



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Integrated Research's Prognosis for Unified Communications 10.5 with Avaya Aura® Session Manager R7.0 and Avaya Aura® System Manager R7.0 - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Prognosis for Unified Communications 10.5 to interoperate with Avaya Aura® Session Manager and System Manager.

Prognosis for Unified Communications 10.5 provides real-time monitoring and management solutions for IP telephony networks. Prognosis for Unified Communications 10.5 provides visibility of Avaya and other vendor's IP Telephony solutions from a single console and enables a significant 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 10.5 (herein after referred to as Prognosis) with Avaya Aura® System R7.0 and Avaya Aura® Session Manager R7.0.

The Prognosis product uses three methods to monitor Avaya Aura® Communication Manager systems.

- Real Time Transport Control Protocol (RTCP) Collection - Prognosis collects RTCP information sent by the Avaya IP Media Processor (MEDPRO) boards, media servers, media gateways and IP Telephones.
- Call Detail Recording (CDR) Collection - The Prognosis collects CDR information by SFTP to the Avaya Aura® Session Manager.
- SNMP Collection – The Prognosis uses SNMP to collect configuration and status information from Avaya Aura® System and Avaya Aura® 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 the 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.

### 2.1. Interoperability Compliance Testing

For feature testing, Prognosis GUI was used to view the configurations of System Manager and Session Manager such as the memory and cpu utilizations, disk usage and status. For the collection of RTCP and CDR information, the endpoints include Avaya H323, SIP, digital and analog telephones. 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:

- PBX name configured on Prognosis needs to have the name matched with that configured on System Manager. Otherwise the right PBX will not be monitored.
- Standard Flat format is supported for Session Manager CDR as default. The other format are Enhanced Flat File and Enhanced XML File which supports incomplete calls or SIP user to user calls records can be supported through customization by Prognosis.
- The correct voice streams were shown when a call is made through the media server. However, the “Type” field is marked with “Unknown” instead of Media Server. Enhancement to be made in the later release. Similar observations was made for Compliance Testing with Communication Manager.

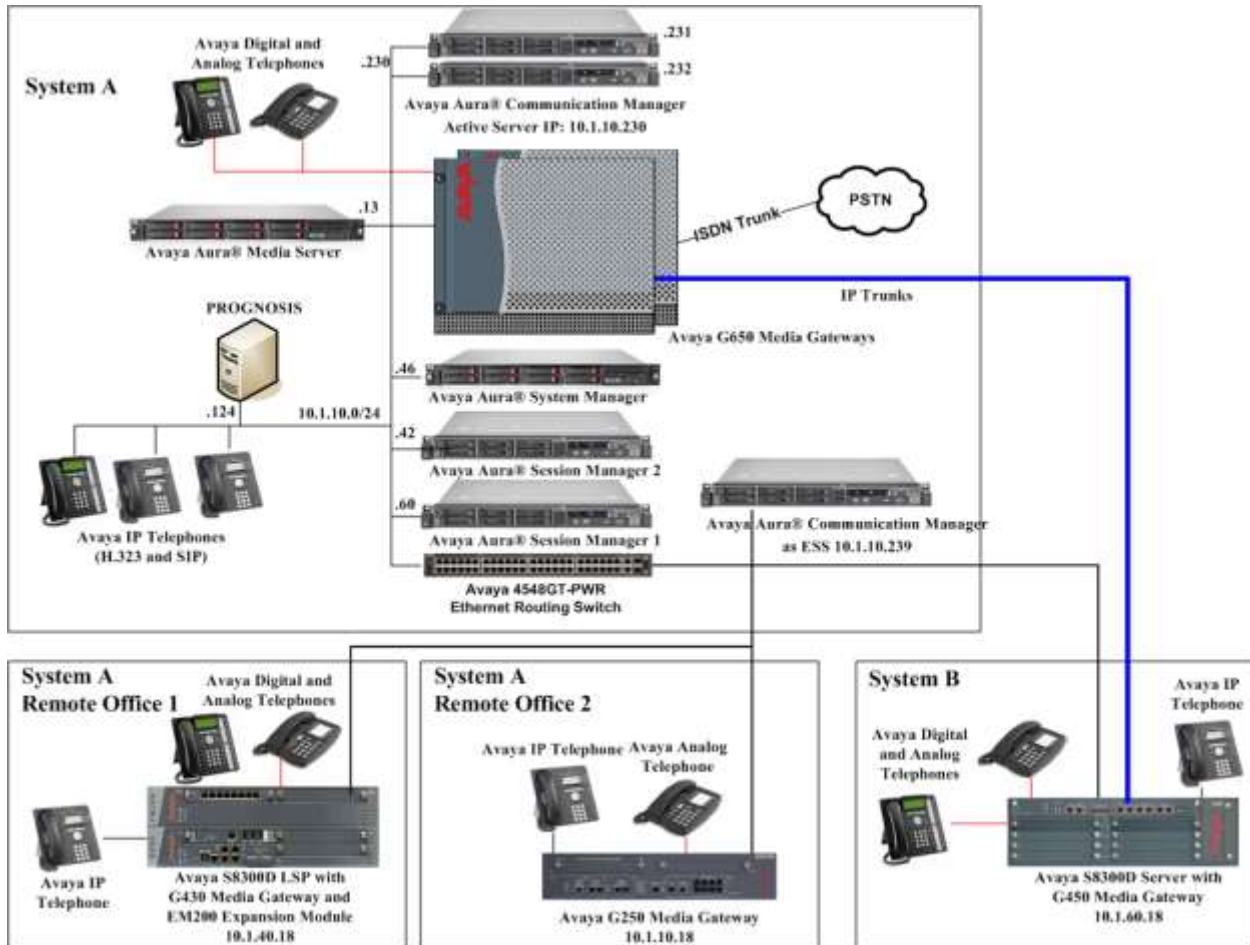
## 2.3. Support

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. It 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 an Avaya G250-BRI Media Gateway. An Enterprise Survivable Server (ESS) was also configured for failover testing. A second Communication Manager system (System B) runs on an Avaya S8300D Server with an Avaya G450 Media Gateway. Both systems have Avaya IP, digital and analog telephones users 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 telephones. Prognosis was installed on a server running Microsoft Windows Server 2008 R2 with Service Pack 1. Both the Monitoring Node and Web Application software are installed on this server. The Avaya 4548GT-PWR Ethernet Routing Switch provides Ethernet connectivity to the servers, media servers, media gateways and IP telephones.



**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)	7.0 SP3.1
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	HW07, FW058 HW01, FW044 HW02 FW066 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW012 HW08, FW016
G250 Media Gateway	30.27.1
Avaya Aura® Communication Manager running on Avaya S8300D Server (G450 Media Gateway – System B)	7.0 SP3.1
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	37.21.0 HW01 FW008 HW07 FW015 HW10 FW099 HW03 FW015 HW11 FW053
Avaya Aura® Communication Manager running on Avaya S8300D Server (G430 Media Gateway - LSP)	7.0 SP3.1
G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	37.21.0 HW04 FW015 HW12 FW098 HW31 FW098 HW05 FW022
Avaya Aura® Communication Manager (ESS)	7.0 SP3.1
Avaya Aura® System Manager	7.0.1.0.064859
Avaya Aura® Session Manager 1	7.0.1.0.701007
Avaya Aura® Session Manager 2	7.0.1.0.701007
Avaya Aura® Messaging	6.3.141.348-1.258129
96xx Series IP Telephones - 9640 - 9620	2.6.14 (SIP) 3.250A (H323)
96x1 Series IP Telephones - 9641G - 9611G	7.0.0.39 (SIP) 6.6029 (H323)

Equipment/Software	Release/Version
1600 Series IP Telephones - 1616 - 1603SW	1.390A (H.323)
Digital Telephones - 1416 - 1408	Rel 4 SP7
Avaya Analog Phones	-
Avaya 4548GT-PWR Ethernet Routing Switch	V5.6.1.052
Prognosis running on Windows 2008 R2 SP1	10.5

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

## 5. Configure System/Session Manager

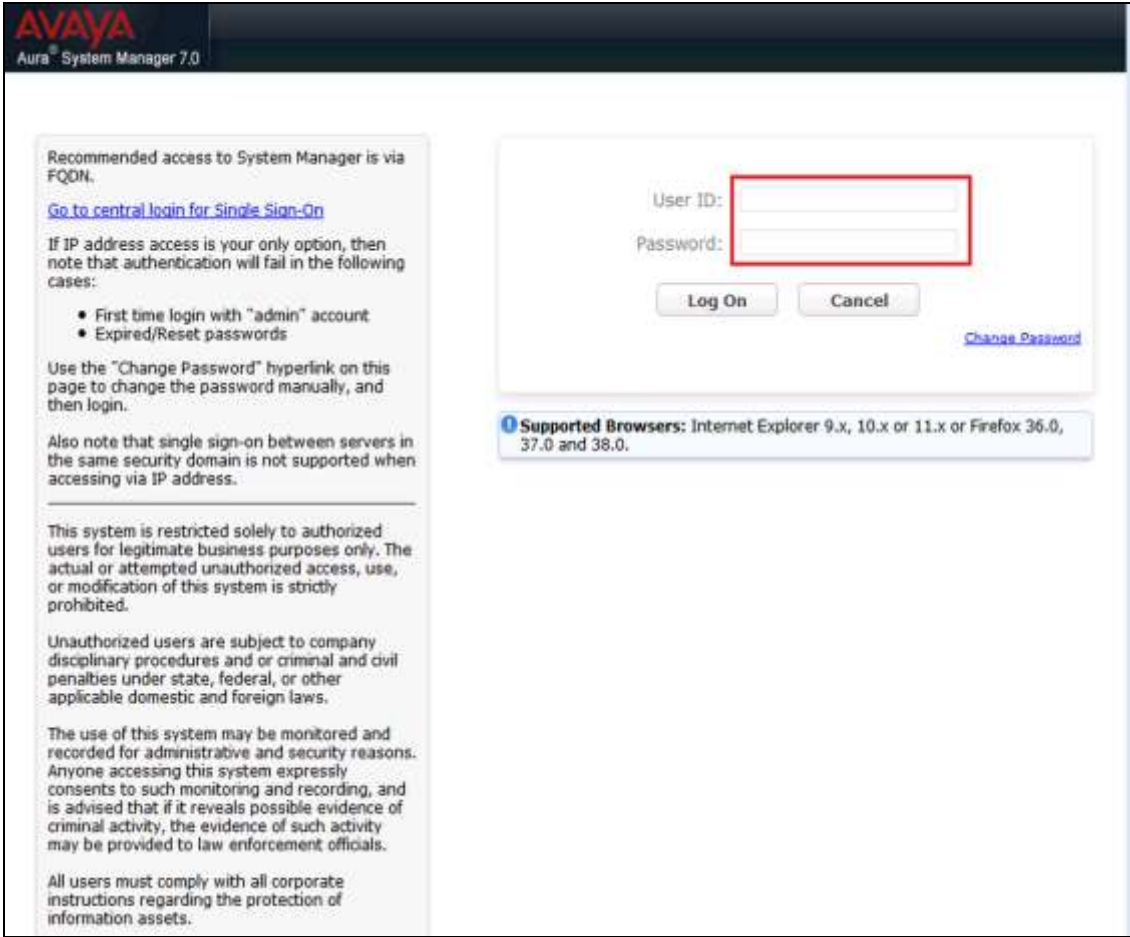
This section describes the steps needed to configure System and Session Manager to interoperate with Prognosis. This includes configuration of the SNMP v3 user profile for System Manager and the CDR user account on both Session Managers. The default SNMP v2c user profile will be used for Session Managers and no configuration is needed here. Configuration of Communication Manager is mentioned in **Reference [7]** and will not be detailed here.

### 5.1. Configure SNMP

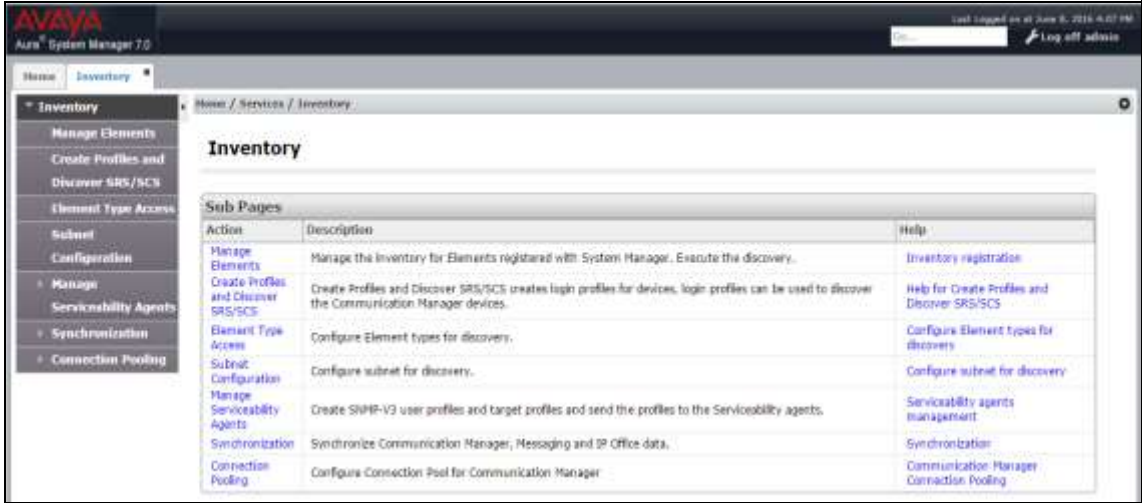
System Manager 7.0 support SNMPV2 for notifications and GET/SET operations will work only for V3. The following shows the steps to create SNMPv3 User Profiles and assigned the profile to System Manager and Session Managers.

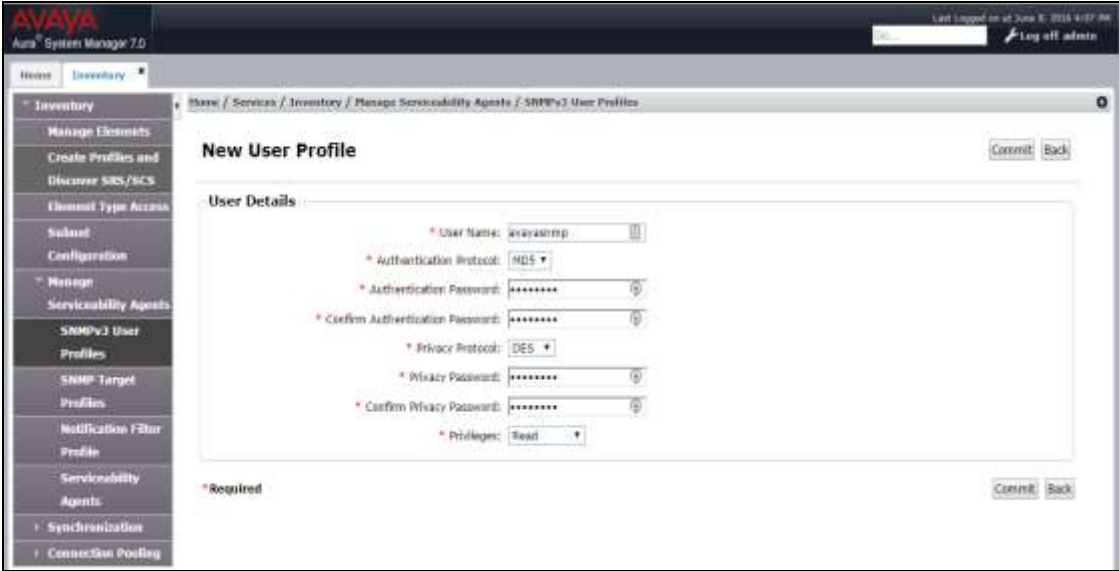
Step	Description
------	-------------

1. 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.



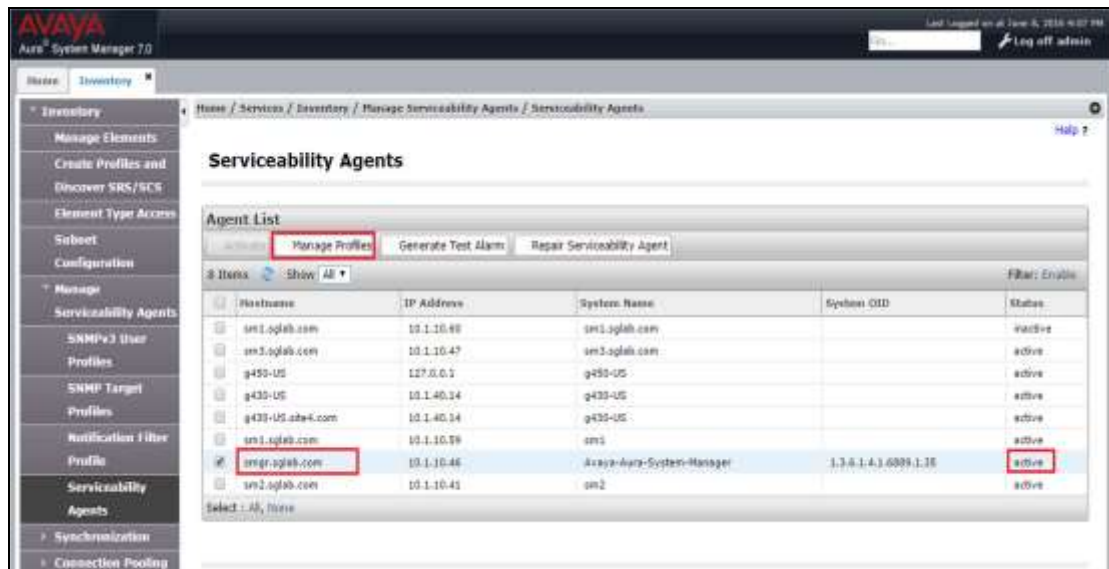


Step	Description																								
2.	<p data-bbox="298 233 1110 264">On the home screen (not shown), select <b>Services</b> → <b>Inventory</b>.</p>  <table border="1" data-bbox="496 495 1386 793"> <thead> <tr> <th>Action</th> <th>Description</th> <th>Help</th> </tr> </thead> <tbody> <tr> <td>Manage Elements</td> <td>Manage the Inventory for Elements registered with System Manager. Execute the discovery.</td> <td><a href="#">Inventory registration</a></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><a href="#">Help for Create Profiles and Discover SRS/SCS</a></td> </tr> <tr> <td>Element Type Access</td> <td>Configure Element types for discovery.</td> <td><a href="#">Configure Element types for discovery</a></td> </tr> <tr> <td>Subnet Configuration</td> <td>Configure subnet for discovery.</td> <td><a href="#">Configure subnet for discovery</a></td> </tr> <tr> <td>Management Serviceability Agents</td> <td>Create SNMP-V3 user profiles and target profiles and send the profiles to the Serviceability agents.</td> <td><a href="#">Serviceability agents management</a></td> </tr> <tr> <td>Synchronization</td> <td>Synchronize Communication Manager, Messaging and IP Office data.</td> <td><a href="#">Synchronization</a></td> </tr> <tr> <td>Connection Pooling</td> <td>Configure Connection Pool for Communication Manager</td> <td><a href="#">Communication Manager Connection Pooling</a></td> </tr> </tbody> </table>	Action	Description	Help	Manage Elements	Manage the Inventory for Elements registered with System Manager. Execute the discovery.	<a href="#">Inventory registration</a>	Create Profiles and Discover SRS/SCS	Create Profiles and Discover SRS/SCS creates login profiles for devices, login profiles can be used to discover the Communication Manager devices.	<a href="#">Help for Create Profiles and Discover SRS/SCS</a>	Element Type Access	Configure Element types for discovery.	<a href="#">Configure Element types for discovery</a>	Subnet Configuration	Configure subnet for discovery.	<a href="#">Configure subnet for discovery</a>	Management Serviceability Agents	Create SNMP-V3 user profiles and target profiles and send the profiles to the Serviceability agents.	<a href="#">Serviceability agents management</a>	Synchronization	Synchronize Communication Manager, Messaging and IP Office data.	<a href="#">Synchronization</a>	Connection Pooling	Configure Connection Pool for Communication Manager	<a href="#">Communication Manager Connection Pooling</a>
Action	Description	Help																							
Manage Elements	Manage the Inventory for Elements registered with System Manager. Execute the discovery.	<a href="#">Inventory registration</a>																							
Create Profiles and Discover SRS/SCS	Create Profiles and Discover SRS/SCS creates login profiles for devices, login profiles can be used to discover the Communication Manager devices.	<a href="#">Help for Create Profiles and Discover SRS/SCS</a>																							
Element Type Access	Configure Element types for discovery.	<a href="#">Configure Element types for discovery</a>																							
Subnet Configuration	Configure subnet for discovery.	<a href="#">Configure subnet for discovery</a>																							
Management Serviceability Agents	Create SNMP-V3 user profiles and target profiles and send the profiles to the Serviceability agents.	<a href="#">Serviceability agents management</a>																							
Synchronization	Synchronize Communication Manager, Messaging and IP Office data.	<a href="#">Synchronization</a>																							
Connection Pooling	Configure Connection Pool for Communication Manager	<a href="#">Communication Manager Connection Pooling</a>																							

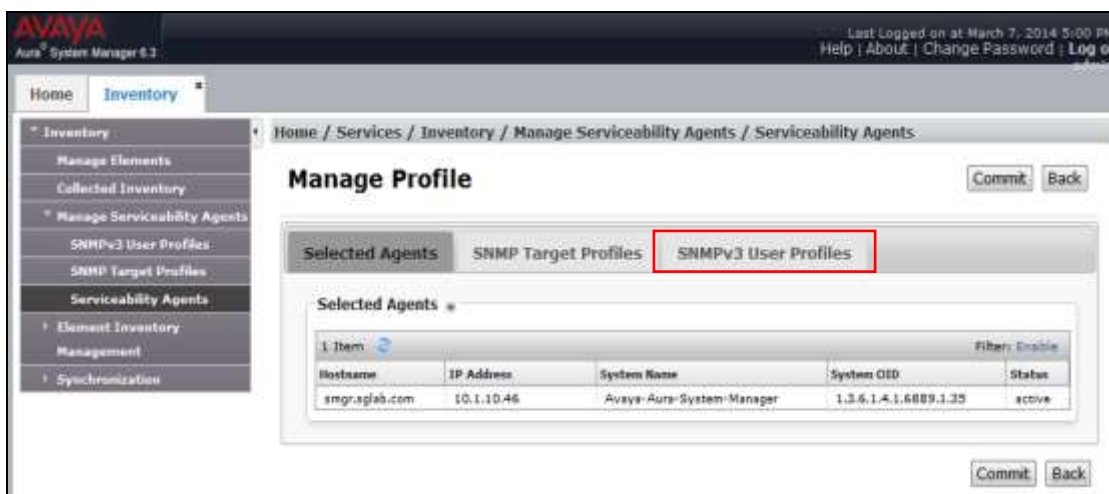
Step	Description
3.	<p>Select and expand on the <b>Manage Serviceability Agents</b> → <b>SNMPv3 User Profiles</b> (not shown) and click <b>New</b> to add a new user profile. Enter the details for the <b>User Profile</b> according to security level required. The user profile will be defined in the Prognosis configuration <b>Section 6 Step 4</b>. For more secured configuration, the profiles can be adjusted here, and the corresponding Prognosis configuration in <b>Section 6 Step 4</b> must then be adjusted as well.</p> <ul style="list-style-type: none"> <li>• <b>User Name:</b> avayasnmp [Enter a descriptive name desired]</li> <li>• <b>Authentication Protocol:</b> [Select MD5 or SHA]</li> <li>• <b>Authentication Password:</b> [Enter and confirm password]</li> <li>• <b>Privacy Protocol:</b> [Select DES or AES]</li> <li>• <b>Privacy Password:</b> [Enter and confirm password]</li> <li>• <b>Privileges:</b> Read</li> </ul> <p>Click <b>Commit</b> to submit. Below is the configuration setup in this compliance testing.</p> 

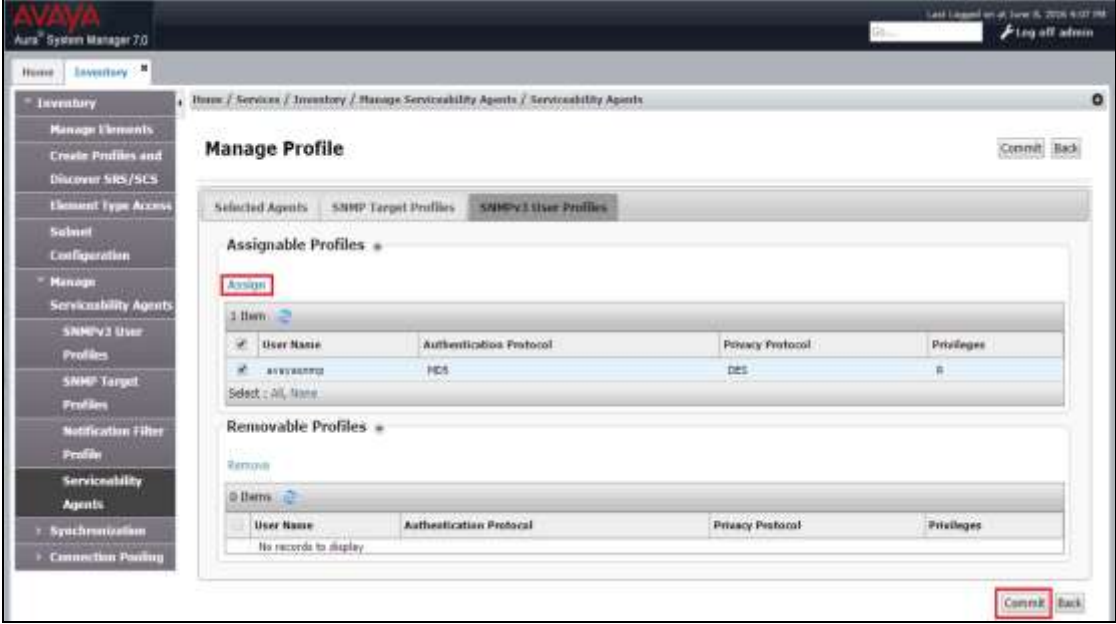
Step	Description
------	-------------

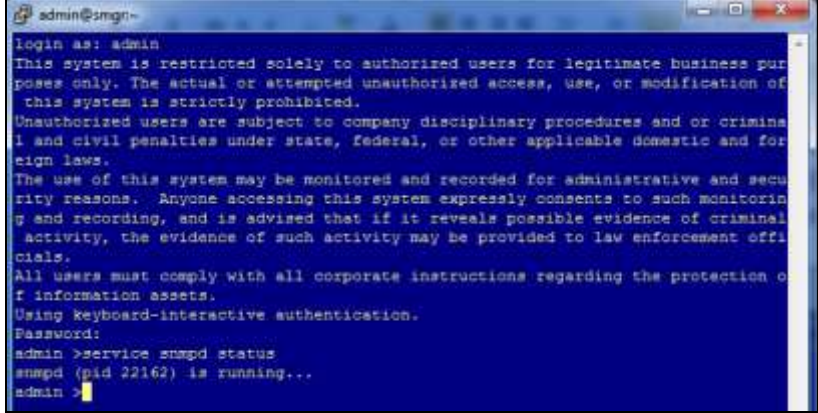
- Navigate to **Inventory** → **Manage Serviceability Agents** → **Serviceability Agents**. Check that the System Manager Agent **Status** is active. Select the System Manager (**smgr.sglab.com**) and select the **Manage Profiles** tab.




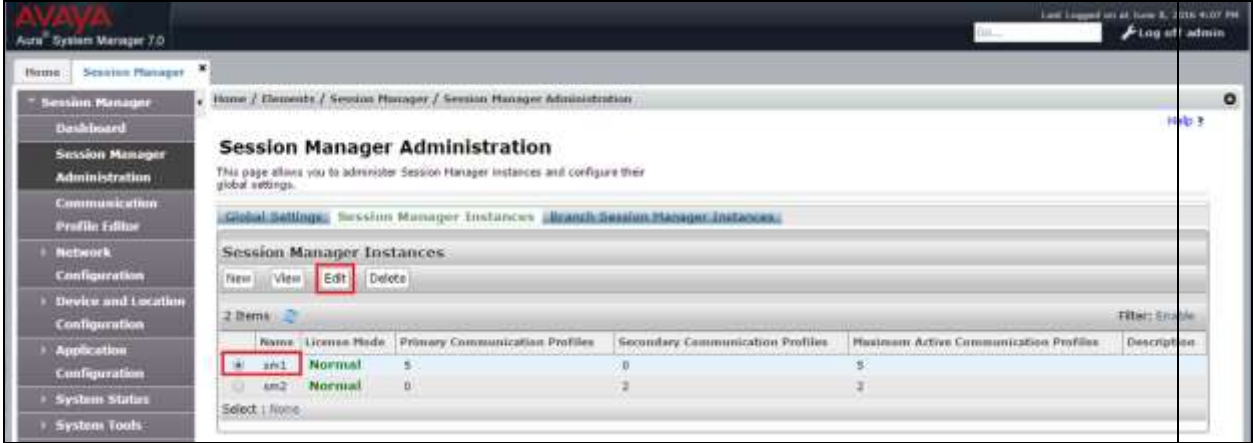
- Select **SNMPv3 User Profiles** tab and the screen will be shown in next step.

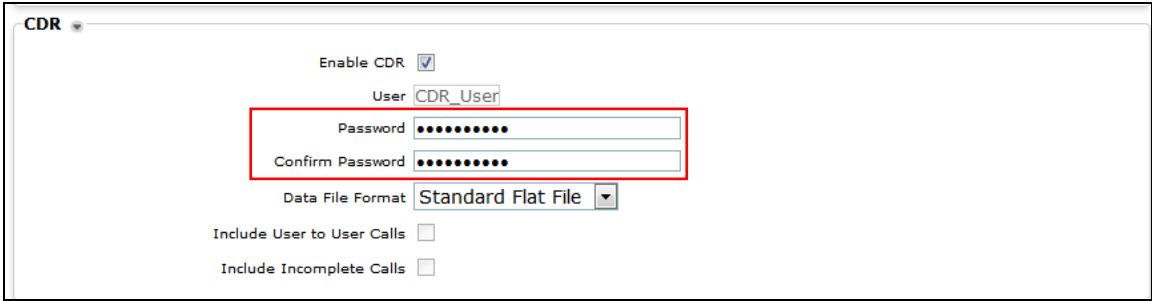


Step	Description
6.	<p>Click <i>down arrow</i> beside <b>Assignable Profiles</b> section if it is not expanded. Select the User Profiles created in <b>Step 3</b> earlier. Click <b>Assign</b> to assign it to the System Manager. The user profile will moved to the <b>Removable Profiles</b> section. Click <b>Commit</b> to submit the changes.</p> 

7.	<p>SSH into the System Manager and log in as valid user. Verify that the SNMP service is running using the command “<b>service snmpd status</b>”. Otherwise, run the command “<b>service snmpd restart/start</b>” to start SNMP service daemon.</p> 
----	--

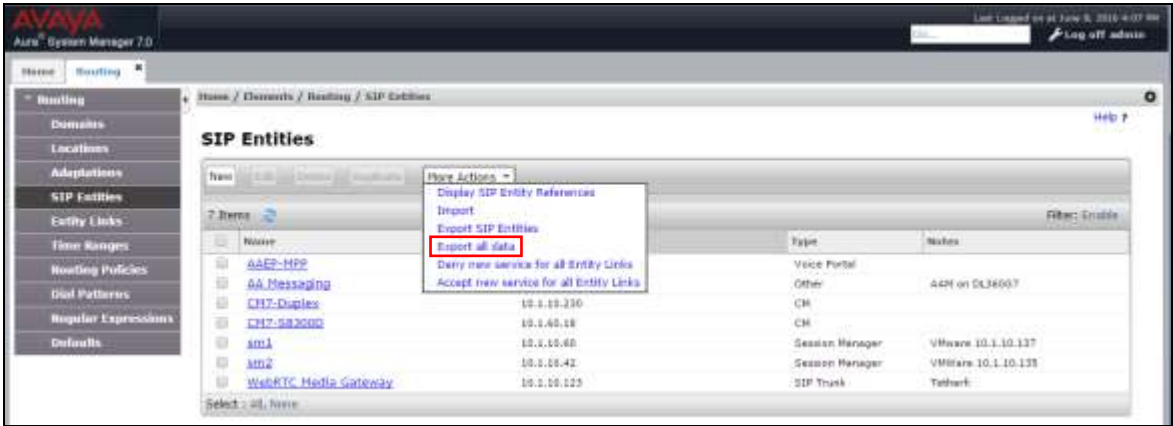
## 5.2. Configure CDR user account for Session Manager

Step	Description																		
1.	<p>From the home screen (not shown), navigate to the Session Manager by clicking <b>Elements</b> → <b>Session Manager</b>.</p> 																		
2.	<p>Click <b>Session Manager</b> → <b>Session Manager Administration</b>. On the right pane, click <b>Session Manager Instances</b> tab and select <b>sm1</b>. Click <b>Edit</b> to make changes.</p>  <table border="1" data-bbox="492 1367 1474 1465"> <thead> <tr> <th>Name</th> <th>License Mode</th> <th>Primary Communication Profiles</th> <th>Secondary Communication Profiles</th> <th>Maximum Active Communication Profiles</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>sm1</td> <td>Normal</td> <td>5</td> <td>0</td> <td>5</td> <td></td> </tr> <tr> <td>sm2</td> <td>Normal</td> <td>0</td> <td>2</td> <td>2</td> <td></td> </tr> </tbody> </table>	Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description	sm1	Normal	5	0	5		sm2	Normal	0	2	2	
Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description														
sm1	Normal	5	0	5															
sm2	Normal	0	2	2															

Step	Description
3.	<p>On the right pane (not shown) under the <b>CDR</b> section, make sure the <b>Enable CDR</b> is checked and set the password for <b>CDR_User</b>. Select <b>Data File Format</b> as <b>Standard Flat File</b> for the default CDR file format. The other formats i.e., Enhanced Flat File and Enhanced XML File are supported but will required customization by Prognosis engineer to accommodate the different formats. For more details, refer to [5] in <b>Additional References</b> Section.</p> 

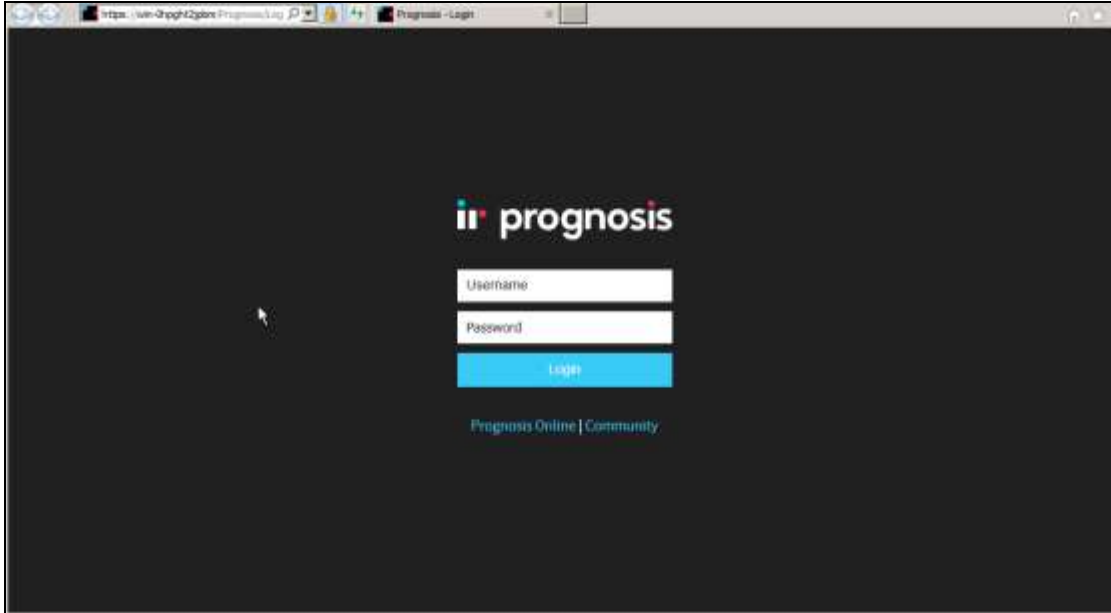
### 5.3. Download Sip Entities and Entity Links XML files.

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

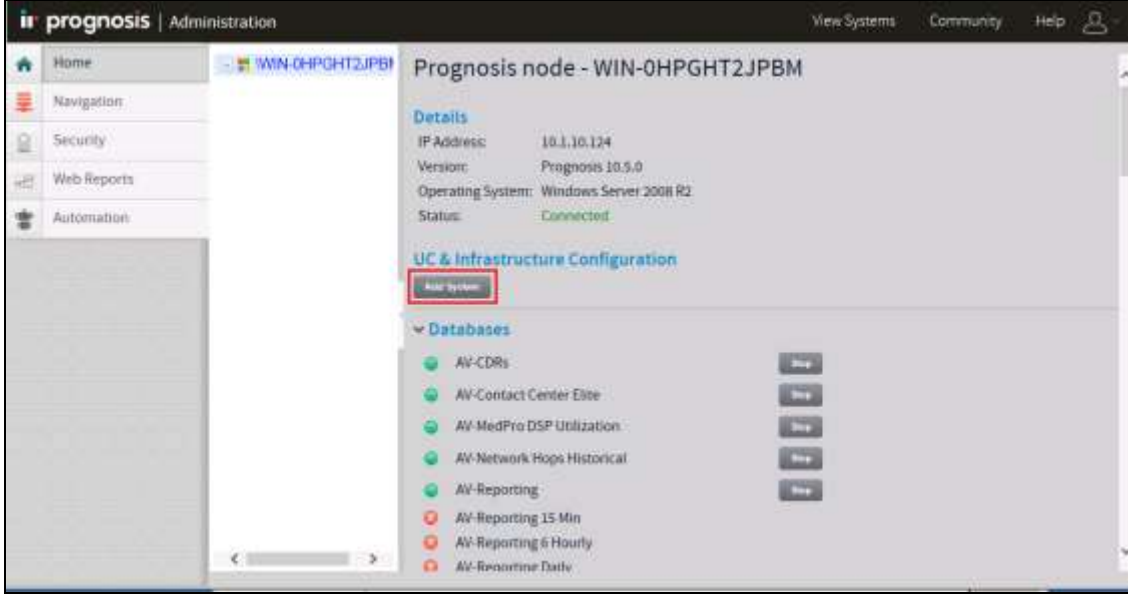

Step	Description
1.	<p>On the System Manager home screen (not shown), select <b>Element</b> → <b>Routing</b>. Click <b>Routing</b> → <b>SIP Entities</b> and select <b>Export all data</b> in the <b>More Actions</b> drop-down menu. Save the zip file into the local hard disk. Extract the files “&lt;user name&gt;EntityLinks.xml” and “&lt;user name&gt;SipEntities.xml”. 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>.</p> 

## 6. Configure Prognosis

This section describes the configuration of Prognosis required to interoperate with System/Session Manager. Configuration of Prognosis to interoperate with Communication Manager is mentioned in **Reference [7]** and will not be detailed here.

Step	Description
1.	<p>Log into the Prognosis server with administrative privileges. Launch the Prognosis Administration by clicking <b>Start → All Programs → Prognosis → Prognosis Administration</b>. Log in with the appropriate password.</p> 



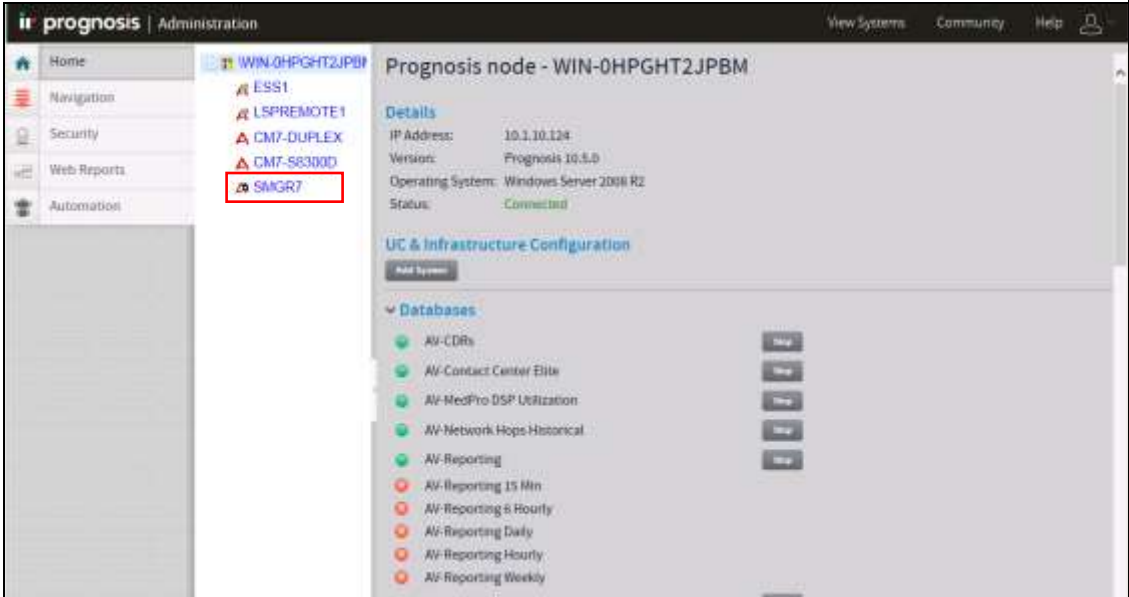
Step	Description
2.	<p>Click <b>Add System</b>.</p>  <p>The screenshot shows the 'Prognosis node - WIN-0HPGHT2JPBM' configuration page. The 'UC &amp; Infrastructure Configuration' section has an 'Add System' button highlighted with a red box. Below it, a 'Databases' section lists various database types with 'Add' buttons next to each.</p>
3.	<p>Click <b>Add</b> to add a new System Manager.</p>  <p>The close-up shows a dropdown menu titled 'System/Session Managers' with 'Avaya System/Session Manager' selected. An 'Add' button is highlighted with a red box.</p>



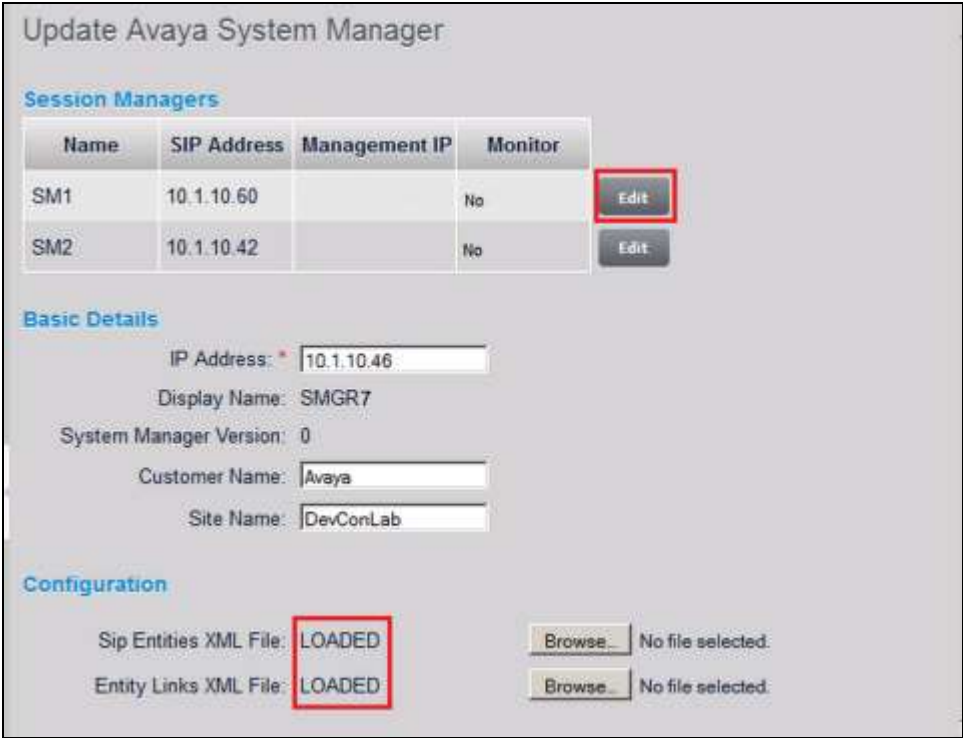
Step	Description
4.	<p>In this test configuration, the following entries are added for System Manager with the Display Name <b>SMGR7</b> and with the IP addresses as <b>10.1.10.46</b>.</p> <p>The following settings were configured during the compliance test.</p> <p><b>Basic Details:</b></p> <ul style="list-style-type: none"> <li>• <b>IP address: 10.1.10.46</b></li> <li>• <b>Display Name: SMGR7</b></li> <li>• <b>Customer Name: Avaya</b></li> <li>• <b>Site Name: DevConLab</b></li> </ul> <p><b>Configuration:</b> Browse for the <b>Sip Entities</b> and <b>Entity Links XML</b> files downloaded in <b>Section 5.3</b> and copied into the Prognosis server.</p> <p><b>SNMP Connection Details:</b> Enter the settings configured in <b>Section 5.1 Step 3</b>.</p> <p>Leave the <b>Databases and Thresholds</b> as checked. Click <b>Add</b> at the bottom (not shown) to effect the addition.</p> <div data-bbox="488 932 1239 1696" style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <p><b>Basic Details</b></p> <p>IP Address: * <input type="text" value="10.1.10.46"/></p> <p>Display Name: <input type="text" value="SMGR7"/></p> <p>System Manager Version: <input type="text" value="0"/></p> <p>Customer Name: <input type="text" value="Avaya"/></p> <p>Site Name: <input type="text" value="DevConLab"/></p> <p><b>Configuration</b></p> <p>Sip Entities XML File: <input type="text"/> <input type="button" value="Browse"/></p> <p>Entity Links XML File: <input type="text"/> <input type="button" value="Browse"/></p> <p><b>SNMP Connection Details</b></p> <p><input type="radio"/> Use SNMP Version 2c  <input checked="" type="radio"/> Use SNMP Version 3</p> <p>Authentication Protocol: <input type="text" value="MD5"/></p> <p>Authentication User Name: * <input type="text" value="avayasnmp"/></p> <p>Authentication Password: * <input type="password" value="*****"/></p> <p>Encryption Method: <input type="text" value="DES"/></p> <p>Encryption Password: * <input type="password" value="*****"/></p> <p><b>Databases and Thresholds</b></p> <p><input checked="" type="checkbox"/> Start standard databases and thresholds</p> </div>

**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.



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



Step	Description
7.	<p>The following settings were configured during the compliance test for <b>SM1</b>.</p> <p><b>Session Manager Details:</b></p> <ul style="list-style-type: none"> <li>• <b>Management IP: 10.1.10.59</b></li> <li>• <b>Site Name: Science Park</b> [Descriptive name of location]</li> </ul> <p><b>CDR Configuration Details (SFTP):</b></p> <ul style="list-style-type: none"> <li>• <b>User Name: CDR_User</b></li> <li>• <b>Password:</b> As configured in <b>Section 5.2</b></li> <li>• <b>Mode: SFTP</b></li> <li>• <b>Port: 22</b> [As default]</li> <li>• <b>Remote Directory: /</b> [As default]</li> </ul> <p><b>SNMP Connection Details:</b></p> <p>Select <b>User SNMP Version 2c</b> and the <b>Community String</b> “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 “<b>Use System Manager SNMP</b>”. Follow similar steps as in <b>Section 5.1 Steps 4-6</b>.</p> <p>Click <b>Update</b> to make the changes. Repeat the above for SM2 with <b>Management IP</b> as <b>10.1.10.41</b>.</p> <div data-bbox="591 974 1135 1797" data-label="Form"> </div>

**Step**    **Description**

8. Access the configuration of the 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 Address set earlier.

**Update Avaya System Manager**

**Session Managers**

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

**Basic Details**

IP Address: \* 10.1.10.46  
Display Name: SMGR7  
System Manager Version: 0  
Customer Name: Avaya  
Site Name: DevConLab

**Configuration**

Sip Entities XML File: LOADED » Browse...  
Entity Links XML File: LOADED » Browse...


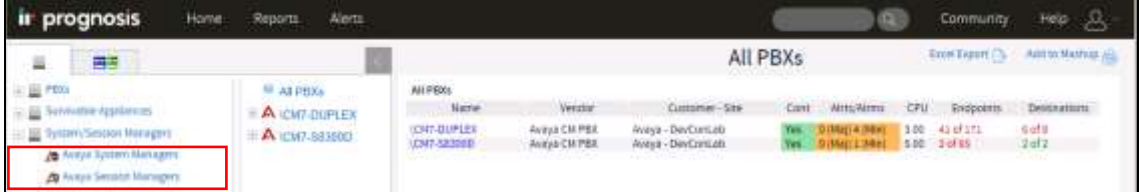
9. SSH into the Session Managers and log in as valid user and su to the root user. Verify that the SNMP service is running using the command “**service snmpd status**”. Otherwise, run the command “**service snmpd restart/start**” to start SNMP service daemon.

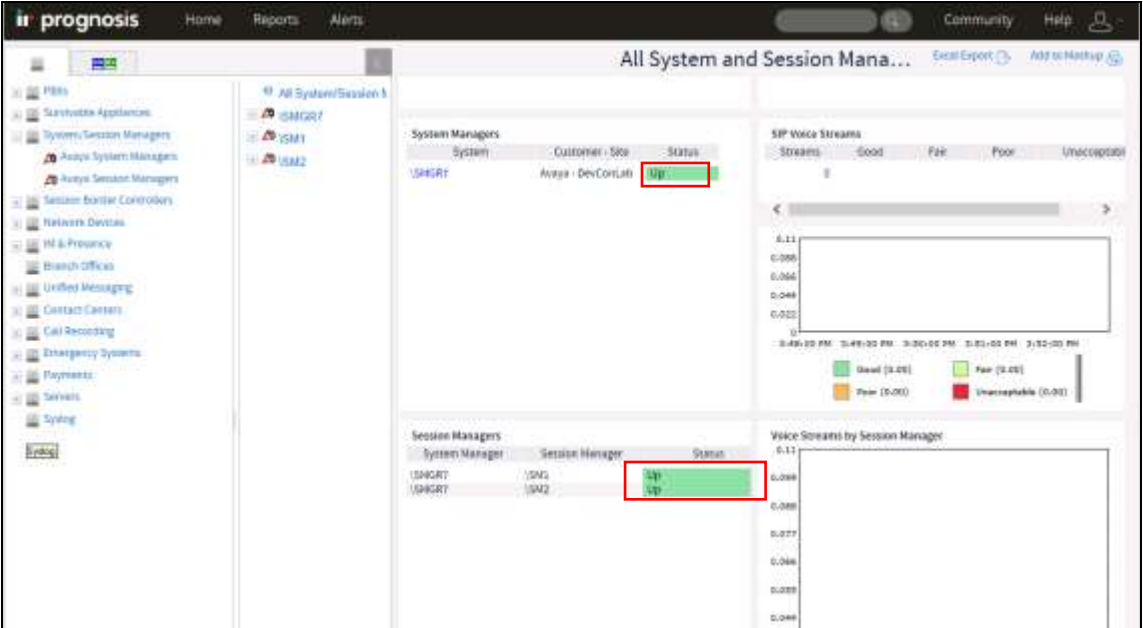
```
root@sm1:~  
[root@sm1 ~]# service snmpd status  
snmpd (pid 1459) is running...  
[root@sm1 ~]#
```

```
root@sm2:~  
[root@sm2 ~]# service snmpd status  
snmpd (pid 9360) is running...  
[root@sm2 ~]#
```

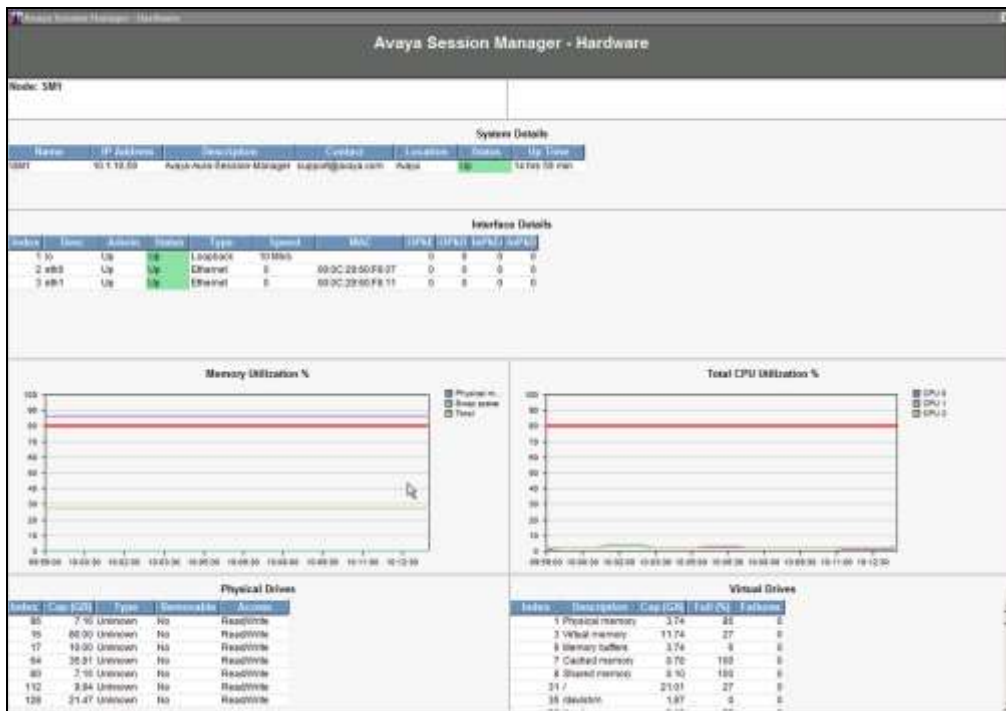
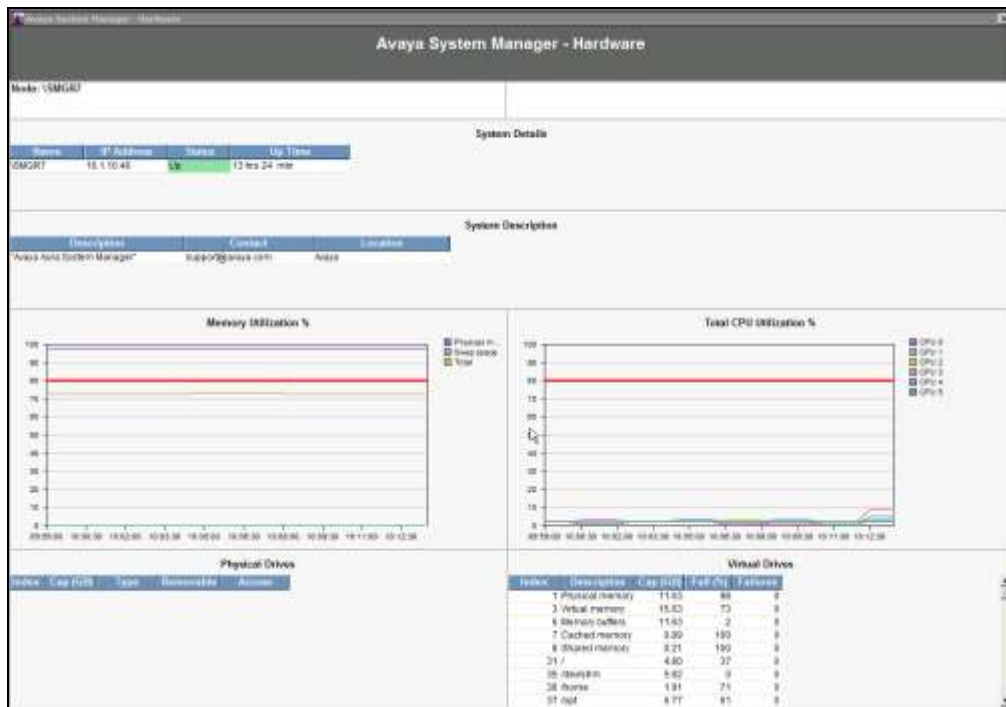
## 7. Verification Steps

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

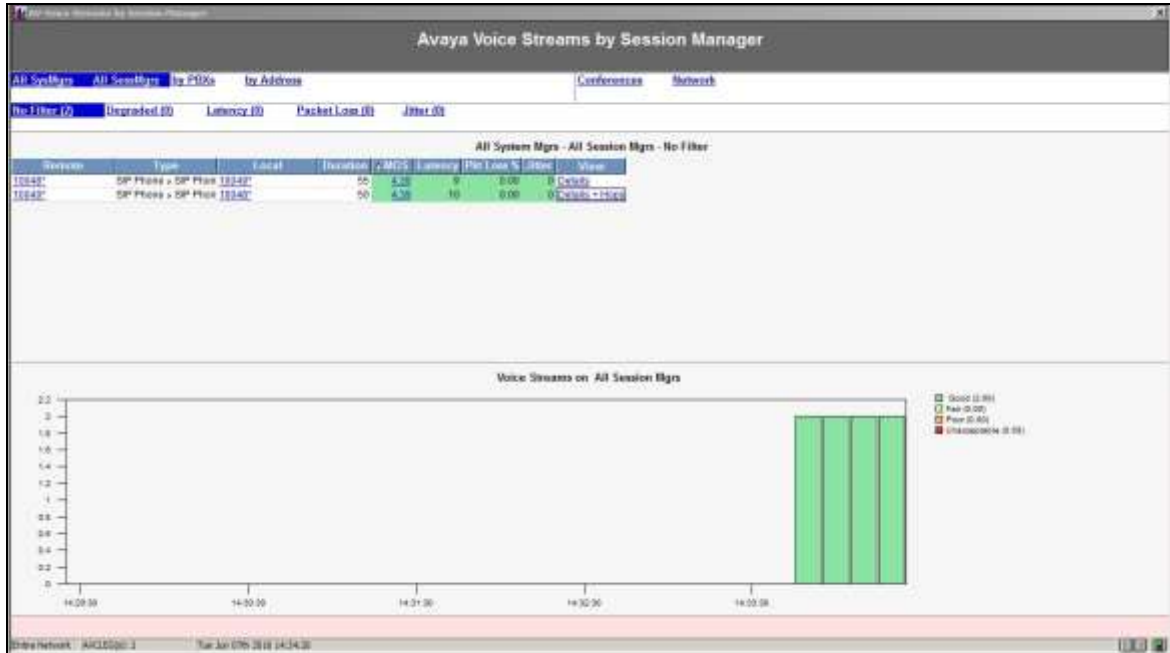
Step	Description																								
1.	<p>After logging into Prognosis webui as in <b>Section 6 Step 1</b>, expand the server “WIN-OHPGHT2JPBM” in the middle pane and verify that the System Manager Display Name <b>SMGR7</b> is created under the server name. Then select View Systems on the top right icon.</p> 																								
2.	<p>Check that the System Managers and Session Managers are created on the left pane.</p>  <table border="1" data-bbox="678 1304 1382 1402"> <thead> <tr> <th>Name</th> <th>Vendor</th> <th>Customer - Site</th> <th>Cont</th> <th>Alerts/Alarms</th> <th>CPU</th> <th>Endpoints</th> <th>Destinations</th> </tr> </thead> <tbody> <tr> <td>CM7-DUPLEX</td> <td>Avaya CM PBE</td> <td>Avaya - DevCentLab</td> <td>Yes</td> <td>0 (0%) 4 (0%)</td> <td>100</td> <td>43 of 171</td> <td>0 of 0</td> </tr> <tr> <td>CM7-SB300D</td> <td>Avaya CM PBE</td> <td>Avaya - DevCentLab</td> <td>Yes</td> <td>0 (0%) 1 (0%)</td> <td>100</td> <td>3 of 85</td> <td>2 of 2</td> </tr> </tbody> </table>	Name	Vendor	Customer - Site	Cont	Alerts/Alarms	CPU	Endpoints	Destinations	CM7-DUPLEX	Avaya CM PBE	Avaya - DevCentLab	Yes	0 (0%) 4 (0%)	100	43 of 171	0 of 0	CM7-SB300D	Avaya CM PBE	Avaya - DevCentLab	Yes	0 (0%) 1 (0%)	100	3 of 85	2 of 2
Name	Vendor	Customer - Site	Cont	Alerts/Alarms	CPU	Endpoints	Destinations																		
CM7-DUPLEX	Avaya CM PBE	Avaya - DevCentLab	Yes	0 (0%) 4 (0%)	100	43 of 171	0 of 0																		
CM7-SB300D	Avaya CM PBE	Avaya - DevCentLab	Yes	0 (0%) 1 (0%)	100	3 of 85	2 of 2																		

Step	Description																	
3.	<p>Verify the System Manager and the two Session Managers <b>Status</b> are <b>Up</b>.</p>  <p>The screenshot displays the Prognosis interface with the following data tables:</p> <p><b>System Managers</b></p> <table border="1"> <thead> <tr> <th>System</th> <th>Customer</th> <th>Site</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>USGR7</td> <td>Avaya</td> <td>DevConLab</td> <td>Up</td> </tr> </tbody> </table> <p><b>Session Managers</b></p> <table border="1"> <thead> <tr> <th>System Manager</th> <th>Session Manager</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>USGR7</td> <td>SM1</td> <td>Up</td> </tr> <tr> <td>USGR7</td> <td>SM2</td> <td>Up</td> </tr> </tbody> </table> <p>The 'Status' column in both tables is highlighted with a red box, showing 'Up' for all entries.</p>	System	Customer	Site	Status	USGR7	Avaya	DevConLab	Up	System Manager	Session Manager	Status	USGR7	SM1	Up	USGR7	SM2	Up
System	Customer	Site	Status															
USGR7	Avaya	DevConLab	Up															
System Manager	Session Manager	Status																
USGR7	SM1	Up																
USGR7	SM2	Up																

- Step**   **Description**
4. Verify the hardware details can be viewed for System Manager and all Session Managers. Only **SM1 (Session Manager 1)** is shown below.



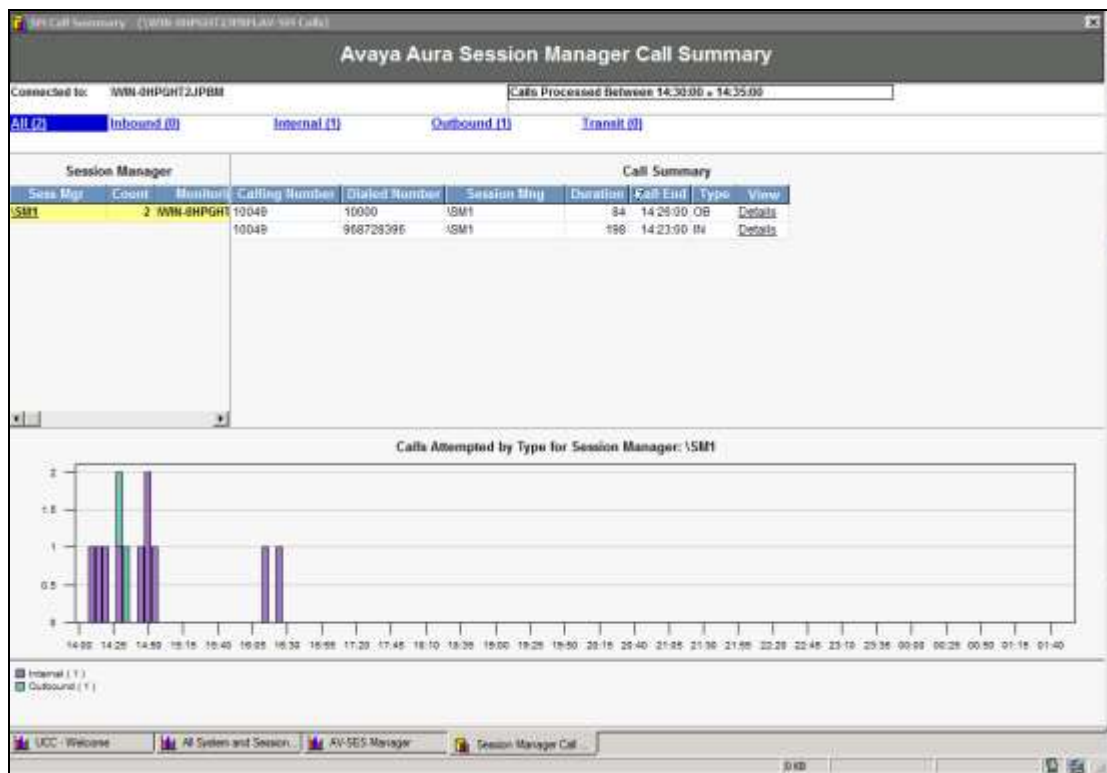
Step	Description
5.	<p>Make a call between two Avaya IP SIP telephones that belong to an IP Network Region that is being configured to send RTCP information to the Prognosis server. Verify that the <b>Voice Streams</b> section shows voice streams reflecting the quality of the call.</p>





Step	Description
------	-------------

- |    |  |
|----|--|
| 6. | Make several calls and look at the call summary. Verify that calls are recorded 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 <b>Section 5.2 Step 3</b> . |
|----|--|



## 8. Conclusion

These Application Notes describe the procedures for configuring the Prognosis to interoperate with Avaya Aura® System Manager and Avaya Aura® Session Manager. In the configuration described in these Application Notes, Prognosis obtained the configuration and status information through SNMP. Prognosis also processed the RTCP information to monitor the quality of IP calls and collected CDR information from each Session Manager as records. 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 7.0.1, Issue 2, May 2016, Document Number 555-245-205.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2, May 2016, Document Number 03-300509.
- [4] *Administering Avaya Aura® Session Manager*, Release 7.0.1, Issue 2, May 2016.
- [5] *Maintaining Avaya Aura® Session Manager, Release 7.0.1, Issue 2, May 2016*.
- [6] *Administering Avaya Aura® System Manager*, Release 7.0.1, Issue 2, May 2016
- [7] *Application Notes for Integrated Research's Prognosis for Unified Communications 10.5 with Avaya Aura® Communication Manager R7.0*.
- [8] *Avaya Aura® System Manager 7.0.1 SNMP Whitepaper*, Issue 1.0, May 2016.

The following Prognosis documentations are provided by Integrated Research. Documents are also provided in the online help that comes with the software Package.

- [9] *Prognosis Deployment and Installation Guide 10.5*, 22<sup>nd</sup> Feb 2016
- [10] *Prognosis for Unified Communications Avaya Aura Communication Manager User Guide, Prognosis 10.5*, 21 Dec 2015
- [11] *Prognosis for Unified Communications Avaya Aura System and Session Manager User Guide, Prognosis 10.5*, 21 Dec 2015

---

**©2016 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).