Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis for Unified Communications R11.4 with Avaya Aura® Session Manager R7.1 and Avaya Aura® System Manager R7.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis for Unified Communications R11.4 to interoperate with Avaya Aura® Session Manager and System Manager R7.1.

Prognosis for Unified Communications R11.4 provides real-time monitoring and management solutions for IP telephony networks. Prognosis for Unified Communications R11.4 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.

Prognosis uses Simple Network Management Protocol (SNMP) to query Session and System Manager for information and status. At the same time, Prognosis processes Real-time Transport Control Protocol (RTCP) from Avaya SIP endpoints and collects Call Detail Recording (CDR) information from each Session Manager.

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 R11.4 (herein after referred to as Prognosis) with Avaya Aura® System Manager R7.1 and Avaya Aura® Session Manager R7.1.

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

- Real Time Transport Control Protocol (RTCP) collection - Prognosis collects RTCP information sent by Avaya SIP 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 System Manager and 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 System Manager and 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 and SNMP but not for RTCP as requested by Integrated Research.

2.1. Interoperability Compliance Testing

For feature testing, Prognosis webui was used to view the configurations of System Manager and Session Manager such as the memory and CPU utilizations, disk usage and status from data collected via SNMP. For the collection of RTCP and CDR information, only SIP endpoints 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, System Manager and Session Managers were also performed during testing.

2.2. Test Results

All test cases passed successfully.

2.3. Support

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

- Hotline: +61 (2) 9921 1524
- Email: support@prognosis.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Prognosis interoperability with System Manager and Session Manager. The configuration consists of a duplex pair of Communication Manager system (System A) with two Avaya G650 Media Gateways, an Avaya G430 Media Gateway with Avaya S8300D Server as a Local Survivability Processor (LSP) and a local Avaya G250-BRI Media Gateway. An Enterprise Survivable Server (ESS) was also configured. A second Communication Manager system (System B) has an Avaya G450 Media Gateway. Both systems have Avaya H323, SIP, digital and analog endpoints 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 2012 R2 with Service Pack 1. Both the Monitoring Node and Web Application software are installed on this server.

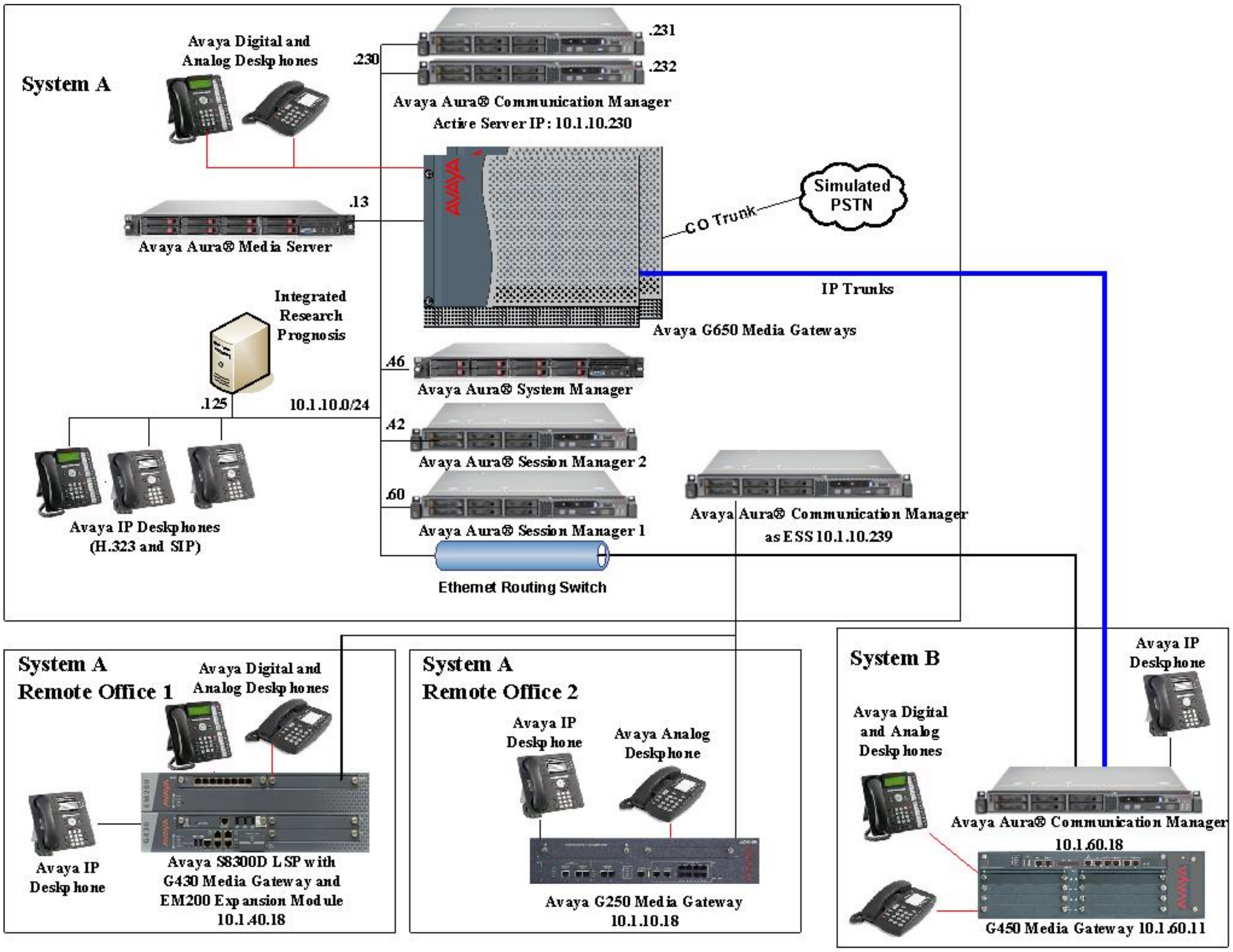

System A
Avaya Digital and Analog Deskphones
.230
.231
.232
Avaya Aura® Communication Manager Active Server IP: 10.1.10.230
.13
Avaya Aura® Media Server
CO Trunk
Simulated PSTN
IP Trunks
Avaya G650 Media Gateways
Integrated Research Prognosis
.125
10.1.10.0/24
.46
Avaya Aura® System Manager
.42
Avaya Aura® Session Manager 2
.60
Avaya Aura® Session Manager 1
Avaya IP Deskphones (H.323 and SIP)
Avaya Aura® Communication Manager as ESS 10.1.10.239
Ethernet Routing Switch
System A Remote Office 1
Avaya Digital and Analog Deskphones
Avaya IP Deskphone
Avaya S8300D LSP with G430 Media Gateway and EM200 Expansion Module 10.1.40.18
System A Remote Office 2
Avaya IP Deskphone
Avaya Analog Deskphone
Avaya G250 Media Gateway 10.1.10.18
System B
Avaya IP Deskphone
Avaya Digital and Analog Deskphones
Avaya Aura® Communication Manager 10.1.60.18
G450 Media Gateway 10.1.60.11

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 (System A)	7.1.2.0.0.532.24184
Avaya Aura® Media Server	7.8.0.333
Avaya G650 Media Gateway - TN2312BP IP Server Interface (x 2) - TN799DP C-LAN Interface (x 4) - TN2602AP IP Media Processor (x 2) - TN2302AP IP Media Processor (x 2) - TN2464BP DS1 Interface - TN2464CP DS1 Interface - TN793CP Analog Line - TN2214CP Digital Line - TN2501AP Announcement	 HW07, FW058 HW01, FW044 HW02 FW066 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW012 HW08, FW016 HW03 FW023
Avaya G250 Media Gateway	30.27.1
Avaya Aura® Communication Manager (System B)	7.1.2.0.0.532.24184
Avaya G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	39.5.0 HW01 FW008 HW07 FW015 HW10 FW099 HW03 FW015 HW11 FW053
Avaya Aura® Communication Manager running on Avaya S8300D Server (G430 Media Gateway - LSP)	7.1.2.0.0.532.24184
Avaya G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	39.5.0 HW04 FW015 HW12 FW098 HW31 FW098 HW05 FW022
Avaya Aura® Communication Manager (ESS)	7.1.2.0.0.532.24184
Avaya Aura® System Manager	7.1.2.0 Build No.– 7.1.0.0.1125193
Avaya Aura® Session Manager (1)	7.1.2.0.712004
Avaya Aura® Session Manager (2)	7.1.2.0.712004
96x1 Series IP Deskphones - 9641G - 9611G	7.1.1.0 (SIP) 6.6506 (H323)

Equipment/Software	Release/Version
Avaya 1600 Series IP Deskphones - 1608-I - 1603SW-I	1.3100 (H.323)
Avaya Digital Deskphones - 1408 - 1416	Rel 4 SP9
Avaya Analog Phones	-
Avaya one-X Communicator	6.2.12.04-SP12 (H.323)
Prognosis running on Windows 2012 R2 SP1	11.4

Note: All Avaya Aura® systems are installed on VMware 5.x or Avaya Virtual Platform for S8300D.

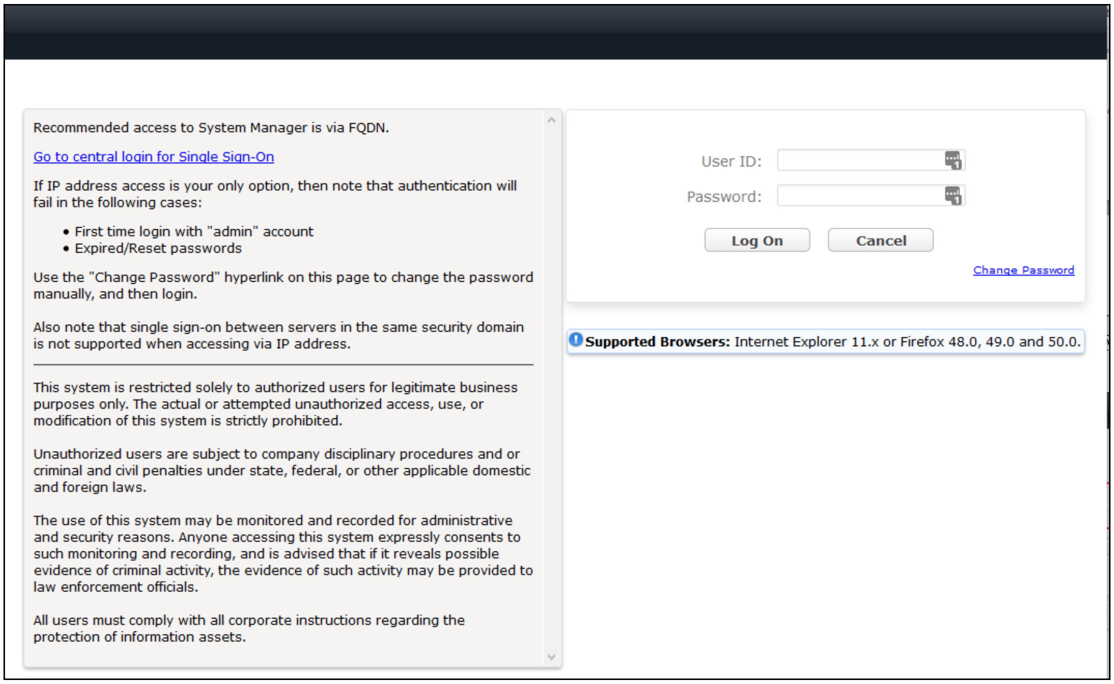
5. Configure Avaya Aura® System and Session Manager

This section describes the steps needed to configure System and Session Manager to interoperate with Prognosis. This includes configuration of the SNMP v3 user profile for System Manager and the CDR user account on both Session Managers. The default SNMP v2c user profile will be used for Session Managers.

5.1. Configure SNMP

The following shows the steps to create SNMPv3 user profiles and assign the profile to System Manager and setup the default Session Managers SNMPv2c profile.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Using a web browser, enter https://<IP address of System Manager> to connect to the System Manager server being configured and log in using appropriate credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

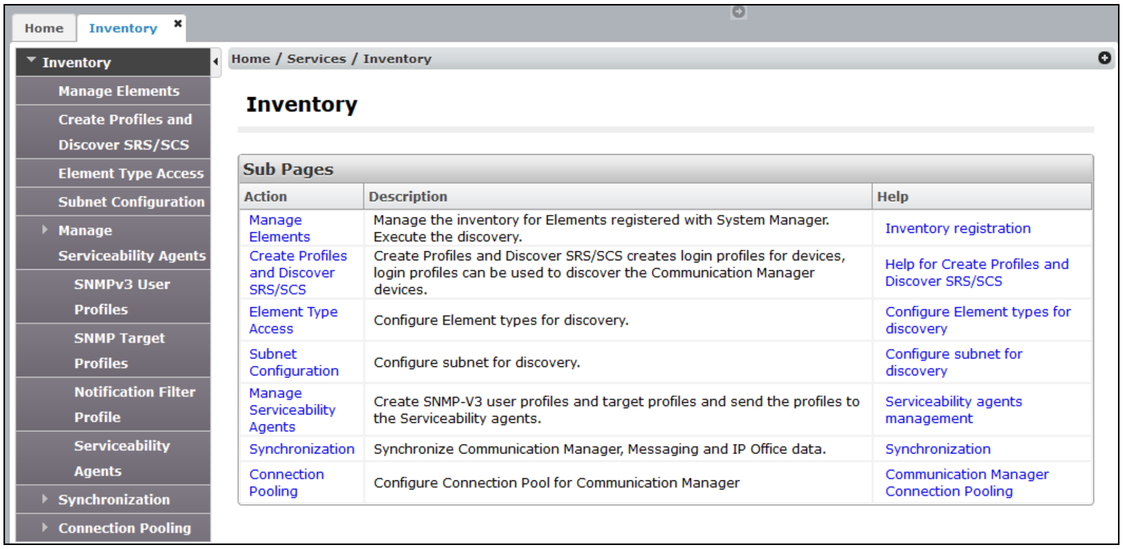
User ID:

Password:

Log On Cancel

Change Password

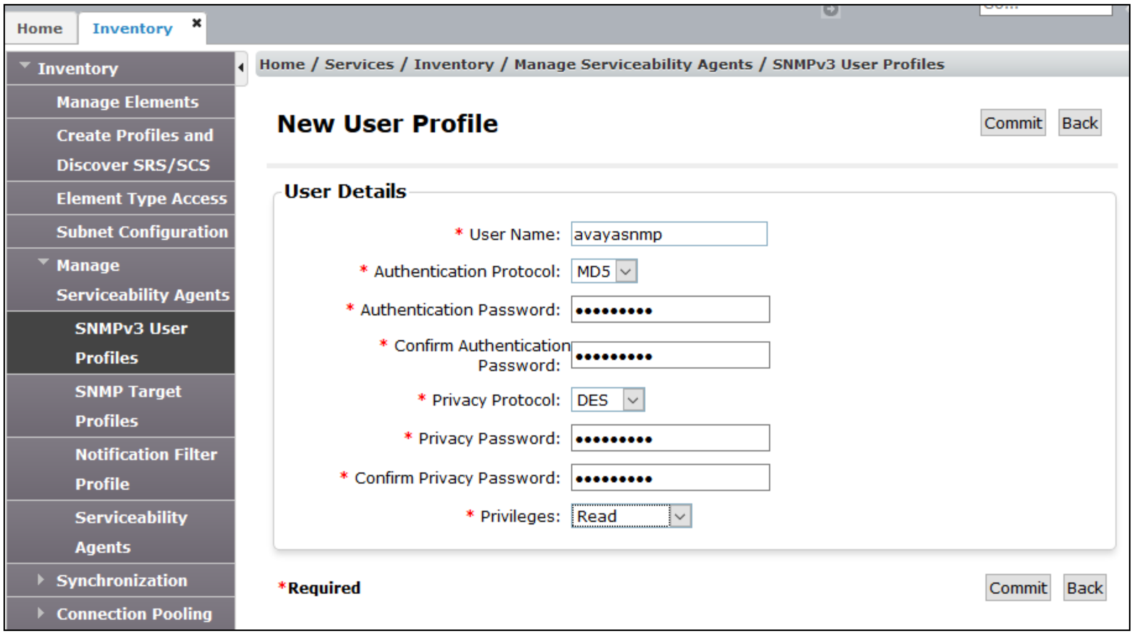
Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.
</td></tr>
<tr><td>2.</td><td>On the home screen (not shown), select <b>Services → Inventory</b>.



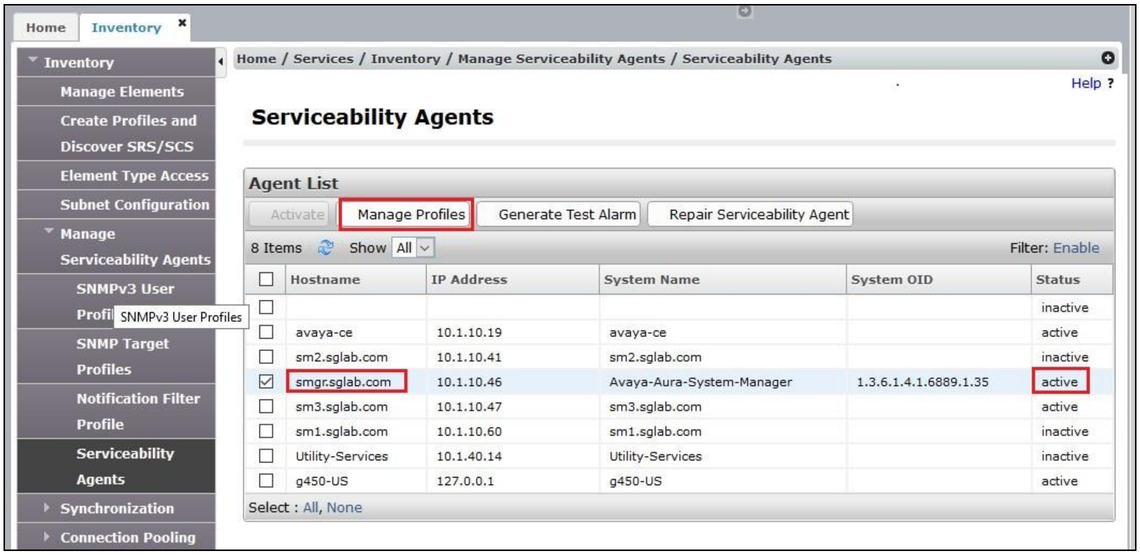
Inventory

Sub Pages

<table>
<tr><th>Action</th><th>Description</th><th>Help</th></tr>
<tr><td>Manage Elements</td><td>Manage the inventory for Elements registered with System Manager. Execute the discovery.</td><td>Inventory registration</td></tr>
<tr><td>Create Profiles and Discover SRS/SCS</td><td>Create Profiles and Discover SRS/SCS creates login profiles for devices, login profiles can be used to discover the Communication Manager devices.</td><td>Help for Create Profiles and Discover SRS/SCS</td></tr>
<tr><td>Element Type Access</td><td>Configure Element types for discovery.</td><td>Configure Element types for discovery</td></tr>
<tr><td>Subnet Configuration</td><td>Configure subnet for discovery.</td><td>Configure subnet for discovery</td></tr>
<tr><td>Manage Serviceability Agents</td><td>Create SNMP-V3 user profiles and target profiles and send the profiles to the Serviceability agents.</td><td>Serviceability agents management</td></tr>
<tr><td>Synchronization</td><td>Synchronize Communication Manager, Messaging and IP Office data.</td><td>Synchronization</td></tr>
<tr><td>Connection Pooling</td><td>Configure Connection Pool for Communication Manager</td><td>Communication Manager Connection Pooling</td></tr>
</table>
</td></tr>
</table>

Step	Description
3.	Select and expand on the **Manage Serviceability Agents → SNMPv3 User Profiles** and click **New** (not shown) to add a new user profile. Enter the details for the **User Details** according to security level required. The user profile will be defined in the Prognosis configuration **Section 6 Step 4**. For more secured configuration, the profiles can be adjusted here, and the corresponding Prognosis configuration in **Section 6 Step 4** must then be adjusted as well. • **User Name**: avayasnmp [Enter a descriptive name desired] • **Authentication Protocol**: [Select MD5 or SHA] • **Authentication Password**: [Enter and confirm password] • **Privacy Protocol**: [Select DES or AES] • **Privacy Password**: [Enter and confirm password] • **Privileges**: Read Click **Commit** to submit. Below is the configuration setup in this compliance test.  Home Inventory Inventory Manage Elements Create Profiles and Discover SRS/SCS Element Type Access Subnet Configuration Manage Serviceability Agents SNMPv3 User Profiles SNMP Target Profiles Notification Filter Profile Serviceability Agents Synchronization Connection Pooling Home / Services / Inventory / Manage Serviceability Agents / SNMPv3 User Profiles Commit Back New User Profile User Details * User Name: avayasnmp * Authentication Protocol: MD5 * Authentication Password: ••••••••• * Confirm Authentication Password: ••••••••• * Privacy Protocol: DES * Privacy Password: ••••••••• * Confirm Privacy Password: ••••••••• * Privileges: Read *Required

Step	Description
4.	Navigate to **Inventory → Manage Serviceability Agents → Serviceability Agents**. Check that the System Manager Agent **Status** is active. Select the System Manager (**smgr.sglab.com**) and select the **Manage Profiles** tab.



Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

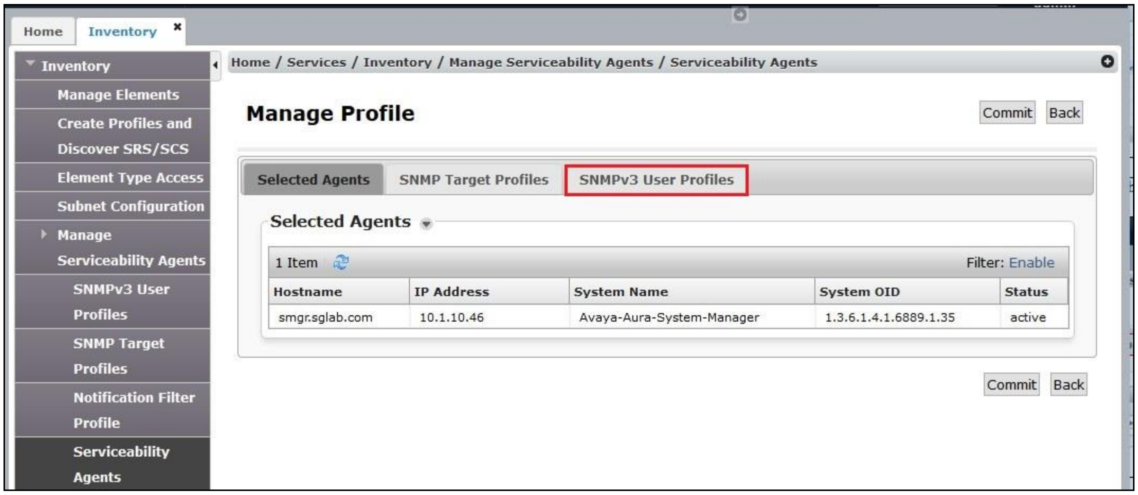
Serviceability Agents

Agent List

8 Items

☐	Hostname	IP Address	System Name	System OID	Status
☐					inactive
☐	avaya-ce	10.1.10.19	avaya-ce		active
☐	sm2.sglab.com	10.1.10.41	sm2.sglab.com		inactive
☑	smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
☐	sm3.sglab.com	10.1.10.47	sm3.sglab.com		active
☐	sm1.sglab.com	10.1.10.60	sm1.sglab.com		inactive
☐	Utility-Services	10.1.40.14	Utility-Services		inactive
☐	g450-US	127.0.0.1	g450-US		active

Step	Description
5.	Select **SNMPv3 User Profiles** tab and the screen will be shown in next step.



Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

Manage Profile

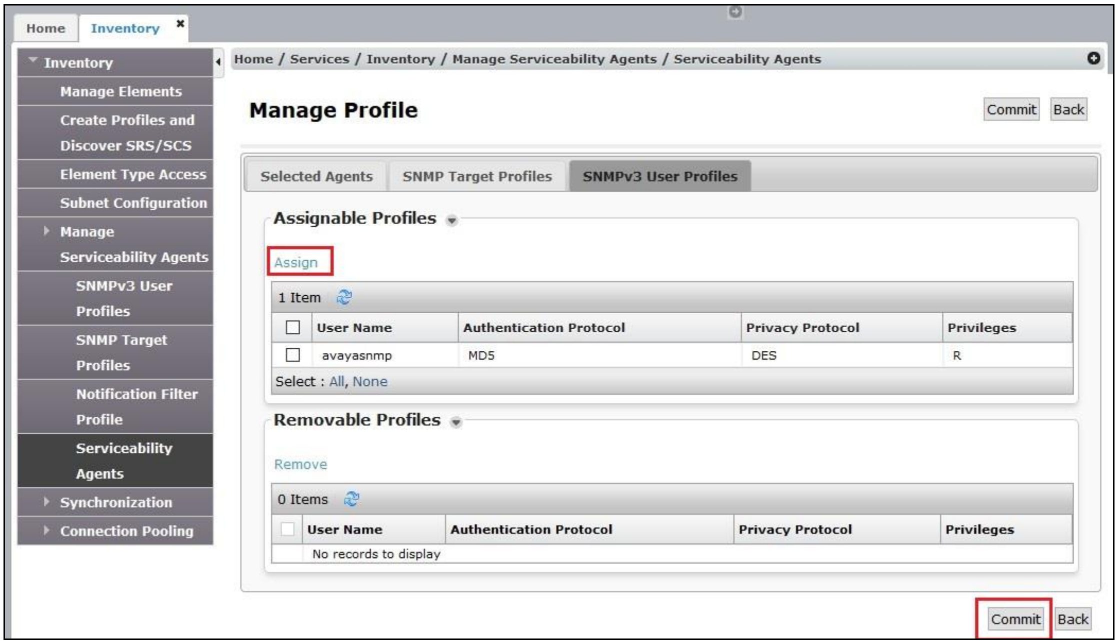
Selected Agents

1 Item

Hostname	IP Address	System Name	System OID	Status
smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>

Click *down arrow* beside **Assignable Profiles** section if it is not expanded. Select the user profile created earlier in **Step 3**. Click **Assign** to assign the profile to System Manager. The user profile will move to the **Removable Profiles** section. Click **Commit** to submit the changes.



Manage Profile

Assignable Profiles

1 Item

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
□	avayasnmp	MD5	DES	R

Select : All, None

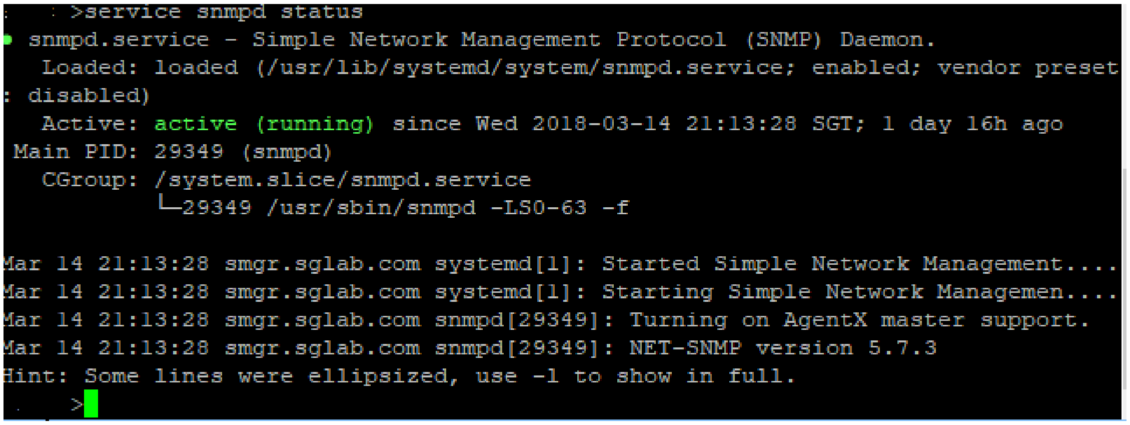
Removable Profiles

0 Items

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
	No records to display			

</td></tr>
<tr><td>7.</td><td>

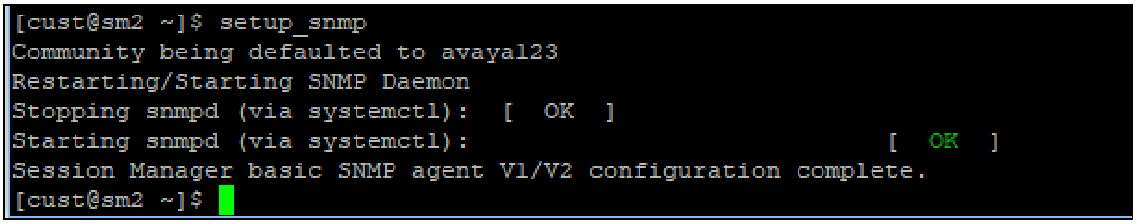
SSH into the System Manager command line interface and log in as valid user. Verify that the SNMP service is running using the command "**service snmpd status**". Otherwise, run the command "**service snmpd restart/start**" to start SNMP service daemon. Login with sufficient privileges to perform this verification.



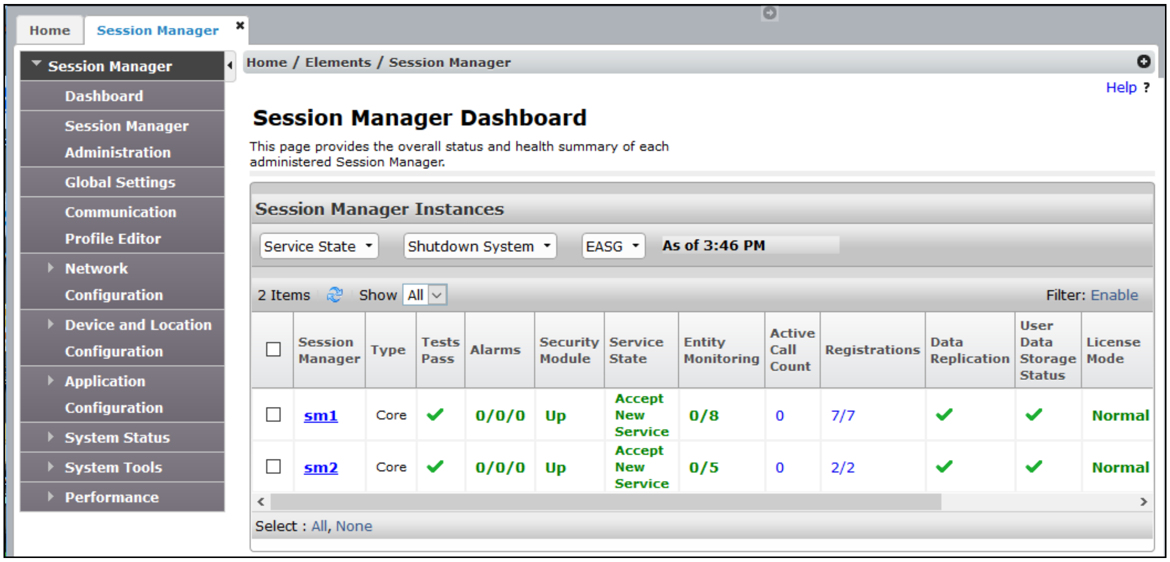
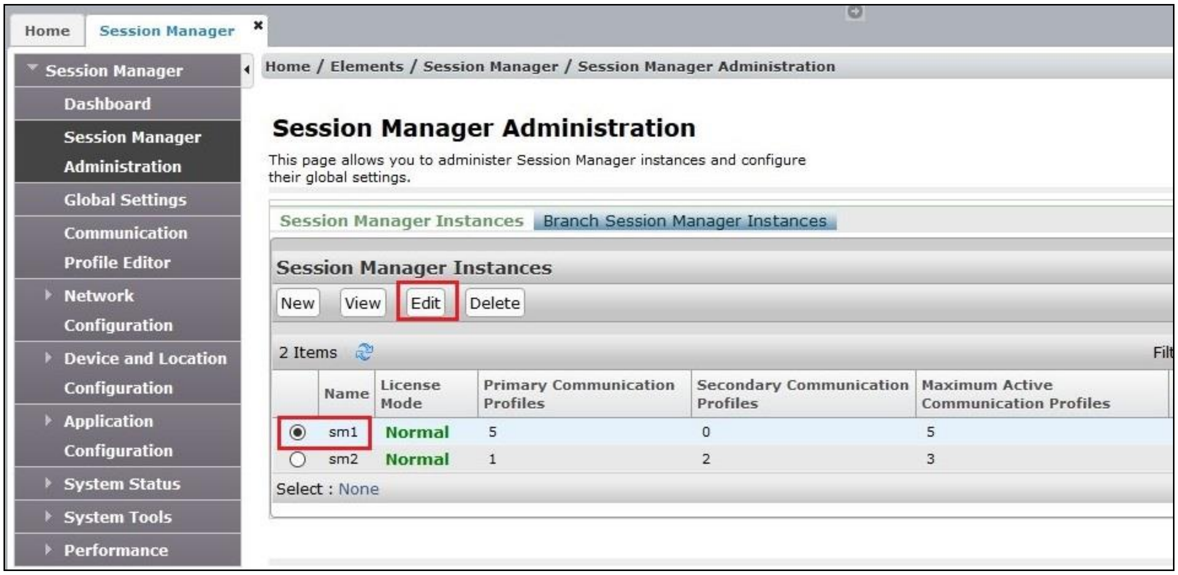
```
:   : >service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset
: disabled)
   Active: active (running) since Wed 2018-03-14 21:13:28 SGT; 1 day 16h ago
 Main PID: 29349 (snmpd)
   CGroup: /system.slice/snmpd.service
           └─29349 /usr/sbin/snmpd -LS0-63 -f

Mar 14 21:13:28 smgr.sglab.com systemd[1]: Started Simple Network Management....
Mar 14 21:13:28 smgr.sglab.com systemd[1]: Starting Simple Network Managemen....
Mar 14 21:13:28 smgr.sglab.com snmpd[29349]: Turning on AgentX master support.
Mar 14 21:13:28 smgr.sglab.com snmpd[29349]: NET-SNMP version 5.7.3
Hint: Some lines were ellipsized, use -l to show in full.
     >
```

</td></tr>
</table>

Step	Description
8.	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

Step	Description
1.	From the home screen (not shown), navigate to Session Manager by clicking **Elements → Session Manager**. 
2.	Click **Session Manager → Session Manager Administration**. On the right pane, click **Session Manager Instances** tab and select **sm1**. Click **Edit** to make changes. 

Home / Elements / Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State ▾ Shutdown System ▾ EASG ▾ As of 3:46 PM

2 Items Show All Filter: Enable

□	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode
□	sm1	Core	✓	0/0/0	Up	Accept New Service	0/8	0	7/7	✓	✓	Normal
□	sm2	Core	✓	0/0/0	Up	Accept New Service	0/5	0	2/2	✓	✓	Normal

Select : All, None

Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Session Manager Instances
Branch Session Manager Instances
New
View
Edit
Delete

Home / Elements / Session Manager / Session Manager Administration

Session Manager Administration

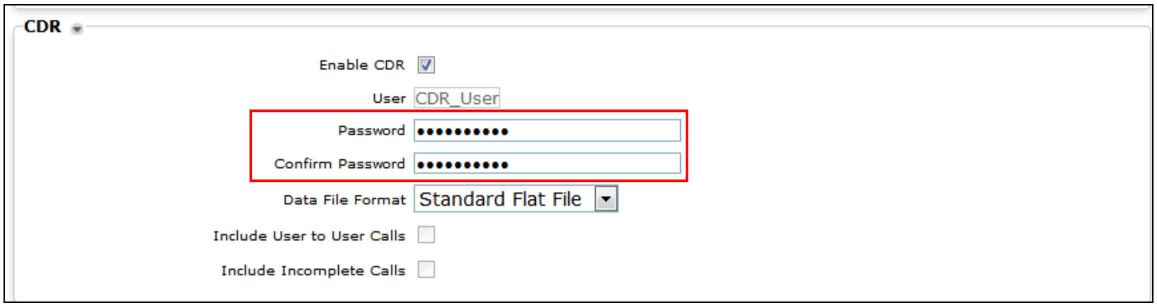
This page allows you to administer Session Manager instances and configure their global settings.

Session Manager Instances

2 Items Filt

	Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles
●	sm1	Normal	5	0	5
○	sm2	Normal	1	2	3

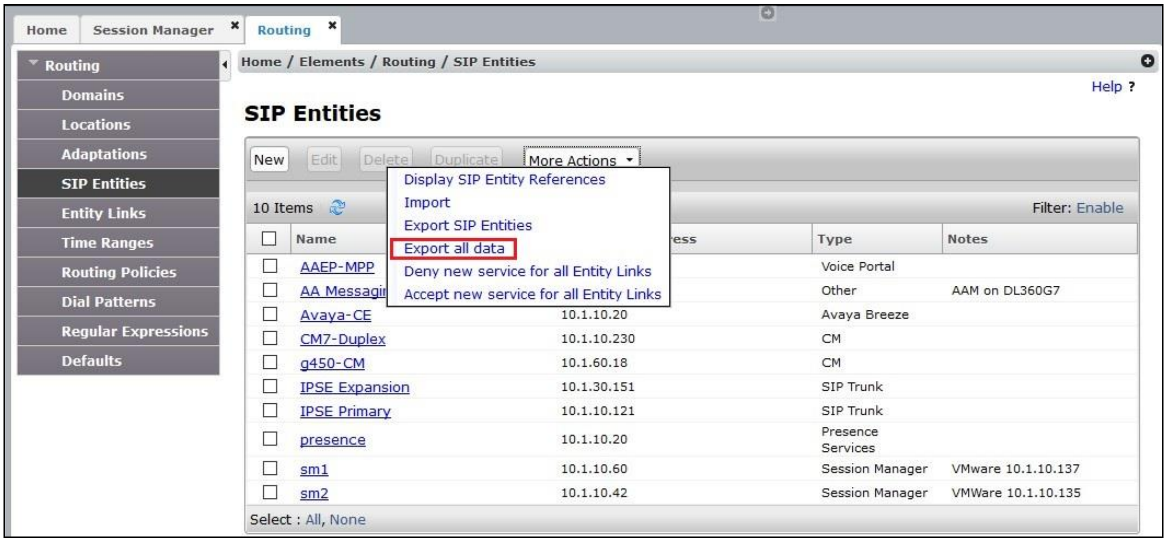
Select : None

Step	Description
3.	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 **[4]** in **Additional References** Section.  CDR Enable CDR ☑ User CDR_User Password ●●●●●●●●●●● Confirm Password ●●●●●●●●●●● Data File Format Standard Flat File Include User to User Calls □ Include Incomplete Calls □
4.	Repeat **Step 2** for sm2 CDR access configuration.

5.3. Download SIP Entities and Entity Links XML Files

The SIP Entities and Entity Links XML files are required for input into Prognosis for configuration of System Manager and Session Manager. These files can be downloaded from System Manager.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>On the System Manager home screen (not shown), select <b>Elements → Routing</b>. Click <b>Routing → SIP Entities</b> and select <b>Export all data</b> in the <b>More Actions</b> drop-down menu. Save the zip file into the local PC hard disk. Extract the files "<i>&lt;user name>EntityLinks.xml</i>" and "<i>&lt;user name>SipEntities.xml</i>". Rename the files without the user name. Upload the renamed files "EntityLinks.xml' and "SipEntities.xml" into the Prognosis server in <b>Section 6 Step 4</b>.



SIP Entities
10 Items

<table>
<tr><th>□</th><th>Name</th><th>ess</th><th>Type</th><th>Notes</th></tr>
<tr><td>□</td><td>AAEP-MPP</td><td></td><td>Voice Portal</td><td></td></tr>
<tr><td>□</td><td>AA Messagi</td><td></td><td>Other</td><td>AAM on DL360G7</td></tr>
<tr><td>□</td><td>Avaya-CE</td><td>10.1.10.20</td><td>Avaya Breeze</td><td></td></tr>
<tr><td>□</td><td>CM7-Duplex</td><td>10.1.10.230</td><td>CM</td><td></td></tr>
<tr><td>□</td><td>g450-CM</td><td>10.1.60.18</td><td>CM</td><td></td></tr>
<tr><td>□</td><td>IPSE Expansion</td><td>10.1.30.151</td><td>SIP Trunk</td><td></td></tr>
<tr><td>□</td><td>IPSE Primary</td><td>10.1.10.121</td><td>SIP Trunk</td><td></td></tr>
<tr><td>□</td><td>presence</td><td>10.1.10.20</td><td>Presence Services</td><td></td></tr>
<tr><td>□</td><td>sm1</td><td>10.1.10.60</td><td>Session Manager</td><td>VMware 10.1.10.137</td></tr>
<tr><td>□</td><td>sm2</td><td>10.1.10.42</td><td>Session Manager</td><td>VMWare 10.1.10.135</td></tr>
</table>
</td></tr>
</table>

5.4. Configure RTCP Monitoring

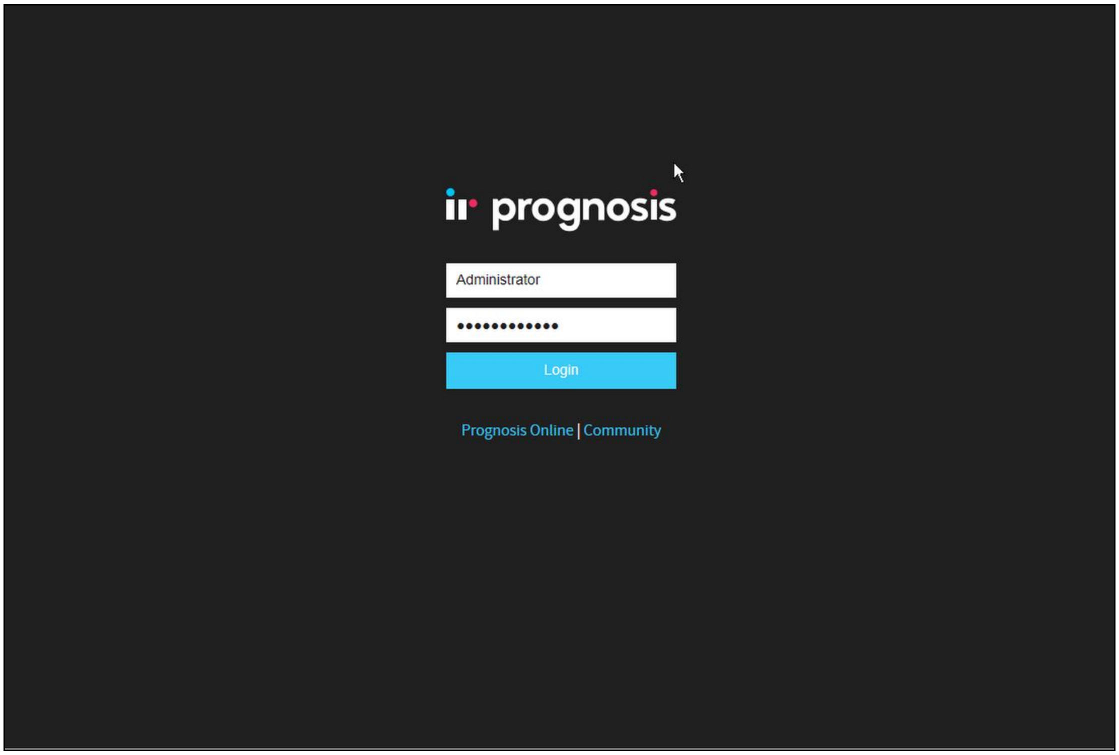
To allow Prognosis to monitor the voice quality of SIP endpoint calls, configure Avaya SIP endpoints to send RTCP reporting to the IP address of the Prognosis server. This is done through the 46xxsettings file.

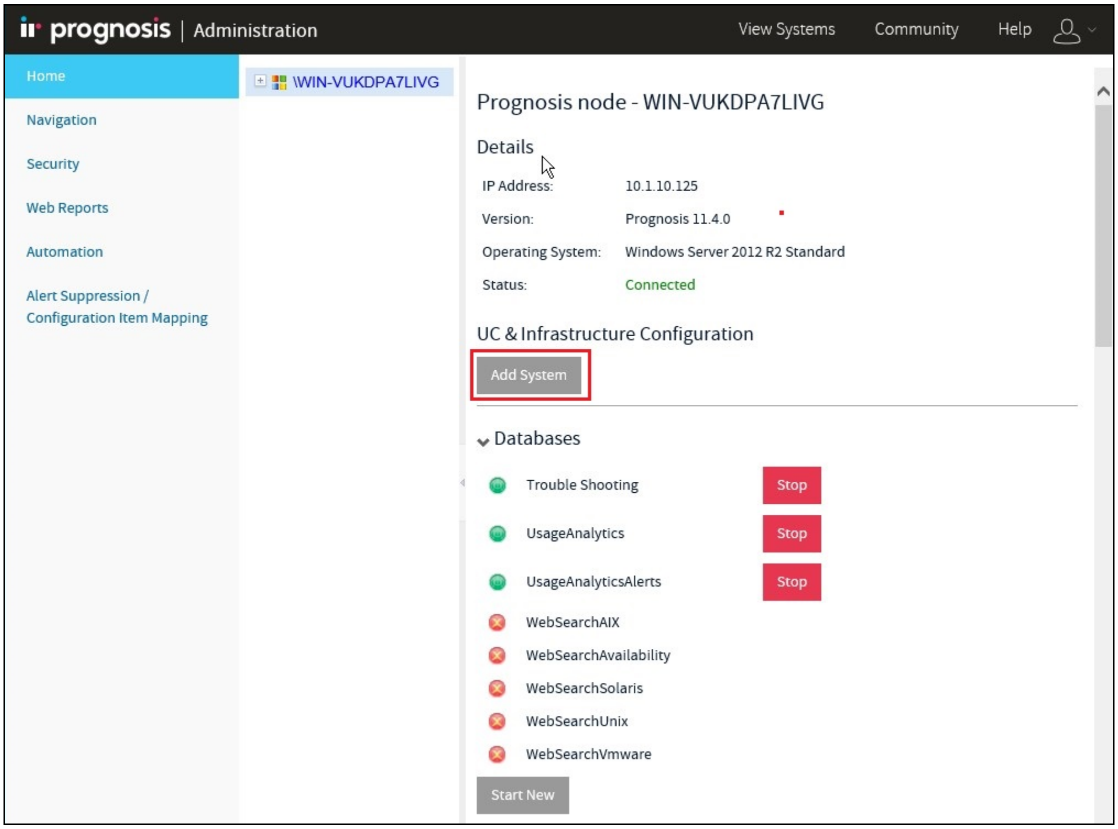
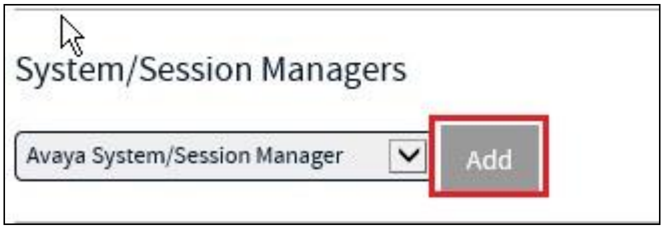
1. Configured **RTCP MONITORING** portion of the 46xxsettings file as below. The SIP endpoints need to be restarted for the configuration to be loaded.

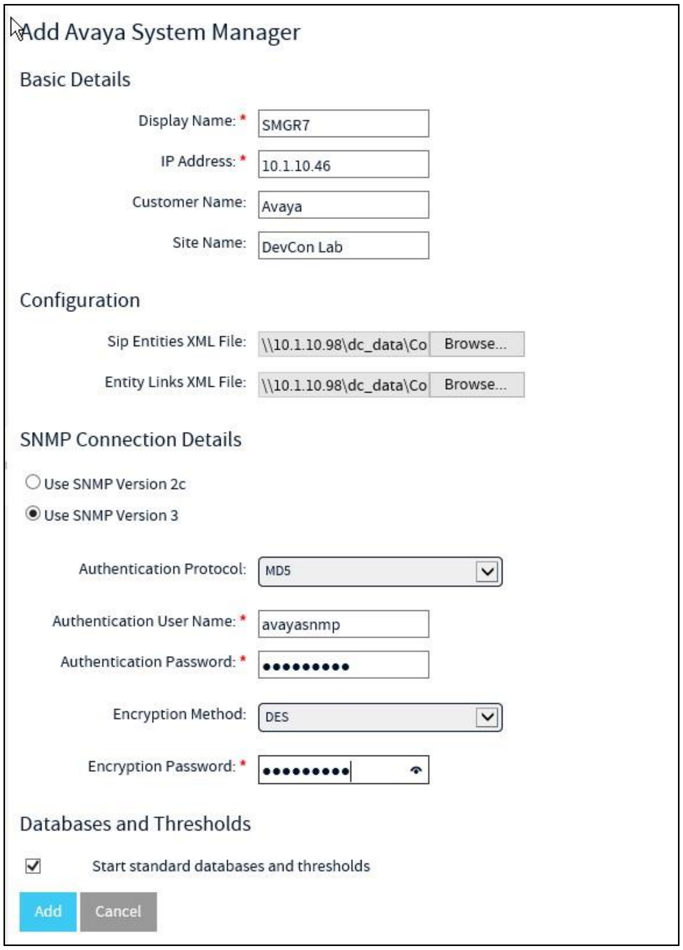
```
###################  RTCP MONITORING  #####################
##
## The RTCP monitor
SET RTCPMON 10.1.10.125
##
SET RTCPMONPORT 5005
##
## RTCP Monitor Report Period
SET RTCPMONPERIOD 5
##
## RTCPCONT specifies whether the sending of RTCP is enabled.
##     0 for No
##     1 for Yes
SET RTCPCONT 1
```

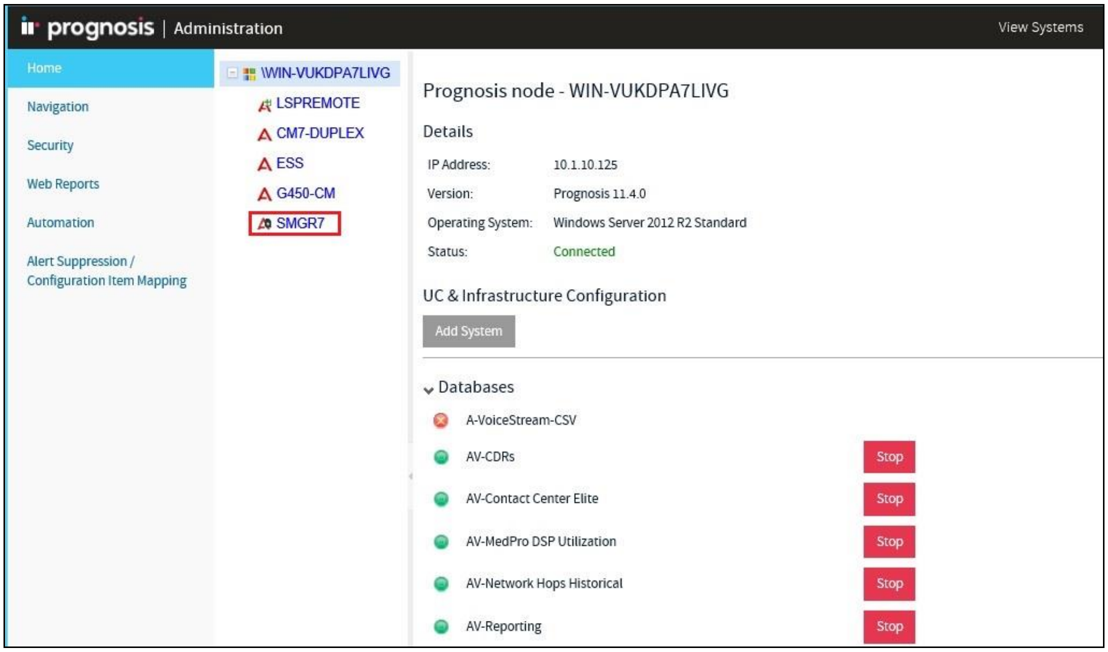
6. Configure Integrated Research Prognosis

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

Step	Description
1.	Log into the Prognosis server with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Prognosis Administration**. Log in with the appropriate password.  Administrator •••••••••••••

Step	Description
2.	Click **Add System**.  prognosis | Administration View Systems Community Help Home Navigation Security Web Reports Automation Alert Suppression / Configuration Item Mapping \WIN-VUKDPA7LIVG Add System Stop Start New Prognosis node - WIN-VUKDPA7LIVG Details IP Address: 10.1.10.125 Version: Prognosis 11.4.0 Operating System: Windows Server 2012 R2 Standard Status: Connected UC & Infrastructure Configuration Databases Trouble Shooting UsageAnalytics UsageAnalyticsAlerts WebSearchAIX WebSearchAvailability WebSearchSolaris WebSearchUnix WebSearchVmware
3.	Select **Avaya System/Session Manager** from the drop-down menu. Click **Add** to add a new System Manager.  System/Session Managers Avaya System/Session Manager

Step	Description
4.	In this test configuration, the following entries are added for System Manager with display name of **SMGR7** and IP address as **10.1.10.46**. The following settings were configured during the compliance test. **Basic Details:** • **IP address: 10.1.10.46** • **Display Name: SMGR7** • **Customer Name: Avaya** • **Site Name: DevCon Lab** **Configuration:** Browse for the SIP Entities and Entity Links XML files downloaded in **Section 5.3** and copy into the Prognosis server. **SNMP Connection Details**: Enter the settings configured in **Section 5.1 Step 3**. Leave the **Databases and Thresholds** as checked. Click **Add** at the bottom to affect the addition.  Add Avaya System Manager Basic Details Display Name: * SMGR7 IP Address: * 10.1.10.46 Customer Name: Avaya Site Name: DevCon Lab Configuration Sip Entities XML File: \\10.1.10.98\dc_data\Co Browse... Entity Links XML File: \\10.1.10.98\dc_data\Co Browse... SNMP Connection Details ○ Use SNMP Version 2c ● Use SNMP Version 3 Authentication Protocol: MD5 Authentication User Name: * avayasnmp Authentication Password: * ●●●●●●●●● Encryption Method: DES Encryption Password: * ●●●●●●●●● Databases and Thresholds ☑ Start standard databases and thresholds Add Cancel

Step	Description
5.	Return to the home screen; check that **SMGR7** is created under the server name in the middle pane. Click on the **SMGR7** to update the Session Manager in the next few steps. 

prognosis | Administration

View Systems

- Home
- Navigation
- Security
- Web Reports
- Automation
- Alert Suppression / Configuration Item Mapping

\WIN-VUKDPA7LIVG
- LSPREMOTE
- CM7-DUPLEX
- ESS
- G450-CM
- SMGR7

Prognosis node - WIN-VUKDPA7LIVG

Details

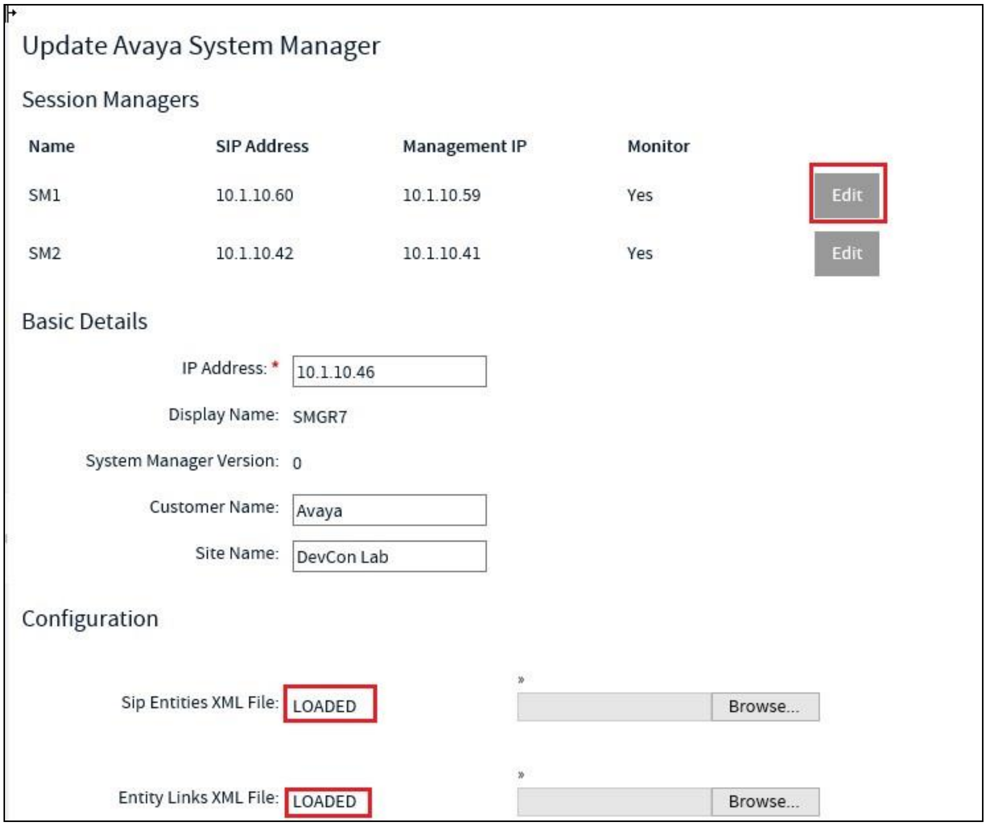
IP Address:	10.1.10.125
Version:	Prognosis 11.4.0
Operating System:	Windows Server 2012 R2 Standard
Status:	Connected

UC & Infrastructure Configuration

Add System

Databases

✕	A-VoiceStream-CSV	
●	AV-CDRs	Stop
●	AV-Contact Center Elite	Stop
●	AV-MedPro DSP Utilization	Stop
●	AV-Network Hops Historical	Stop
●	AV-Reporting	Stop

Step	Description
6.	Check that the **Sip Entities XML File** and **Entity Links XML File** are **LOADED**. Click **Edit** on **SM1**. 

Update Avaya System Manager

Session Managers

Name	SIP Address	Management IP	Monitor	
SM1	10.1.10.60	10.1.10.59	Yes	Edit
SM2	10.1.10.42	10.1.10.41	Yes	Edit

Basic Details

IP Address: * 10.1.10.46

Display Name: SMGR7

System Manager Version: 0

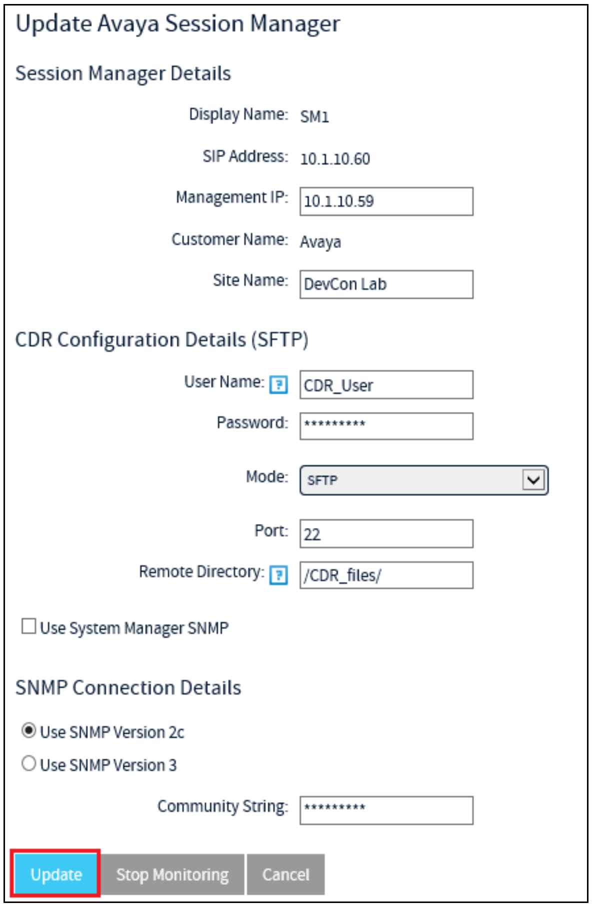
Customer Name: Avaya

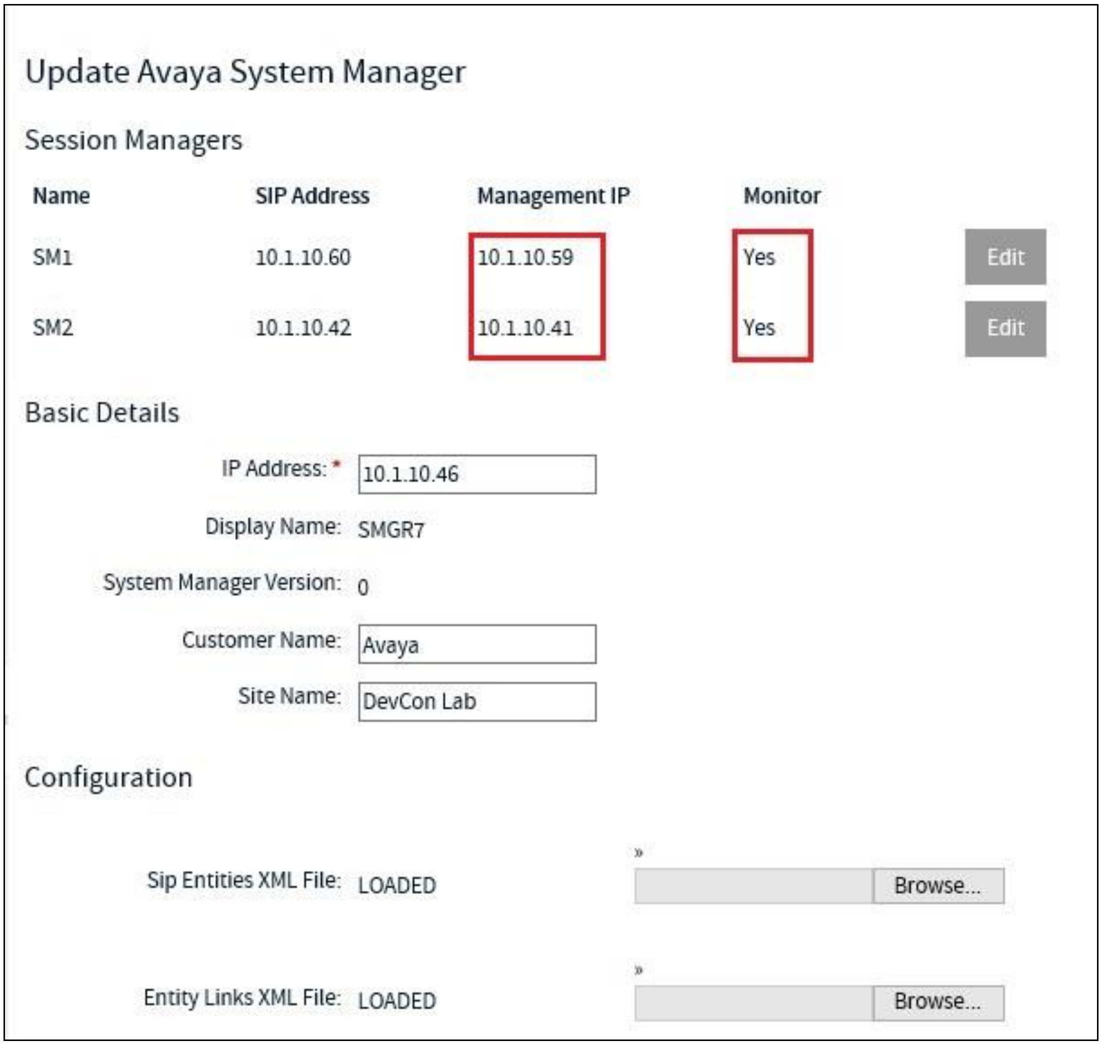
Site Name: DevCon Lab

Configuration

Sip Entities XML File: LOADED

Entity Links XML File: LOADED

Step	Description
7.	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 Steps 4-6**. Click **Update** to make the changes. Repeat the above for SM2 with **Management IP** as **10.1.10.41**.  Update Avaya Session Manager Session Manager Details Display Name: SM1 SIP Address: 10.1.10.60 Management IP: 10.1.10.59 Customer Name: Avaya Site Name: DevCon Lab CDR Configuration Details (SFTP) User Name: CDR_User Password: ********* Mode: SFTP Port: 22 Remote Directory: /CDR_files/ ☐ Use System Manager SNMP SNMP Connection Details ● Use SNMP Version 2c ○ Use SNMP Version 3 Community String: *********

Step	Description
8.	Access the configuration of System Manager in **Step 5**. Verify that the **Monitor** column for the Session Manager is set to **Yes** and the **Management IP** reflects the IP addresses set earlier. 

Update Avaya System Manager

Session Managers

Name	SIP Address	Management IP	Monitor	
SM1	10.1.10.60	10.1.10.59	Yes	Edit
SM2	10.1.10.42	10.1.10.41	Yes	Edit

Basic Details

IP Address: * 10.1.10.46

Display Name: SMGR7

System Manager Version: 0

Customer Name: Avaya

Site Name: DevCon Lab

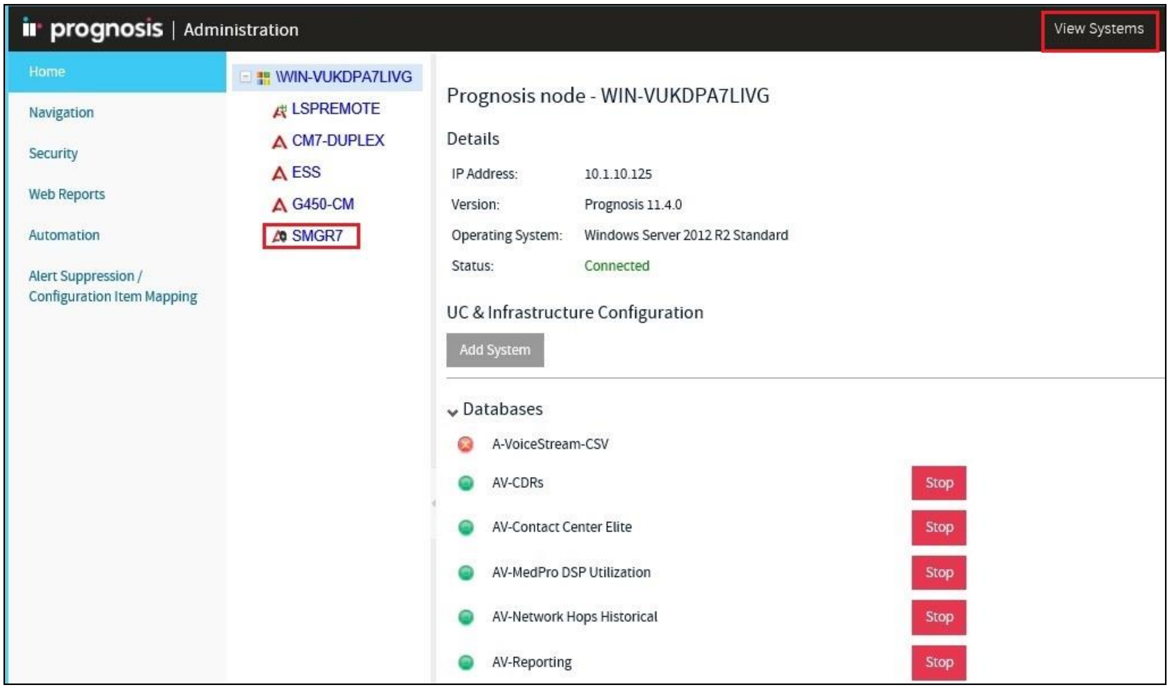
Configuration

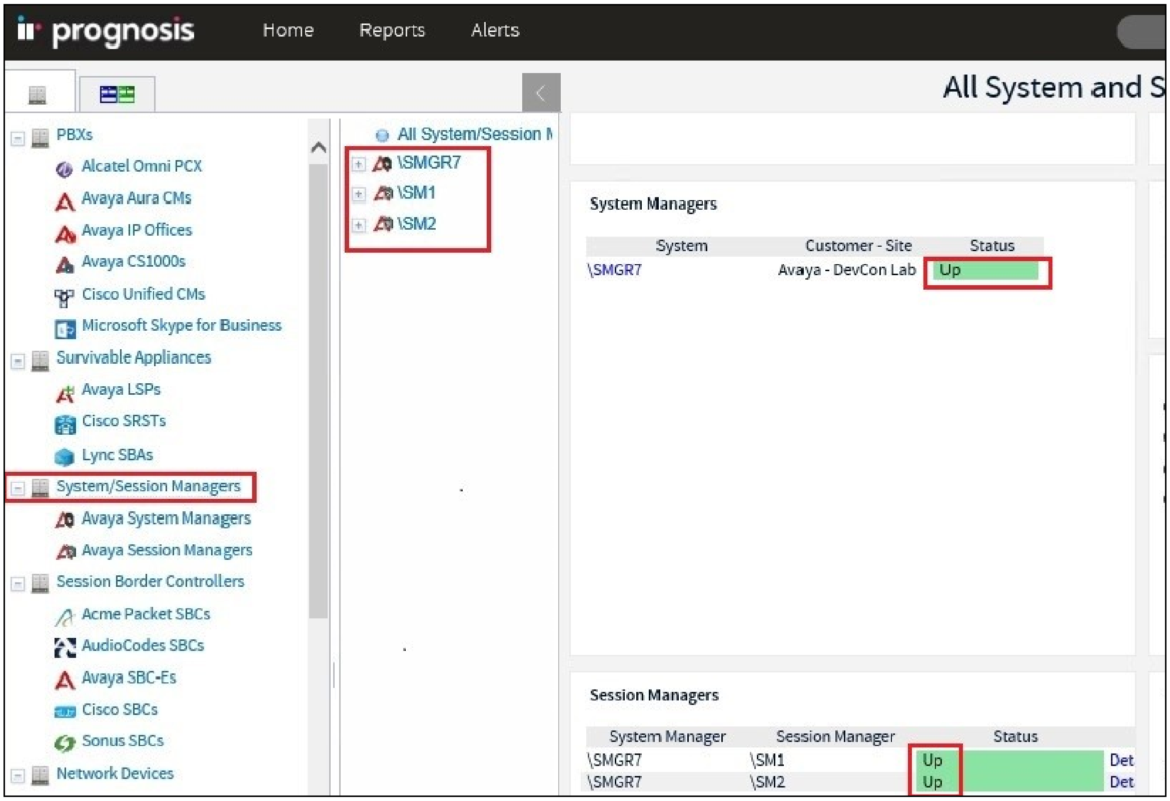
Sip Entities XML File: LOADED

Entity Links XML File: LOADED

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.

Step	Description
1.	After logging into Prognosis webui as in **Section 6 Step 1**, expand the server "WIN-VUKDPA7LIVG" in the middle pane and verify that the System Manager **SMGR7** is listed. Then select **View Systems** on the top right icon.  prognosis | Administration View Systems Home Navigation Security Web Reports Automation Alert Suppression / Configuration Item Mapping WIN-VUKDPA7LIVG LSPREMOTE CM7-DUPLEX ESS G450-CM SMGR7 Add System Stop Prognosis node - WIN-VUKDPA7LIVG Details IP Address: 10.1.10.125 Version: Prognosis 11.4.0 Operating System: Windows Server 2012 R2 Standard Status: Connected UC & Infrastructure Configuration Databases A-VoiceStream-CSV AV-CDRs AV-Contact Center Elite AV-MedPro DSP Utilization AV-Network Hops Historical AV-Reporting

Step	Description
2.	Select **System/Session Manager**s on the left pane. Check that the System Manager and Session Managers created earlier i.e., **SMGR7**, **SM1** and **SM2** are shown. Verify also the System Manager and the Session Managers **Status** is **Up**. 

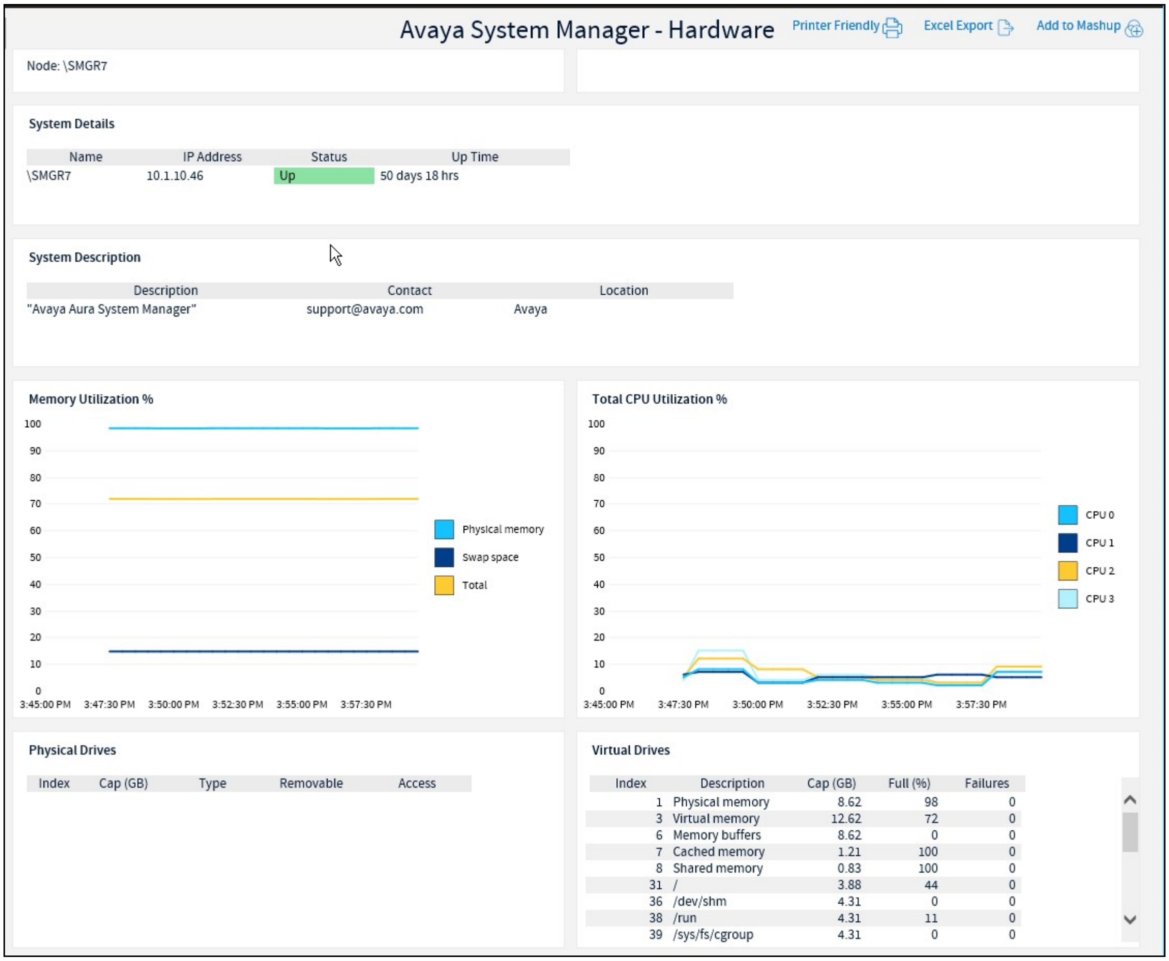
System Managers

System	Customer - Site	Status
\SMGR7	Avaya - DevCon Lab	Up

Session Managers

System Manager	Session Manager	Status	
\SMGR7	\SM1	Up	Det
\SMGR7	\SM2	Up	Det

3. Verify the hardware of System Manager.



Avaya System Manager - Hardware

Node: \SMGR7

System Details

Name	IP Address	Status	Up Time
\SMGR7	10.1.10.46	Up	50 days 18 hrs

System Description

Description	Contact	Location
"Avaya Aura System Manager"	support@avaya.com	Avaya

Memory Utilization %

Total CPU Utilization %

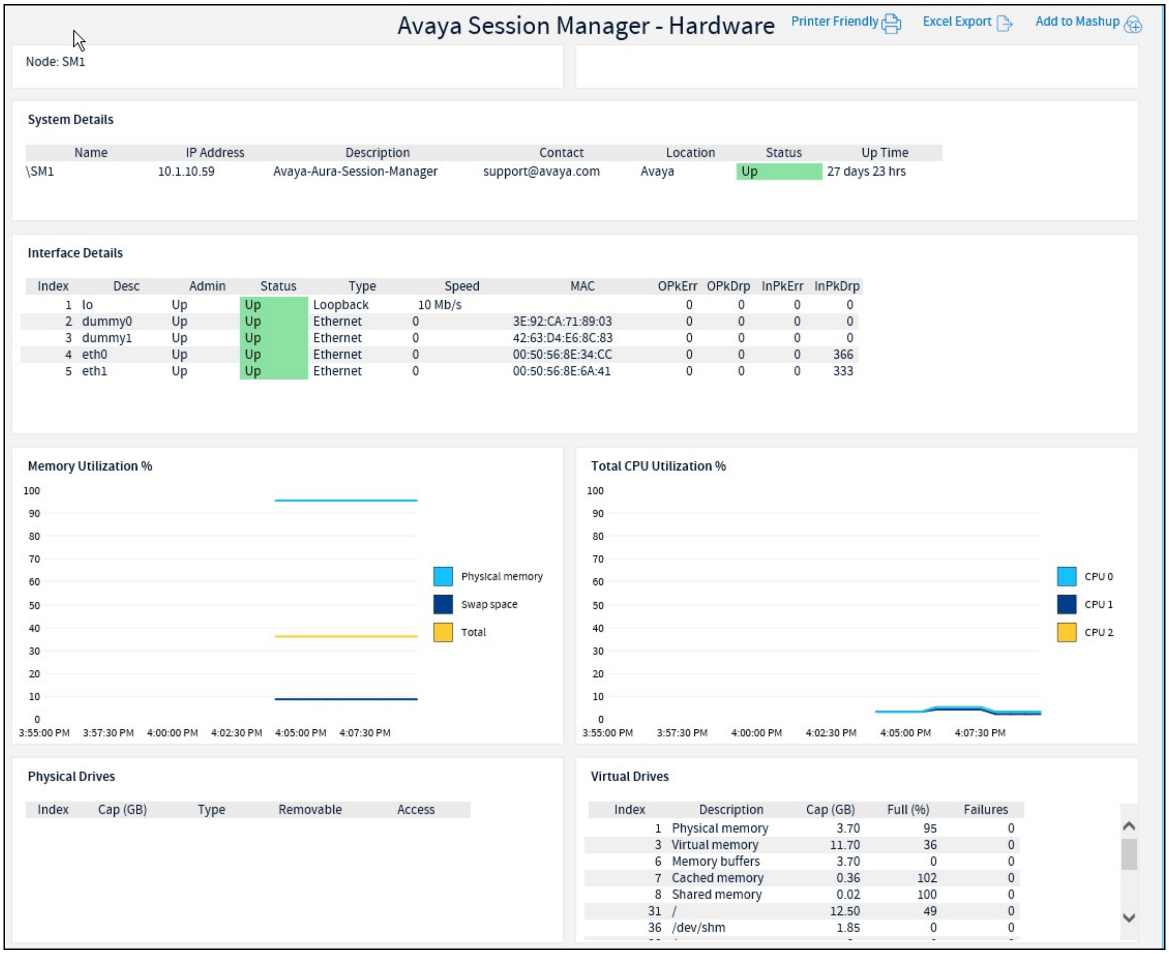
Physical Drives

Index	Cap (GB)	Type	Removable	Access

Virtual Drives

Index	Description	Cap (GB)	Full (%)	Failures
1	Physical memory	8.62	98	0
3	Virtual memory	12.62	72	0
6	Memory buffers	8.62	0	0
7	Cached memory	1.21	100	0
8	Shared memory	0.83	100	0
31	/	3.88	44	0
36	/dev/shm	4.31	0	0
38	/run	4.31	11	0
39	/sys/fs/cgroup	4.31	0	0

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



Avaya Session Manager - Hardware

Node: SM1

System Details

Name	IP Address	Description	Contact	Location	Status	Up Time
\SM1	10.1.10.59	Avaya-Aura-Session-Manager	support@avaya.com	Avaya	Up	27 days 23 hrs

Interface Details

Index	Desc	Admin	Status	Type	Speed	MAC	OPkErr	OPkDrp	InPkErr	InPkDrp
1	lo	Up	Up	Loopback	10 Mb/s		0	0	0	0
2	dummy0	Up	Up	Ethernet	0	3E:92:CA:71:89:03	0	0	0	0
3	dummy1	Up	Up	Ethernet	0	42:63:D4:E6:8C:83	0	0	0	0
4	eth0	Up	Up	Ethernet	0	00:50:56:8E:34:CC	0	0	0	366
5	eth1	Up	Up	Ethernet	0	00:50:56:8E:6A:41	0	0	0	333

Memory Utilization %

Total CPU Utilization %

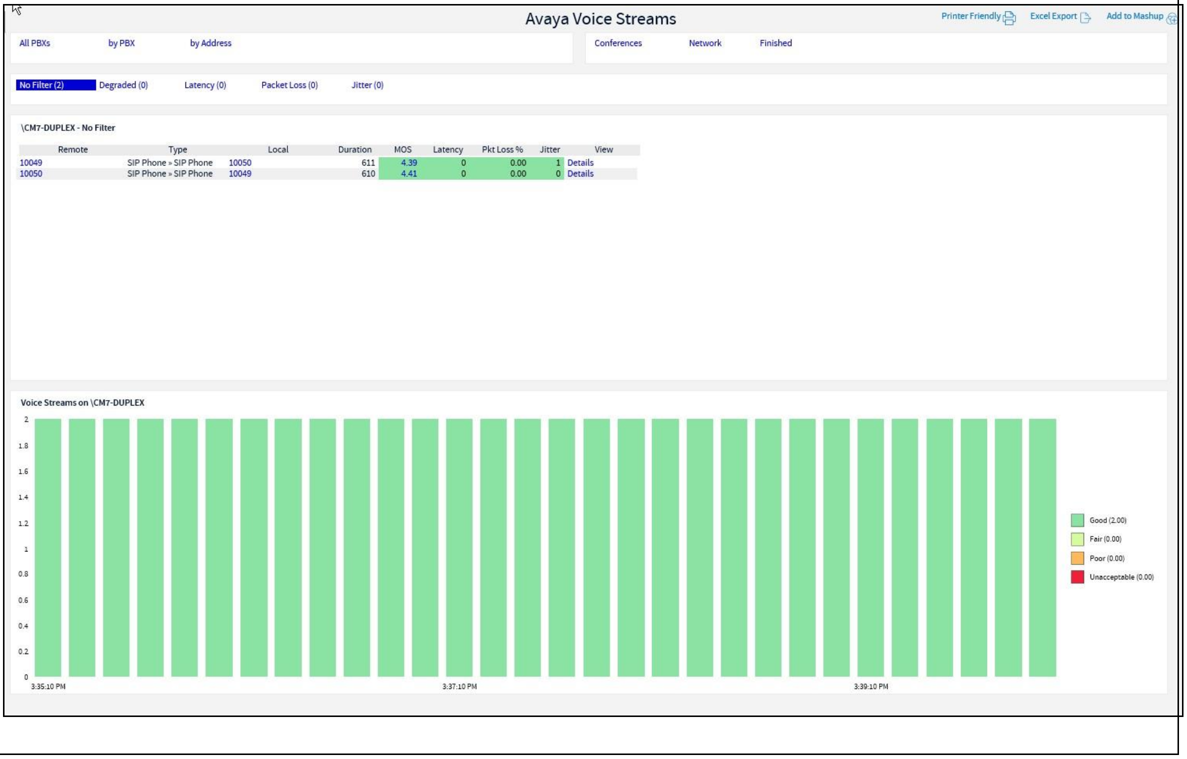
Physical Drives

Index	Cap (GB)	Type	Removable	Access

Virtual Drives

Index	Description	Cap (GB)	Full (%)	Failures
1	Physical memory	3.70	95	0
3	Virtual memory	11.70	36	0
6	Memory buffers	3.70	0	0
7	Cached memory	0.36	102	0
8	Shared memory	0.02	100	0
31	/	12.50	49	0
36	/dev/shm	1.85	0	0

5. 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 **Voice Streams** section shows voice streams reflecting the quality of the call.



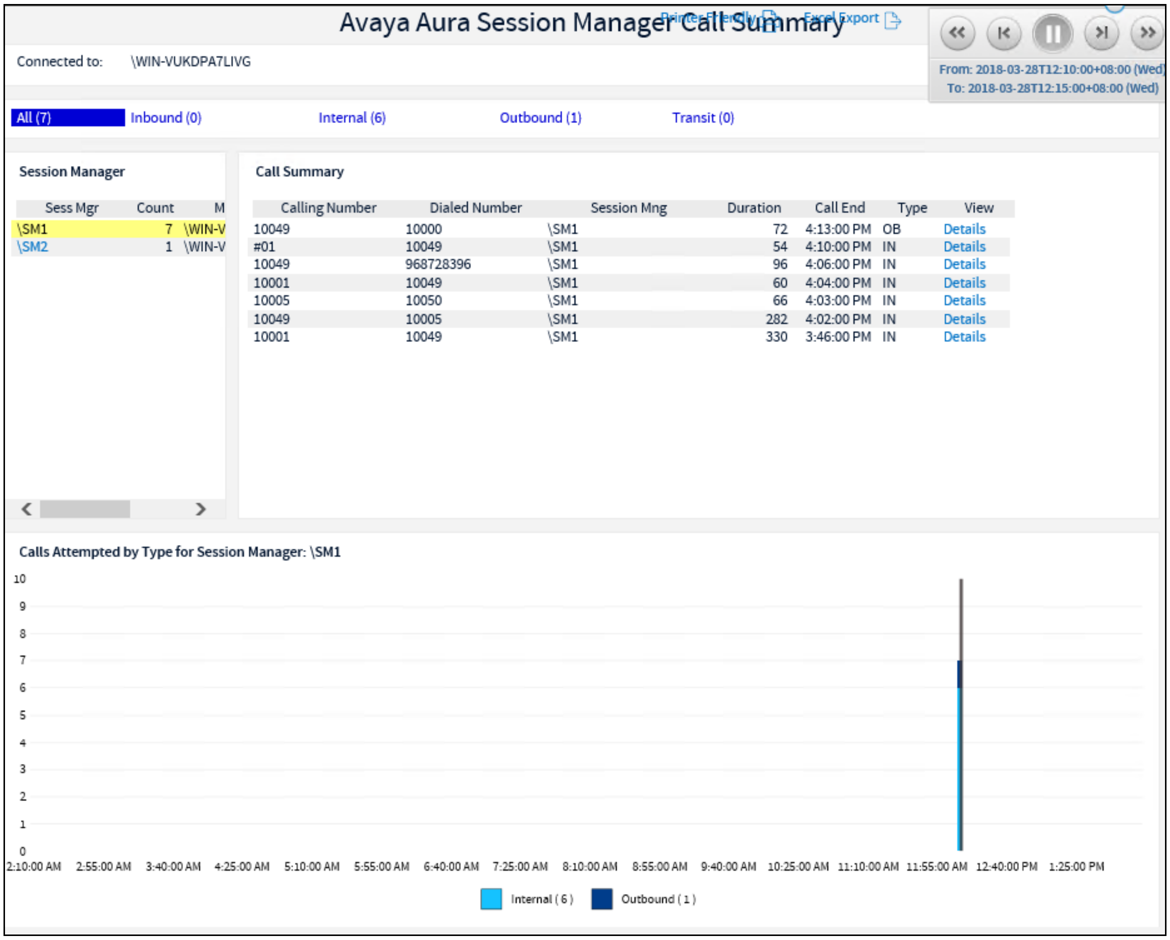
Avaya Voice Streams

\CM7-DUPLEX - No Filter

Remote	Type	Local	Duration	MOS	Latency	Pkt Loss %	Jitter	View
10049	SIP Phone » SIP Phone	10050	611	4.39	0	0.00	1	Details
10050	SIP Phone » SIP Phone	10049	610	4.41	0	0.00	0	Details

Voice Streams on \CM7-DUPLEX

6. 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 Step 3**.



Avaya Aura Session Manager Call Summary

Connected to: \WIN-VUKDPA7LIVG

From: 2018-03-28T12:10:00+08:00 (Wed)
To: 2018-03-28T12:15:00+08:00 (Wed)

All (7) Inbound (0) Internal (6) Outbound (1) Transit (0)

Session Manager

Sess Mgr	Count	M
\SM1	7	\WIN-V
\SM2	1	\WIN-V

Call Summary

Calling Number	Dialed Number	Session Mng	Duration	Call End	Type	View
10049	10000	\SM1	72	4:13:00 PM	OB	Details
#01	10049	\SM1	54	4:10:00 PM	IN	Details
10049	968728396	\SM1	96	4:06:00 PM	IN	Details
10001	10049	\SM1	60	4:04:00 PM	IN	Details
10005	10050	\SM1	66	4:03:00 PM	IN	Details
10049	10005	\SM1	282	4:02:00 PM	IN	Details
10001	10049	\SM1	330	3:46:00 PM	IN	Details

Calls Attempted by Type for Session Manager: \SM1

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis R11.4 to interoperate with Avaya Aura® System Manager 7.1 and Avaya Aura® Session Manager 7.1. In the configuration described in these Application Notes, Prognosis obtained the configuration and status information through SNMP from System Manager and each 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] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.2, Issue 5, Feb 2018.
[2] *Administering Avaya Aura® Communication Manager*, Release 7.1.2, Issue 4, Jan 2018.
[3] *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 4, Mar 2018.
[4] *Maintaining Avaya Aura® Session Manager*, Release 7.1, Issue 1, May 2017.
[5] *Administering Avaya Aura® System Manager*, Release 7.1.2, Issue 11, Mar 2018
[6] *Application Notes for Integrated Research's Prognosis for Unified Communications 11.4 with Avaya Aura® Communication Manager R7.1.*
[7] *Avaya Aura® System Manager 7.0.1 SNMP Whitepaper*, Issue 1.0, May 2016.

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.