AVAYA

Application Notes for Integrated Research's Prognosis for Unified Communications 10 with Avaya Aura® Session Manager and Avaya Aura® System Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Prognosis for Unified Communications 10 to interoperate with Avaya Aura® Session Manager and System Manager.

Prognosis for Unified Communications 10 provides real-time monitoring and management solutions for IP telephony networks. Prognosis for Unified Communications 10 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.

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.

LYM; Reviewed:
SPOC 03/26/2014
Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
1 of 28
PROG-SM_SMGR

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Prognosis for Unified Communications 10 (herein after referred to as Prognosis) with Avaya Aura® System and Session Manager.

The Prognosis product uses three methods to monitor a Communication Manager system.

- Real Time Transport Control Protocol (RTCP) Collection - Prognosis collects RTCP information sent by the Avaya IP Media Processor (MEDPRO) boards, media gateways, IP Telephones.

- Call Detail Recording (CDR) Collection - The Prognosis collects CDR information by SFTP to the Session Manager.

- SNMP Collection – The Prognosis uses SNMP to collect configuration and status information from Avaya Aura® System 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 the System Manager and Session Manager. Calls were placed between Avaya SIP endpoints and 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, drives and status. For the collection of RTCP and CDR information, the endpoints included 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.

LYM; Reviewed:
SPOC 03/26/2014
Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
2 of 28
PROG-SM_SMGR

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 Avaya Aura® System Manager and Avaya Aura® Session Manager. It consists of a Communication Manager system (System A) running on a pair of Avaya S8800 Servers 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) running on Avaya S8800 Server 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. Avaya Aura® System Manager and Avaya Aura® 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 gateways and IP telephones.
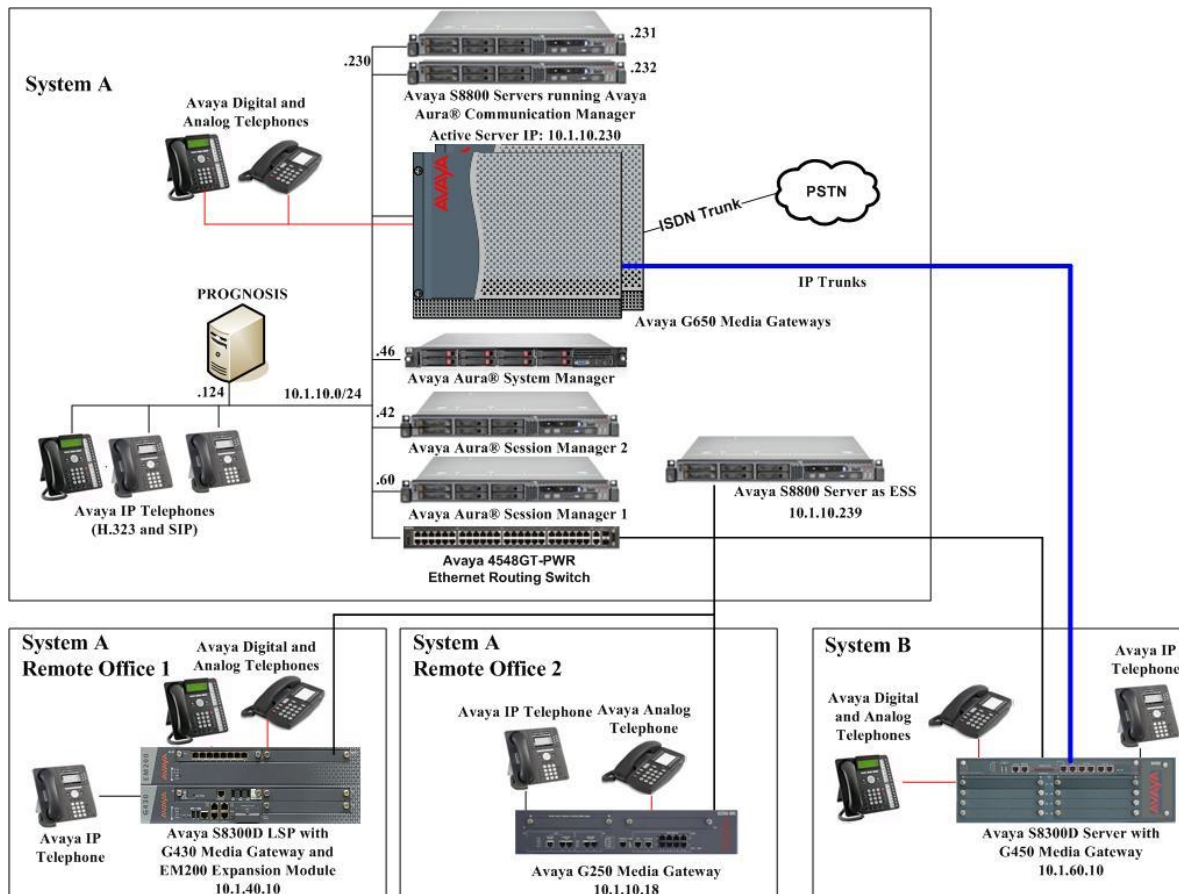
Figure 1: Test Configuration

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 running on Avaya S8800 Servers (System A)	6.3 SP3
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, FW057 HW01, FW043 HW02 FW064 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW011 HW08, FW016
G250 Media Gateway	30.27.1
Avaya Aura® Communication Manager running on Avaya S8300D Server (G450 Media Gateway – System B)	6.3 SP3
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	34.5.1 HW01 FW008 HW07 FW015 HW10 FW098 HW03 FW015 HW11 FW052
Avaya Aura® Communication Manager running on Avaya S8300D Server (G430 Media Gateway - LSP)	6.3 SP3
G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	34.5.1 HW04 FW015 HW12 FW098 HW31 FW098 HW05 FW022
Avaya Aura® Communication Manager running on Avaya S8800 Server (ESS)	6.3 SP3
HP DL360 G7 running Avaya Aura® System Manager	6.3 SP5 Patch 1
Avaya S8800 Server running Avaya Aura® Session Manager 1	6.3 SP5
Avaya S8800 Server running Avaya Aura® Session Manager 2 on VMware 5.1	6.3 SP5
Avaya Aura® Messaging	6.2 SP3
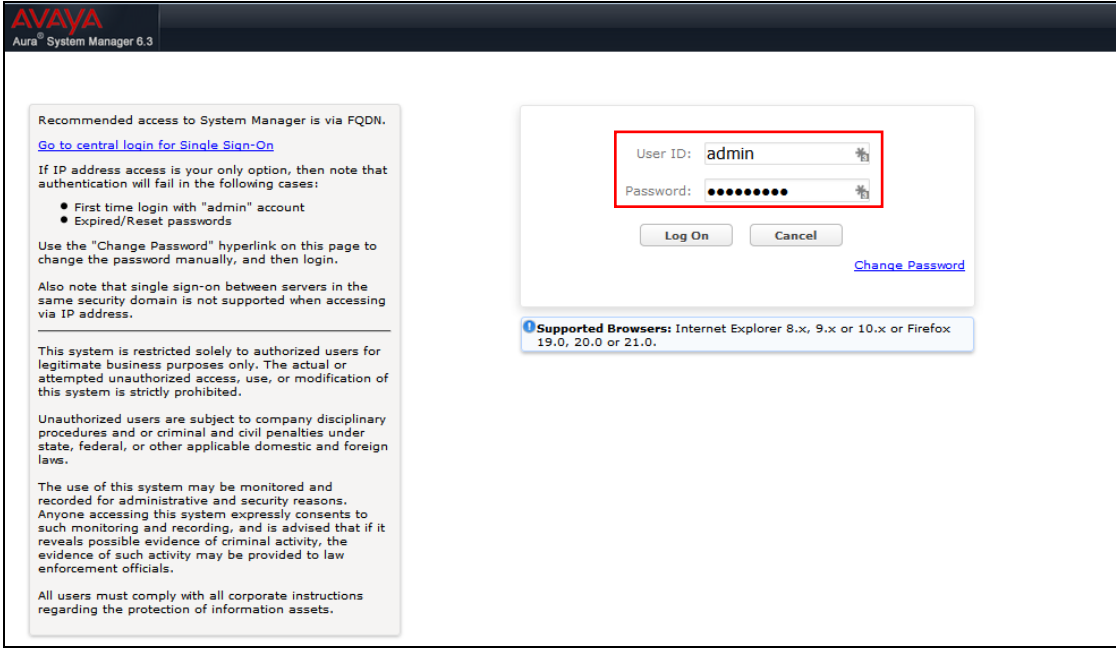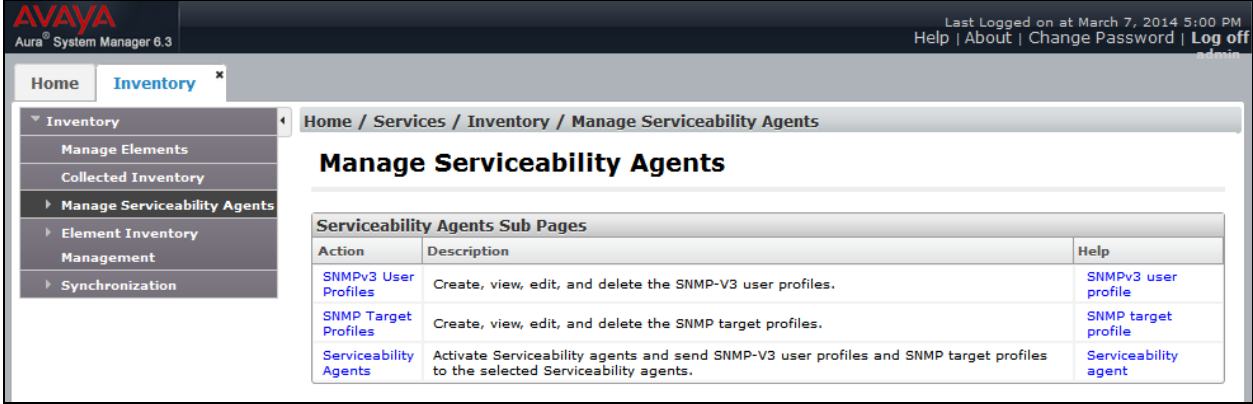
Equipment/Software	Release/Version
96xx Series IP Telephones - 9640 - 9620	2.6 SP11 (SIP) 3.2.1 (H323)
96x1 Series IP Telephones - 9641G - 9611G	6.3 (SIP) 6.3.1 (H323)
1600 Series IP Telephones - 1616 - 1603SW	1.34 (H.323)
Digital Telephones - 1416 - 1408	SP1
Avaya Analog Phones	-
Avaya 4548GT-PWR Ethernet Routing Switch	V5.6.1.052
Prognosis on Windows 2008 R2 SP1	Windows 2008 R2 SP1
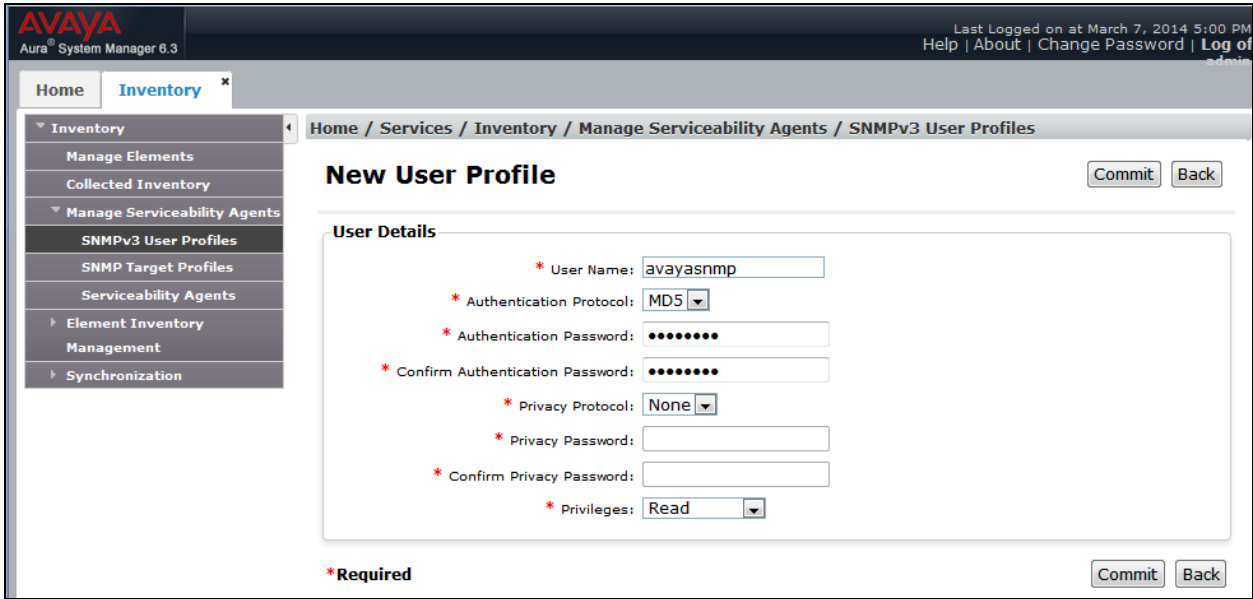
5. Configure System/Session Manager
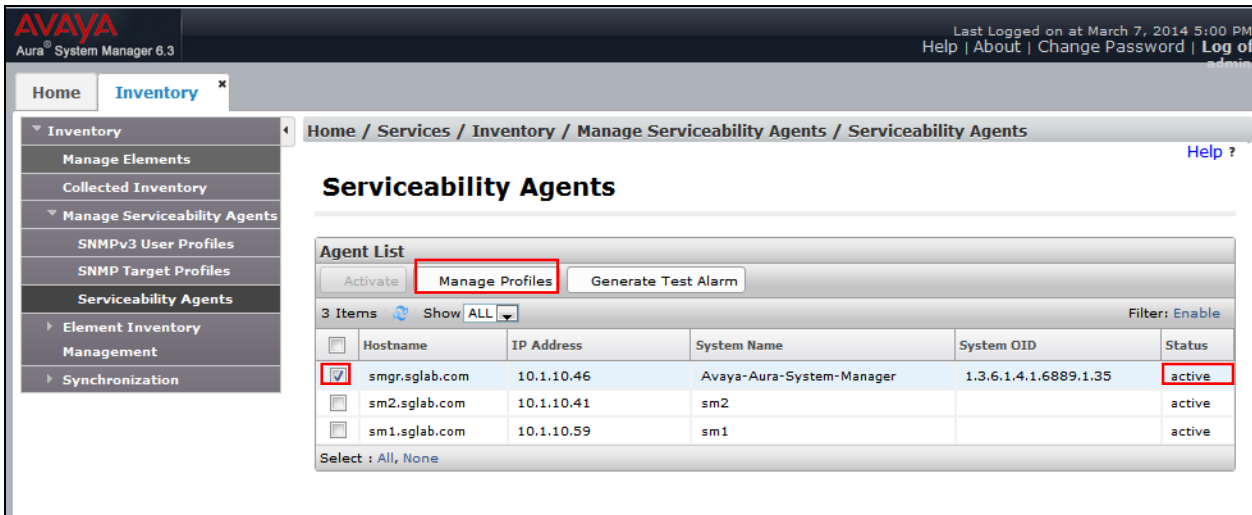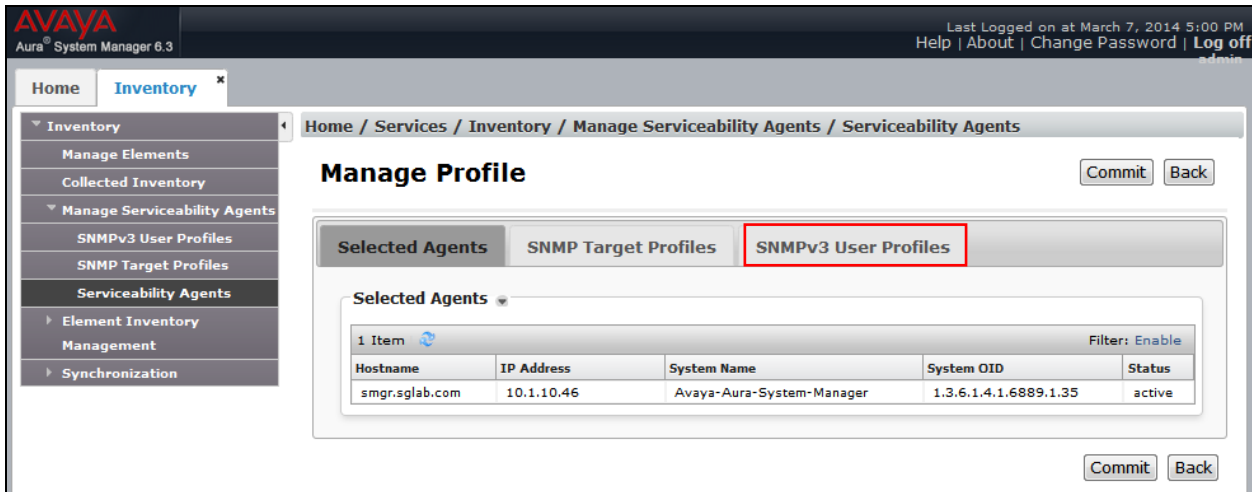
This section describes the steps needed to configure System and Session Manager to interoperate with Prognosis. This includes configuration of the SNMP v3 user profile for System Manager and the CDR user account on both Session Managers. The default SNMP v2c user profile will be used for Session Managers and no configuration is needed here. Configuration of Communication Manager is mentioned in **Reference [4]** and will not be detailed here.
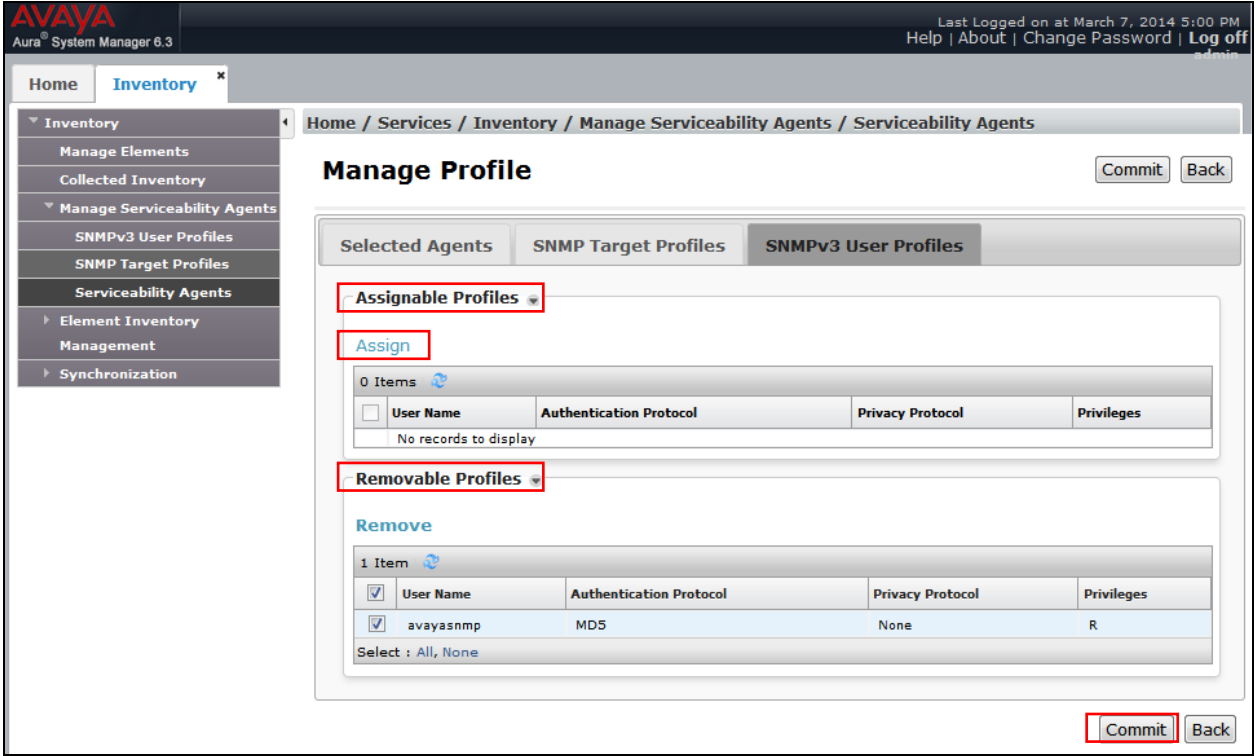
5.1. Configure SNMP

System Manager 6.3 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.
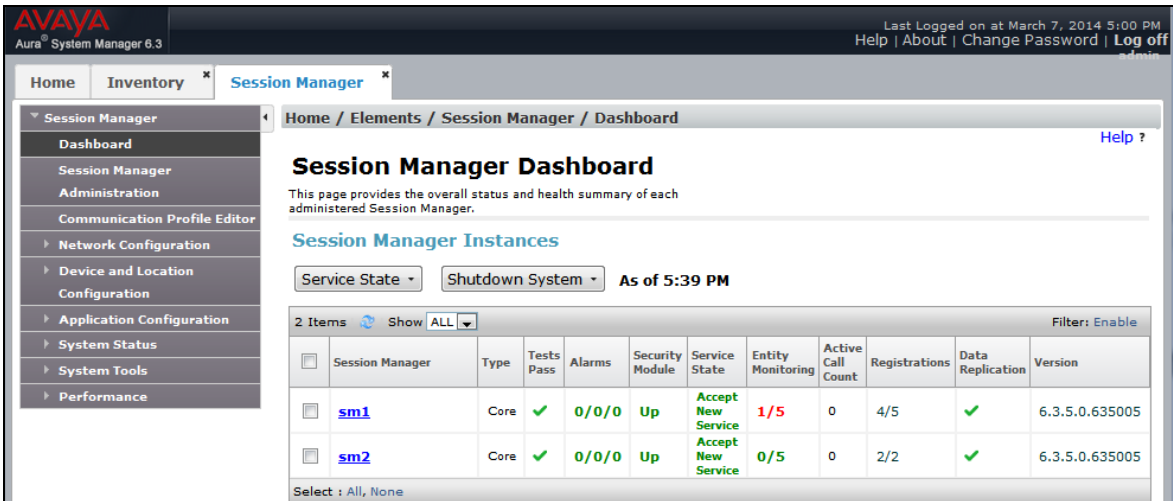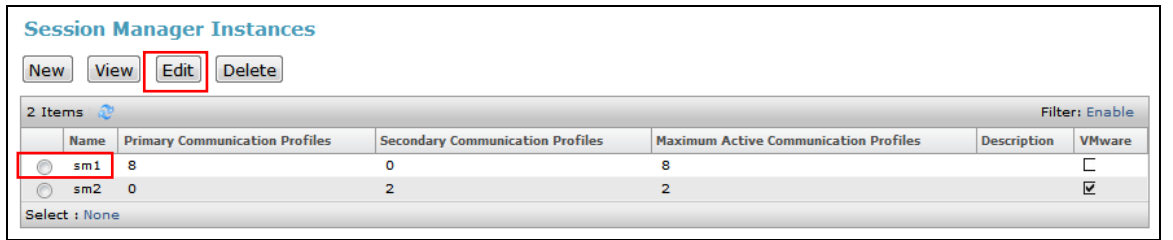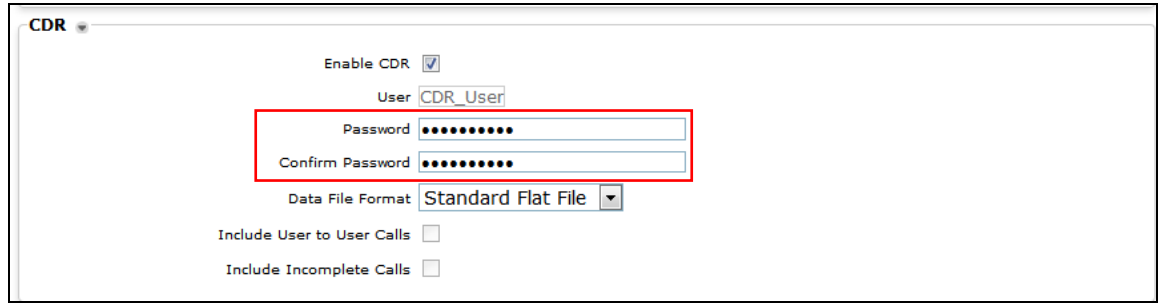
Step	Description
1.	Using a web browser, enter https://<IP address of System Manager> to connect to the System Manager Server being configured and log in using appropriate credentials.
2.	On the home screen (not shown), select **Services → Inventory**.

Step	Description
3.	Expand on the **Manage Serviceability Agents → SNMPv3 User Profiles** (not shown). Click **New** to add a new user profile. Enter the following details for the **User Profile**. 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 • **Authentication Protocol**: MD5 • **Authentication Password**: avaya123 • **Privacy Protocol**: None • **Privileges**: Read Click **Commit** to submit.

LYM; Reviewed:
SPOC 03/26/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

9 of 28
PROG-SM_SMGR

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 click **Manage Profiles**.

| 5. | Select **SNMPv3 User Profiles** and click **Commit** below. |

LYM; Reviewed:
SPOC 03/26/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

10 of 28
PROG-SM_SMGR

Step	Description
6.	Click *down arrow* beside **Assignable Profiles** section if it is not expanded. Click **Assign** to assign it to the System Manager. The user profile is moved to the **Removable Profiles** section as below. The user profile has been assigned to the System Manager. Click **Commit** to submit the changes.

5.2. Configure CDR user account for Session Manager

Step	Description
1.	From the home screen, navigate to the Session Manager by clicking **Elements → Session Manager.**
2.	Click **Session Manager → Session Manager Administration**. On the right pane under the **Session Manager Instances** section, click **sm1** and then **Edit**.
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 which is the current CDR file format supported by Prognosis.
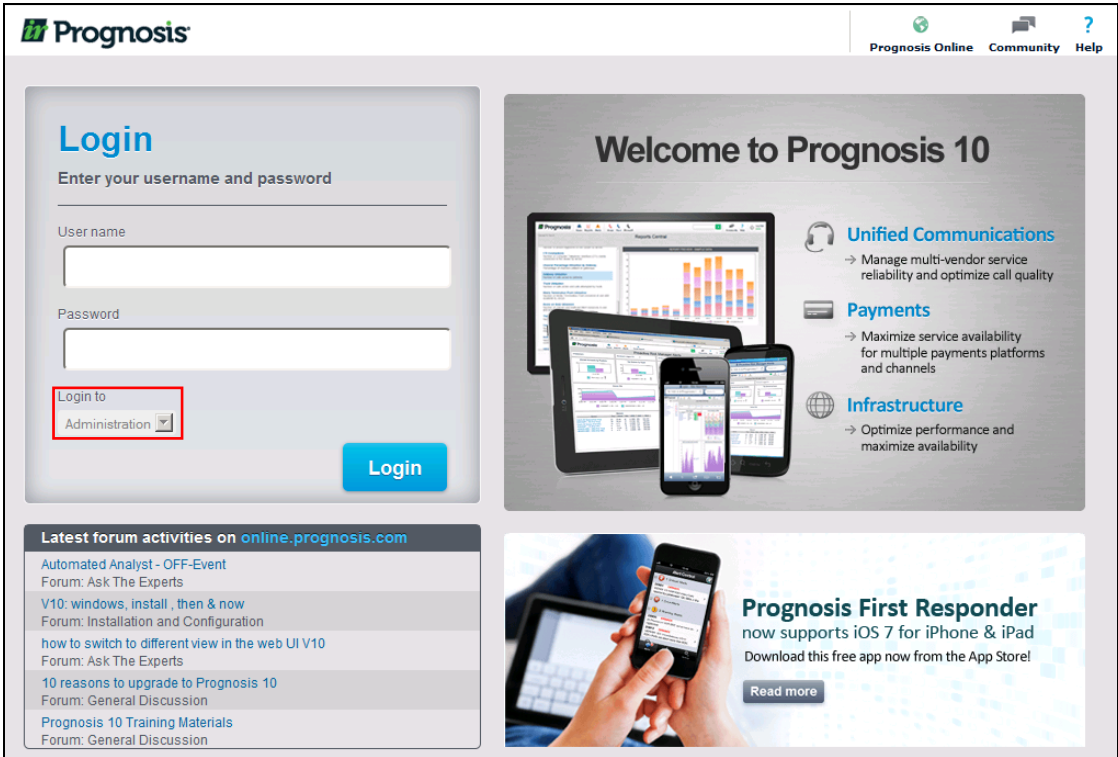
5.3. Download Sip Entities and Entity Links XML files.
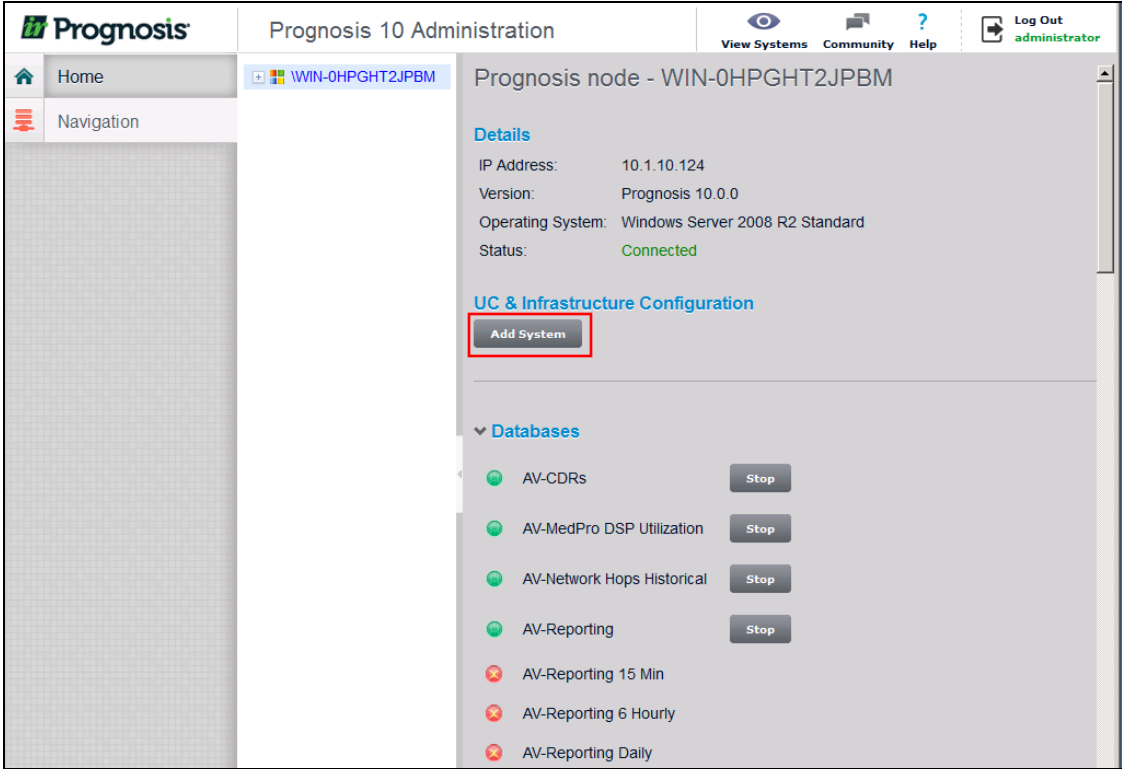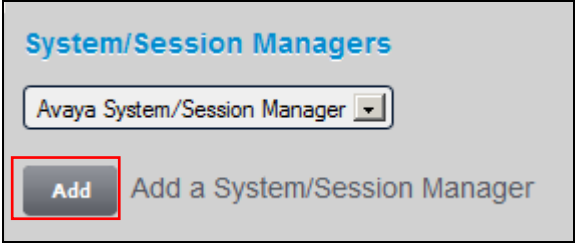
The Sip Entities and Entity Links XML files are required for input into Prognosis for configuration of System and Session Manager. These files can be downloaded from System Manager.

Step	Description
1.	On the System Manager home screen (not shown), select **Element → Routing.** Click **Routing → SIP Entities** and select **Export SIP Entities** in the drop-down menu. Save the SIP Entities file into the local hard disk for uploading into the Prognosis in **Section 6 Step 4**.
2.	On the same page above, click **Entity Links** and select **Export Entity Links** in the drop-down menu. Save the Entity Links file into the local hard disk for uploading into the Prognosis also in **Section 6 Step 4**.

LYM; Reviewed:
SPOC 03/26/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

14 of 28
PROG-SM_SMGR

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 [4]** and will not be detailed here.

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

LYM; Reviewed:
SPOC 03/26/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

15 of 28
PROG-SM_SMGR

Step	Description
2.	Click **Add System**.
3.	Click **Add** to add a new System Manager.

Step	Description
4.	In this test configuration, the following entries are added for System Manager with the Display Name **SMGR63SP5** and with the IP addresses as **10.1.10.46.** The following settings were configured during the compliance test. **Basic Details:** • **IP address: 10.1.10.46** • **Display Name: SMGR63SP5** • **Customer Name: Avaya** • **Site Name: DevConLab** **Configuration:** Browse for the **Sip Entities** and **Entity Links XML** files downloaded in **Section 5.3** and copy into the Prognosis server. Ensure that the xml files have been uploaded to the Avaya folder: PROGNOSIS_HOME/Server/Configurations/IPTM/ **SNMP Connection Details**: Enter the settings configured in **Section 5.1 Step 3** Leave the **Databases and Thresholds** as checked. Click **Add** to effect the addition. **Add Avaya System Manager** **Basic Details** IP Address: * `10.1.10.46` Display Name: * `SMGR63SP5` Customer Name: `Avaya` Site Name: `DevConLab` **Configuration** Sip Entities XML File:　Browse…　No file selected. Entity Links XML File:　Browse…　No file selected. **SNMP Connection Details** ○ Use SNMP Version 2c ◉ Use SNMP Version 3 Authentication Protocol:　MD5 ▾ Authentication User Name: * `avayasnmp` Authentication Password: * •••••••• Encryption Method:　None ▾ **Databases and Thresholds** ☑　Start standard databases and thresholds Add　Cancel

Step	Description
5.	Return to the home screen; check that **SMGR63SP5** is created under the server name. Click on the **SMGR63SP5** to update the Session Manager.
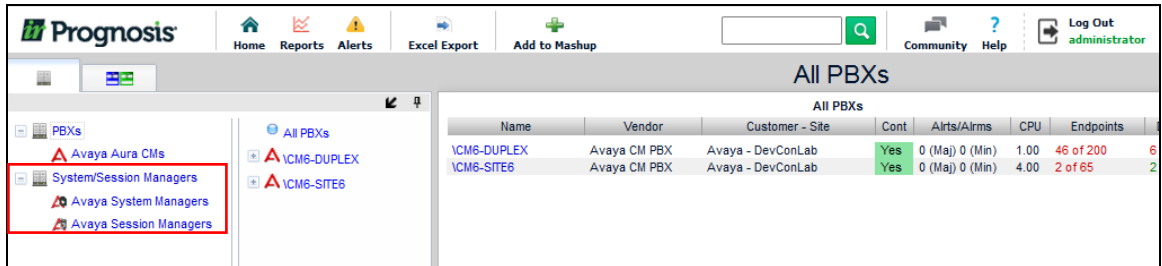
Step	Description
6.	Check that the Sip Entities and Entity Links XML files are **LOADED**. Click **Edit** on **SM1**.

LYM; Reviewed:
SPOC 03/26/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

19 of 28
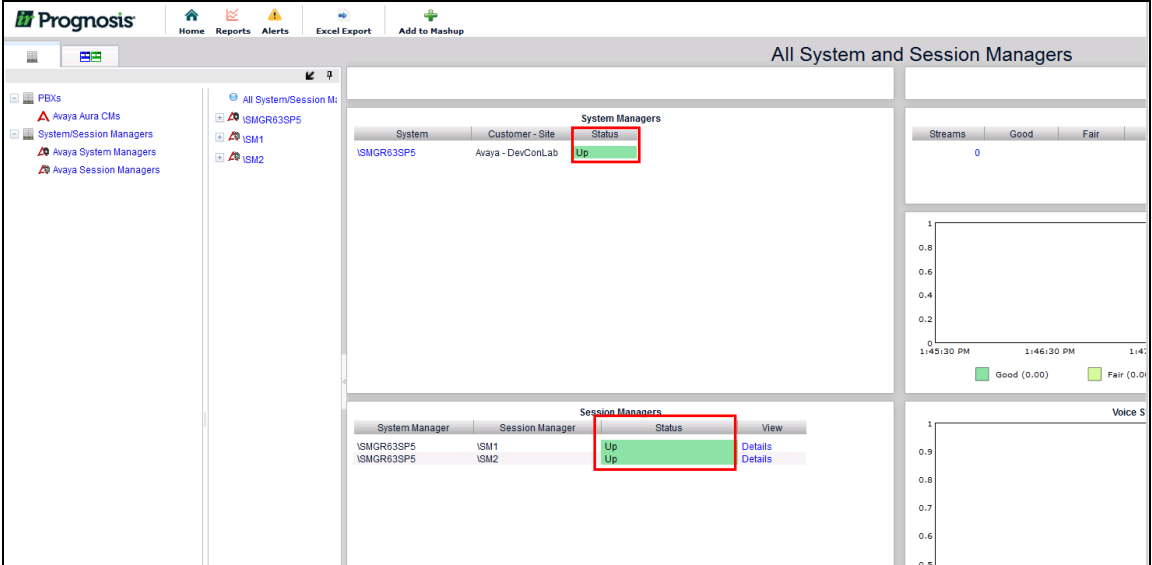PROG-SM_SMGR

Step	Description
7.	The following settings were configured during the compliance test.

Session Manager Details:
- **Management IP: 10.1.10.59**
- **Site Name: Location1**

CDR Configuration Details (SFTP):
- **User Name: CDR_User**
- **Password:** As configured in Section 5.2
- **Mode: SFTP**
- **Port: 22**
- **Remote Directory: /** (As default)

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.

Click **Update** to make the changes. Repeat the **Step 6-7** 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: Location1

CDR Configuration Details (SFTP)
User Name: [?] CDR_User
Password: ********

Mode: SFTP

Port: 22
Remote Directory: [?] /

☐ Use System Manager SNMP

SNMP Connection Details
⦿ Use SNMP Version 2c
○ Use SNMP Version 3
Community String: ********

[Update] [Stop Monitoring] [Cancel]

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.

Step	Description
9.	SSH into the Session Managers and log in as 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.

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**, verify that the System Manager Display Name **SMGR63SP5** is created under the server name. Then select View Systems on the top right icon.
2.	Check that the System Managers and Session Managers are created on the left pane.

Step	Description
3.	Verify the System Manager and the 2 Session Managers **Status** are **Up**.

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

Avaya System Manager - Hardware

Node: \SMGR63SP5

System Details

Name	IP Address	Status	Up Time
\SMGR63SP5	10.1.10.46	Up	8 days 21 hrs

System Description

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

Memory Utilization %

Physical memory
Swap space
Total

Total CPU Utilization %

CPU 0
CPU 1
CPU 2
CPU 3

Physical Drives

Index	Cap (GB)	Type	Removable	Access

Virtual Drives

Index	Description	Cap (GB)	Full (%)	Failures
1	Physical memory	9.00	99	0
3	Virtual memory	11.00	81	0
6	Memory buffers	9.00	3	0
7	Cached memory	1.30	100	0
8	Shared memory	0.00		0
31	/	28.94	40	0
32	/boot	0.10	14	0
33	/perfdata	29.53	1	0
34	/emdata	1.97	3	0

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	62 days 3 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	usb0	Down	Down	Ethernet	0	E6:1F:13:29:4A:BB	0	0	0	0
3	eth0	Up	Up	Ethernet	1 Gb/s	E4:1F:13:2F:FA:B8	0	0	0	0
4	eth1	Up	Down	Ethernet	0	E4:1F:13:2F:FA:BA	0	0	0	0
5	eth2	Up	Up	Ethernet	1 Gb/s	00:21:5E:08:EA:E4	0	0	0	0
6	eth3	Down	Down	Ethernet	0	00:21:5E:08:EA:E6	0	0	0	0

Memory Utilization %

Total CPU Utilization %

CPU 0
CPU 1
CPU 10
CPU 11
CPU 12
CPU 13
CPU 14
CPU 15
CPU 2
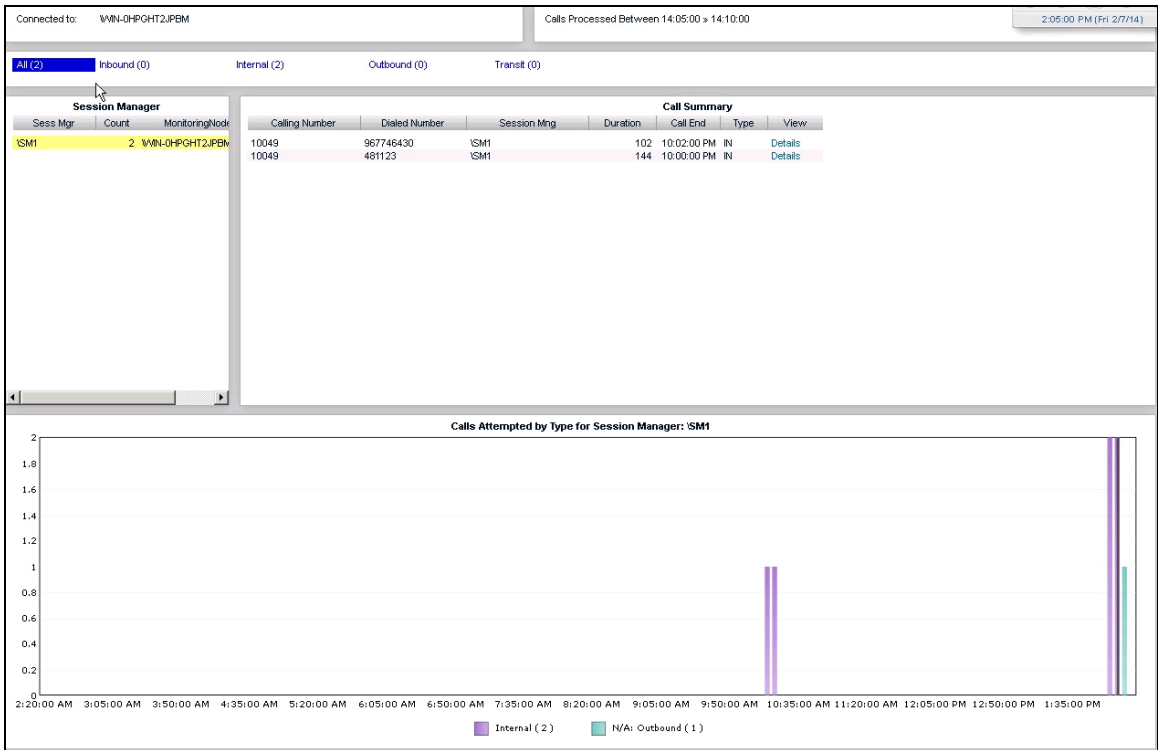
Physical Drives

Index	Cap (GB)	Type	Removable	Access
16	135.97	Unknown	No	Read/Write
64	78.00	Unknown	No	Read/Write

Virtual Drives

Index	Description	Cap (GB)	Full (%)	Failures

LYM; Reviewed:
SPOC 03/26/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

24 of 28
PROG-SM_SMGR

Step	Description
5.	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 **Voice Streams** section shows two active voice streams reflecting the quality of the call.

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

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 **Section 5.2 Step 3**.

LYM; Reviewed:
SPOC 03/26/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

26 of 28
PROG-SM_SMGR

8. Conclusion

These Application Notes describe the procedures for configuring the Prognosis to interoperate with Avaya Aura® System and 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.

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 6.3, Issue 10.0, May 2013, Document Number 555-245-205.
[2] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 9.0, October 2013, Document Number 03-300509.
[3] *Application Notes for Integrated Research Prognosis IP Telephony Manager 9.6.1 with Avaya Aura® Communication Manager 6.2.*
[4] *Application Notes for Integrated Research's Prognosis IP Telephony Manager 10 with Avaya Aura® Communication Manager.*

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

[3] *Prognosis 10 Deployment and Installation Guide*, 31st October 2013.

©2014 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.