Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis for Unified Communications R11.7 with Avaya Aura® Session Manager R8.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis for Unified Communications R11.7 to interoperate with Avaya Aura® Session Manager.

Prognosis for Unified Communications R11.7 provides real-time monitoring and management solutions for IP telephony networks. Prognosis for Unified Communications R11.7 provides visibility of Avaya and other vendor's IP Telephony solutions from a single console and enables a reduction in complexity when managing complex IP telephony environments.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Prognosis for Unified Communications R11.7 (herein after referred to as Prognosis) with Avaya Aura® Session Manager R8.1.

The Prognosis product uses three integration methods to monitor Session Manager.

- Real Time Transport Control Protocol (RTCP) collection - Prognosis collects RTCP information sent by Avaya resources including IP Media Processor (MEDPRO) boards, media servers, media gateways and IP Deskphones.
- Call Detail Recording (CDR) collection - Prognosis collects CDR information via SFTP connection to Session Manager.
- SNMP collection –Prognosis uses SNMP to collect configuration and status information from Session Manager.

2. General Test Approach and Test Results

The general test approach was to use Prognosis web interface (webui) to display the hardware details of Session Manager. Calls were placed between Avaya SIP endpoints with other endpoints and Prognosis Webui was used to display the RTCP and CDR information collected.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Prognosis utilized enabled capabilities of SFTP by Integrated Research but not for RTCP and SNMP.

2.1. Interoperability Compliance Testing

For feature testing, Prognosis Webui was used to view the configurations of Session Manager such as the memory and CPU utilizations, disk usage and status. For the collection of RTCP and CDR information, only SIP endpoint is included. The types of calls made included intra-switch calls, inbound and outbound trunk calls.

For serviceability testing, reboots were applied to the Prognosis and Session Managers to simulate system unavailability. Loss of network connectivity to both Prognosis and Session Managers were also performed during testing.

2.2. Test Results

All test cases passed successfully with the following being observed:

- Voice Stream for Avaya IX Workplace SIP Deskphone is not shown on Session Manager SIP Voice Streams panel but on the Avaya PBX Voice Stream screen panel for calls made/received except where far end is a local SIP endpoint.
- RTCP-XR is not supported for Voice Streams from SIP phone.

2.3. Support

For technical support on Prognosis, contact the Integrated Research Support Team at:

- Hotline: +61 (2) 9966 1066
- Email: support@ir.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Prognosis interoperability with Session Manager. The configuration consists of a duplex pair of Communication Manager system (System A) with two Avaya G650 Media Gateways and an Avaya G430 Media Gateway with Communication Manager as a Local Survivability Processor (LSP). A simplex Enterprise Survivable Server (ESS) was also configured. A second Communication Manager system (System B) has an Avaya G450 Media Gateway. Avaya H323, SIP, digital and analog endpoints, and Avaya one-X® Communicator user were configured for making and receiving calls. IP trunks connect the two systems together to allow calls between them. System Manager and Session Manager provided SIP support to the Avaya SIP endpoints. Prognosis was installed on a server running Microsoft Windows Server 2016. Both the Monitoring Node and Web Application software are installed on this server. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution.

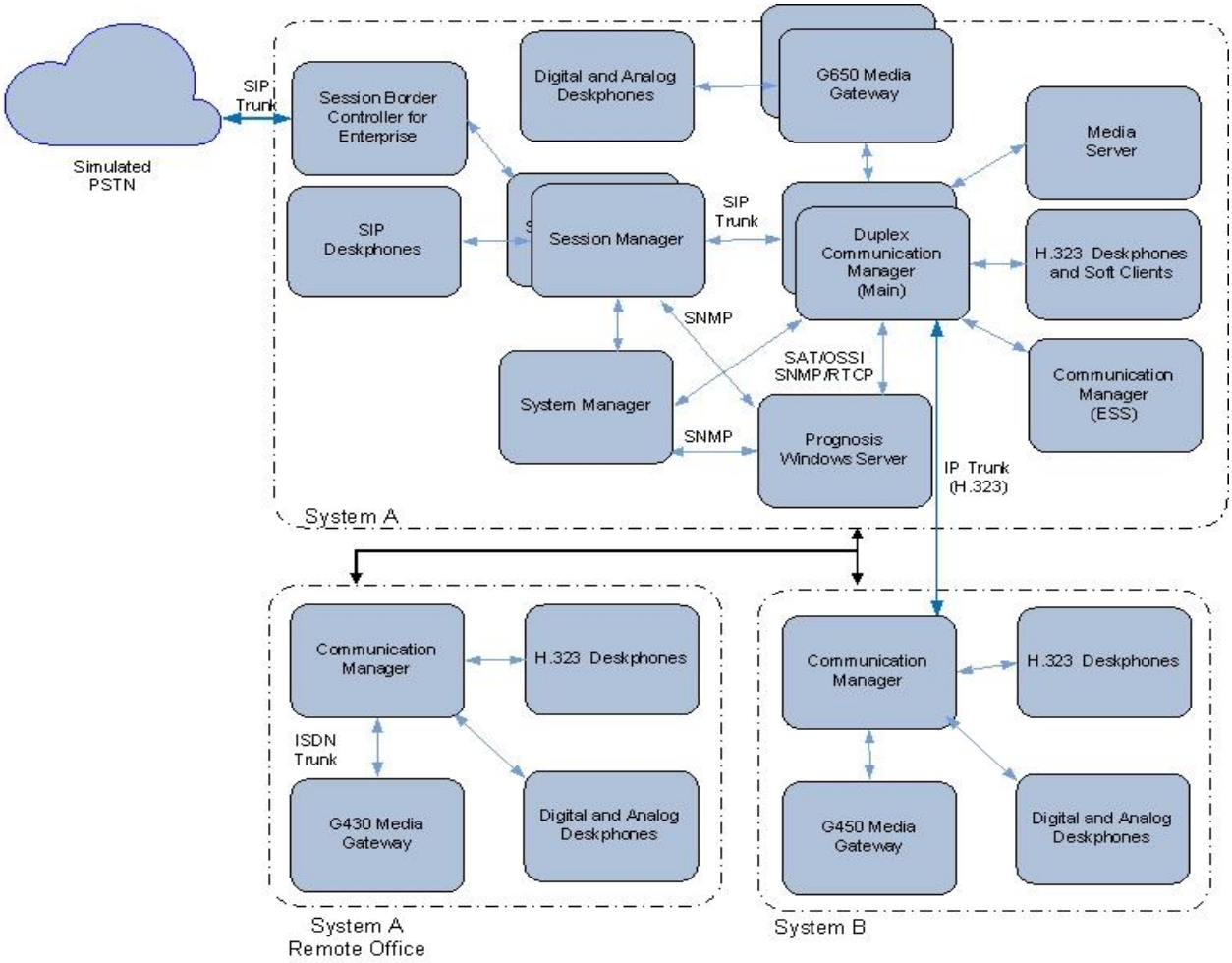


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
Avaya Aura® Media Server	R8.0.1.121
G650 Media Gateway - TN2312BP IP Server Interface - TN799DP C-LAN Interface - TN2602AP IP Media Processor - TN2302AP IP Media Processor - TN2464BP DS1 Interface - TN2464CP DS1 Interface - TN793CP Analog Line - TN2214CP Digital Line - TN2501AP Announcement	 HW07, FW058 HW01, FW044 HW02 FW067 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW012 HW08, FW016 HW03 FW023
Avaya Aura® Communication Manager	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	41.16.0 HW01 FW008 HW07 FW015 HW10 FW0104 HW03 FW015 HW11 FW054
Avaya Aura® Communication Manager	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
G430 Media Gateway - MM712AP DCP MM - MM716AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	41.16.0 HW04 FW015 HW12 FW104 HW31 FW104 HW05 FW022
Avaya Aura® Communication Manager	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
Avaya Aura® System Manager	System Manager 8.1.1.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.1.0.0310912 Feature Pack 1

Equipment/Software	Release/Version
Avaya Aura® Session Manager	Session Manager R8.1 FP1 Build No. – 8.1.0.0.810021
J100 Series IP Telephones - J179 - J129	 4.0.2.1.3 (SIP) 6.8202 (H323)
96x1 Series IP Telephones - 9641G - 9611G	 7.1.6.1.3 (SIP) 6.8202 (H323)
Avaya IX Workplace	3.7.0.102.3 (SIP)
1600 Series IP Telephones - 1616 - 1603SW	1.312 (H.323)
Digital Telephones - 9408	 R20
Avaya Analog Phones	-
Desktop PC with Avaya one-X Communicator	6.2.13.04 SP13 (H.323)
Prognosis running on Microsoft Windows Server 2016	11.7

Note: All Avaya Aura® systems and Prognosis runs on VMware 6.x virtual platform.

5. Configure Avaya Aura® Session Manager

This section describes the steps needed to configure Session Manager to interoperate with Prognosis. This includes configuration of the CDR user account on both Session Managers. The default SNMP v2c user profile will be used for Session Managers.

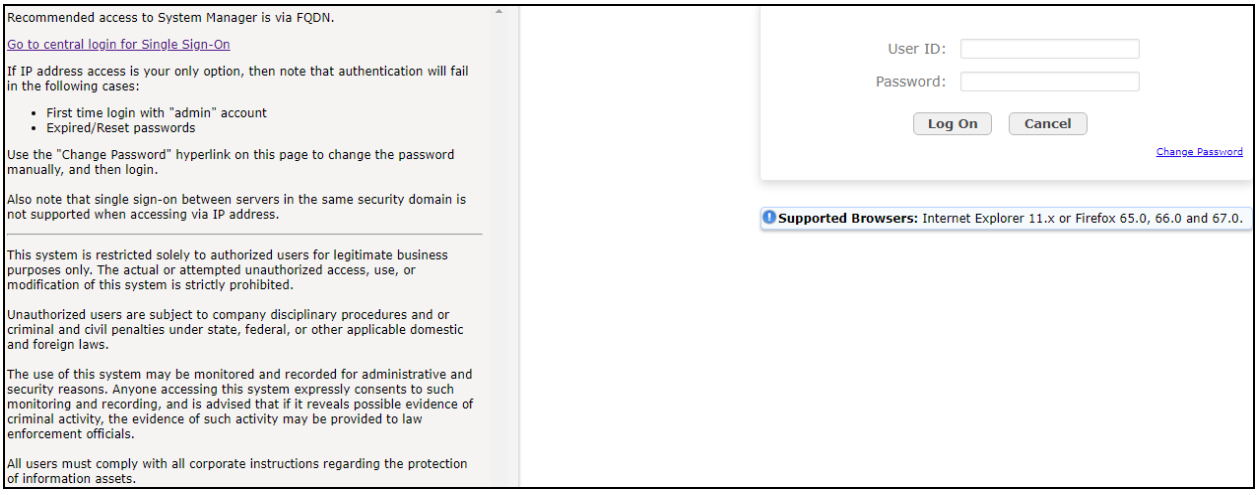
5.1. Configure SNMP for Session Manager

SSH into each Session Manager and log in as valid user. Setup the SNMP in Session Manager using the command "**setup_snmp <Community String>**". The default community string is set as **avaya123** if no community string is provided. The SNMP service is also restarted by this command.

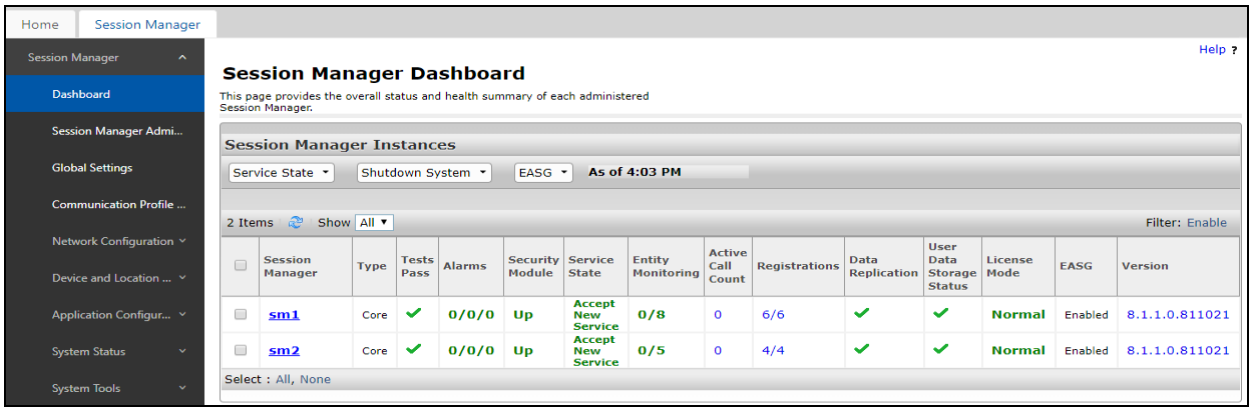
```
[cust@sm2 ~]$ setup_snmp
Community being defaulted to avaya123
Restarting/Starting SNMP Daemon
Stopping snmpd (via systemctl):  [  OK  ]
Starting snmpd (via systemctl):                            [  OK  ]
Session Manager basic SNMP agent V1/V2 configuration complete.
[cust@sm2 ~]$
```

5.2. Configure CDR User Account for Session Manager

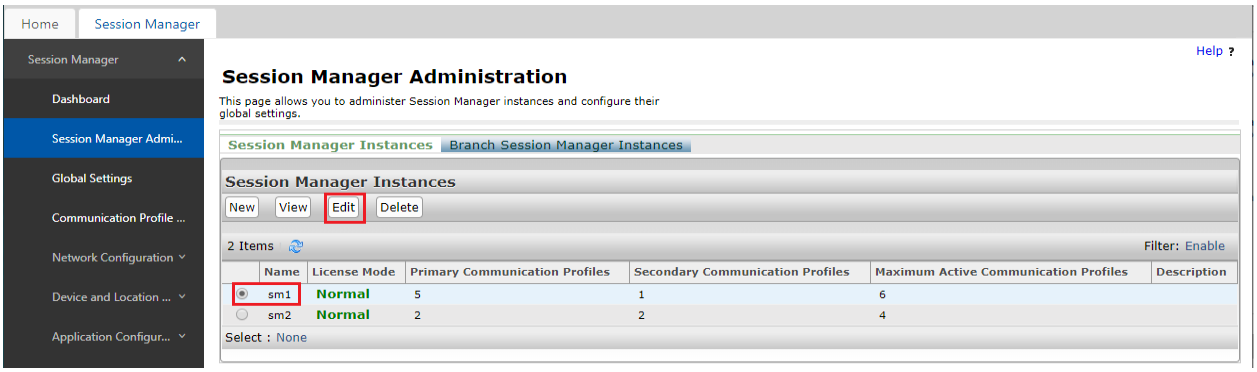
Using a web browser, enter https://<IP address of System Manager> to connect to the System Manager and log in using appropriate credentials.



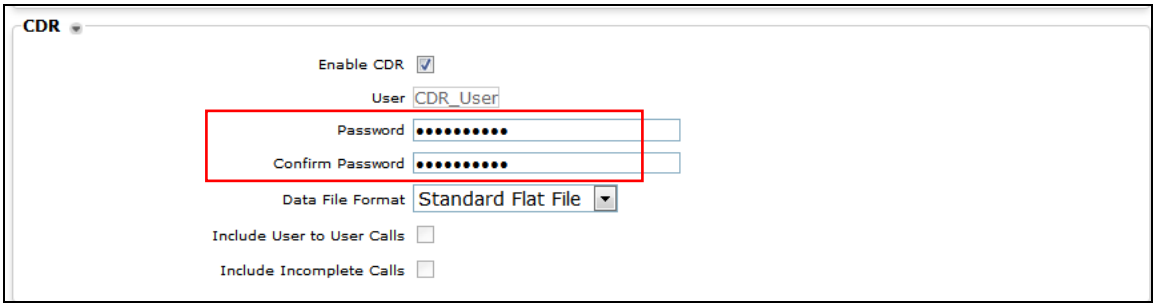
From the home screen (not shown), navigate to Session Manager by clicking **Elements → Session Manager → Dashboard**.



Click **Session Manager → Session Manager Administration**. On the right pane, click **Session Manager Instances** tab and select **sm1** (this may show as a different name, depending on the system in question). Click **Edit** to make changes.



On the right pane (not shown) under the **CDR** section, make sure the **Enable CDR** is checked and set the password for **CDR_User**. Select **Data File Format** as **Standard Flat File** for the default CDR file format. The other formats i.e., Enhanced Flat File and Enhanced XML File are supported but will require customization by Prognosis engineer to accommodate the different formats. For more details, refer to **[1]** in **Additional References** section.



Repeat above for SM2 CDR access configuration.

5.3. Configure VoIP/RTCP Monitoring server for SIP endpoint

The Prognosis will be the VoIP/RTCP Monitoring server for SIP endpoints and this is configured via System Manager. All other Avaya resources including IP Media Processor (MEDPRO) boards, media servers, media gateways and H.323 IP Deskphones will be configurated from Communication Manager. Refer to references **[4]** for setup of Communication Manager.

From the home screen, click **Elements → Session Manager → Device and Location Configuration → Device Settings Groups** (not shown). Under **Location Groups**, click **New**.

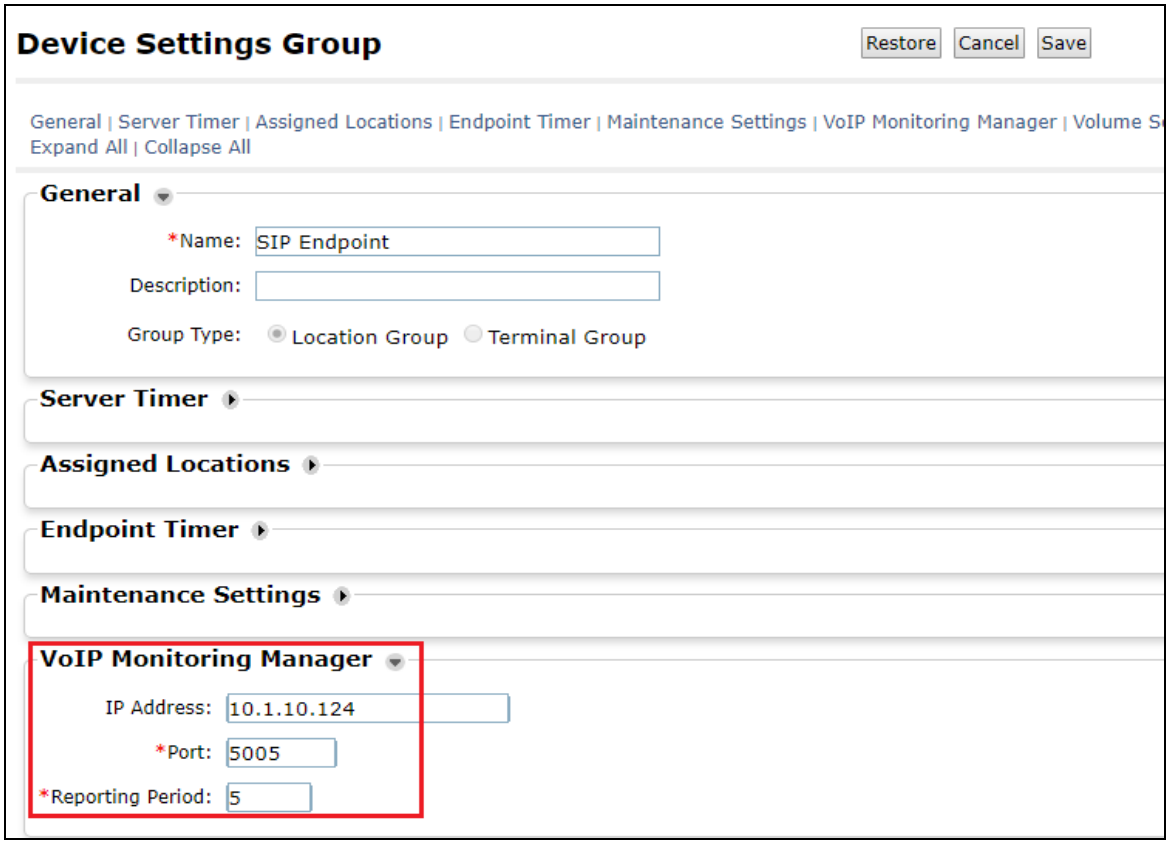
The following settings were configured:
General:

- **Name**: SIP Endpoint [Enter descriptive name of Location Group]
- **Description**: [Optional]
- **Group Type**: [Select Location Group]

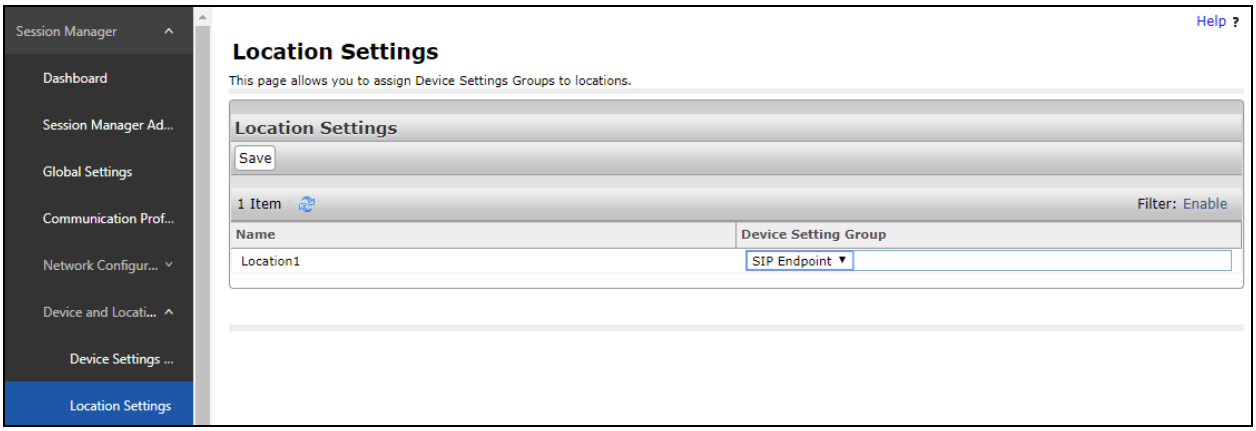
VoIP Monitoring Manager:

- **IP Address**: [IP address of Prognosis]
- **Port**: 5005 [Leave as Default]
- **Reporting Period**: 5 [Leave as Default]

Leave the rest of the parameters settings as default. Click **Save**.



From the home screen, click **Elements → Session Manager → Device and Location Configuration → Location Settings**. Depending on the locations created for the system, assigned the Location Group in the appropriate location. In this example, there is only one default location i.e., "Location1". Select the "SIP Endpoint" Location Group created earlier under **Device Setting Group** and click **Save**.

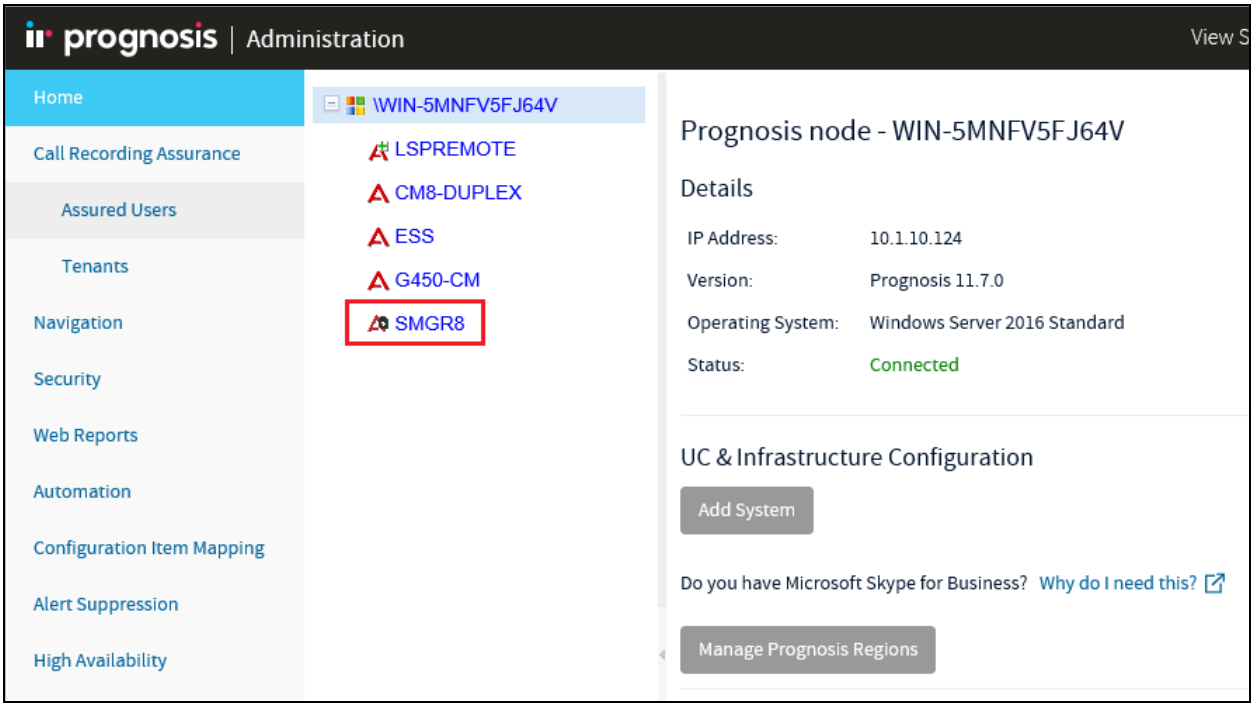


6. Configure Integrated Research Prognosis

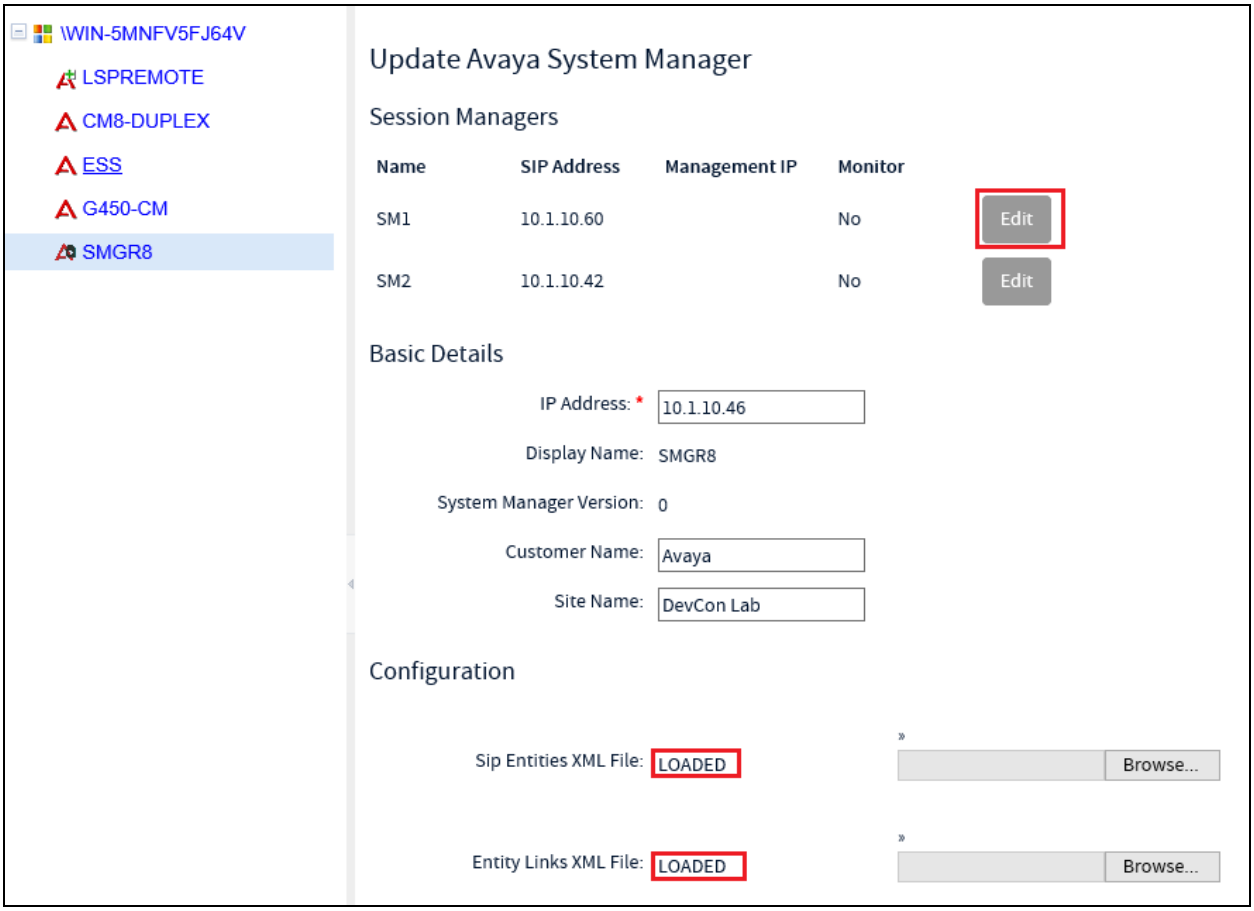
This section describes the configuration of Prognosis required to interoperate with Session Manager.

Log into the Prognosis Windows 2016 server with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Prognosis Administration**. Log in with the appropriate password.

From the home screen, click + below to expand the Server “WIN-5MNFV5FJ64V” in the middle pane. Refer to references **[5]** for setup of System Manager. Assuming System Manager has been added, click on the **SMGR8** to update the Session Manager in the next few steps.



The information for the Session Managers were provided in the entities XML files downloaded from System Manager. Check that the **Sip Entities XML File** and **Entity Links XML File** are **LOADED**. Click **Edit** on **SM1**.



The following settings were configured during the compliance test for **SM1**.

Session Manager Details:

- **Management IP: 10.1.10.59** [Management IP address of Session Manager]
- **Site Name: DevCon Lab** [Descriptive name of location]

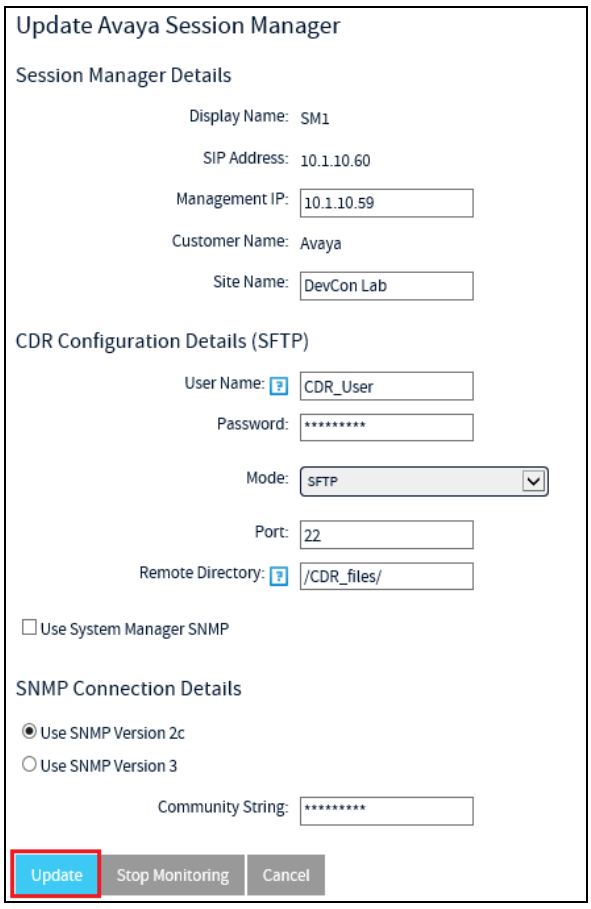
CDR Configuration Details (SFTP):

- **User Name: CDR_User**
- **Password:** As configured in **Section 5.2**
- **Mode: SFTP**
- **Port: 22** [As default]
- **Remote Directory: /CDR_files/**

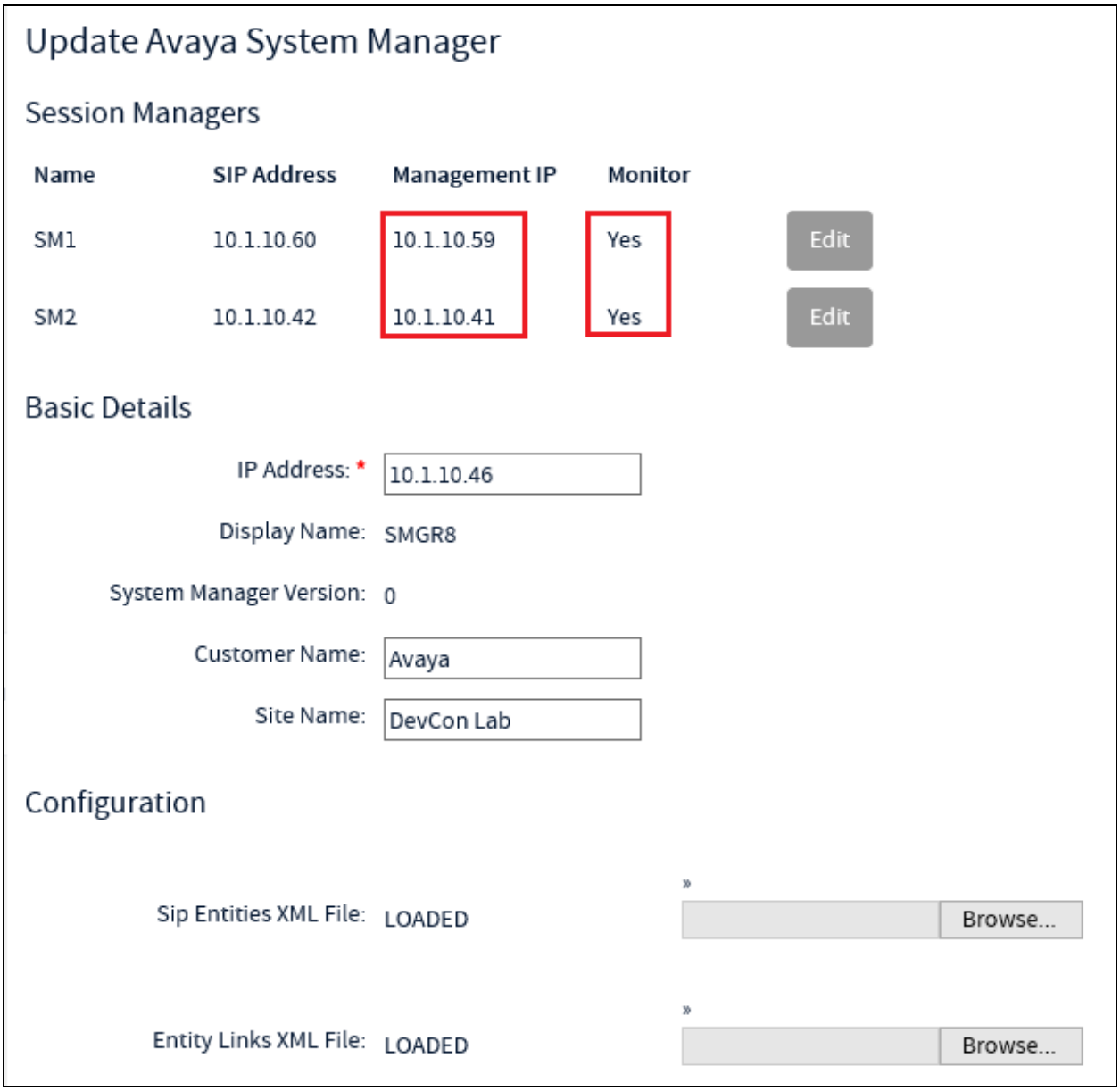
SNMP Connection Details:

Select **User SNMP Version 2c** and the **Community String** "avaya123". This is the default SNMP version and community string for Session Manager. However, if the Session Manager SNMP V3 is configured with System Manager web console, check the "**Use System Manager SNMP**". Follow similar steps as in **Section 5.1**.

Click **Update** to make the changes. Repeat the above for SM2 with **Management IP** as **10.1.10.41**.



Access the configuration of System Manager. Verify that the **Monitor** column for the Session Manager is set to **Yes** and the **Management IP** reflects the IP addresses set earlier.

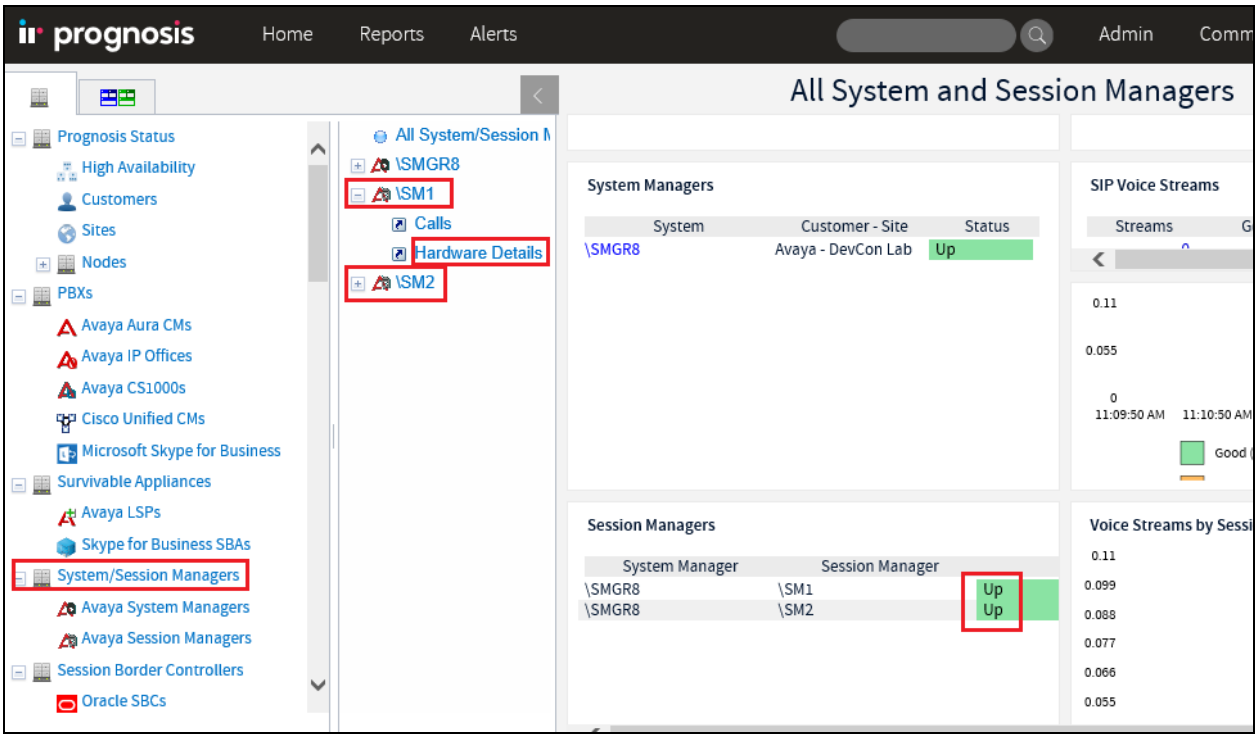


7. Verification Steps

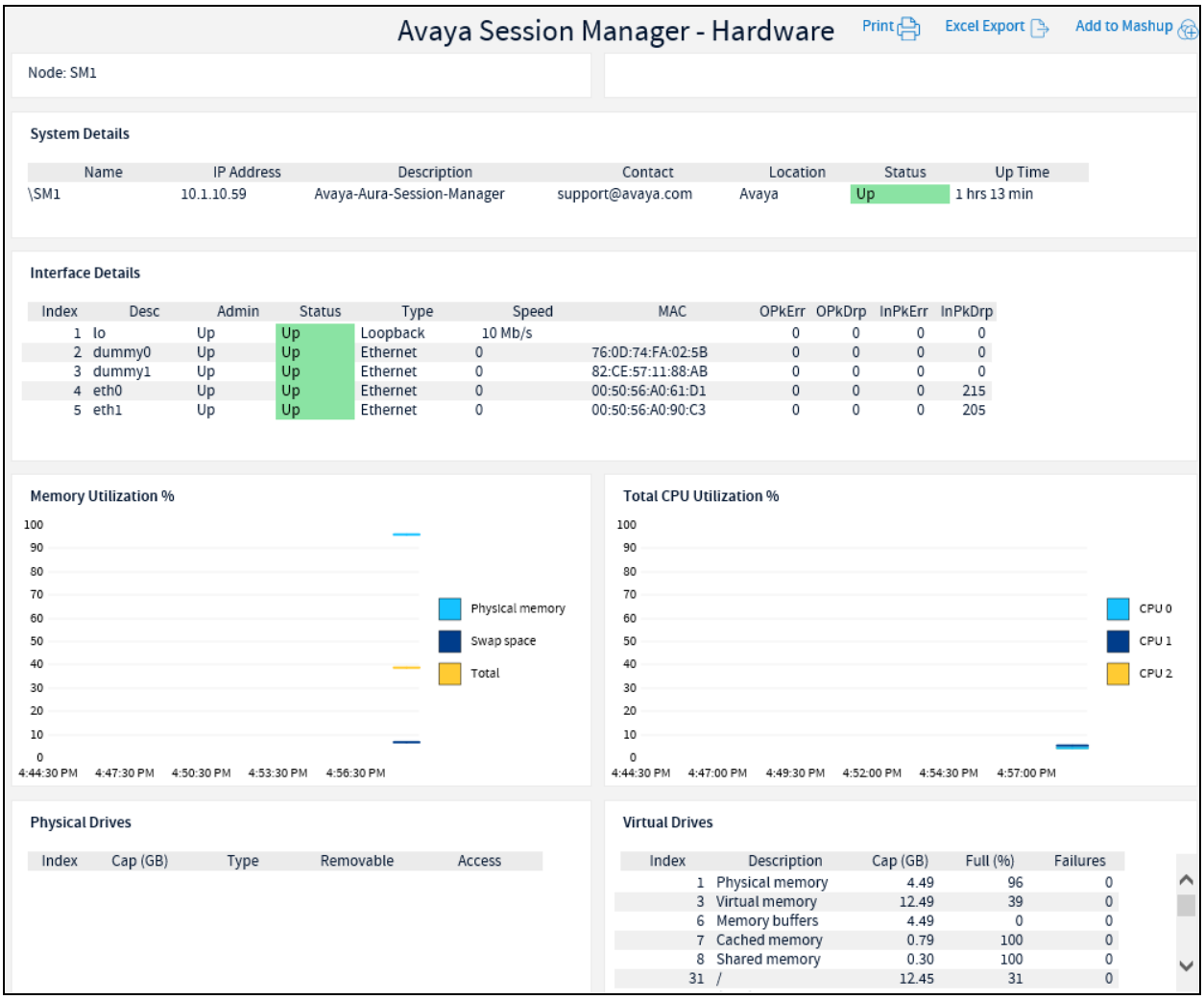
This section provides the tests that can be performed to verify proper configuration of Prognosis. The following steps are done using the Prognosis webui.

Log into the Prognosis Windows 2016 server with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Prognosis View Systems**. Log in with the appropriate password.

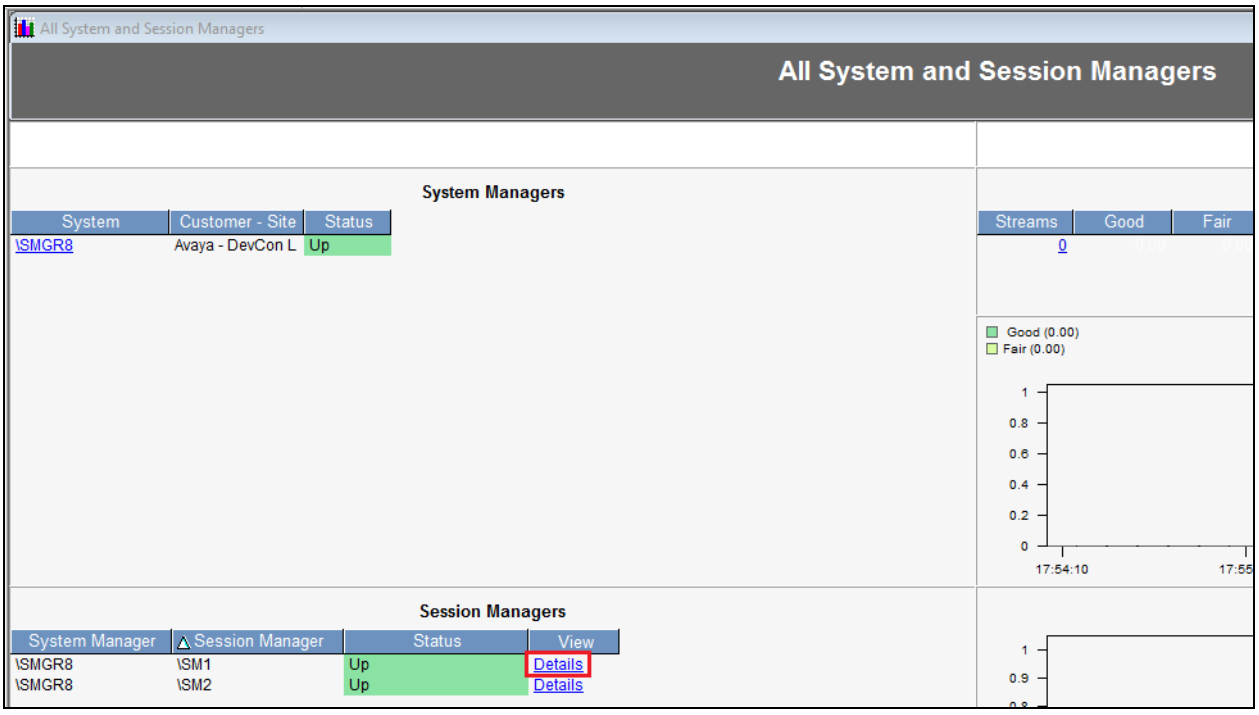
Select **System/Session Manager**s on the left pane. Check that the Session Managers created earlier i.e., **SM1** and **SM2** are shown below the System Manager **SMGR8**. Verify also the Session Managers **Status** is **Up**. Expand **SM1** by clicking the + symbol and select **Hardware Details**.



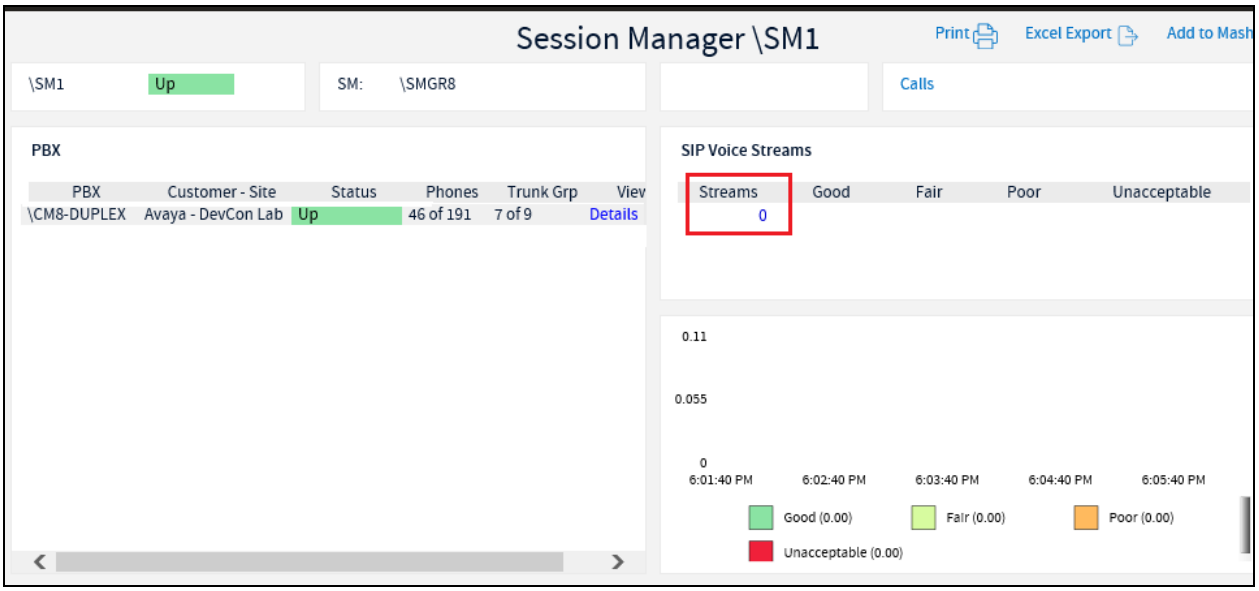
Verify hardware details of all Session Managers. Only **SM1 (Session Manager 1)** is shown below.



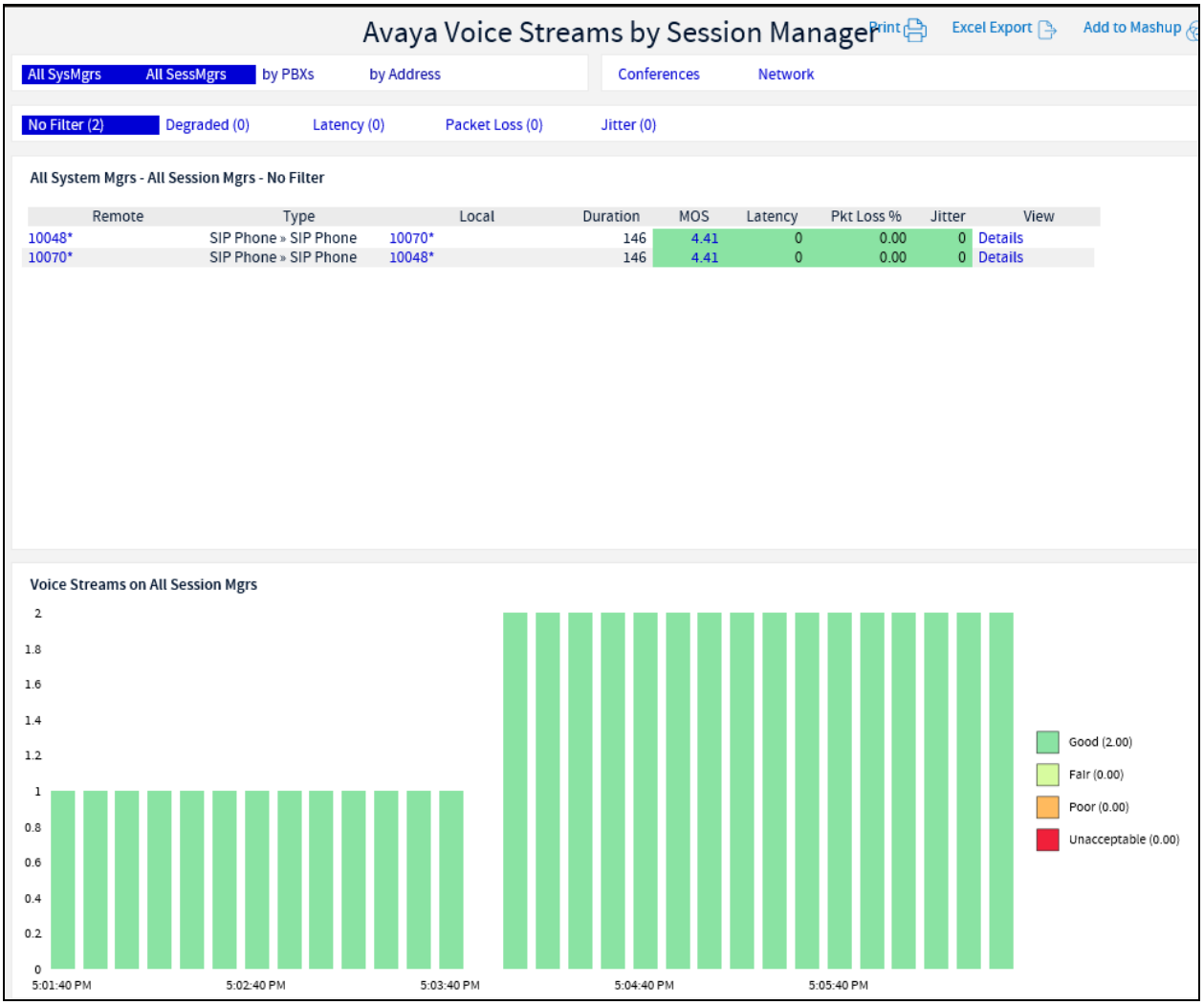
From the View System home screen, click on the **Details** of **SM1**.



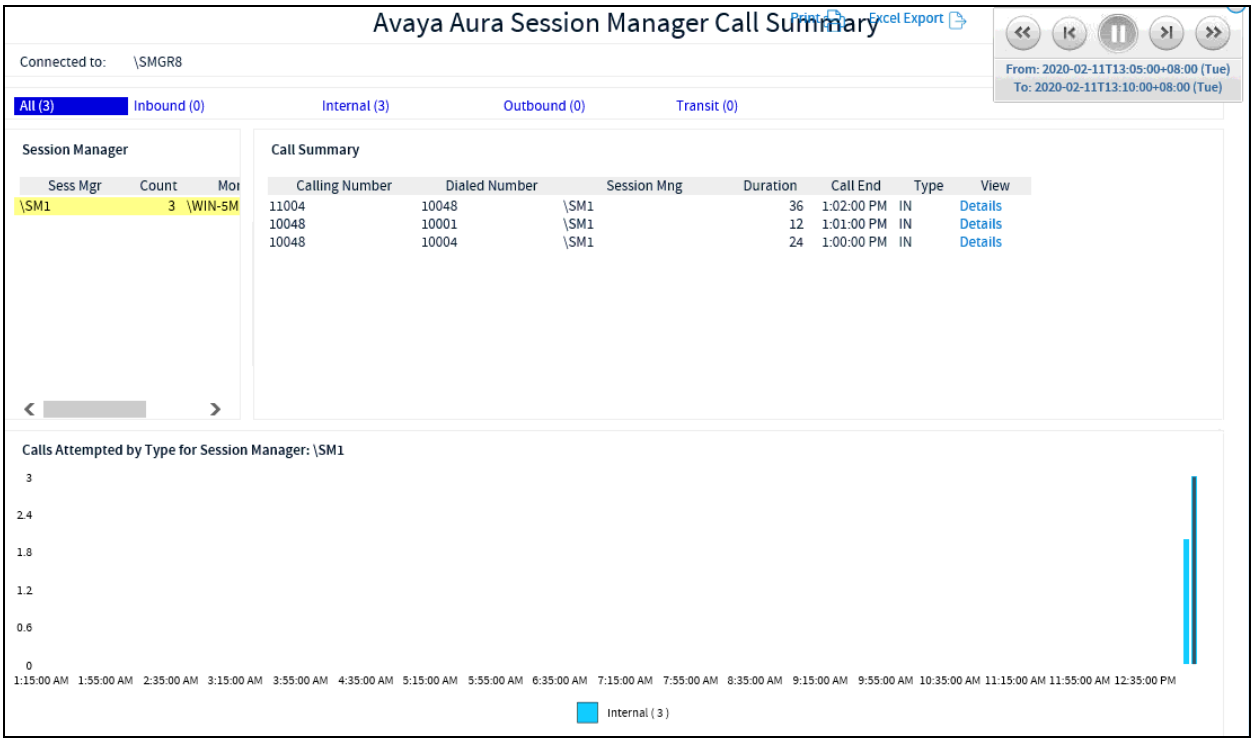
Verify that Avaya Aura® Communication Manager (PBX) that is connected to the Session Manager can be monitored from the next screen below.



Make a call between two Avaya IP SIP endpoints that belong to an IP Network Region that is being configured to send RTCP information to the Prognosis server. Verify that the **SIP Voice Streams** section on previous screen shows voice streams **count**. Click the highlighted count when there are voice streams count, show the details. Below is the screen of two Avaya IP SIP endpoints reflecting the quality of the call.



Make several calls and look at the **Call Summary**. Verify that calls are reported on the CDR data retrieved from each Session Manager. Compare with the records in the Session Manager CDR files and verify that they match. The CDR files can be retrieved by remotely logging into the Session Manager using the SFTP protocol with the account created in **Section 5.2**.



8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis R11.7 to interoperate with Avaya Aura® Session Manager 8.1. In the configuration described in these Application Notes, Prognosis obtained the configuration and status information through SNMP for Session Manager. Prognosis also processed the RTCP information to monitor the quality of SIP endpoint calls and collected CDR information from each Session Manager. During compliance testing, all test cases were completed successfully with observations in **Section 2.2**.

9. Additional References

The following Avaya documentations can be obtained on the http://support.avaya.com.

[1] *Administering Avaya Aura® Session Manager*, Release 8.1.1, Issue 2, Oct 2019.
[2] *Maintaining Avaya Aura® Session Manager*, Release 8.1, Issue 1, Jun 2019.
[3] *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 3, Jul 2019
[4] *Application Notes for Integrated Research's Prognosis for Unified Communications 11.7 with Avaya Aura® Communication Manager R8.1.*
[5] *Application Notes for Integrated Research Prognosis for Unified Communications R11.7 with Avaya Aura® System Manager R8.1.*

Prognosis documentations are provided in the online help that comes with the software package.

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 DevConnect Program at devconnect@avaya.com.