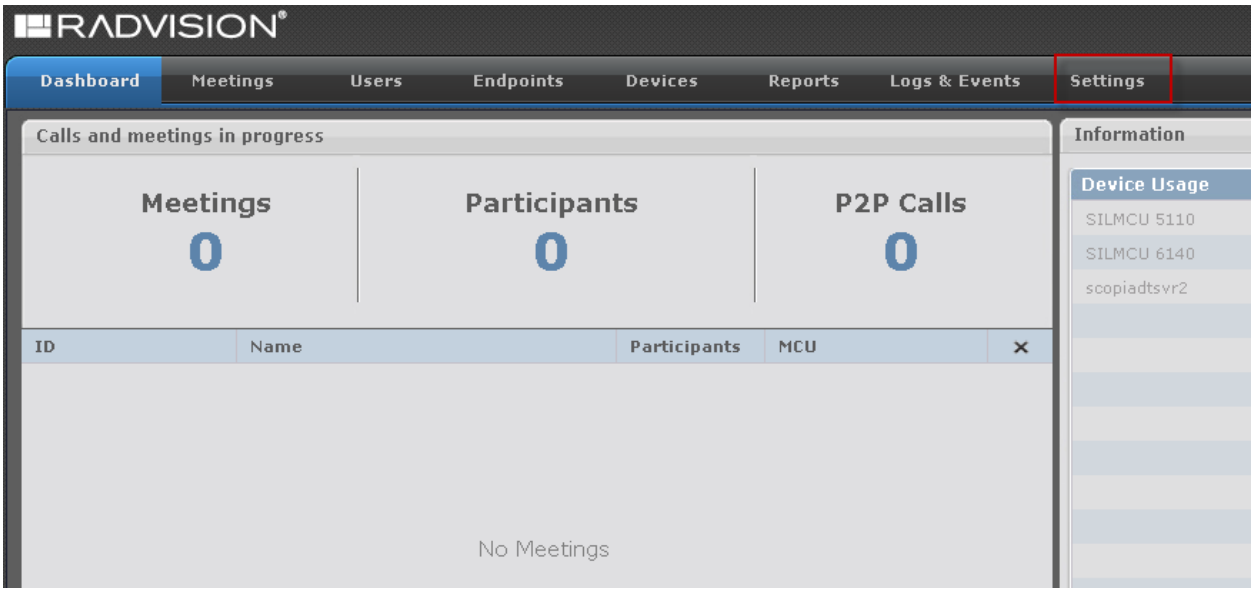
The following screen shows the Avaya Aura® Conferencing integration settings.



6.1.2. Configure the Meeting Types

Perform this procedure to configure the Avaya Aura® Conferencing integration for a meeting type. With this procedure, you can enable automatic dial out from a Radvision SCOPIA conference to an Avaya Aura® Conferencing conference for a selected meeting type.

From the options on the top of the administrator console, select the **Settings** tab.



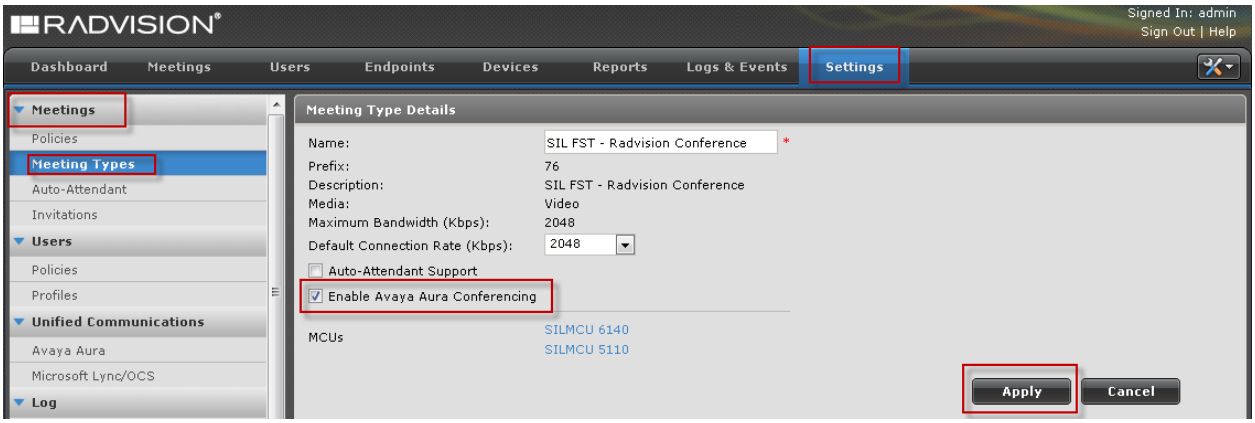
To add Meeting Types, select **Meetings → Meeting Type** and select the appropriate Name of the Meeting Type of interest. In this sample configuration "**SIL FST - Radvision Conference**" was selected

Note: The Meeting Types listed are not created here but created directly on the Radvision Scopia Elite MCU and pushed here via the **Synchronize** button and is out of the scope for this Application Note.

The following screen shows the Meeting Types.

After selecting the relevant Meeting Type from the previous screen the Meeting Type Details are displayed. Select the **Enable Avaya Aura Conferencing** check box.

Press **Apply**.



6.1.3. Configure Session Manager SIP Entity Link on SCOPIA Management

With this procedure you can create a SIP entity link between SCOPIA Management and Session Manager.

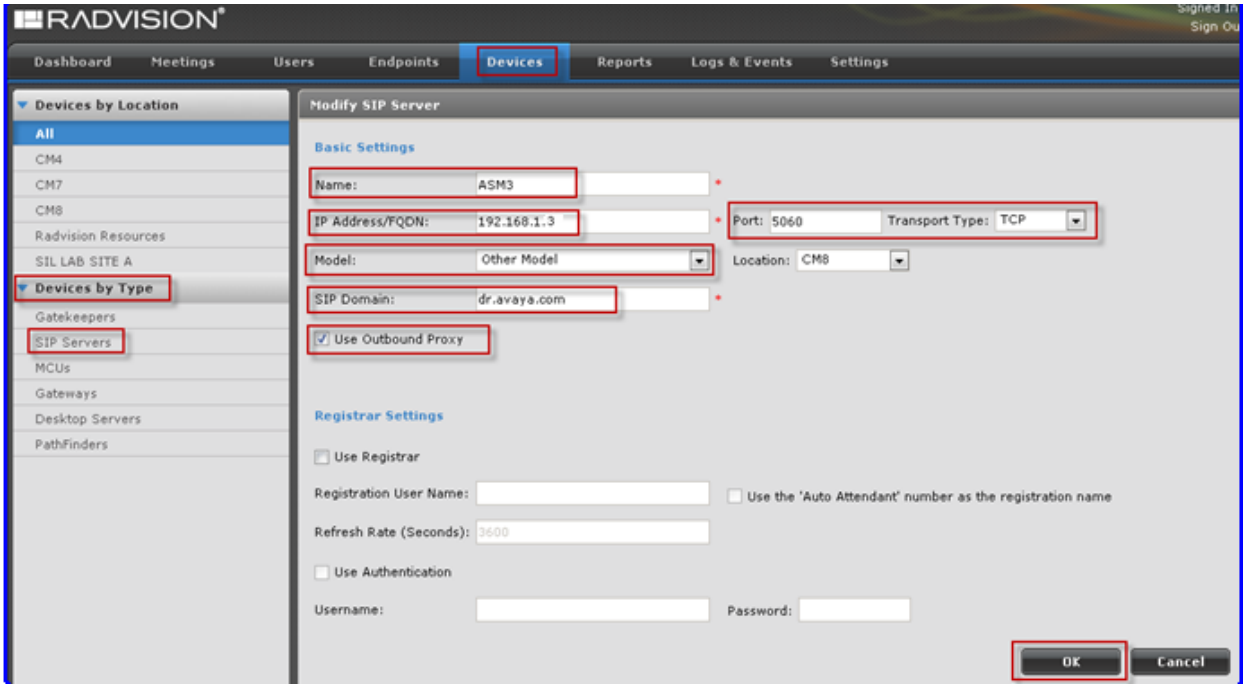
From the options on the top of the administrator console, select the **Devices** tab → **Devices by Type** → **SIP Server**.to add a new SIP server entry.

Press **Add**. Enter the following values**.**

- **Name:** Enter an identifier for the Session Manager instance. In the sample configuration, "**ASM3**" was used.
- **IP Address/FQDN:** Enter the IP address of the Session Manager SIP service.
- **Port:** Enter the Port of the Session Manager SIP service.
- **Transport Type:** Enter the Transport Type to connect to the Session Manager SIP service.
- **Model:** Select "**Other Model**".
- **SIP Domain:** Enter the SIP Domain of Avaya Aura® Conferencing.
- **Use Outbound Proxy:** Select the check box.

Press **OK**.

The following screen shows the SIP server details.



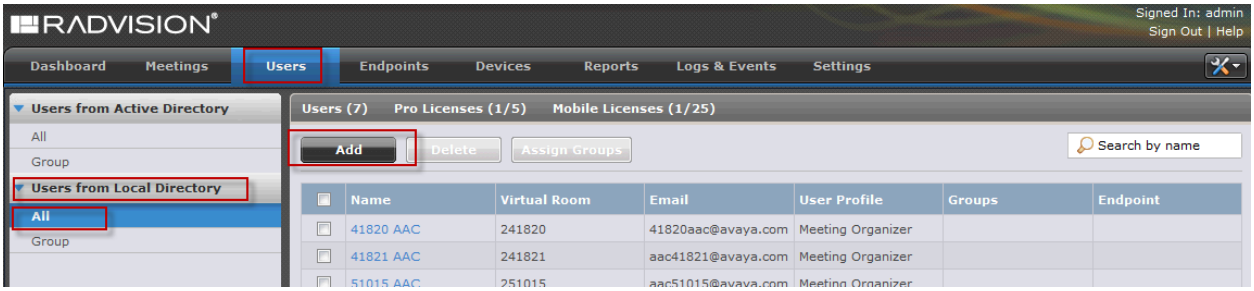
6.1.4. Configure the Subscriber Virtual Room

This procedure describes the steps to add a new user and configure a virtual room for the user. With a dedicated virtual room, Radvision SCOPIA users can avoid dialing a steering code or a prefix. Ensure that the virtual room number of each user corresponds to the Avaya Aura® Conferencing participant security code of the user.

Do not use the moderator code for a virtual room number.

From the options on the top of the administrator console, select the **Users** tab → **Users from Local Directory** → **All**.

The following screen shows all of the Users.

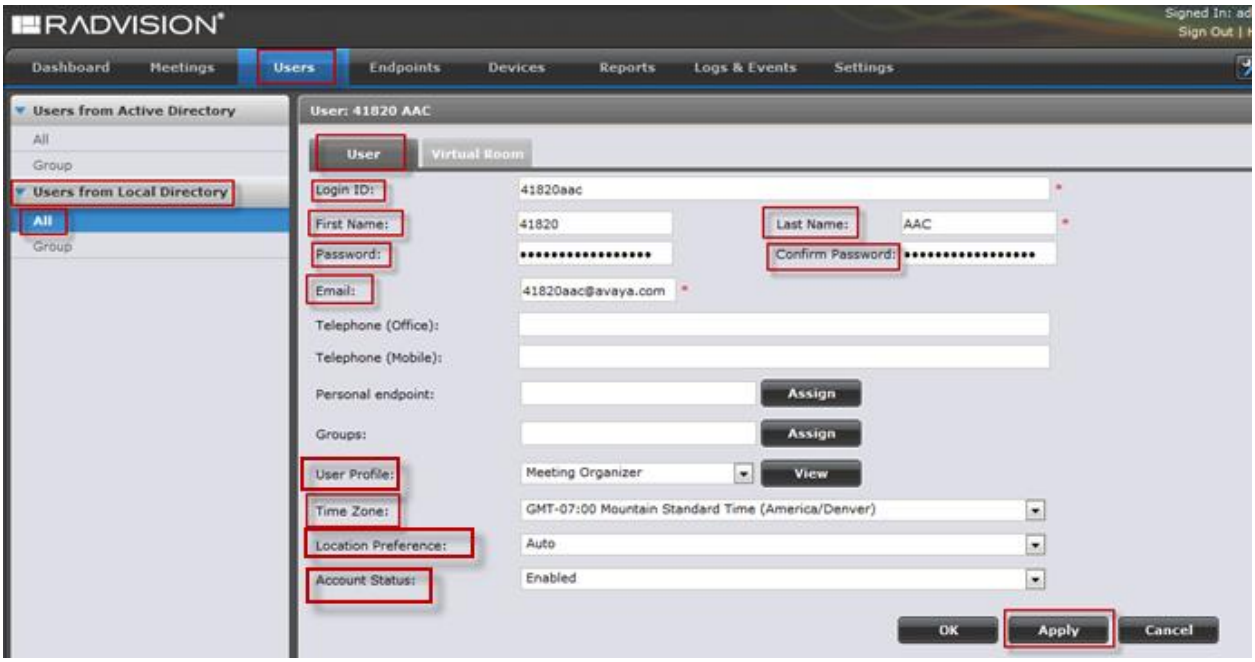


Press **Add**. Enter the following values**.**

- **Login ID:** Enter a unique Login ID.
- **First Name:** Enter the First Name.
- **Last Name:** Enter the Last Name.
- **Password:** Enter a password
- **Confirm Password:** Enter the password again.
- **Email:** Enter a valid email address.
- **User Profile:** Use the default value "**Meeting Organizer**".
- **Time Zone:** Select the appropriate Time Zone.
- **Location Preference:** Use the default value "**Auto**".
- **Account Status:** Use the default value "**Enabled**".

Press **Apply**.

The following screen shows the Users details.



Select the **Virtual Room** tab.

Enter the following values**.**

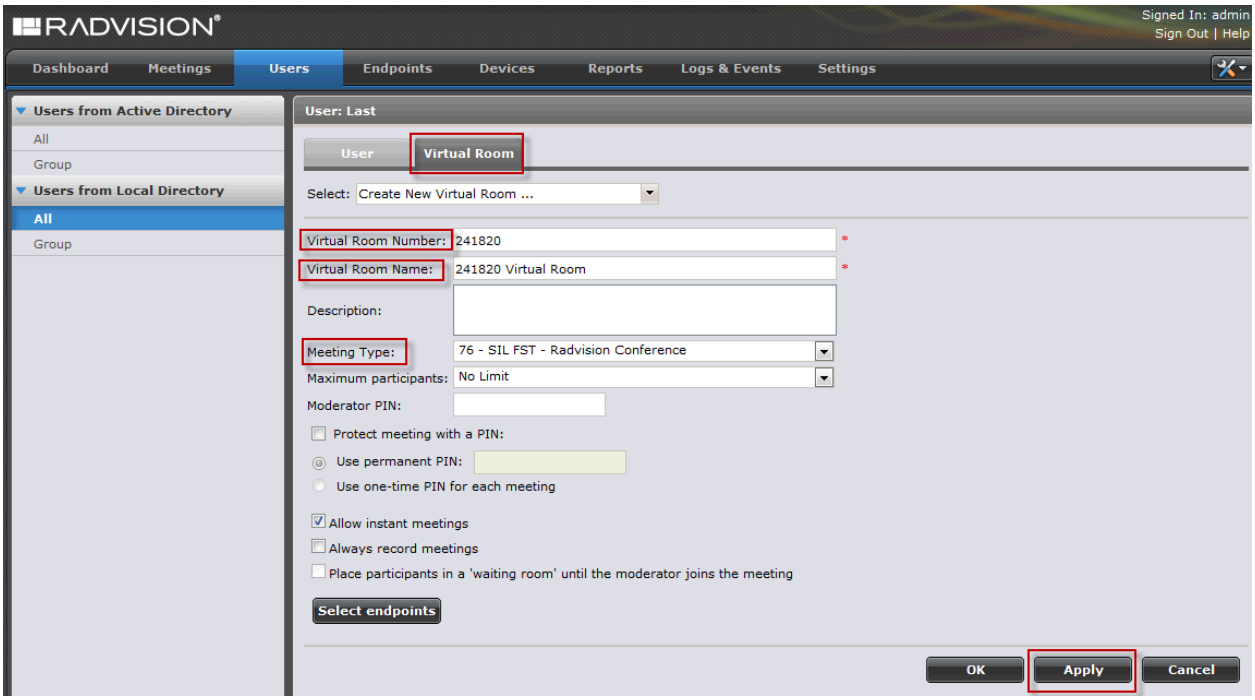
- **Virtual Room Number:** Enter the virtual room number for the user.
- **Virtual RoomName:** Enter the Name for the virtual room.
- **Meeting Type:** Select the Meeting Type that was configured in **Section 6.1.2.**

Note:
Ensure that the virtual room number corresponds to the Avaya Aura® Conferencing participant security code of the subscriber.

Depending on the dial plan requirements, a prefix may need to be added to the virtual room number. If the dial plan requires a prefix, ensure that the value of the Virtual Room Number field contains the prefix.

Press **Apply**.

The following screen shows the User's Virtual Room details.



6.1.5. Configure the Virtual Conference Room Prefix Translation

Perform this procedure to enable translation of dialed digits when accessing a Radvision SCOPIA Virtual Room conference. Radvision SCOPIA applies the prefix translation to the digits in the outgoing call to Avaya Aura® Conferencing.

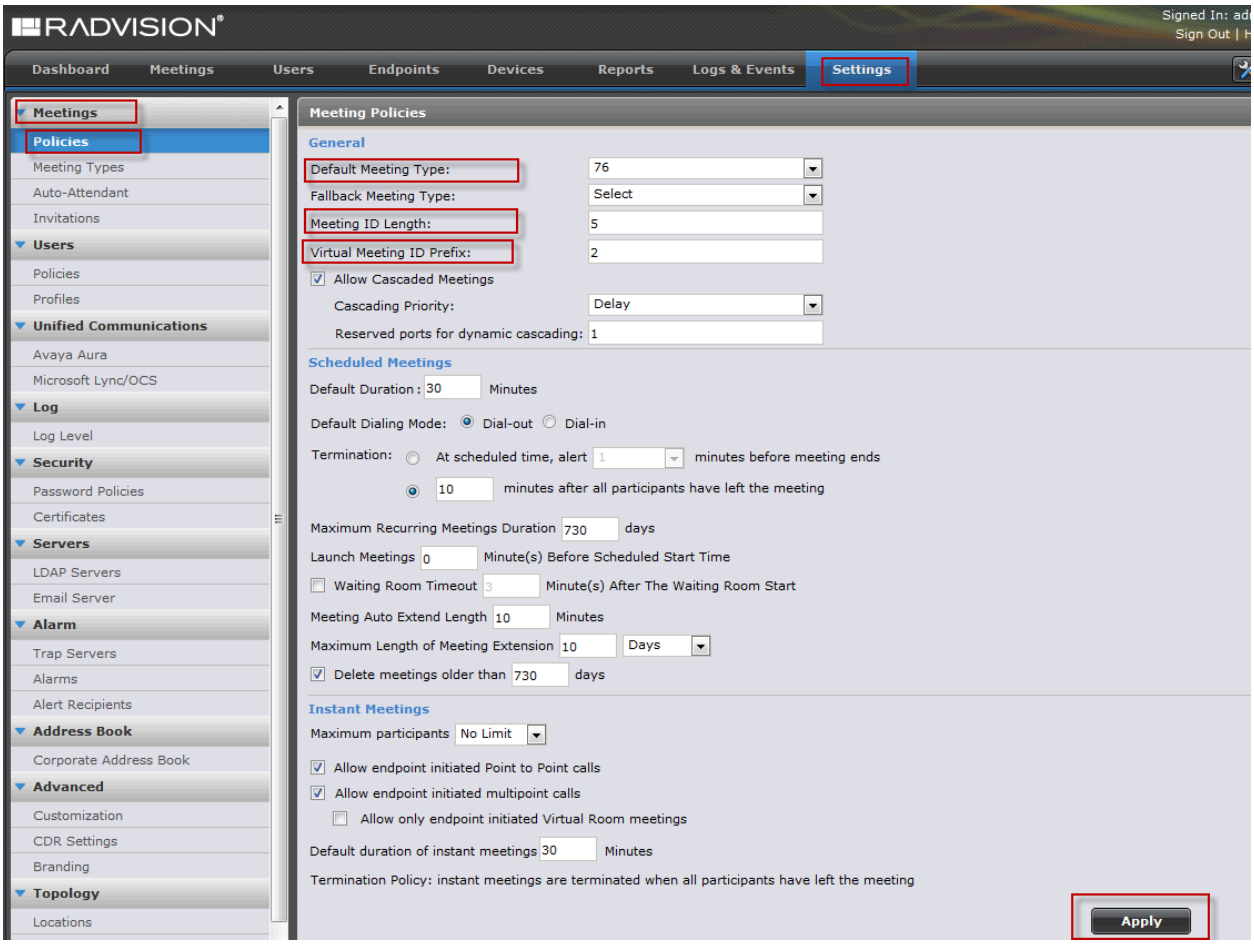
From the options on the top of the administrator console, select the **Settings** tab → **Meetings** → **Policies**.

Enter the following values**.**

- **Default Meeting Type:** Select the appropriate Default Meeting Type. In the sample configuration "**76**" was used, which is the Meeting Type defined in **Section 6.1.2**.
- **Meeting ID Length:** Enter the number of digits in the Meeting ID.
- **Virtual Meeting ID Prefix:** Enter the Prefix digits.

Press **Apply**.

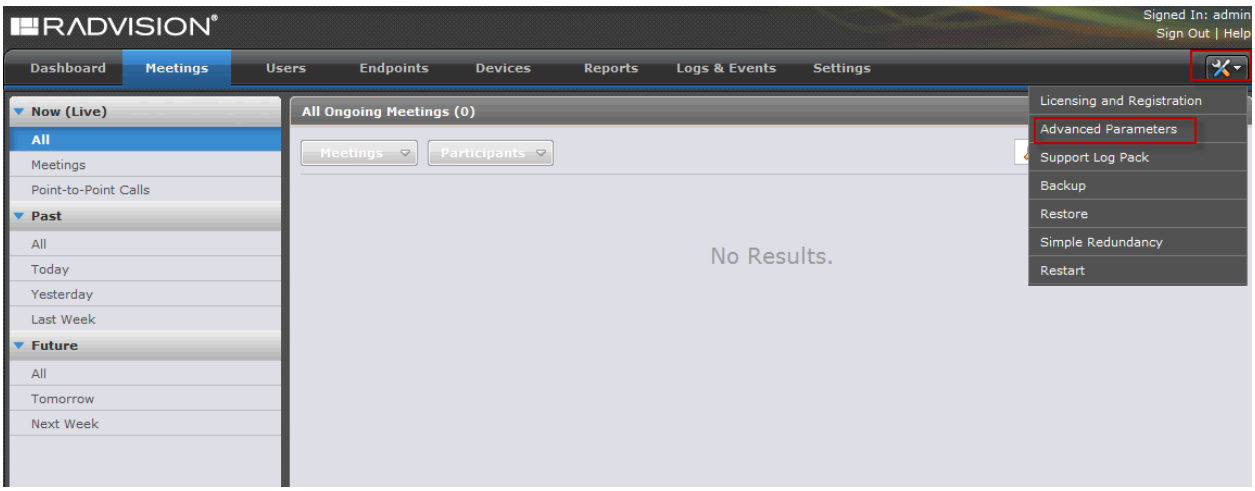
The following screen shows the Meeting Policies details.



6.1.6. Configure the Media Trunk Label

Perform this procedure to change the name that Radvision endpoints display for the video stream from Avaya Aura® Conferencing.

From the options on the top of the administrator console, select the **Tools** icon on the top right corner. Select **Advanced Parameters**.

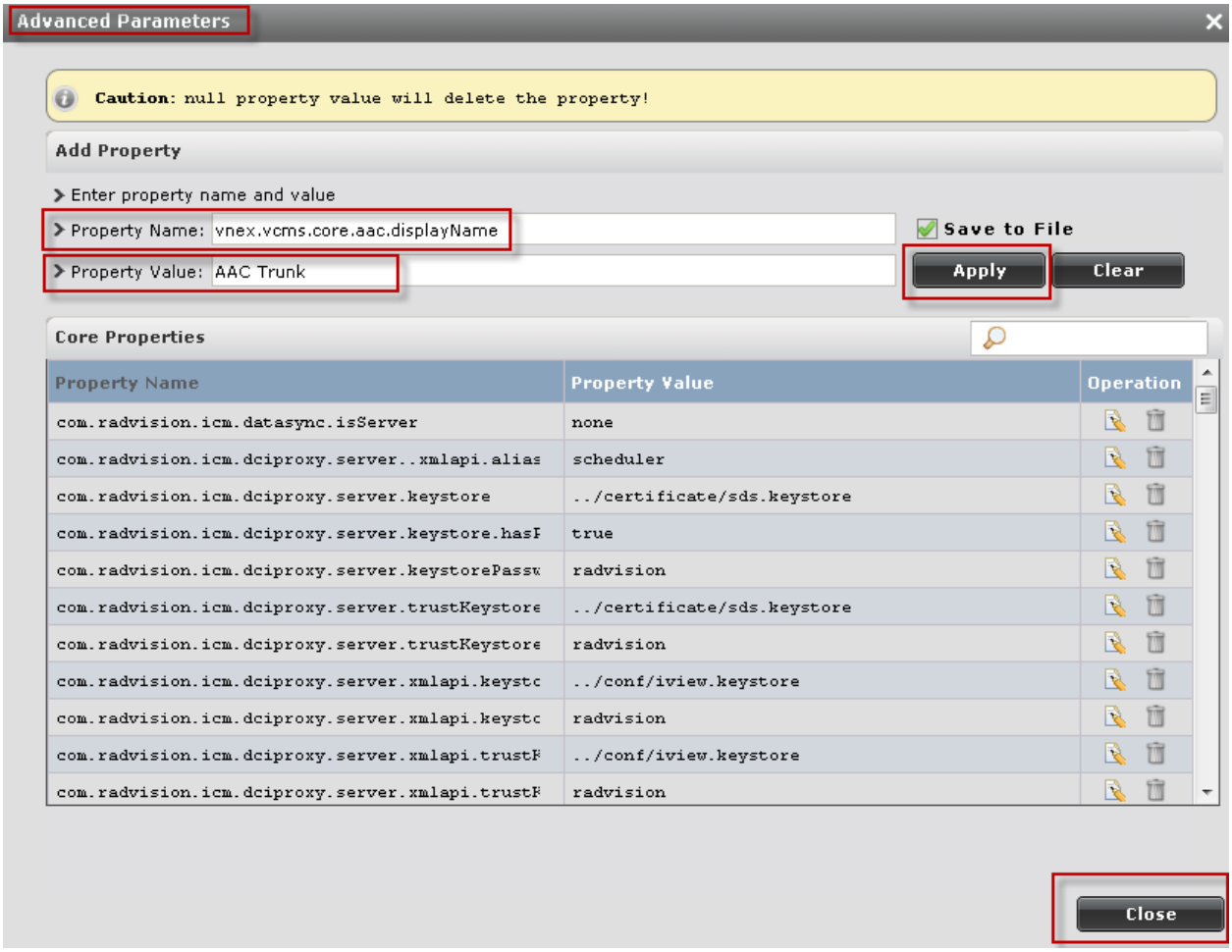


Enter the following values**.**

- **Property Name:** Enter **vnex.vcms.core.aac.displayName** This is the variable used for the media trunk label.
- **Property Value:** Enter the display name to represent the link to Avaya Aura® Conferencing. In this sample configuration "**AAC Trunk**" was used. The default value of this field is **Audio Link**.

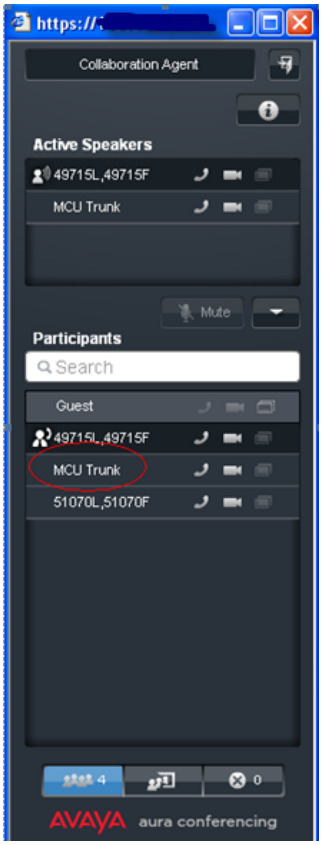
Press **Apply**.
Press **Close**.

The following screen shows the Advanced Parameters details.

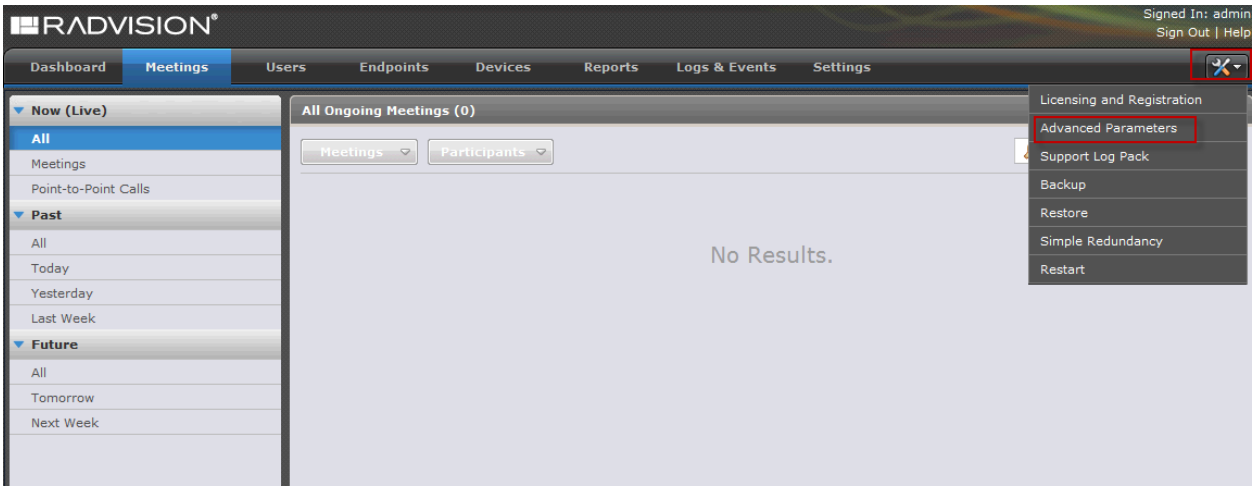


6.1.7. Configure the Roster Label

Perform this procedure to change the name that Avaya Aura® Conferencing displays to represent the conference link to Scopia Elite MCU in the Collaboration Agent roster.



From the options on the top of the administrator console, select the **Tools** icon on the top right corner. Select **Advanced Parameters**.

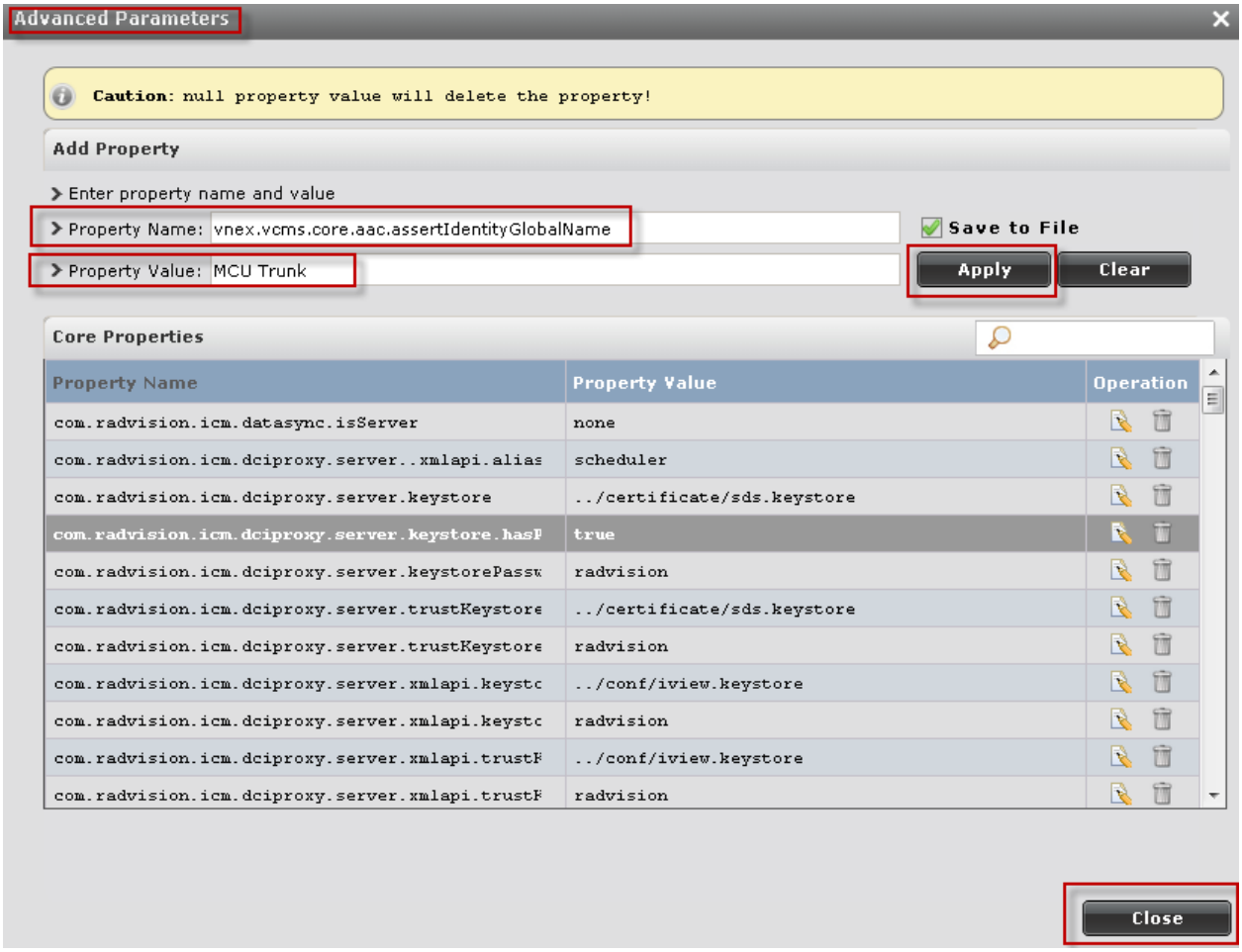


Enter the following values**.**

- **Property Name:** Enter **vnex.vcms.core.aac.assertIdentityGlobalName** This is the variable used for the roster label.
- **Property Value:** Enter the display name to represent the link to Scopia Elite MCU on the Avaya Aura® Conferencing roster.

Press **Apply**.
Press **Close**.

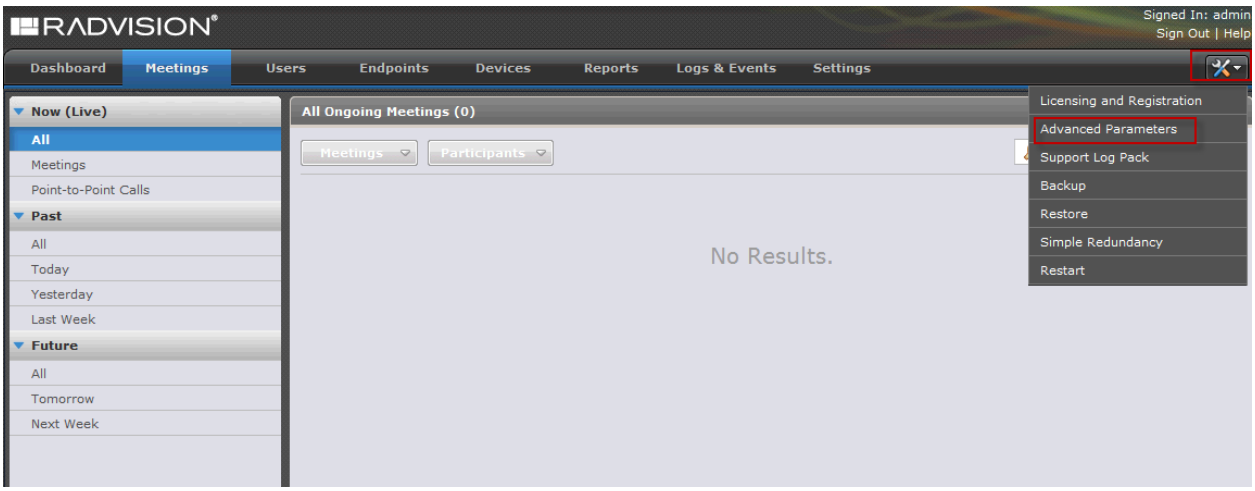
The following screen shows the Advanced Parameters details.



6.1.8. Administer the Conference Default Domain

Perform this procedure to administer the SIP domain name that Scopia Elite MCU uses when dialing in to the Avaya Aura® Conferencing conference.

From the options on the top of the administrator console, select the **Tools** icon on the top right corner. Select **Advanced Parameters**.

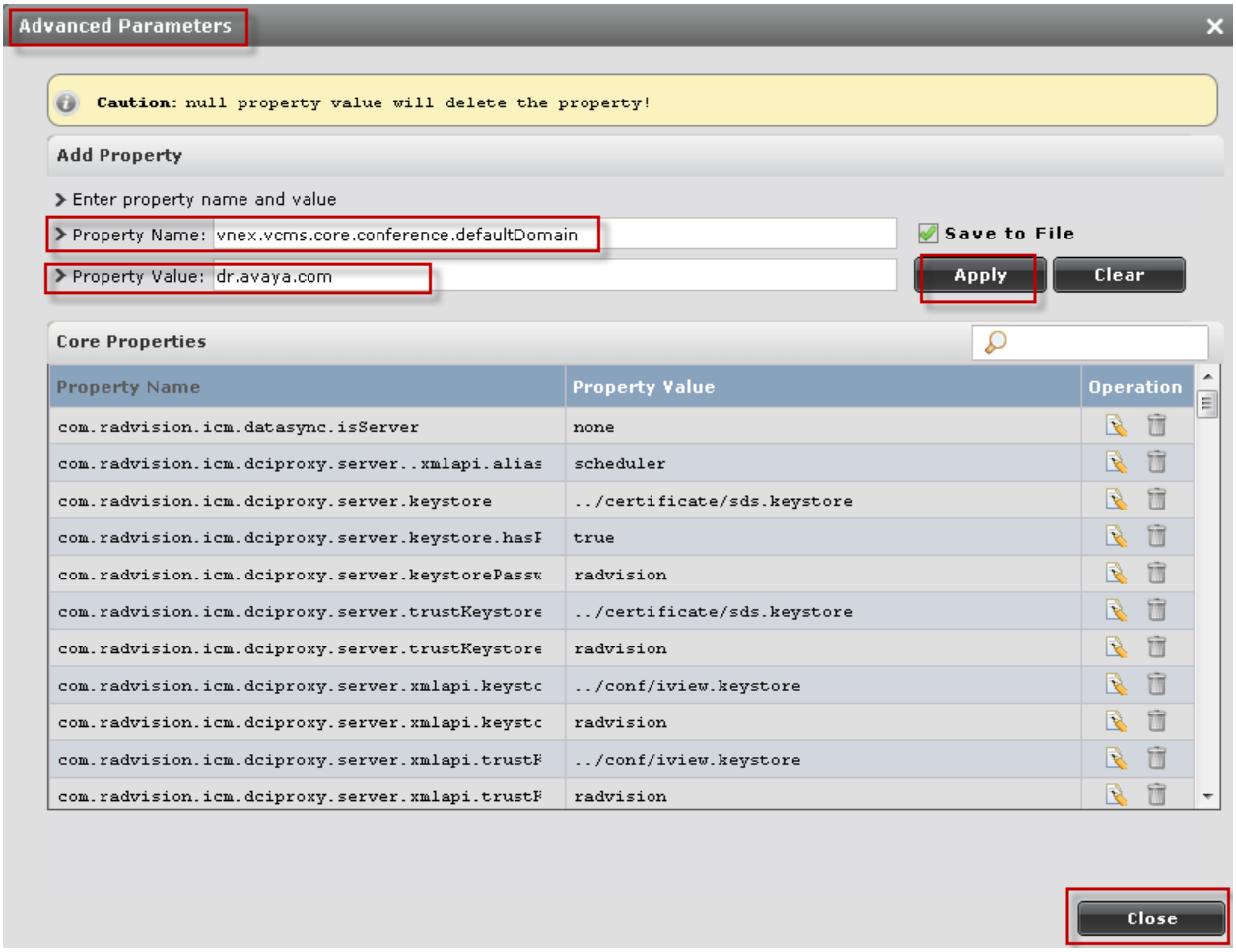


Enter the following values**.**

- **Property Name:** Enter **vnex.vcms.core.conference.defaultDomain**
  This is the variable used for the conference default domain.
- **Property Value:** Enter the SIP domain name for calls to Avaya Aura® Conferencing.

Press **Apply**.
Press **Close**.

The following screen shows the Advanced Parameters details.

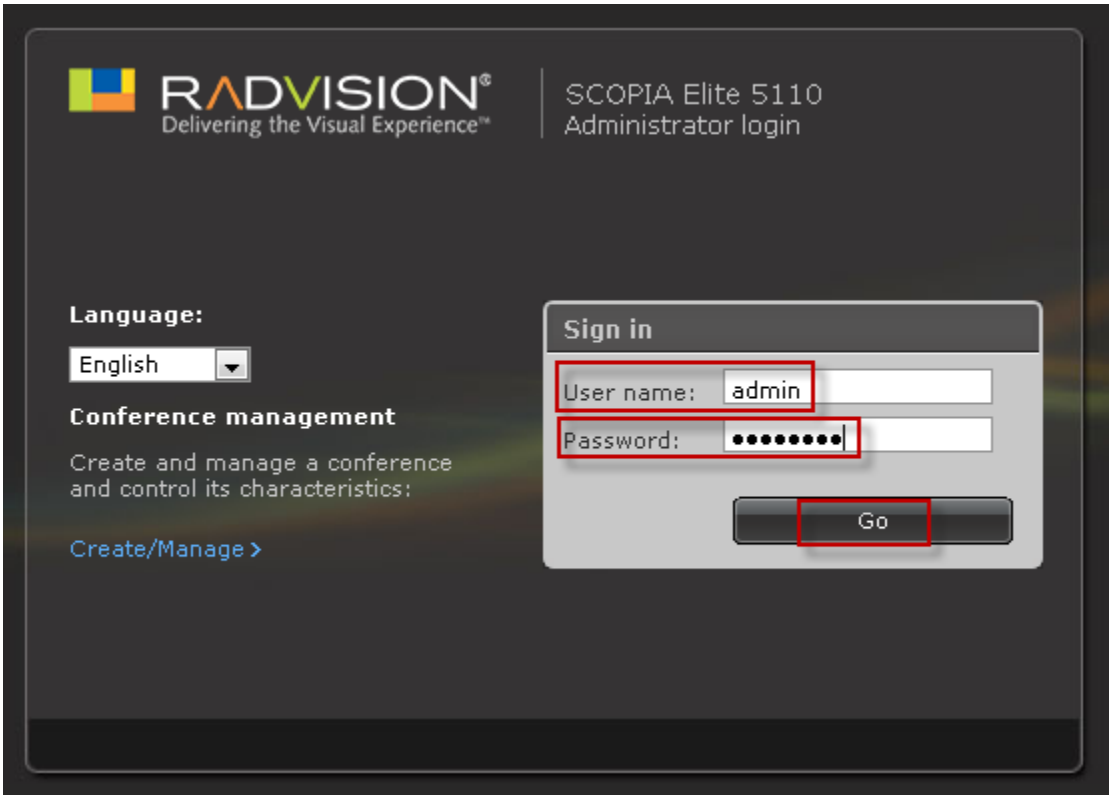


6.2. Logging in to SCOPIA Elite MCU

To log in to SCOPIA Elite MCU, in the browser address bar, enter the SCOPIA Elite MCU IP Address or FQDN in the following format:

http://<IP_or_FQDN_of_iVIEW>

Enter a valid **User name** and **Password**. Press **Go**.



6.2.1. Administer DNS on SCOPIA Elite MCU

Perform this procedure to enable the DNS search on Scopia Elite MCU.

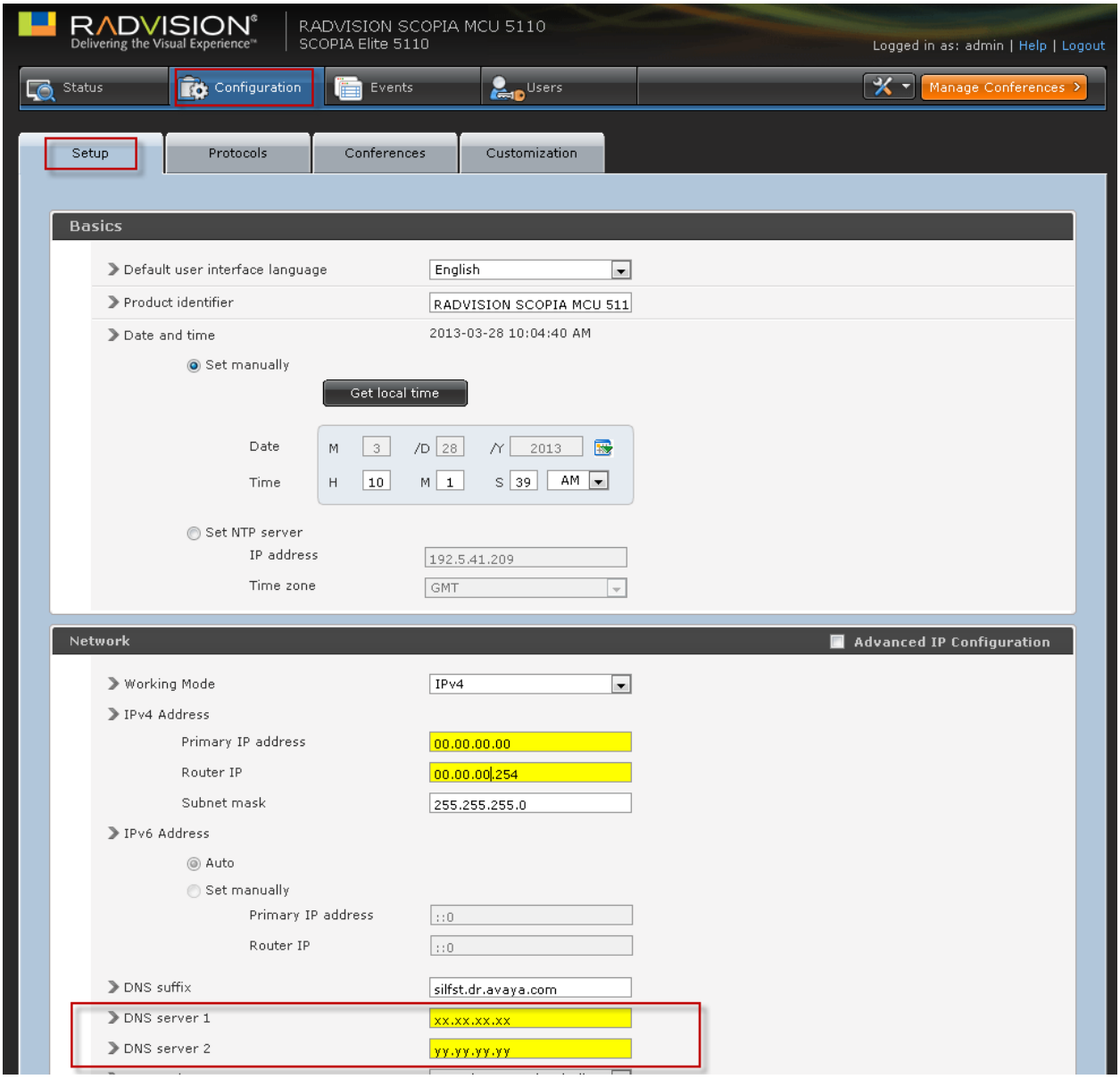
The DNS search resolves addresses of SIP headers and fields that contain FQDNs.

From the options on the top of the Scopia Elite 5000 MCU Web-based interface, select **Configuration → Setup**.

Enter the following values**.**

- **DNS server 1:** Enter the IP address of the primary DNS server
- **DNS server 2:** Enter the IP address of the secondary DNS server

Press **Apply** (not shown).



7. Advantages

With the Avaya Aura® Conferencing and Radvision Scopia interoperability configuration, users can:

- Connect to a Radvision Scopia conference through Avaya Flare Experience.
  Note:
  The Flare Experience user only receives video. The roster and content sharing is not yet integrated with Flare Experience.

- Automatically connect an Avaya Aura® Conferencing video conference with a Radvision Scopia conference.
- Use the room systems and video endpoints connected to Scopia Elite MCU to connect to an Avaya Aura® Conferencing conference.
- Use the Avaya endpoints, such as Flare Experience, one-X® Communicator, desk phones, to connect to a Scopia Elite MCU conference.

8. Limitations

The Avaya Aura® Conferencing and Radvision Scopia interoperability configuration has the following limitations:

- Conference participants cannot use the Avaya Aura® Conferencing moderator security code to join a conference from a Scopia endpoint.
    - If an Avaya Aura® Conferencing conference owner joins a conference from a Scopia endpoint, the conference owner must use the participant security code or the Virtual Room number.
    - Participants can use the moderator conference controls of an Avaya Aura® Conferencing conference only through Collaboration Agent.
- The Avaya Aura® Conferencing conference and Radvision Scopia conference roster and conference controls are not integrated between these conferences.
    - The Avaya Aura® Conferencing Collaboration Agent and TUI conference controls impact only the Avaya Aura® Conferencing conference.
    - The Radvision Scopia conference control API impacts only the Radvision Scopia conference.
    - The operator conference controls are not integrated between Avaya Aura® Conferencing and Radvision Scopia conferences. Administrators must separately configure the Avaya Aura® Conferencing and the Scopia Elite MCU operator conference controls. The operators must access the conference controls using independent TUI commands.
    - The Radvision Scopia conference participants cannot use TUI conference controls to moderate the Avaya Aura® Conferencing conference. The conference participants must use Collaboration Agent to use the moderator conference controls.
    - Conference participants cannot use the Avaya Aura® Conferencing conference TUI controls through DTMF on the Scopia endpoints.
- The Avaya Aura® Conferencing conference does not automatically connect to the Scopia conferencing if:
    - The MeetMe conference does not have any participants.
    - Scopia Desktop starts the conference in the Presentation-only mode.
    - Scopia endpoints are connected to the waiting room.
- The SIP trunk between the Avaya Aura® Conferencing conference and Radvision Scopia conference does not support continuous presence. A single participant video stream is shared between the Avaya Aura® Conferencing conference and the Radvision Scopia conference.
    - The SIP trunk to Scopia Elite MCU is processed as a participant for bandwidth usage monitoring.
    - If the trunk from Scopia Elite MCU to Avaya Aura® Conferencing is not established, the trunk to Avaya Aura® Conferencing fails without any notification.
    - The moderator does not receive a notification that the trunk to Avaya Aura® Conferencing is not available. An administrator can view the trunk failure in the Scopia Elite MCU or the

Scopia Management logs. Scopia Desktop users can view the failure of the trunk to Avaya Aura® Conferencing in the conference roster.

  - The SIP trunk between Avaya Aura® Conferencing does not support the PSTN overflow because there is no mechanism to provide the Avaya Aura® Conferencing access code.
  - The SIP trunk between Avaya Aura® Conferencing and Scopia Elite MCU does not support TLS and SRTP.

- The Dial out feature of Avaya Aura® Conferencing cannot dial out to the Scopia endpoints.
- The conference participants can share data from the Avaya Aura® Conferencing conference to the Scopia Elite MCU endpoints using a physical connection, such as a video cable, between a computer running Collaboration Agent and a Scopia endpoint.
- Avaya Aura® Conferencing does not monitor the bandwidth usage between Scopia Elite MCU and Scopia endpoints.

9. Feature Integration

The following table lists the integration status of the key interoperability features:

Feature	Avaya Aura® Conferencing	Radvision Scopia	Integration
Audio bridging	Yes	Yes	Yes
Video bridging	Yes	Yes	Yes, only Active Speaker
Content sharing	Yes	Yes	No, a Scopia subscriber must log in to Avaya Aura® Conferencing Collaboration Agent to view and share content in the Radvision Scopia conference by sharing the Collaboration Agent display through the Presenter mode in Scopia Desktop.
Participant controls	Yes	Yes	No, the moderators of the Avaya Aura® Conferencing conference or the Radvision Scopia conference can perform limited management of the other conference, which is processed as a participant. The moderators cannot perform management tasks on individual participants in conferences.
High definition video	Yes	Yes	The video resolution depends on the Avaya Aura® Conferencing administration. • In Avaya Aura® Conferencing Release 7.0, using H.264 SVC, Avaya Aura® Conferencing and Radvision Scopia subscribers view each other in the 360p resolution. • In Avaya Aura® Conferencing Release 7.0, using H.264 AVC with

			720p resolution, Avaya Aura® Conferencing and Radvision Scopia subscribers view each other in the 720p resolution. Avaya endpoints that support only the SVC video codec do not receive video. • In Avaya Aura® Conferencing Release 7.2, using SVC without inter-layer prediction, Avaya Aura® Conferencing subscribers view the Radvision Scopia subscribers in the 360p resolution while Radvision Scopia subscribers view Avaya Aura® Conferencing subscribers in the 720p resolution. Avaya endpoints that support only the SVC video codec also receive video.

10. Conference Controls

Conference controls are not integrated between Avaya Aura® Conferencing and Radvision Scopia.

- The moderator conference controls from a Radvision Scopia endpoint or a Web-based user portal impact only the Radvision Scopia conference.
- The Avaya Aura® Conferencing moderator conference controls from an Avaya Aura® Conferencing endpoint or Collaboration Agent impact only the Avaya Aura® Conferencing conference.
- An Avaya Aura® Conferencing subscriber hosting a conference from a Radvision Scopia endpoint must use Collaboration Agent to moderate the Avaya Aura® Conferencing conference.
- The Avaya Aura® Conferencing Mute All moderator control mutes only the participants of the Avaya Aura® Conferencing conference. You can mute the participants of the Radvision Scopia conference only from a Scopia endpoint or a Web-based user portal.

11. Use Cases

11.1. Scopia Endpoint User Joins a Conference as a Participant

Prerequisites

- The Avaya Aura® Conferencing MeetMe conference number is 79001.
- User A is an Avaya Aura® Conferencing subscriber with the 123456 participant security code and the 654321 moderator code.
- User B is a Radvision Scopia subscriber using a Scopia endpoint.
- The Virtual Meeting ID prefix is 76, the Meeting ID length is 5.

- Avaya Aura® Conferencing Integration is enabled for the provisioned Scopia Default Meeting Type

Actions

1) User A dials the 79001 Avaya Aura® Conferencing MeetMe conference number and joins the conference using the 654321 moderator code.
2) User B dials 76123456 from the Scopia endpoint.

Results

1) User A enters the Avaya Aura® Conferencing conference as a moderator.
2) User B enters the 76123456 Scopia Elite MCU Instant Meeting room.
3) A call is automatically initiated from Scopia Management to connect the Scopia Elite MCU Instant Meeting to the Avaya Aura® Conferencing conference with the 123456 embedded access code.
4) User A and User B can hear and see each other.

Variations

If User B arrives before User A:

- The Avaya Aura® Conferencing MeetMe conference starts automatically.
- The conference functions as a Fast Start conference.

11.2. Scopia Endpoint user Joins a Conference as a Moderator

Prerequisites

- The Avaya Aura® Conferencing MeetMe conference number is 79001.
- User A is a Radvision Scopia subscriber using a Scopia endpoint.
- User B is an Avaya Aura® Conferencing subscriber using an Avaya Flare client.
- The Virtual Meeting ID prefix is 76, the Meeting ID length is 5.
- Avaya Aura® Conferencing Integration is enabled for the provisioned Scopia Default Meeting Type

Actions

1) User A dials 76123456 from the Scopia endpoint.
2) User B dials the 79001 Avaya Aura® Conferencing MeetMe conference number and joins the conference using the 123456 participant security code.

Results

1) User A enters the 88123456 Scopia Elite MCU Instant Meeting room.
2) A call is automatically initiated from Scopia Management to connect the Scopia Elite MCU Instant Meeting to the Avaya Aura® Conferencing conference with the 123456 embedded access code.
3) User B enters the Avaya Aura® Conferencing conference.
4) User A and User B can hear and see each other.

Note:
The moderator code is not required in this scenario. The connection of the Scopia Elite MCU trunk to the Avaya Aura® Conferencing conference starts the conference automatically.

Variations
If User B connects before User A, User B can join the conference even if User A has not enabled the Fast Start feature.

11.3. Avaya Aura® Conferencing User Hosts a Conference from a Scopia Endpoint

Prerequisites

- The Avaya Aura® Conferencing MeetMe conference number is 79001.
- User A is an Avaya Aura® Conferencing subscriber with the 123456 participant security code and the 654321 moderator code.
- User B is a Radvision Scopia subscriber using a Scopia endpoint.
- User C is an Avaya Aura® Conferencing subscriber using an Avaya Flare client.
- The Virtual Meeting ID prefix is 76, the Meeting ID length is 5.
- Avaya Aura® Conferencing Integration is enabled for the provisioned Scopia Default Meeting Type

Actions

1) User A dials the 76123456 prefix and the participant security code from a Scopia endpoint.
2) User B dials 76123456 from the Scopia endpoint.
3) User C dials the 79001 Avaya Aura® Conferencing MeetMe conference number and joins the conference using the 123456 participant security code.

Results

1) User A enters the 76123456 Scopia Elite MCU Instant Meeting room.
2) A call is automatically initiated from Scopia Management to connect the Scopia Elite MCU Instant Meeting to the Avaya Aura® Conferencing conference with the 123456 embedded access code.
3) User B enters the 76123456 Scopia Elite MCU Instant Meeting room.
4) User A and User B can hear and see each other.
5) User C enters the Avaya Aura® Conferencing conference.
6) Users A, B, and C can hear and see each other.

Note:

The moderator code is not required in this scenario. The connection of the Scopia Elite MCU trunk to the Avaya Aura® Conferencing conference starts the conference automatically.

Variations

- If User C arrives before User A and User B, User C can only join the conference if User A has enabled the Fast Start feature.
- If User B arrives first, User C can join the conference even if the Fast Start feature is not enabled.

12. Verification Steps

12.1. Verify Avaya Aura® Session Manager Configuration

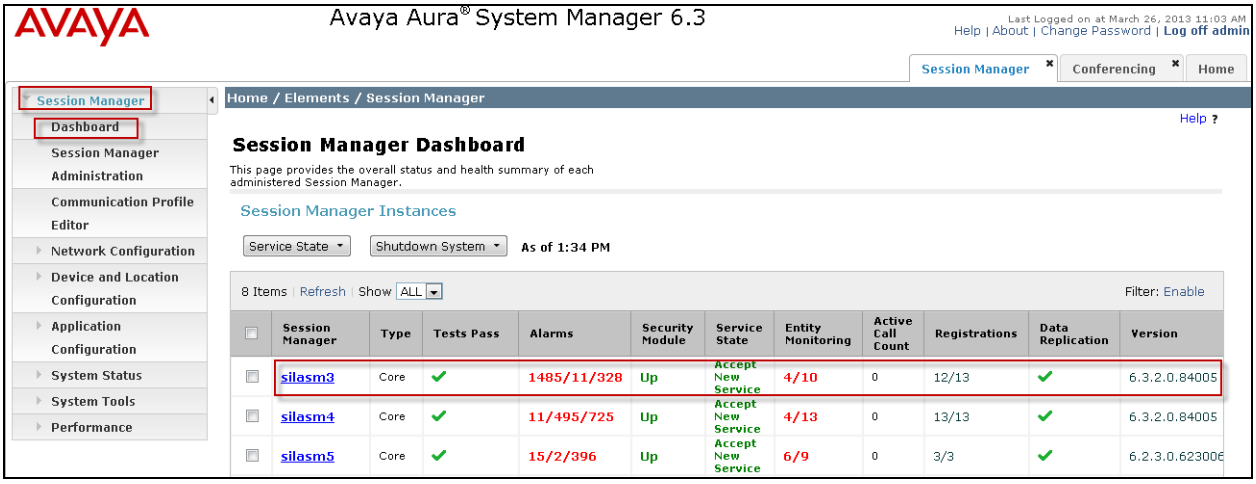
Step 1: Verify Avaya Aura® Session Manager is Operational

Expand **Elements → Session Manager** and select **Dashboard** to verify the overall system status for both of the Session Manager servers.

Specifically, verify the status of the following fields as shown below:

- **Tests Pass** ✔
- **Security Module** Up
- **Service State** Accept New Service

- **Data Replication** ✔



Step 2: Verify SIP Entity Link Status

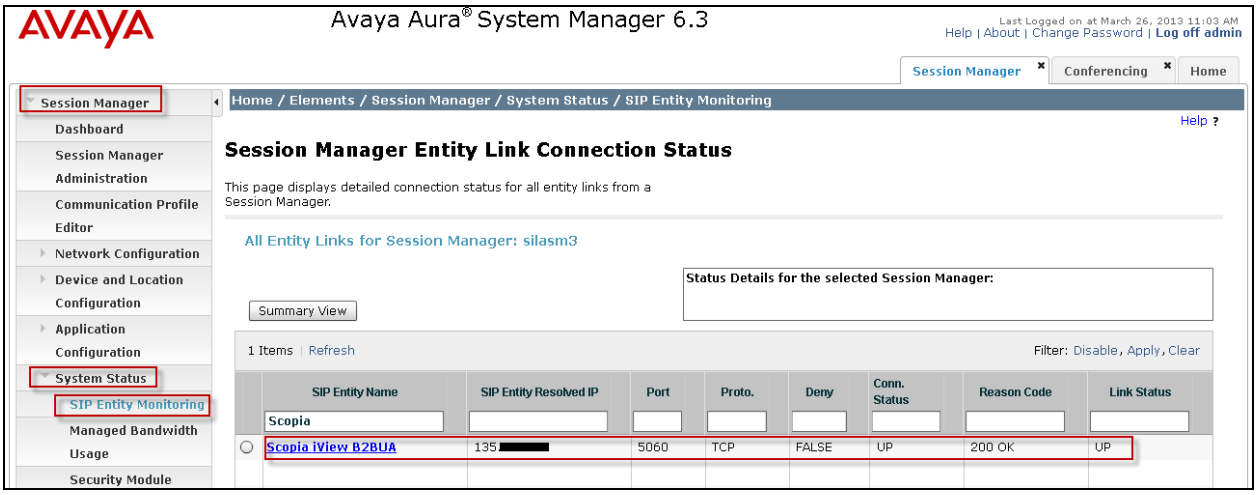
Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** to view more detailed status information for the specific SIP Entity Links used.

Select the SIP Entity for Communication Manager Evolution Server from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: silasm3** table, verify the **Conn. Status** and **Link Status** for both links is "**Up**" for Scopia iView B2BUA.

Click **Show** to view more information associated with the selected Entity Link.

Note: IP addresses and additional fields have been partially hidden for security.



13. Conclusion

These Application Notes describe the integration of Avaya Aura® Conferencing feature of Scopia Management which allows for configuring interoperability between Avaya Aura® Conferencing and Radvision Scopia.

Enterprise customers require a dedicated video conferencing solution along with a unified communications solution. By installing Avaya Aura® Conferencing and Scopia Elite MCU, customers can choose the optimal solution for conferencing and collaboration and leverage the features of both these products.

Avaya Aura® Conferencing Release 7.2 and Radvision Scopia Release 8.0 are the releases involved in the first phase of the integration between these products. The products are integrated through a transparent bridging of the audio and video stream and the Avaya Aura® Conferencing conference with Scopia Elite MCU.

14. Additional References

The following documentation may be obtained from http://support.avaya.com.

Avaya Aura® Conferencing

1) Avaya Aura® Conferencing 7.2 Overview and Specification
2) Avaya Aura® Conferencing 7.2 Planning and Design
3) Avaya Aura® Conferencing 7.2 Security
4) Avaya Aura® Conferencing 7.2 Accounting Records Reference
5) Avaya Aura® Conferencing 7.2 Alarms and Logs Reference
6) Avaya Aura® Conferencing 7.2 Operational Measurements Reference
7) Avaya Aura® Conferencing Collaboration Agent Quick Reference
8) Deploying Avaya Aura® Conferencing 7.2
9) Administering Avaya Aura® Conferencing 7.2
10) Maintaining and Troubleshooting Avaya Aura® Conferencing 7.2
11) Using Avaya Aura® Conferencing Collaboration Agent

Avaya Aura® Session Manager

1) Avaya Aura® Session Manager Overview, Doc ID 100068105.
2) Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473.
3) Avaya Aura® Session Manager Case Studies, Doc ID 03-603478.
4) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325.
5) Administering Avaya Aura® Session Manager, Doc ID 03-603324.

Avaya Aura® Communication Manager

1) SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206.
2) Administering Avaya Aura® Communication Manager, Doc ID 03-300509.
3) Administering Avaya Aura® Communication Manager Server Options, Doc ID 03-603479.
4) Implementing Avaya Aura Communication Manager, Doc ID 03-603558.

Avaya Application Notes

1) Application Notes for Radvision Scopia® XT 5000 Series Endpoint with Multi Avaya Aura® Communication Manager and Multi Avaya Aura® Session Manager Integration – Issue 1.0
2) Application Notes for Configuring Avaya Aura® Conferencing 7.0 Application Server, Media Server, and Web Conferencing Server with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Session Manager 6.2 - Issue 1.0
3) Application Notes for Configuring Avaya Flare® Experience on iPad device with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Session Manager 6.2 – Issue 1.0
4) Application Notes for Configuring Avaya Flare® Experience for Windows with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Session Manager 6.2 – Issue 1.0

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com