



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Integrated Research's Collaborate - Prognosis Server 12.1 with Avaya Aura® System Manager R10.1 - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Collaborate - Prognosis Server R12.1 (Prognosis) to interoperate with Avaya Aura® System Manager R10.1.

Prognosis provides real-time monitoring and management solutions for IP telephony networks. Prognosis 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 Collaborate - Prognosis Server R12.1 (herein after referred to as Prognosis) with Avaya Aura® System Manager R10.1.

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 and System Manager were also performed during testing.

## 2.2. Test Results

All test cases passed successfully with the following being observed:

- Communication Manager's 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.

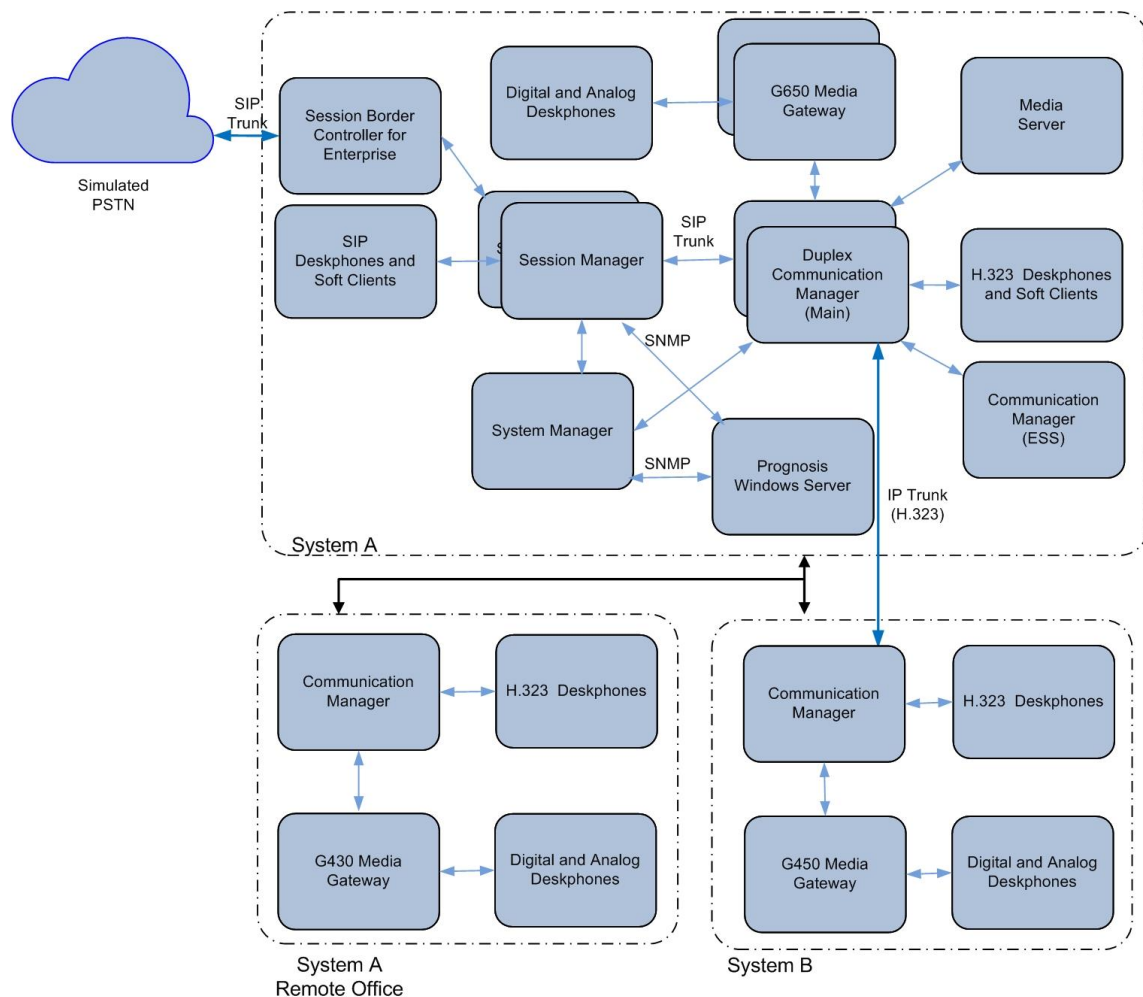
## 2.3. Support

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, Avaya Workplace Client (SIP) and Avaya Agent for Desktop (H.323) 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 2019. 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 (System A)	10.1 (10.1.0.0.0.974.27293)
Avaya Aura® Media Server	8.0.2.218
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 (LSP)	10.1 (10.1.0.0.0.974.27293)
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	42.4.0 HW01 FW008 HW10 FW0104 HW03 FW015 HW11 FW054
Avaya Aura® Communication Manager (System B)	10.1 (10.1.0.0.0.974.27293)
G430 Media Gateway - MM712AP DCP MM - MM716AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	42.4.0 HW04 FW015 HW12 FW104 HW31 FW104 HW05 FW022
Avaya Aura® Communication Manager (ESS)	10.1 (10.1.0.0.0.974.27293)
Avaya Aura® System Manager	10.1 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya Aura® Session Manager	10.1 (10.1.0.0.1010019)
J100 Series IP Telephones - J179 - J129	4.0.11.0 (SIP) 6.8511 (H323)
96x1 Series IP Telephones - 9611G - 9641G	6.8511 (H323)

Equipment/Software	Release/Version
Avaya Workplace Client for Windows	3.26 (SIP)
1600 Series IP Telephones - 1616 - 1603SW	1.312 (H.323)
Digital Telephones - 1400 Series	R48
Avaya Analog Phones	-
Avaya Agent for Desktop	2.0.6.20.3007 (H.323)
Collaborate – Prognosis Server running on Microsoft Windows Server 2019	12.1

**Note:** All Avaya Aura® systems and Prognosis runs on VMware 6.7 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 10.1 supports SNMP v2 for notifications and GET/SET operations will work only for SNMP 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.

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

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

AVAYA  
ura® System Manager 10.1

Users ▾ Elements ▾ **Services** ▾ Widgets ▾ Shortcuts ▾ Search | admin

**Disk Space Utilization**

Category	Free	Normal	Warning	Critical
opt	15	10	0	0
var	10	0	0	0
emldata	15	0	0	0
tmp	10	0	0	0
perfdata	20	0	0	0
swlibrary	45	5	0	0
home	10	0	0	0
pgsql	15	0	0	0

**Alarms**

Severity: ▾

SourceIP	Description
----------	-------------

**Application State**

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

**Services**

- Backup and Restore
- Bulk Import and Export
- Configurations
- Events
- Geographic Redundancy
- Inventory**
- Licenses
- Replication
- Reports
- Scheduler
- Security
- Shutdown
- Solution Deployment Manager

**Inventory**

- Manage Elements
- Create Profiles and Discover SRS/SCS
- Element Type Access
- Subnet Configuration
- Manage Serviceability Agents**
- Synchronization
- Connection Pooling

**Manage Serviceability Agents**

- SNMPv3 User Profiles**
- SNMP Target Profiles
- Notification Filter Profile
- Serviceability Agents

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:

\* Authentication Protocol:

\* Authentication Password:

\* Confirm Authentication Password:

\* Privacy Protocol:

\* Privacy Password:

\* Confirm Privacy Password:

\* Privileges:

\*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.

The screenshot shows the 'Serviceability Agents' page. The 'Agent List' table contains the following data:

Hostname	IP Address	System Name	System OID	Status
<input type="checkbox"/> g450-US	127.0.0.1	g450-US		active
<input type="checkbox"/> Utility-Services	10.1.40.14	Utility-Services		inactive
<input type="checkbox"/> sm1.sglab.com	10.1.10.60	sm1.sglab.com		inactive
<input type="checkbox"/> sm1.sglab.com	10.1.10.59	Session Manager	.1.3.6.1.4.1.6889.1.36	active
<input type="checkbox"/> sm3.sglab.com	10.1.10.47	sm3.sglab.com		active
<input checked="" type="checkbox"/> smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
<input type="checkbox"/> sm2.sglab.com	10.1.10.41	Session Manager	.1.3.6.1.4.1.6889.1.36	active
<input type="checkbox"/> avaya-ce-sm100	10.1.10.19	avaya-ce-sm100		active

Select **SNMPv3 User Profiles** tab. 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.

The screenshot shows the 'Manage Profile' page with the 'SNMPv3 User Profiles' tab selected. The 'Removable Profiles' section contains the following data:

User Name	Authentication Protocol	Privacy Protocol	Privileges
<input type="checkbox"/> avayasmp	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.

```
root >service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor prese>
   Active: active (running) since Tue 2022-06-14 09:54:13 +08; 3 weeks 3 days a>
 Main PID: 1254 (snmpd)
    Tasks: 1 (limit: 75255)
   Memory: 19.5M
    CGroup: /system.slice/snmpd.service
           └─1254 /usr/sbin/snmpd -LS0-63 -f
```

## 5.2. Download SIP Entities and Entity Links XML Files

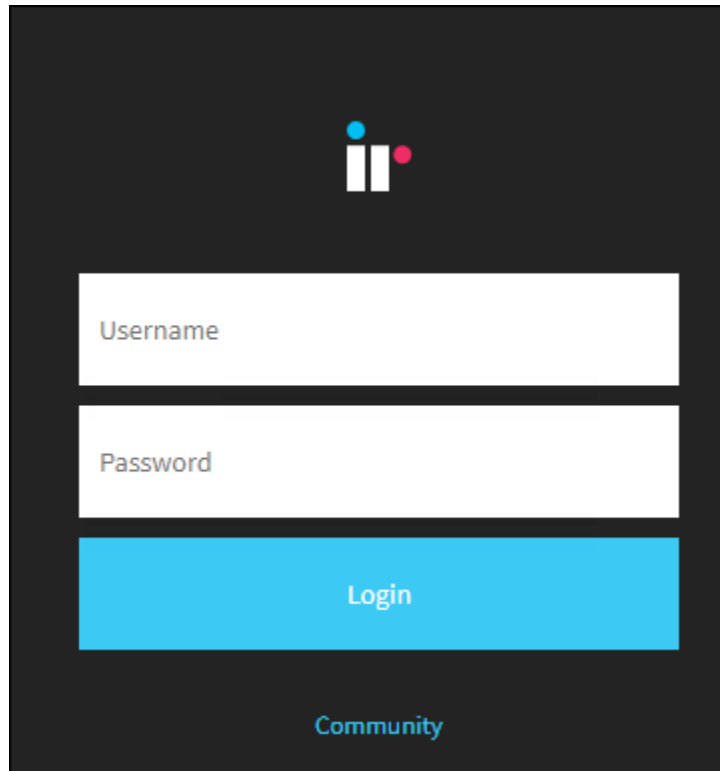
The SIP Entities and Entity Links XML files are required for input into Prognosis for configuration of all the SIP Entities and Entity Links. These files can be downloaded from System Manager.

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” from the zip file downloaded into the PC. Rename the files without the user’s name i.e., “EntityLinks.xml” and “SipEntities.xml”. Upload the renamed files into the Prognosis server in **Section 6**.

## 6. Configure Integrated Research Prognosis

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

Log into the Prognosis Windows 2019 server with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Prognosis Administration**. Log in with the appropriate password.



The screenshot shows a login window with a dark background. At the top center is a logo consisting of three vertical bars of varying heights and colors (blue, white, red). Below the logo are two white input fields: the first is labeled 'Username' and the second is labeled 'Password'. Below these fields is a large blue button labeled 'Login'. At the bottom center of the window is a link labeled 'Community'.

Click **Add System**.

The screenshot shows the Administration console interface. The left sidebar contains navigation links: Home, Call Recording Assurance, Assured Users, Tenants, Navigation, Security, Web Reports, Automation, Configuration Item Mapping, Alert Suppression, and High Availability. The main content area is titled 'Prognosis node - WIN-KKHMESF8NFQ' and includes a 'Details' section with the following information: IP Address: 10.1.10.125, Version: Prognosis 12.1.0, Operating System: Windows Server 2019 Standard, and Status: Connected. Below this is the 'UC & Infrastructure Configuration' section, where the 'Add System' button is highlighted with a red box. Other buttons in this section include 'Manage Prognosis Regions'. At the bottom, there is a 'Databases' section with a list of databases and their status: AV-CDRs, AV-Contact Center Elite, AV-MedPro DSP Utilization, AV-Network Hops Historical, and AV-Reporting, each with a 'Stop' button.

Scroll down to **System/Session Managers**. Select **Avaya System/Session Manager** from the drop-down menu. Click **Add** to add a new System Manager.

The screenshot shows a dropdown menu titled 'System/Session Managers'. The selected item is 'Avaya System/Session Manager'. To the right of the dropdown is a blue 'Add' button, which is highlighted with a red box.

In this test configuration, the following entries are added for System Manager with display name of **SMGR10** and IP address as **10.1.10.46**.

The following settings were configured during the compliance test.

**Basic Details:**

- **Display Name: SMGR10**
- **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: \* SMGR10

IP Address: \* 10.1.10.46

Customer Name: Avaya

Site Name: DevCon Lab

**Configuration**

Sip Entities XML File:  SipEntities.xml

Entity Links XML File:  EntityLinks.xml

**System Manager Administrator Web Interface Credentials**

Username: admin

Password: ●●●●●●●●

**SNMP Connection Details**

Use SNMP Version 2c

Use SNMP Version 3

User Name: \* avayasnmp

Authentication Protocol: MD5

Authentication Password: \* ●●●●●●●●

Encryption Method: AES

Encryption Password: \* ●●●●●●●●

**Databases and Thresholds**

Start standard databases and thresholds

Return to the home screen; check that **SMGR10** is created under the Windows server name.

Click on the **SMGR10** highlighted below.

WIN-KKHMESF8NFQ

Prognosis node - WIN-KKHMESF8NFQ

Details

IP Address: 10.1.10.125

Version: Prognosis 12.1.0

Operating System: Windows Server 2019 Standard

Status: Connected

UC & Infrastructure Configuration

Add System

Do you have Microsoft Skype for Business? [Why do I need this?](#)

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

Basic Details

IP Address: \* 10.1.10.46

Display Name: SMGR10

System Manager Version: 0

Customer Name: Avaya

Site Name: DevCon Lab

Configuration

Sip Entities XML File: **LOADED** » Choose File No file chosen

Entity Links XML File: **LOADED** » Choose File No file chosen

System Manager Administrator Web Interface Credentials

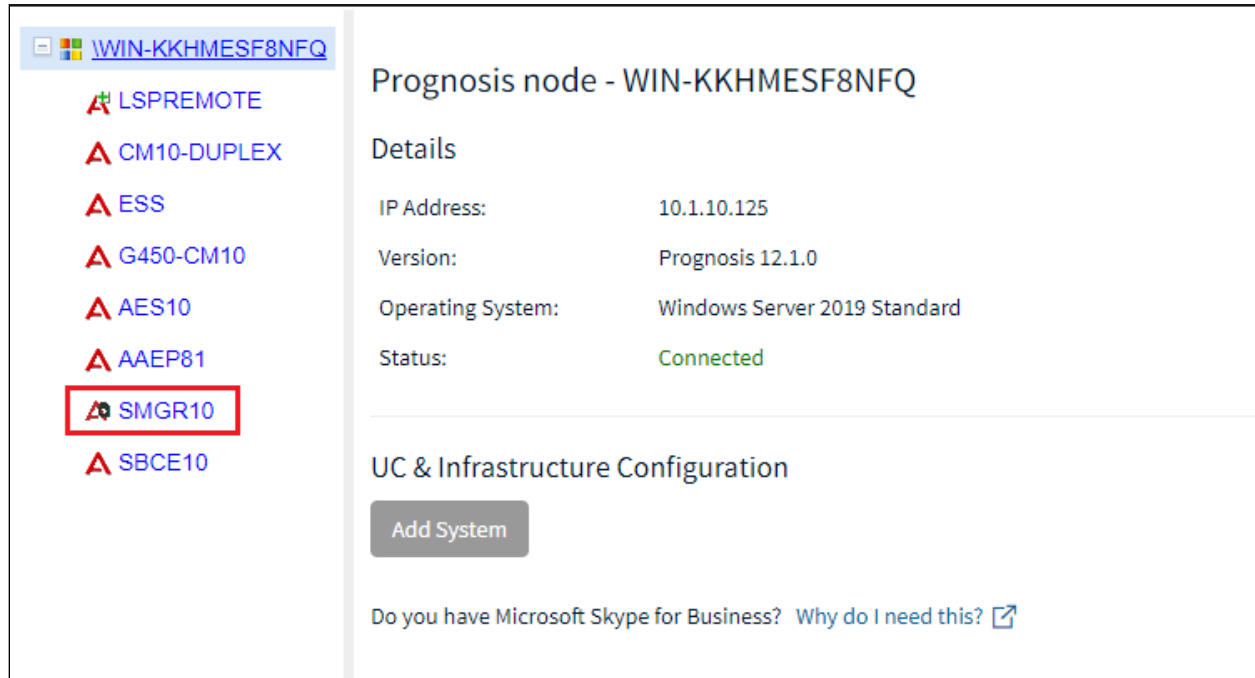
Username: admin

Password: \*\*\*\*\*

## 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-KKHMESF8NFQ” in the middle pane and verify that the System Manager **SMGR10** is listed. Then select **View Systems** on the top right (not shown) of the home screen.



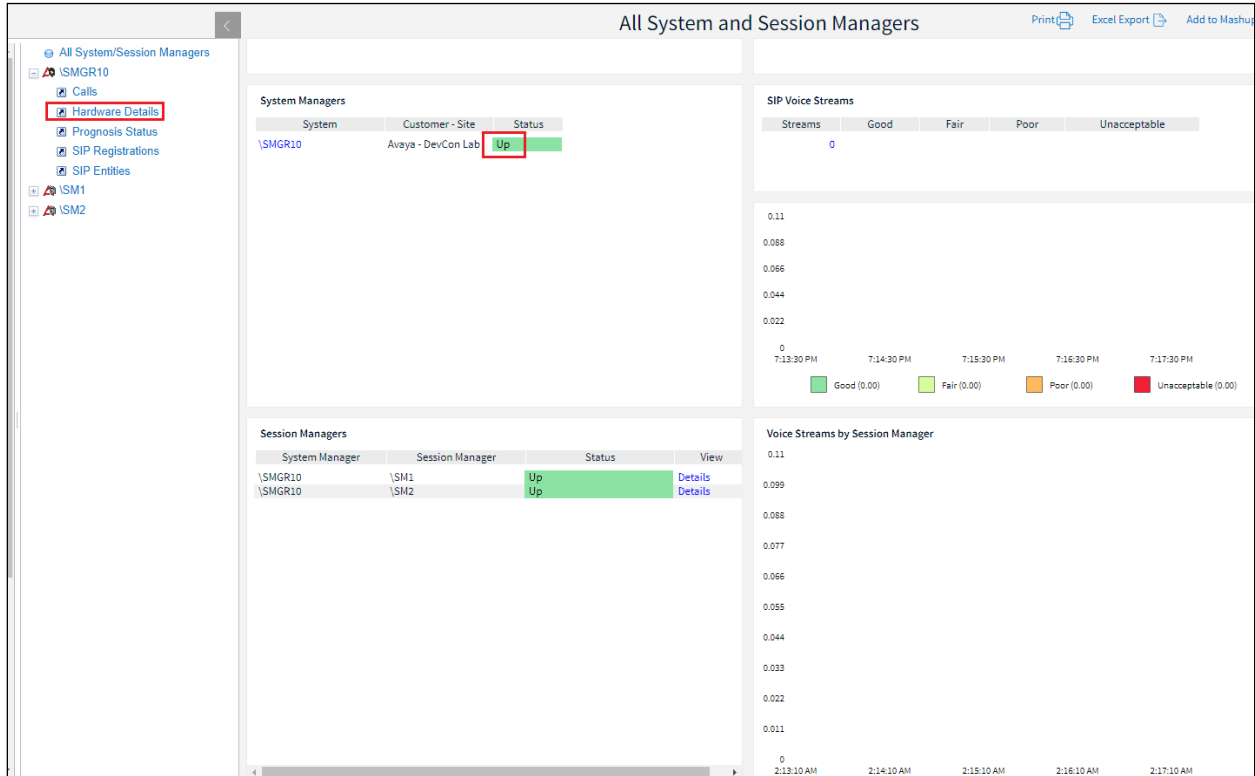
The screenshot displays the Prognosis web interface. On the left, a sidebar lists several systems under the node 'WIN-KKHMESF8NFQ'. The system 'SMGR10' is highlighted with a red box. On the right, the 'Details' section for the selected node shows the following information:

Prognosis node - WIN-KKHMESF8NFQ	
Details	
IP Address:	10.1.10.125
Version:	Prognosis 12.1.0
Operating System:	Windows Server 2019 Standard
Status:	Connected

Below the details, there is a section for 'UC & Infrastructure Configuration' with an 'Add System' button and a link: 'Do you have Microsoft Skype for Business? [Why do I need this?](#)'



Select **System/Session Managers** on the left pane. Check that the System Manager created earlier i.e., **SMGR10** is shown. Verify the System Manager **Status** is **Up**. Expand **SMGR10** by clicking the + symbol and select **Hardware Details**.



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

Avaya System Manager - Hardware

Node: \SMGR10

System Details

Name	IP Address	Status	Up Time
\SMGR10	10.1.10.46	Up	15 days 1 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
1	11.52	Physical memory		
3	15.52	Virtual memory		
6	11.52	Memory buffers		
7	2.55	Cached memory		
8	0.55	Shared memory		
11	2.08	Available memory		
35	5.76	/dev/shm		
37	5.76	/run		
38	5.76	/sys/fs/cgroup		

Virtual Drives

Index	Description	Cap (GB)	Full (%)	Failures
1	Physical memory	11.52	97	0
3	Virtual memory	15.52	73	0
6	Memory buffers	11.52	0	0
7	Cached memory	2.55	100	0
8	Shared memory	0.55	100	0
11	Available memory	2.08	0	0
35	/dev/shm	5.76	0	0
37	/run	5.76	6	0
38	/sys/fs/cgroup	5.76	0	0

Verify other available data like **SIP Entities** (shown below) or **SIP Registrations**.

Avaya System Manager - SIP Entities

Node: \SMGR10

Number of Session Managers	Number of PBXs	Number of Gateways	Total number of SIP Entities
2	2	0	11

SIP Entities

Entity Name	IP Address / FQDN
AAEP-MPP-8.1	10.1.10.84
Avaya-CE	10.1.10.20
CM10-Duplex	10.1.10.230
IPSE Expansion	10.1.10.110
IPSE Primary	10.1.10.121
IX_Msg	10.1.10.62
SBCE	10.1.10.65
g450-CM	10.1.60.18
presence	10.1.10.20
sm1	10.1.10.60
sm2	10.1.10.42

Entity Links

Link Name	Protocol	SIP Entity 1	Port 1	SIP Entity 2	Port 2	Server Status
SM1 to IPSE Exp	UDP	sm1	5060	IPSE Expansion	5060	normal
SM1 to IPSE Primary	UDP	sm1	5060	IPSE Primary	5060	normal
SM1 to SM2	TLS	sm1	5061	sm2	5061	normal
SM1_To_Presence	TLS	sm1	5062	presence	5061	normal
SM1_to_Breeze	TLS	sm1	5061	Avaya-CE	5061	normal
sm1-to-cm-duplex	TLS	sm1	5061	CM10-Duplex	5061	normal
sm1_SBCE_5061_TLS_IPv4	TLS	sm1	5061	SBCE	5061	normal
sm1_To_IXMsg	TCP	sm1	5060	IX_Msg	5060	normal
sm1_to_AAEP-MPP8	TCP	sm1	5060	AAEP-MPP-8.1	5060	normal
sm2 to AAEP-MPP8	TCP	sm2	5060	AAEP-MPP-8.1	5060	normal
sm2-to-cm-duplex	TLS	sm2	5061	CM10-Duplex	5061	normal
sm2-to-site6	TLS	sm2	5061	g450-CM	5061	normal

## 8. Conclusion

These Application Notes describe the procedures for configuring Integrated Research's Collaborate - Prognosis Server R12.1 to interoperate with Avaya Aura® System Manager 10.1. 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 10.1, Issue 1, Dec 2021.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1, Issue 3, Feb 2022.
- [3] *Application Notes for Integrated Research's Collaborate - Prognosis Server R12.1 with Avaya Aura® Communication Manager R10.1*.
- [4] *Application Notes for Integrated Research Collaborate - Prognosis Server R12.1 with Avaya Aura® Session Manager R10.1*.
- [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.

---

**©2022 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).