Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis for Unified Communications R11.7 to interoperate with Avaya Aura® System Manager R8.1.

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

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

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

1. Introduction

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

The Prognosis product uses Simple Network Management Protocol (SNMP) to collect configuration and status information from System 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.

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 did not include use of any specific encryption features as requested by Integrated Research.

2.1. Interoperability Compliance Testing

For feature testing, Prognosis Webui was used to view the configurations of System Manager such as the memory and CPU utilizations, disk usage and status.

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

2.2. Test Results

All test cases passed successfully with the following being observed:

- Communication Manager name configured on Prognosis needs to have the name matched with that configured on System Manager SIP entities. Otherwise the correct PBX will not be monitored.

2.3. Support

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

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

3. Reference Configuration

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

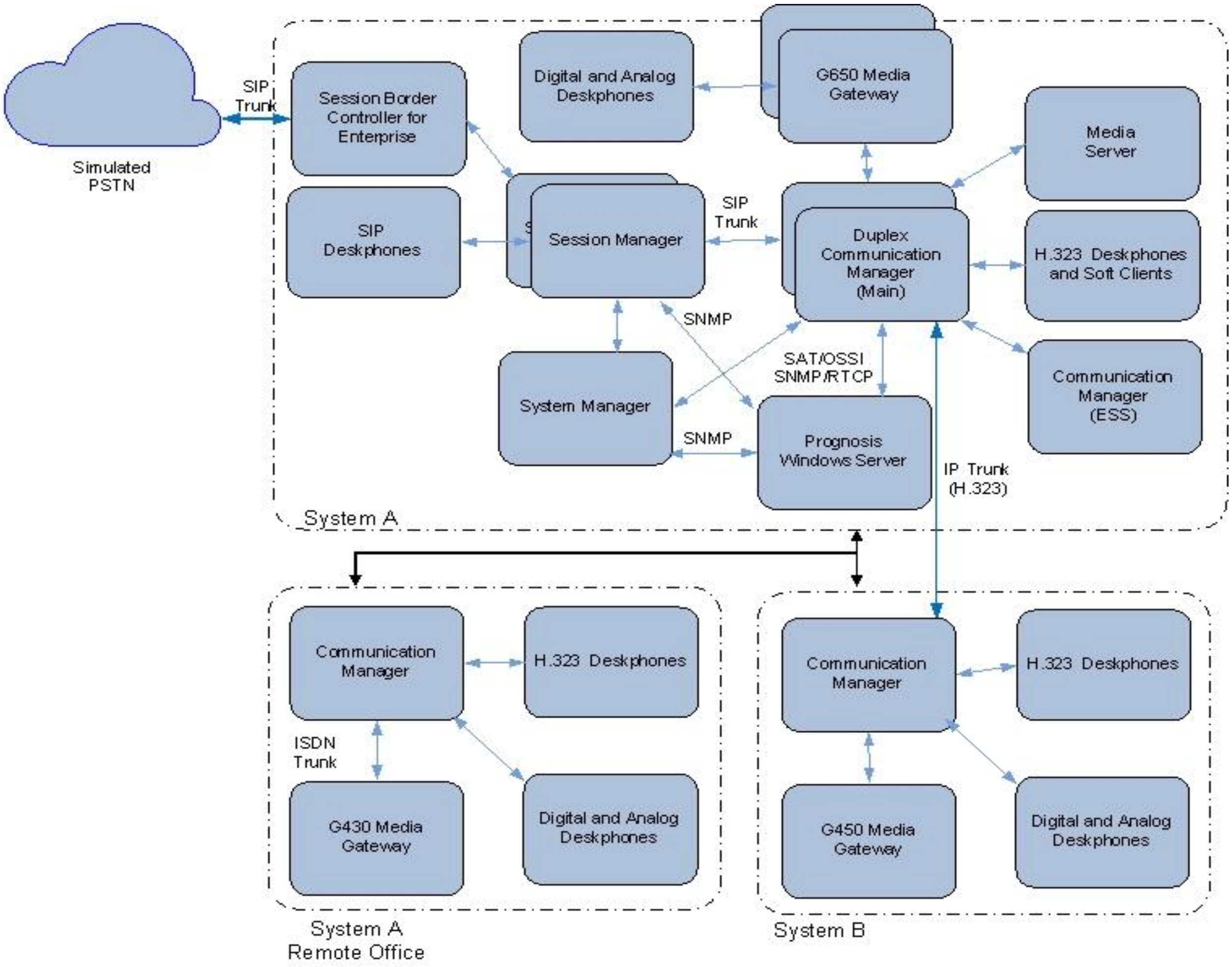


Figure 1: Test Configuration

4. Equipment and Software Validated

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

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

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

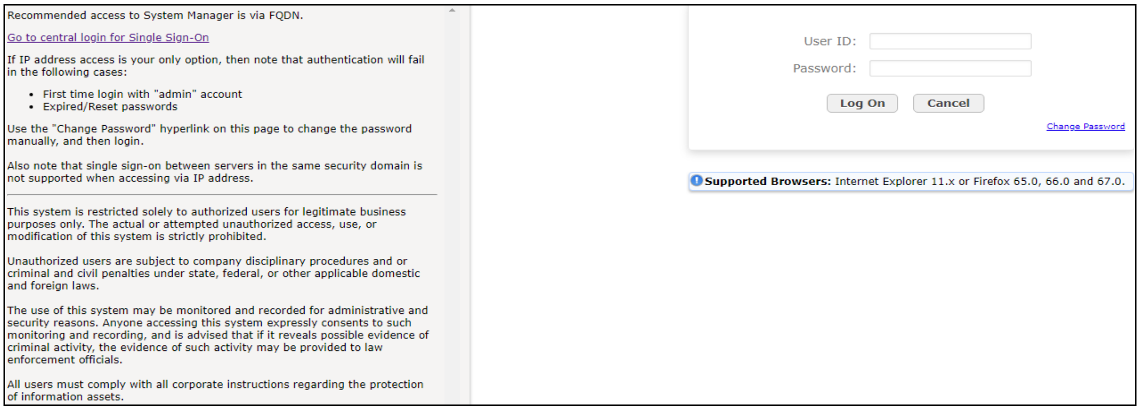
Note: All Avaya Aura® systems and Prognosis runs on VMware 6.x virtual platform.

5. Configure Avaya Aura® System Manager

This section describes the steps needed to configure System Manager to interoperate with Prognosis. This includes configuration of the SNMP v3 user profile for System Manager.

5.1. Configure SNMP for Avaya Aura® System Manager

System Manager 8.1 supports SNMPv2 for notifications and GET/SET operations will work only for V3. The following shows the steps to create SNMPv3 user profiles and assign the profile to System Manager. 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.

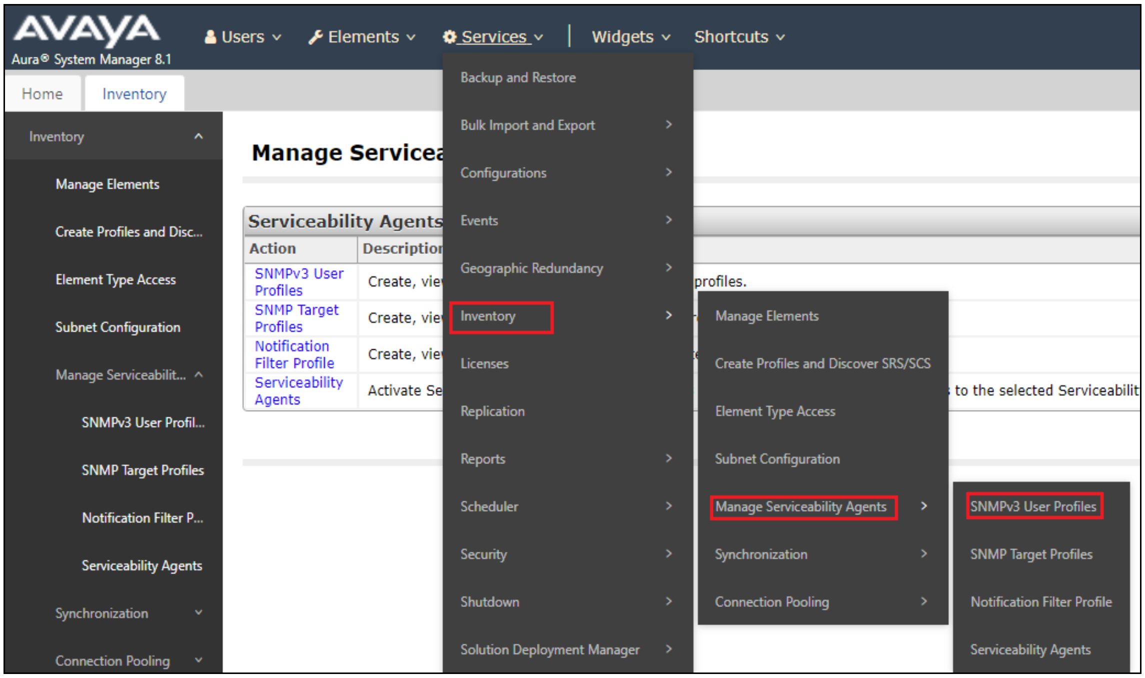
Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

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.

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

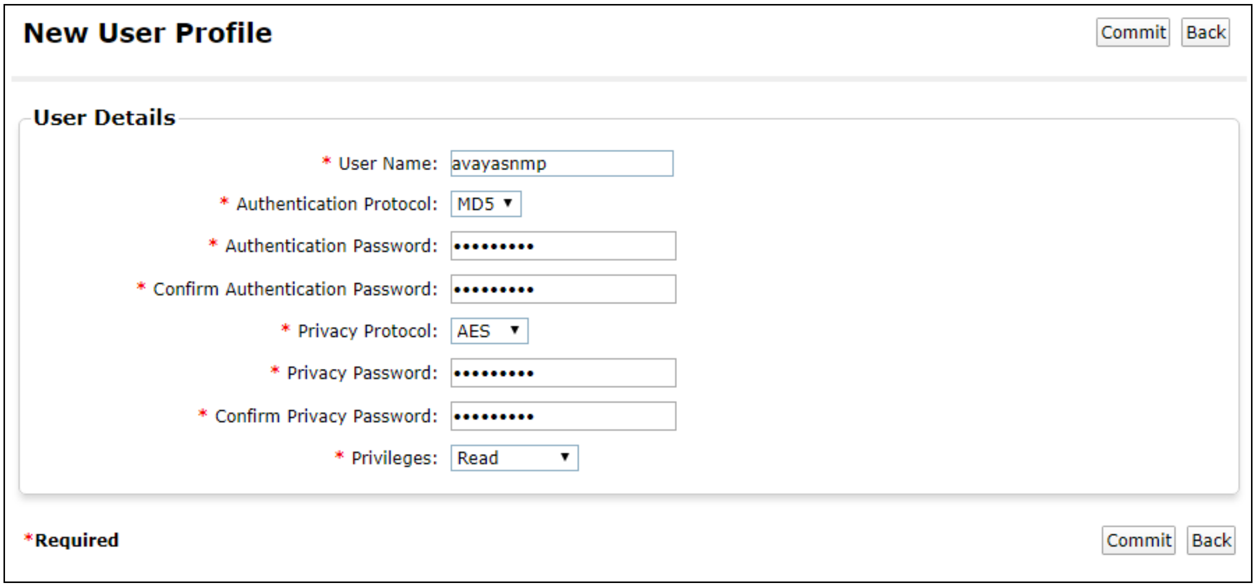
On the home screen, select **Services → Inventory → Manage Serviceability Agents → SNMPv3 User Profiles**.



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**. For more secured configuration, the profiles can be adjusted here, and the corresponding Prognosis configuration in **Section 6** 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.



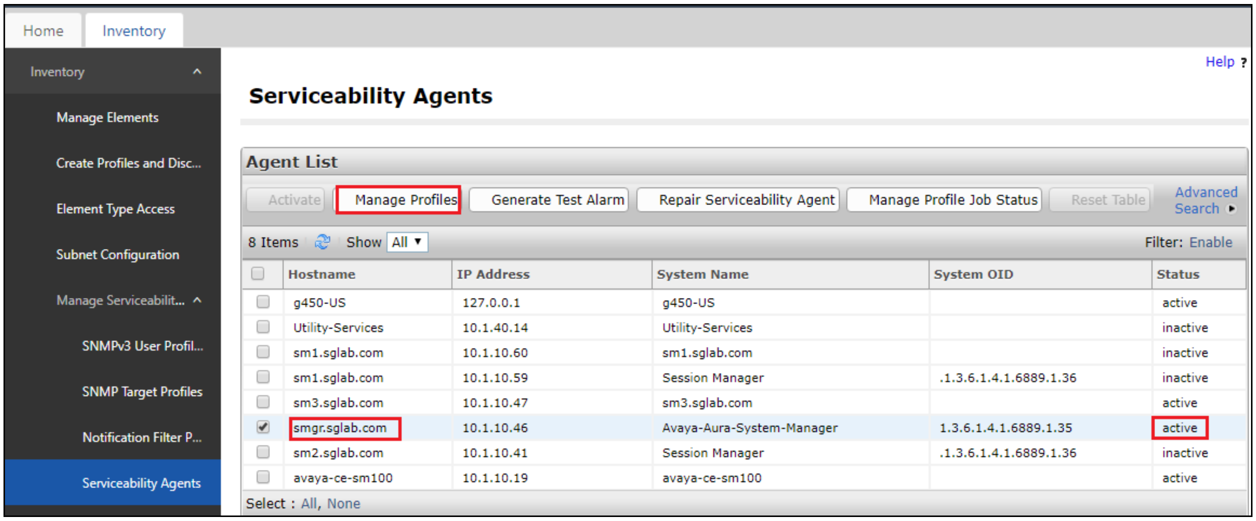
New User Profile

User Details

* User Name:	avayasnmp
* Authentication Protocol:	MD5
* Authentication Password:	•••••••••
* Confirm Authentication Password:	•••••••••
* Privacy Protocol:	AES
* Privacy Password:	•••••••••
* Confirm Privacy Password:	•••••••••
* Privileges:	Read

*Required

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.



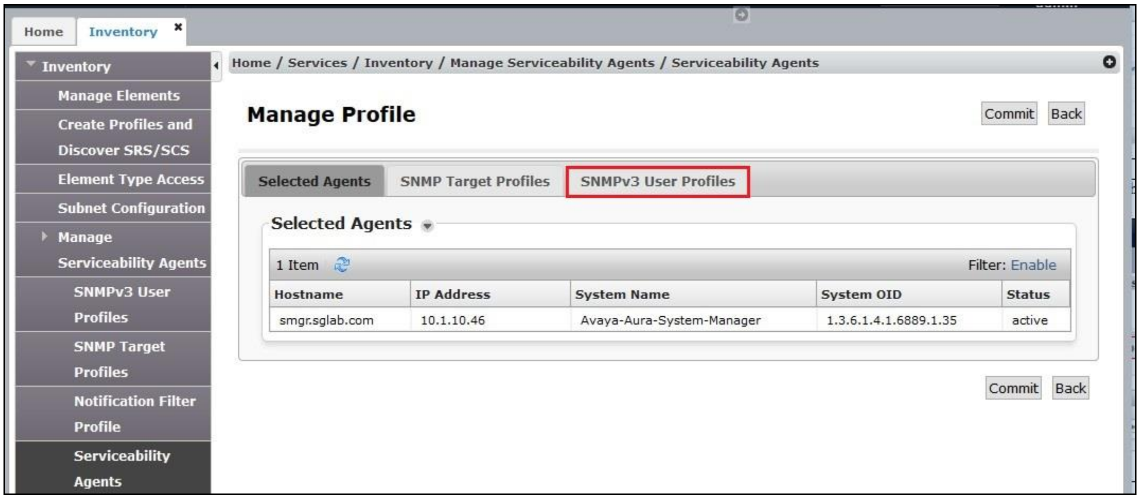
Serviceability Agents

Agent List

8 Items Show All

☐	Hostname	IP Address	System Name	System OID	Status
☐	g450-US	127.0.0.1	g450-US		active
☐	Utility-Services	10.1.40.14	Utility-Services		inactive
☐	sm1.sglab.com	10.1.10.60	sm1.sglab.com		inactive
☐	sm1.sglab.com	10.1.10.59	Session Manager	.1.3.6.1.4.1.6889.1.36	inactive
☐	sm3.sglab.com	10.1.10.47	sm3.sglab.com		active
☑	smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
☐	sm2.sglab.com	10.1.10.41	Session Manager	.1.3.6.1.4.1.6889.1.36	inactive
☐	avaya-ce-sm100	10.1.10.19	avaya-ce-sm100		active

Select **SNMPv3 User Profiles** tab.



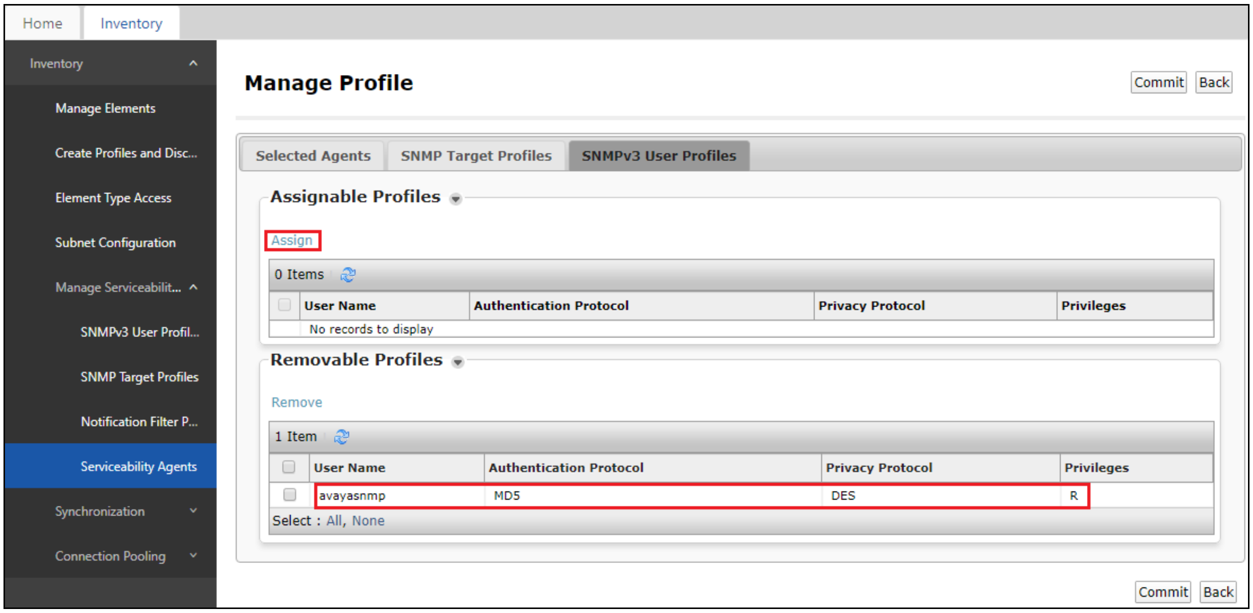
Manage Profile

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

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



Manage Profile

Assignable Profiles

0 Items

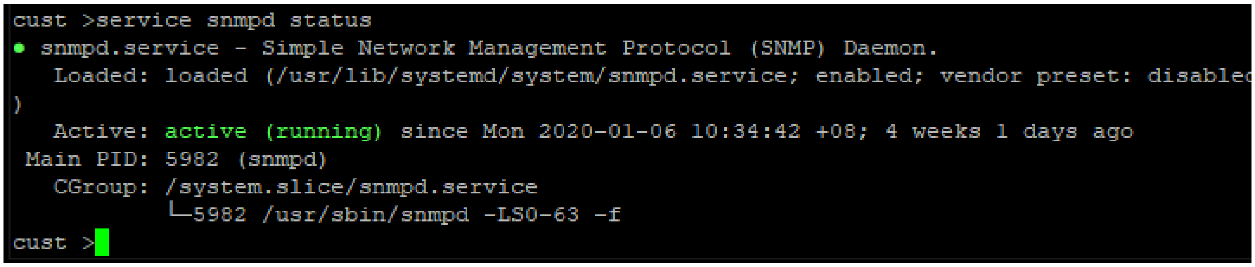
□	User Name	Authentication Protocol	Privacy Protocol	Privileges
	No records to display			

Removable Profiles

1 Item

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

SSH into the System Manager command line interface and log in as valid user. Verify that the SNMP service is **active (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.

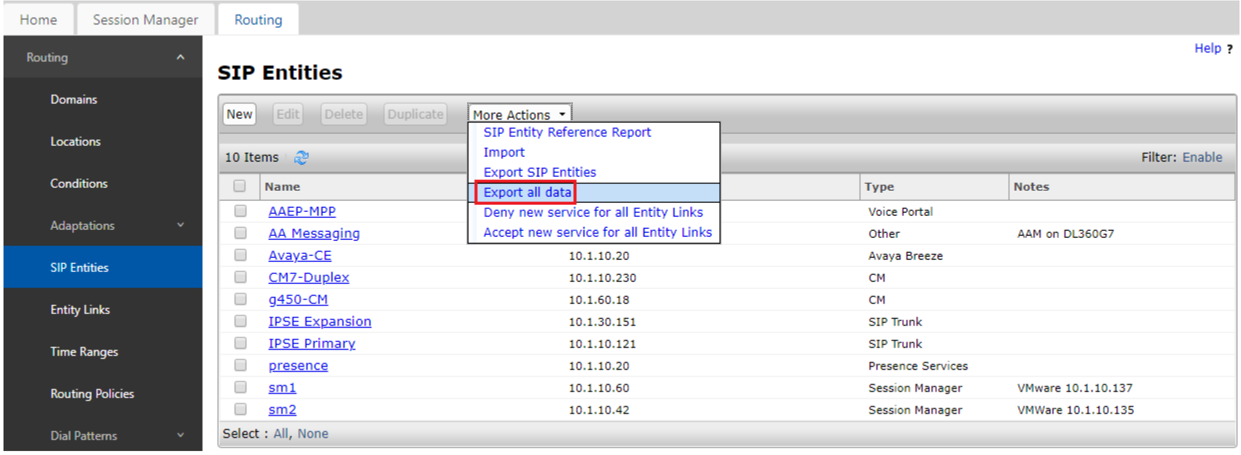


```
cust >service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset: disablec
)
   Active: active (running) since Mon 2020-01-06 10:34:42 +08; 4 weeks 1 days ago
 Main PID: 5982 (snmpd)
   CGroup: /system.slice/snmpd.service
           └─5982 /usr/sbin/snmpd -LS0-63 -f
cust >
```

5.2. 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 all the SIP Entities and Entity Links. These files can be downloaded from System Manager.

On the System Manager home screen (not shown), select **Elements → Routing → SIP Entities** and select **Export all data** in the **More Actions** drop-down menu. Save the zip file into the local PC hard disk. Extract the files "*<user name>EntityLinks.xml*" and "*<user name>SipEntities.xml*". Rename the files without the user name. Upload the renamed files "EntityLinks.xml' and "SipEntities.xml" into the Prognosis server in **Section 6**.



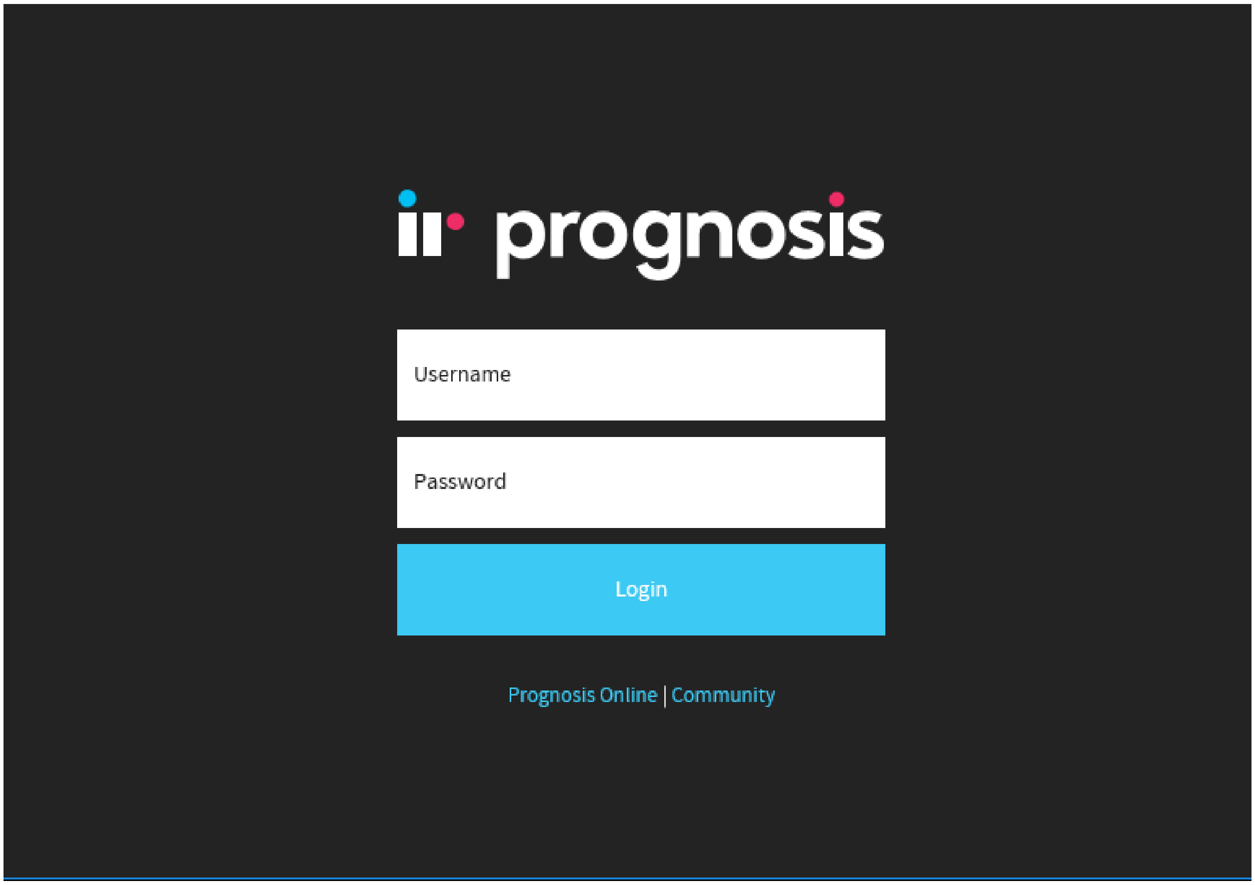
□	Name		Type	Notes
□	AAEP-MPP		Voice Portal	
□	AA Messaging		Other	AAM on DL360G7
□	Avaya-CE	10.1.10.20	Avaya Breeze	
□	CM7-Duplex	10.1.10.230	CM	
□	g450-CM	10.1.60.18	CM	
□	IPSE Expansion	10.1.30.151	SIP Trunk	
□	IPSE Primary	10.1.10.121	SIP Trunk	
□	presence	10.1.10.20	Presence Services	
□	sm1	10.1.10.60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

Select : All, None

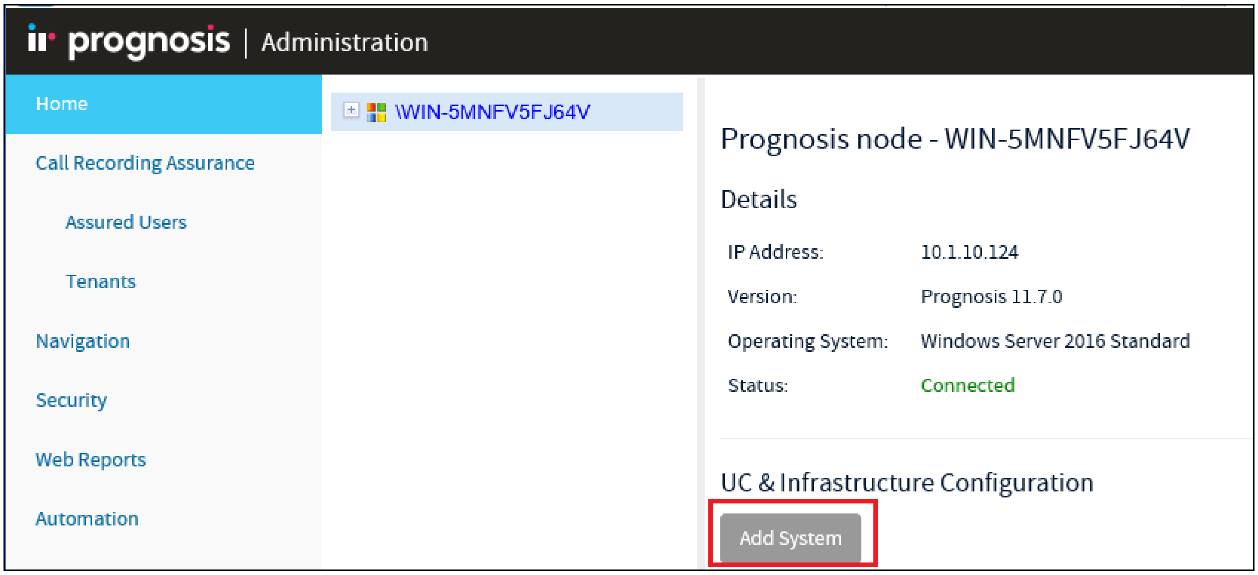
6. Configure Integrated Research Prognosis

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

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



Click **Add System**.



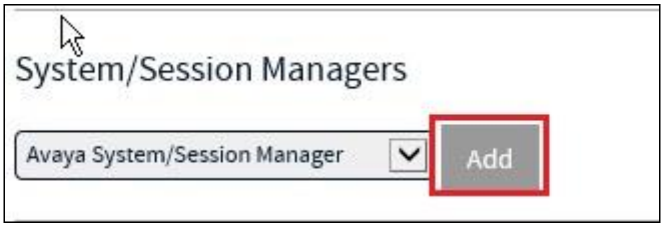
Prognosis node - WIN-5MNFV5FJ64V

Details

IP Address:	10.1.10.124
Version:	Prognosis 11.7.0
Operating System:	Windows Server 2016 Standard
Status:	Connected

UC & Infrastructure Configuration

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

In this test configuration, the following entries are added for System Manager with display name of **SMGR8** and IP address as **10.1.10.46**.

The following settings were configured during the compliance test.

Basic Details:

- **Display Name: SMGR8**
- **IP address: 10.1.10.46**
- **Customer Name: Avaya**
- **Site Name: DevCon Lab**

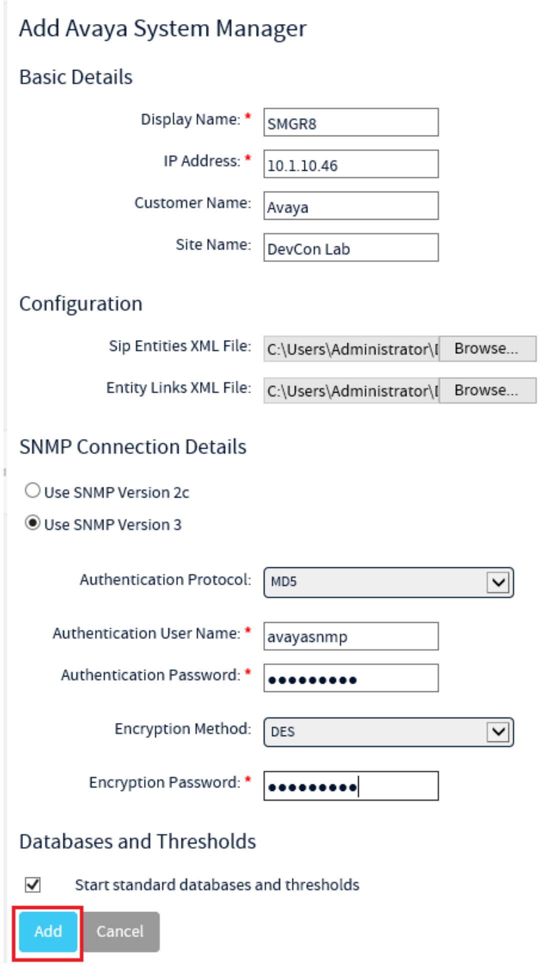
Configuration:

Browse for the SIP Entities and Entity Links XML files downloaded in **Section 5.2** and copy into the Prognosis server.

SNMP Connection Details:

Select "Use SNMP Version 3" and enter the settings as configured in **Section 5.1**.

Leave the **Databases and Thresholds** as checked. Click **Add** at the bottom to affect the addition.



Add Avaya System Manager

Basic Details

Display Name: * SMGR8

IP Address: * 10.1.10.46

Customer Name: Avaya

Site Name: DevCon Lab

Configuration

Sip Entities XML File: C:\Users\Administrator\I Browse...

Entity Links XML File: C:\Users\Administrator\I Browse...

SNMP Connection Details

○ Use SNMP Version 2c

● Use SNMP Version 3

Authentication Protocol: MD5

Authentication User Name: * avayasnmp

Authentication Password: * •••••••••

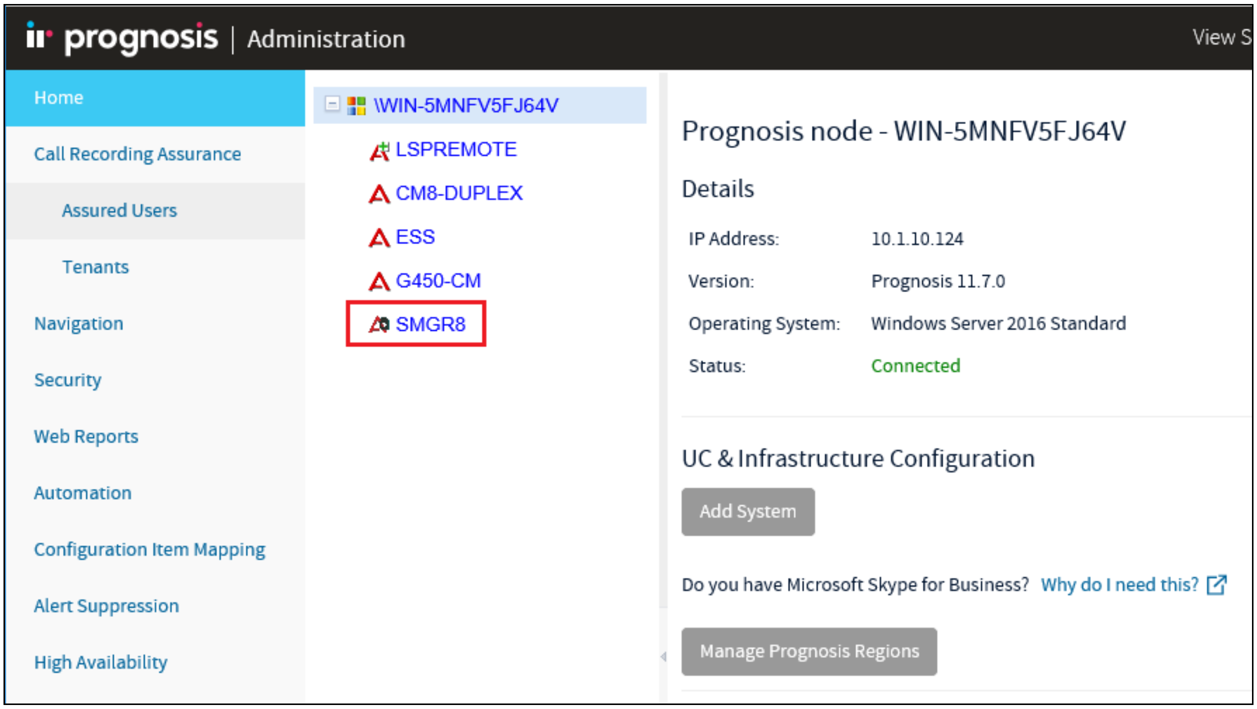
Encryption Method: DES

Encryption Password: * •••••••••

Databases and Thresholds

☑ Start standard databases and thresholds

Return to the home screen; check that **SMGR8** is created under the server name in the middle pane. Click on the **SMGR8** highlighted below.



Prognosis node - WIN-5MNFV5FJ64V

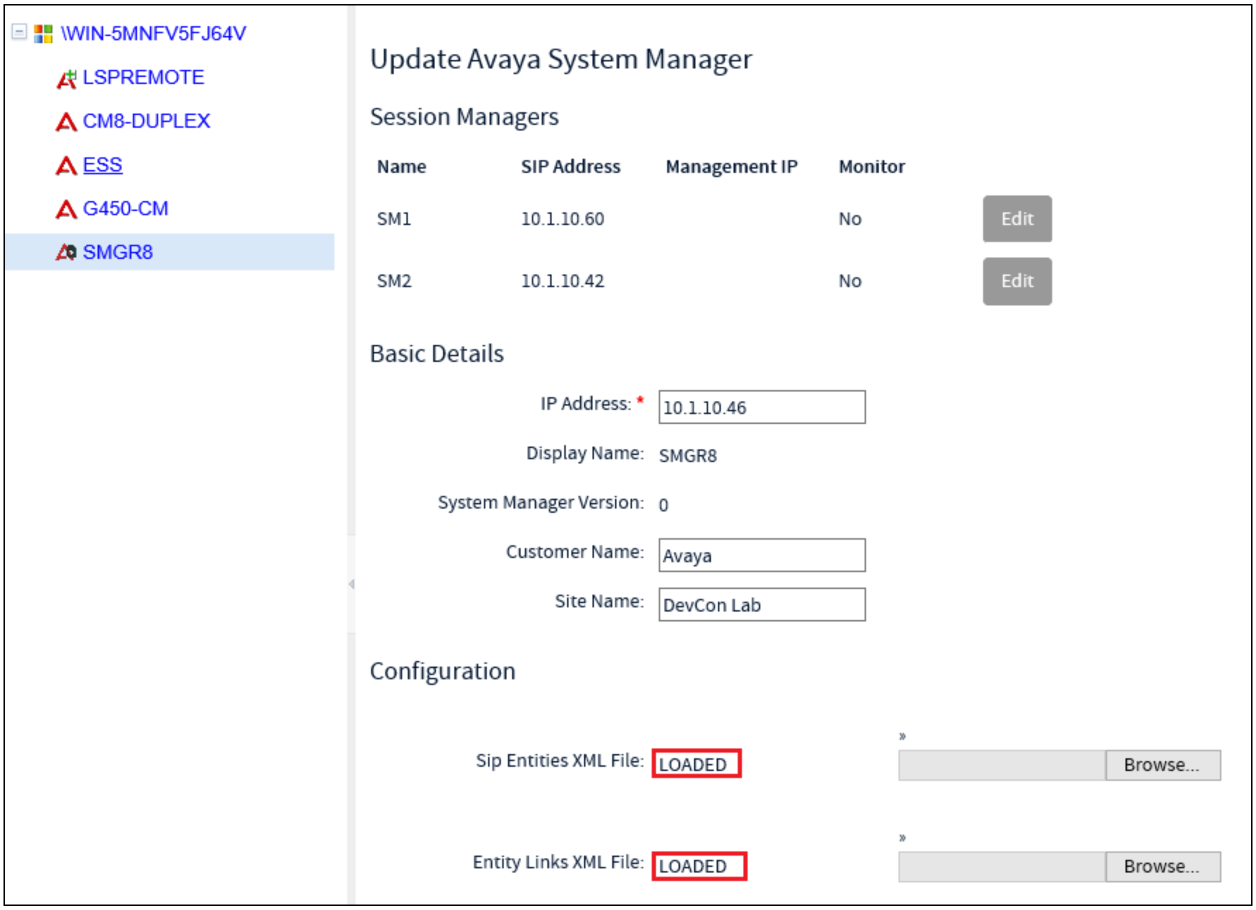
Details

IP Address:	10.1.10.124
Version:	Prognosis 11.7.0
Operating System:	Windows Server 2016 Standard
Status:	Connected

UC & Infrastructure Configuration

Do you have Microsoft Skype for Business?

On the right pane, check that the **Sip Entities XML File** and **Entity Links XML File** are **LOADED**.



Update Avaya System Manager

Session Managers

Name	SIP Address	Management IP	Monitor	
SM1	10.1.10.60		No	Edit
SM2	10.1.10.42		No	Edit

Basic Details

IP Address: * 10.1.10.46

Display Name: SMGR8

System Manager Version: 0

Customer Name: Avaya

Site Name: DevCon Lab

Configuration

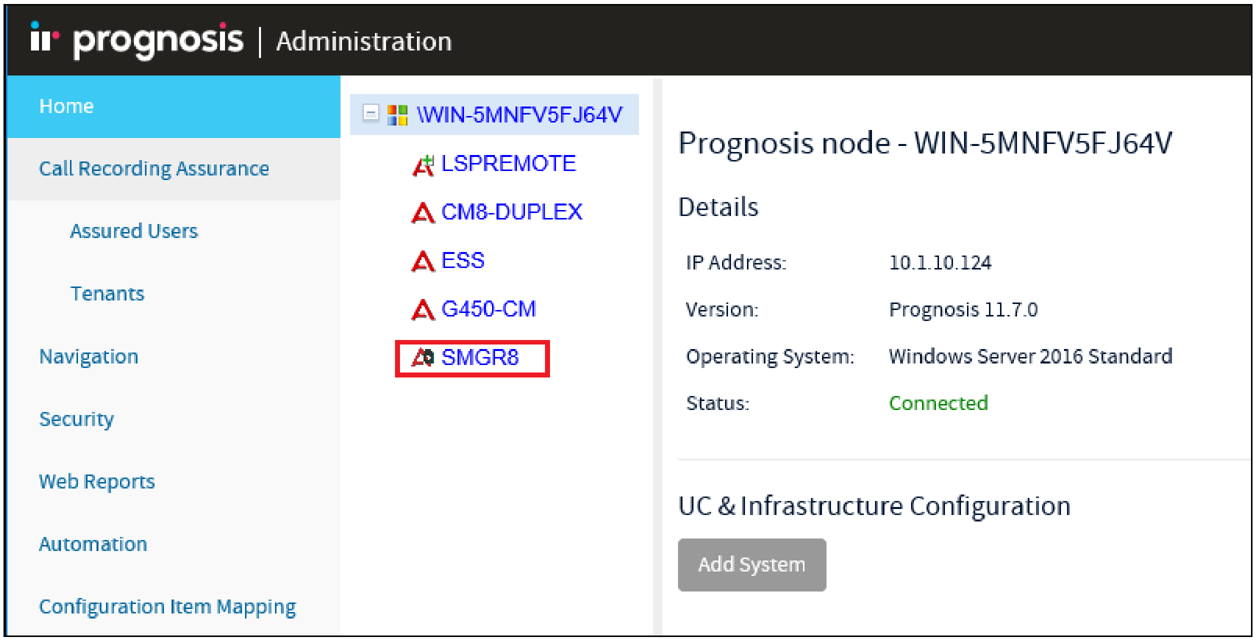
Sip Entities XML File: LOADED

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.

After logging into Prognosis webui as in **Section 6**, expand the server "WIN-5MNFV5FJ64V" in the middle pane and verify that the System Manager **SMGR8** is listed. Then select **View Systems** on the top right icon (not shown).



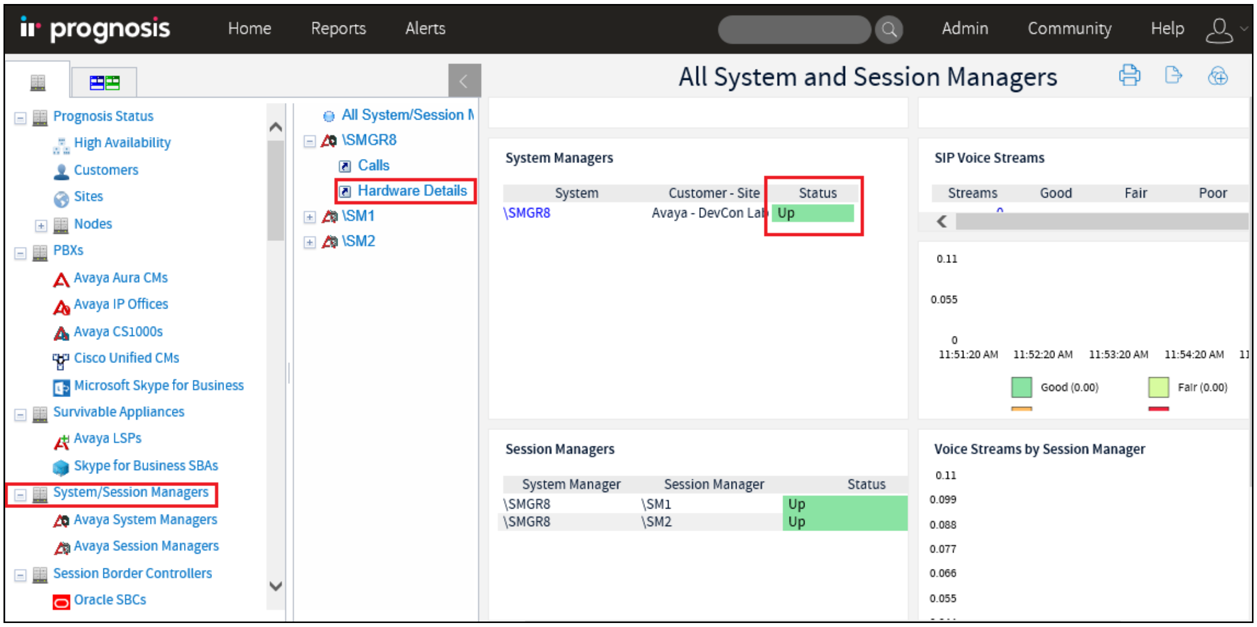
Prognosis node - WIN-5MNFV5FJ64V

Details

IP Address:	10.1.10.124
Version:	Prognosis 11.7.0
Operating System:	Windows Server 2016 Standard
Status:	Connected

UC & Infrastructure Configuration

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



All System and Session Managers

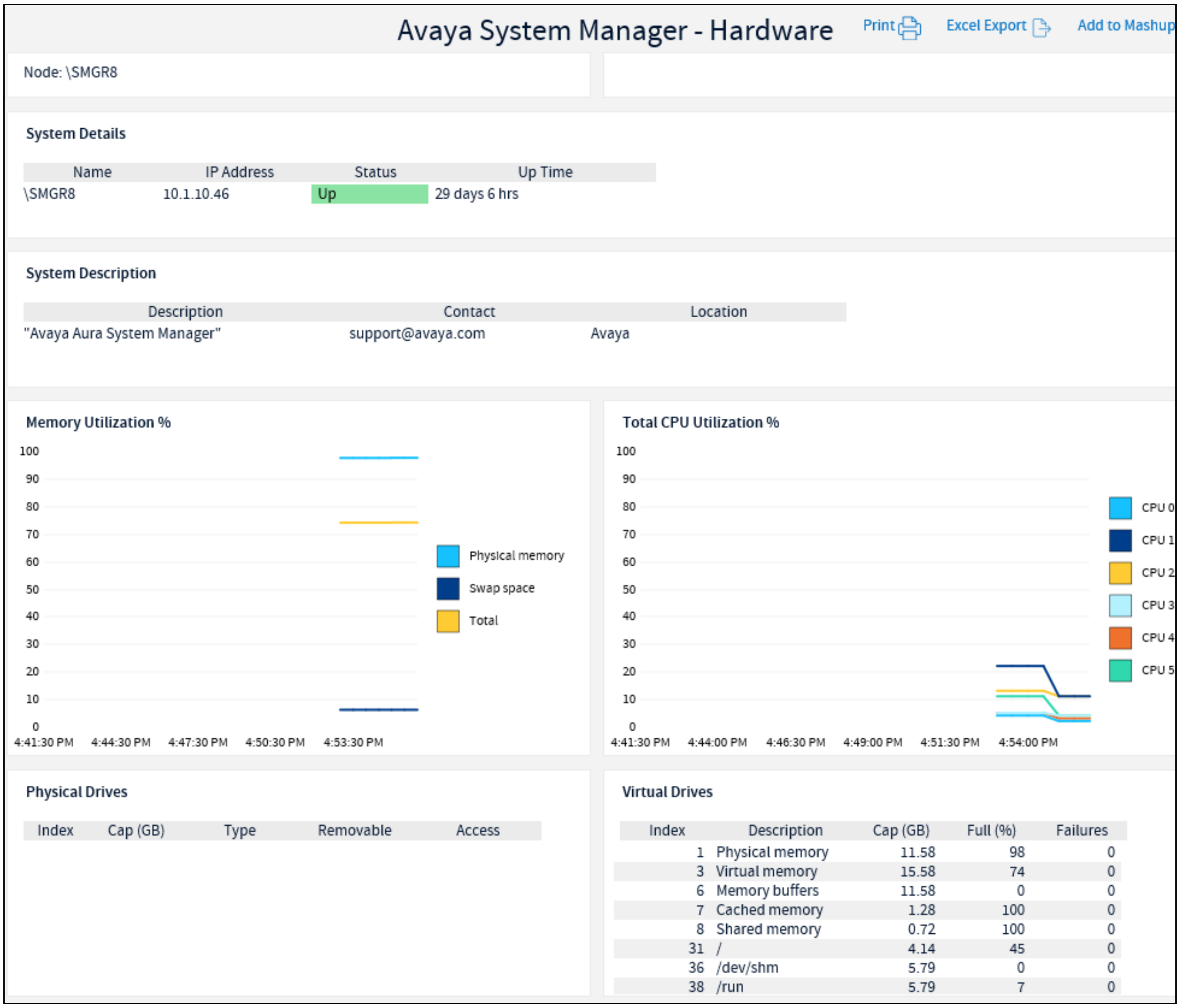
System Managers

System	Customer - Site	Status
\SMGR8	Avaya - DevCon Lab	Up

Session Managers

System Manager	Session Manager	Status
\SMGR8	\SM1	Up
\SMGR8	\SM2	Up

Verify the hardware of System Manager and it has the correct IP Address.



Avaya System Manager - Hardware

Node: \SMGR8

System Details

Name	IP Address	Status	Up Time
\SMGR8	10.1.10.46	Up	29 days 6 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	11.58	98	0
3	Virtual memory	15.58	74	0
6	Memory buffers	11.58	0	0
7	Cached memory	1.28	100	0
8	Shared memory	0.72	100	0
31	/	4.14	45	0
36	/dev/shm	5.79	0	0
38	/run	5.79	7	0

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis R11.7 to interoperate with Avaya Aura® System Manager 8.1. In the configuration described in these Application Notes, Prognosis obtained the configuration and status information through SNMP from System Manager. During compliance testing, all test cases were completed successfully with observations in **Section 2.2**.

9. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 5, Nov 2019.

[2] *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 3, Jul 2019

[3] *Application Notes for Integrated Research's Prognosis for Unified Communications 11.7 with Avaya Aura® Communication Manager R8.1.*

[4] *Application Notes for Integrated Research Prognosis for Unified Communications 11.7 with Avaya Aura® Session Manager R8.1*.

[5] *Avaya Aura® System Manager 7.1 SNMP Whitepaper*, Issue 1.0, Apr 2017.

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.