Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research’s Collaborate - Prognosis Server 12.1 with Avaya Aura® Experience Portal R8.1.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Collaborate - Prognosis Server R12.1 to interoperate with Avaya Aura® Experience Portal R8.1.1.

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. Prognosis monitors directly to Experience Portal using SNMP connection.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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® Experience Portal (AAEP) R8.1.1. Experience Portal comprises Experience Portal Manager (EPM) and Media Processing Platform (MPP) servers.

Prognosis is a multi-vendor software product designed to provide a comprehensive monitoring and management platform for Unified Communications (UC) environments. It does this by collecting data, filtering as required and then presenting in a 'user-friendly' format, all in real time.

In the testing, Prognosis uses the following methods to collect and monitor an Experience Portal system.

- Web Services (SOAP) to be setup on Experience Portal to collect a range of call data.
- Data from the SNMP MIB: AV-VOICE-PORTAL-MIB.
- SNMP Trap.

2. General Test Approach and Test Results

The general test approach was to verify Prognosis using Web Services (SOAP) and Simple Network Management Protocol (SNMP) connection to monitor and display call information from Experience Portal.

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

The feature test of the interoperability compliance testing was to verify Prognosis using Web Services and SNMP to display real-time information and to monitor status of operation on Experience Portal. There are 4 kinds of information on Experience Portal that Prognosis obtains and display on the web user interface.

- Application: display all applications and its related information such as DNIS, application name etc.
- Call Load: display call statistic information such as Unused SIP Sessions, Unused H323 Sessions, MPP Today, SIP Requests Processed, H323 Requests Processed, MPP Active Calls, CCXML Event Sent, CCXML Requests Processed, and VXML Requests Processed.
- MPP (Media Processing Platform): display MPP server statistic.
- Traps: display all SNMP traps sent from Experience Portal system.

2.2. Test Results

All test cases were passed and met the requirements as shown in **Section 2.1** with following observation:

- No Auxiliary EPM server was created for this test and so cannot be viewed.

2.3. Support

For technical support on Integrated Research 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 the Prognosis application with Avaya Aura® Experience Portal. The configuration consists of a duplex Avaya Aura® Communication Manager with an Avaya G430 Media Gateway and Avaya Aura® Media Server, providing virtual H.323 endpoints to Experience Portal. Avaya Aura® Session Manager was configured via Avaya Aura® System Manager to provide SIP trunk to Experience Portal. SIP and H.323 endpoints were used to place/receive call to/from Experience Portal. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution.

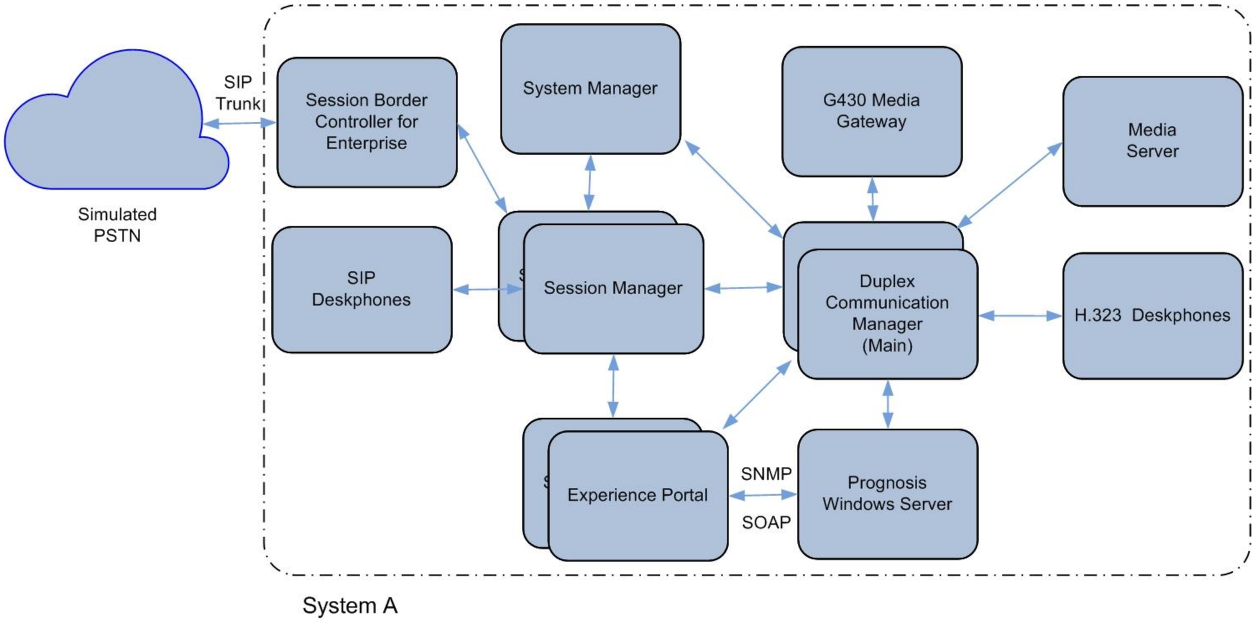


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

The following equipment and software were used for the compliance test provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1 (10.1.0.0.0.974.27293)
Avaya Aura® Media Server	10.1.0.77
Avaya G430 Media Gateway - MGP	42.4.0
Avaya Aura® Enablement Services	10.1 (10.1.0.0.2.11-0)
Avaya Aura® Experience Portal – EPM/MPP	8.1.1.0.0251
Avaya G450 Media Gateway - MGP	42.4.0
Avaya Aura® System Manager	10.1 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Collaborate – Prognosis Server running on Windows Server 2019	12.1

Note: All Avaya Aura® systems and Prognosis runs on VMware 6.7 virtual platform.

5. Configure Avaya Aura® Communication Manager

The configuration of Communication Manager for Experience Portal is assumed to be in place and will not be discussed in this document. For more information of how to configure Communication Manager and Experience Portal, please refer to **Section 11**.

6. Configure Avaya Aura® Session Manager

The configuration of Session Manager for Experience Portal is assumed to be in place and will not be discussed in this document. For more information of how to configure Session Manager and Experience Portal, please refer to **Section 11**.

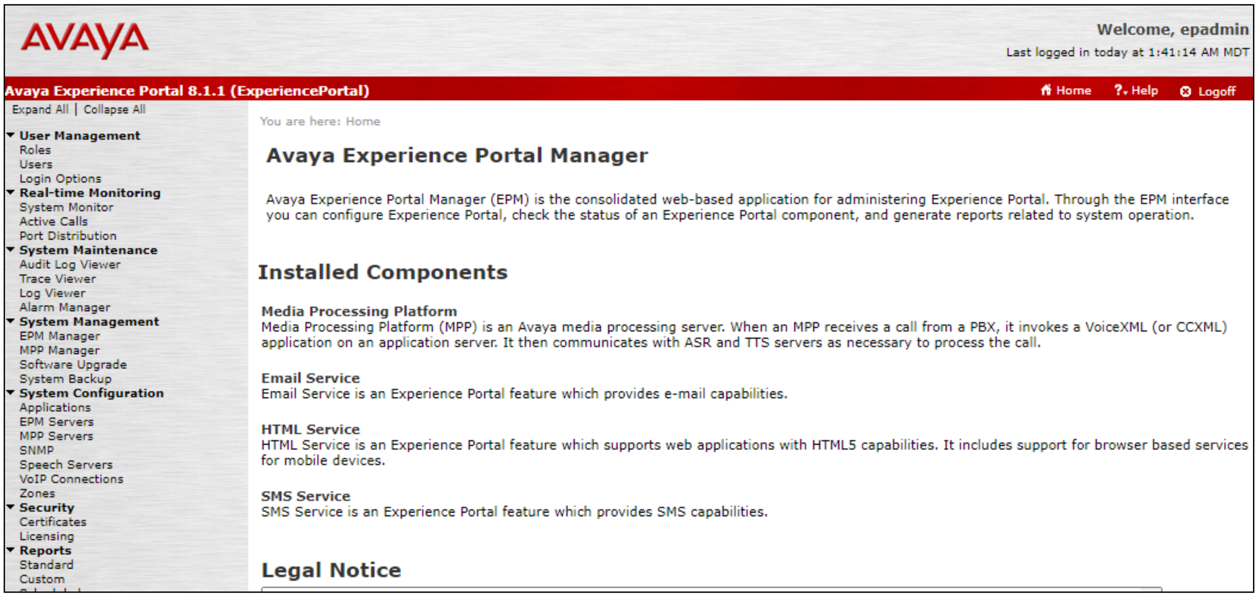
7. Configure Avaya Aura® Experience Portal

The initial administration of Experience Portal and the configuration of the H.323 VoIP connection to Communication Manager and the SIP VoIP connection to Session Manager are assumed to be in place and will not be covered here. This section only covers the configuration of Experience Portal that is required for the purpose of administering Prognosis. The following steps will be covered:

- Configure SNMP connection
- Configure outcall authentication for web services
- Configure applications

Experience Portal is configured via the Experience Portal Management (EPM) web interface. To access the web interface, enter https://<ip-addr>/ as the URL in an internet browser, where <ip-addr> is the IP address of the EPM. Log in using the appropriate credentials. The screen shown below is displayed.

Note: All the screens in this section are shown after the Experience Portal had been configured. Save the screen parameters after configuring Experience Portal.



Avaya Experience Portal Manager

Avaya Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

Installed Components

Media Processing Platform
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

Email Service
Email Service is an Experience Portal feature which provides e-mail capabilities.

HTML Service
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes support for browser based services for mobile devices.

SMS Service
SMS Service is an Experience Portal feature which provides SMS capabilities.

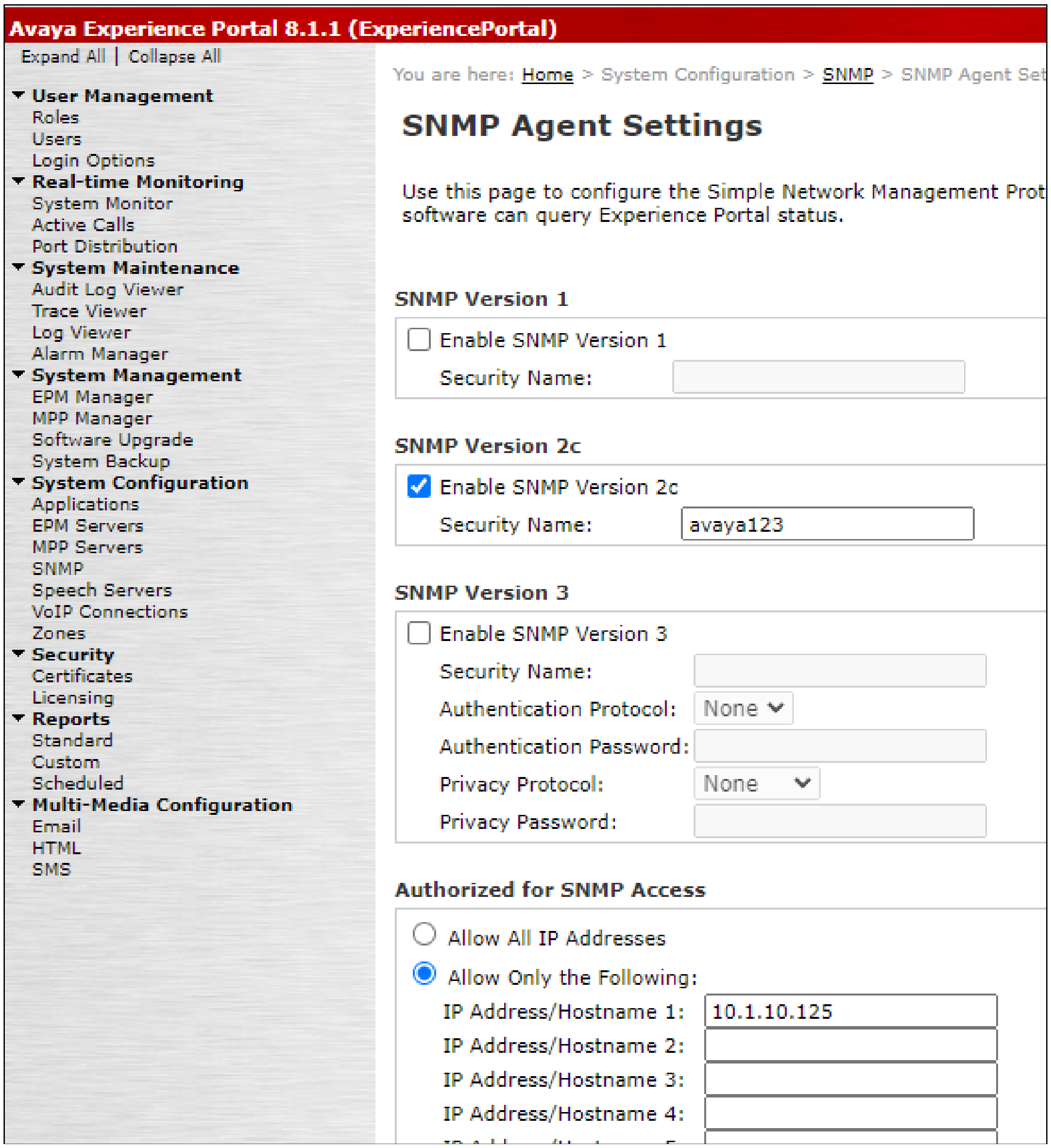
Legal Notice

7.1. Configure SNMP Connection

To configure SNMP connection, navigate to **System Configuration → SNMP** on the left pane. The SNMP page is displayed in the right (not shown) and click on **SNMP Agent Settings**.

Configure the following parameters as shown below.

- Check on the **Enable SNMP Version 2c** and enter the **Security Name** as **avaya123**, this security name can be any name and it will be used in Prognosis configuration.
- **Authorized for SNMP Access** – select **Allow Only the Following** and enter the Prognosis server IP Address.



SNMP Agent Settings

Use this page to configure the Simple Network Management Prot
software can query Experience Portal status.

SNMP Version 1

☐ Enable SNMP Version 1

Security Name:

SNMP Version 2c

☑ Enable SNMP Version 2c

Security Name: avaya123

SNMP Version 3

☐ Enable SNMP Version 3

Security Name:

Authentication Protocol: None

Authentication Password:

Privacy Protocol: None

Privacy Password:

Authorized for SNMP Access

○ Allow All IP Addresses

● Allow Only the Following:

IP Address/Hostname 1: 10.1.10.125

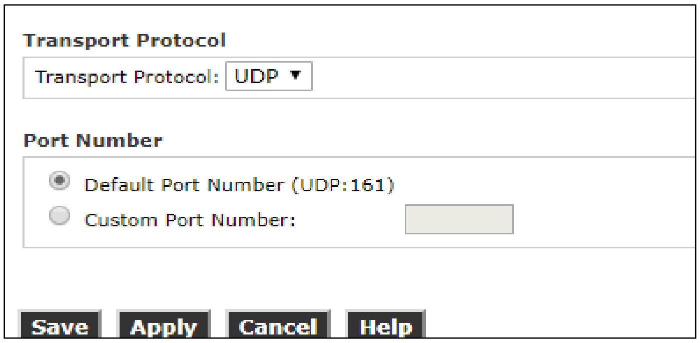
IP Address/Hostname 2:

IP Address/Hostname 3:

IP Address/Hostname 4:

- **Transport Protocol** – Select **UDP**.
- **Port Number** – Select Default Port Number (**UDP: 161**).

Click **Apply** and **Save** to save configuration.



Transport Protocol

Transport Protocol: UDP

Port Number

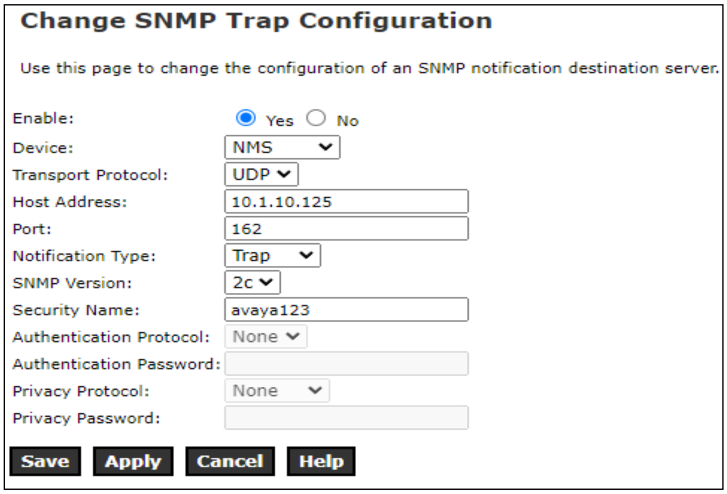
● Default Port Number (UDP:161)

○ Custom Port Number:

Navigate to **System Configuration → SNMP** page, click on **Add** button (not shown) to configure Prognosis server as destination server which Experience Portal sends SNMP notifications to. The screen below shows the parameters after completing the **Add SNMP Trap Configuration**.

- **Enable** – Select **Yes**.
- **Device** – Select **NMS**.
- **Transport Protocol** – Select **UDP**.
- **Host Address** – Enter the IP address of Prognosis server.
- **Port** – Use the port **162**.
- **Notification Type** – Select **Trap**.
- **SNMP Version** – Select version **2c**.
- **Security Name** – In this case for SNMP 2c, it is the community name i.e., **"avaya123"**.

Click the **Save** button to complete the creation and save the configuration.



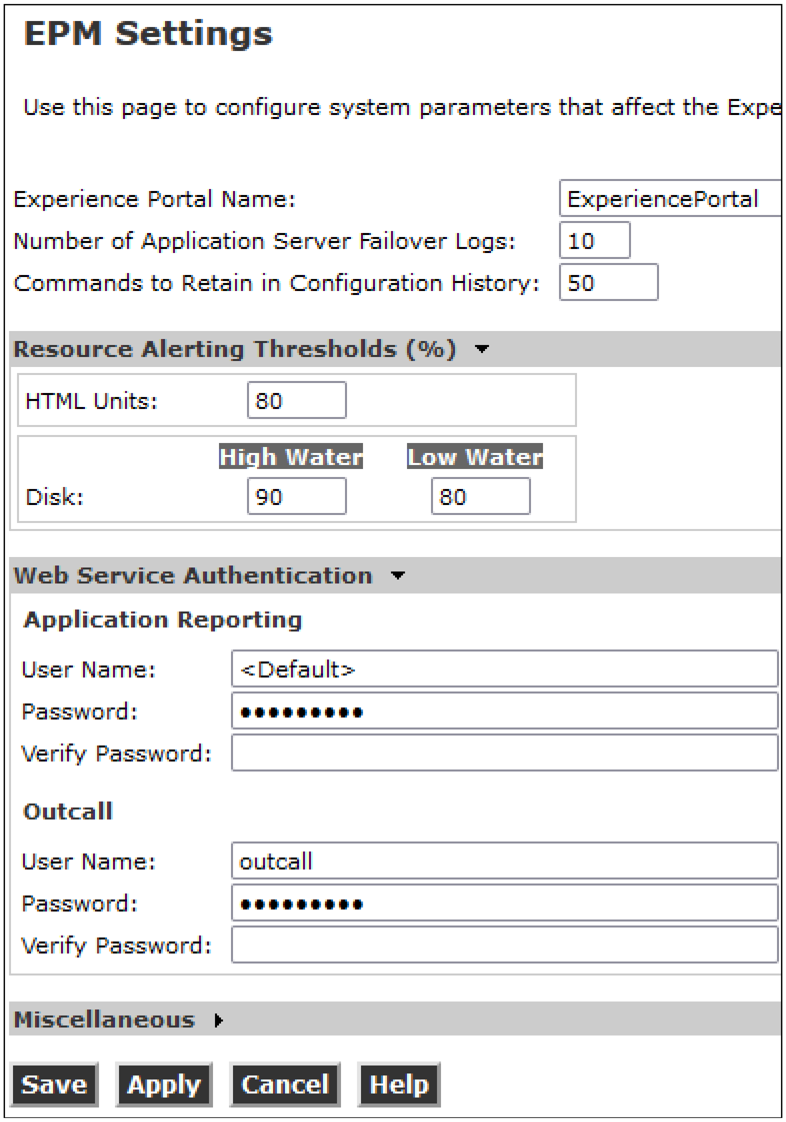
Change SNMP Trap Configuration

Use this page to change the configuration of an SNMP notification destination server.

Enable:	● Yes ○ No
Device:	NMS
Transport Protocol:	UDP
Host Address:	10.1.10.125
Port:	162
Notification Type:	Trap
SNMP Version:	2c
Security Name:	avaya123
Authentication Protocol:	None
Authentication Password:	
Privacy Protocol:	None
Privacy Password:	

7.2. Configure Outcall Authentication for Web Services

To configure the outcall authentication, navigate to **System Configuration →EPM Servers**. The EPM Servers page is displayed in the right (not shown), click on **EPM** button and the **EPM Settings** below. The **EPM Settings** page is displayed. In the **Outcall** sub-section of the **Web Service Authentication** section, enter username **outcall** in the **User Name** field and its password e.g., **avaya123** in the **Password** field, keep other fields at default values. Note that the outcall authentication username can be any desired value, but the password must not have username as part of the password string. Click **Apply** and **Save** button to save the configuration.



EPM Settings

Use this page to configure system parameters that affect the Expe

Experience Portal Name:	ExperiencePortal
Number of Application Server Failover Logs:	10
Commands to Retain in Configuration History:	50

Resource Alerting Thresholds (%) ▾

	High Water	Low Water
HTML Units:	80	
Disk:	90	80

Web Service Authentication ▾

Application Reporting

User Name:	<Default>
Password:	●●●●●●●●●
Verify Password:	

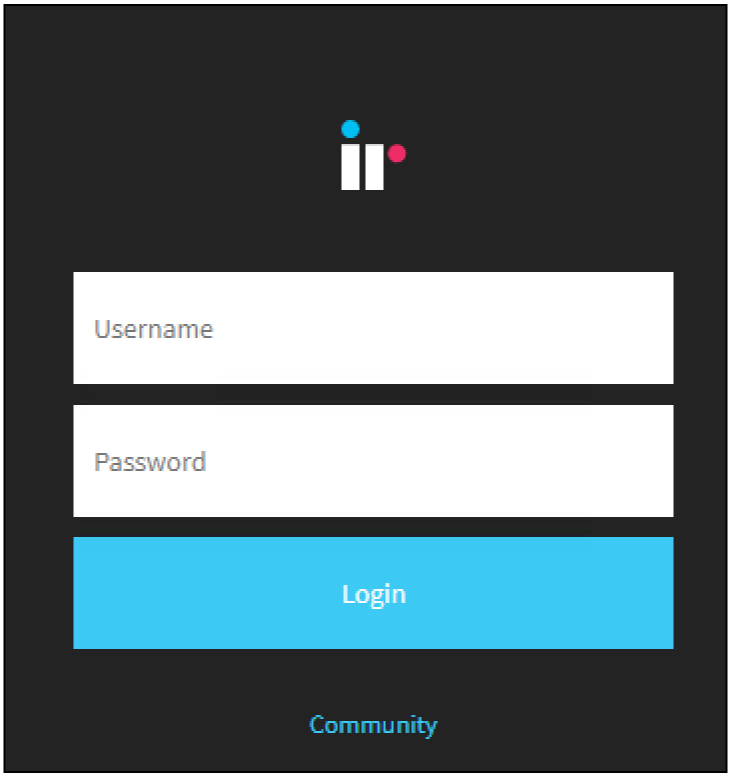
Outcall

User Name:	outcall
Password:	●●●●●●●●●
Verify Password:	

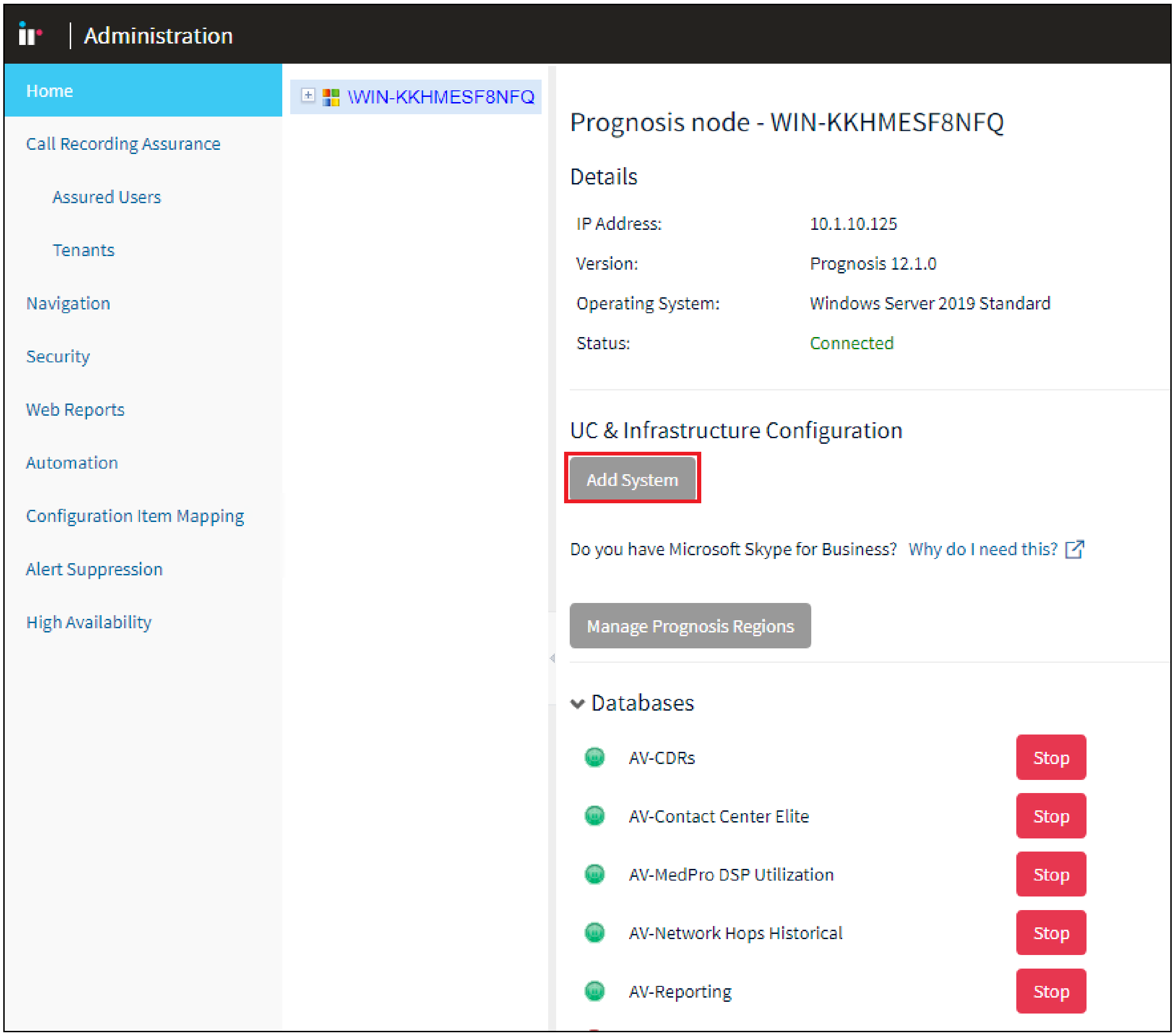
8. Configure Prognosis

This section describes the configuration of Prognosis required to interoperate with Experience Portal.

Log in to the Prognosis Windows Server 2019 with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Administration** and log in with the appropriate password.



The **Prognosis Administration** homepage is displayed as shown below.



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

Do you have Microsoft Skype for Business? Why do I need this?

Databases

AV-CDRs

AV-Contact Center Elite

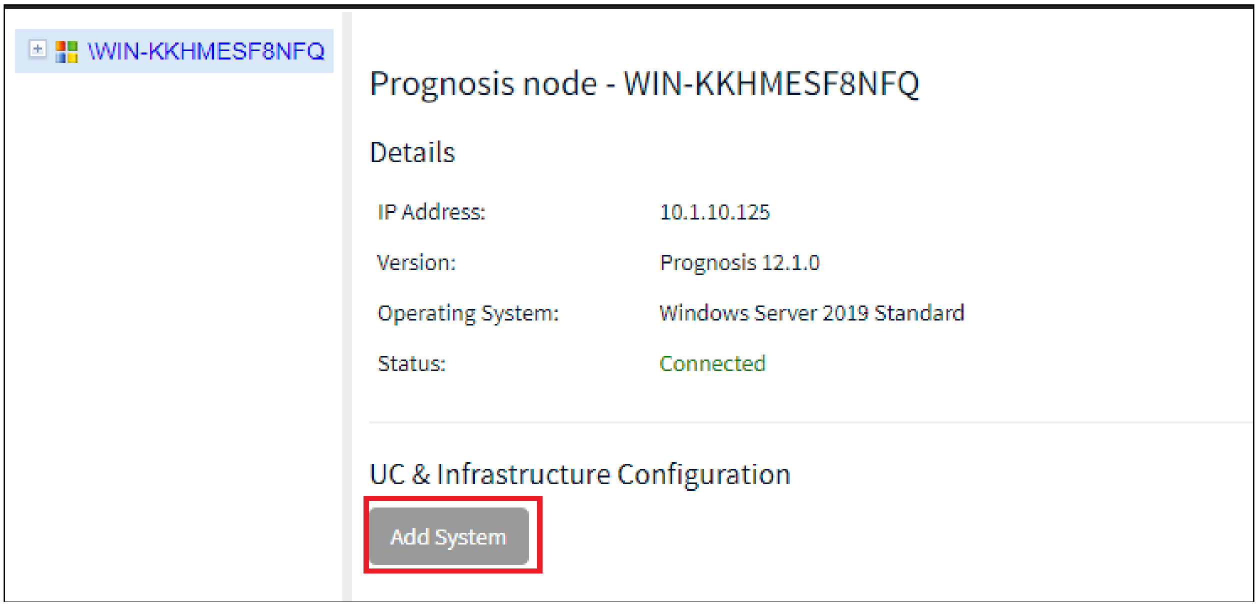
AV-MedPro DSP Utilization

AV-Network Hops Historical

AV-Reporting

8.1. Administer Avaya Aura® Experience Portal Service Configuration

Click **Add System**.



WIN-KKHMESF8NFQ

Prognosis node - WIN-KKHMESF8NFQ

Details

IP Address: 10.1.10.125

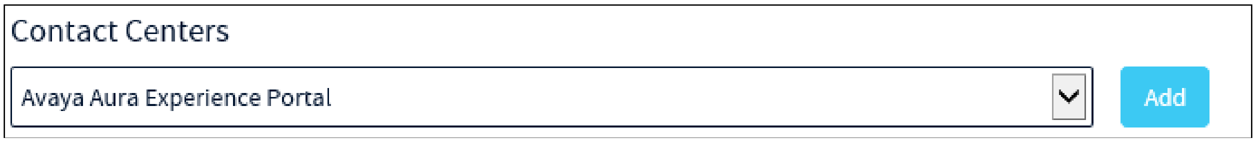
Version: Prognosis 12.1.0

Operating System: Windows Server 2019 Standard

Status: Connected

UC & Infrastructure Configuration

Scroll below to **Contact Centers**. Select **Avaya Aura Experience Portal** from drop-down menu. Click **Add** to add a new Experience Portal.



Contact Centers

Avaya Aura Experience Portal

In this test configuration, the following entries are added for Experience Portal with display name of **AAEP81** and with IP addresses of **10.1.10.81**.

The following settings were used during the compliance test.

Basic Details:

- **Display Name: AAEP81**
- **IP address: 10.1.10.82** [EPM IP Address]
- **Customer Name: Avaya**
- **Site Name: DevCon Lab**

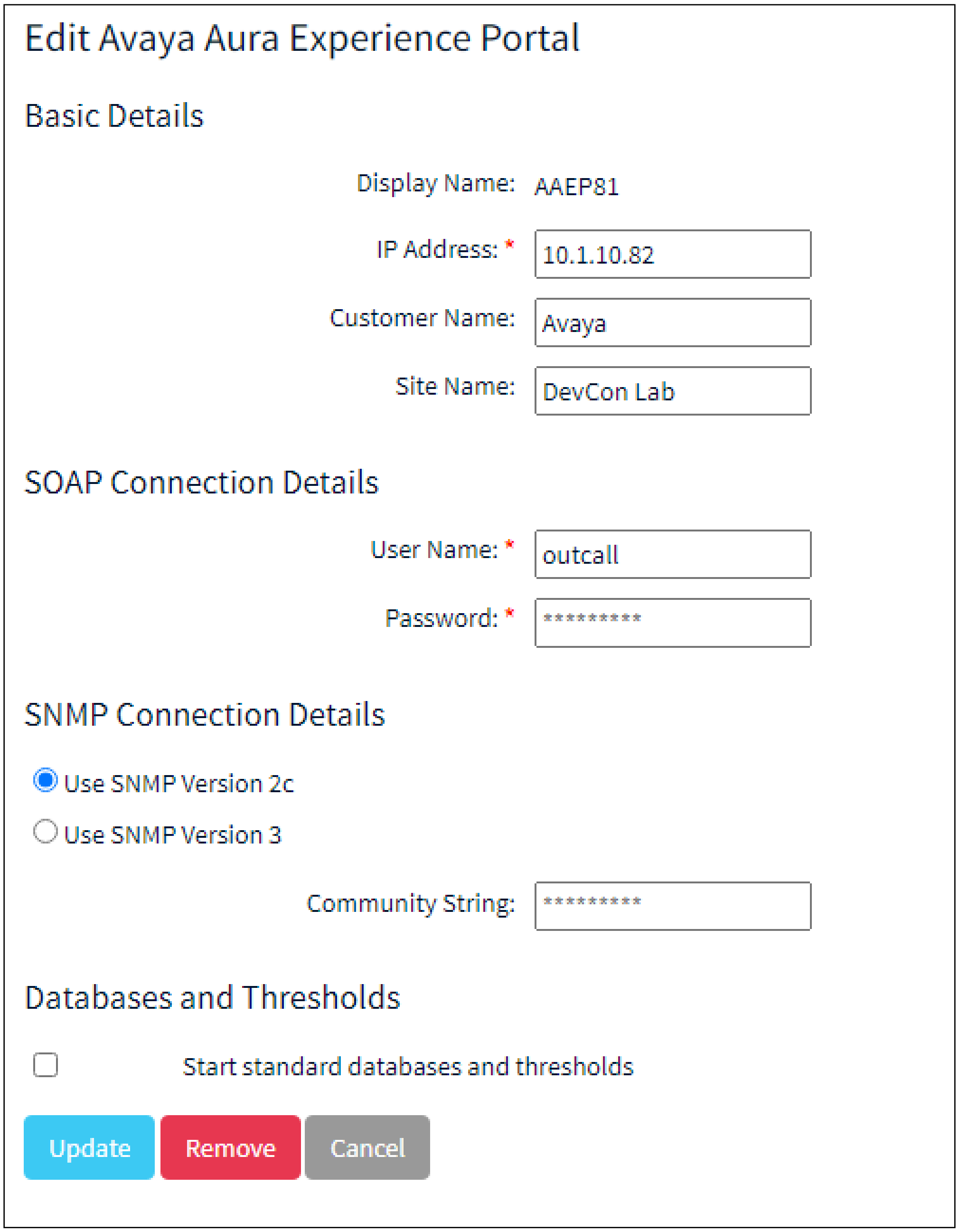
SOAP Connection Details:

- **User Name: outcall**
- **Password:** As configured in **Section 7.2**.

SNMP Connection Details:

- Select **Use SNMP Version 2c**
- **Community String:** As configured in **Section 7.1**.

Leave the **Databases and Thresholds** as checked and click **Add** to affect the addition. Below shows the updated screenshot.



Edit Avaya Aura Experience Portal

Basic Details

Display Name: AAEP81

IP Address: * 10.1.10.82

Customer Name: Avaya

Site Name: DevCon Lab

SOAP Connection Details

User Name: * outcall

Password: * *********

SNMP Connection Details

● Use SNMP Version 2c

○ Use SNMP Version 3

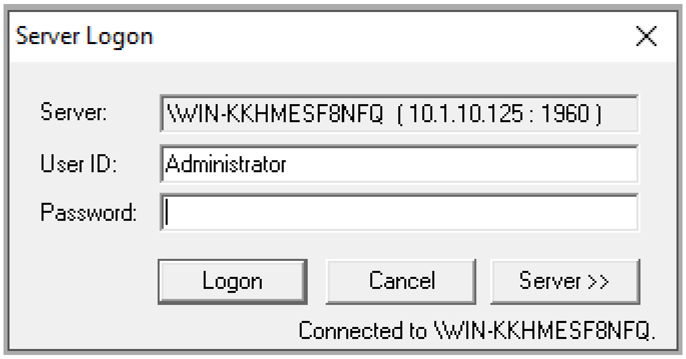
Community String: *********

Databases and Thresholds

□ Start standard databases and thresholds

8.2. Verifying Configurations with Prognosis Client

On Prognosis server, click **Start → All Programs → Prognosis → Prognosis Client** to start the Windows Client application (not shown). Log in with the appropriate credentials.



Server Logon

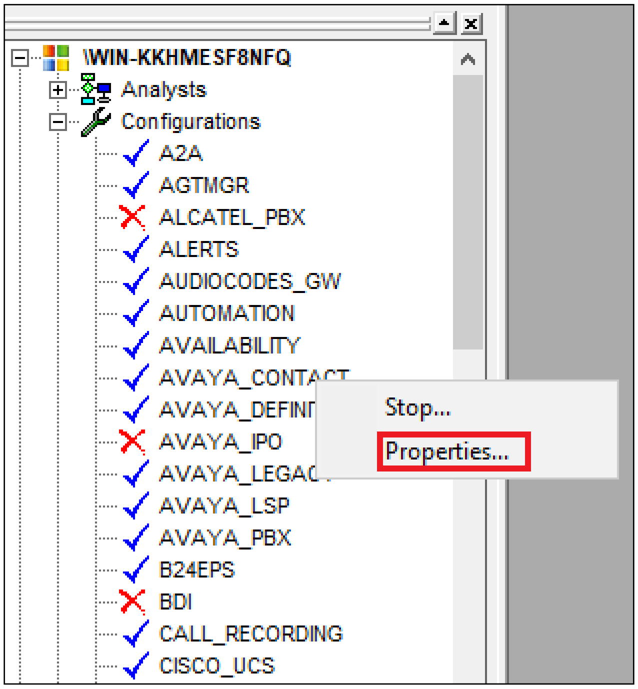
Server: \\WIN-KKHMESF8NFQ (10.1.10.125 : 1960)

User ID: Administrator

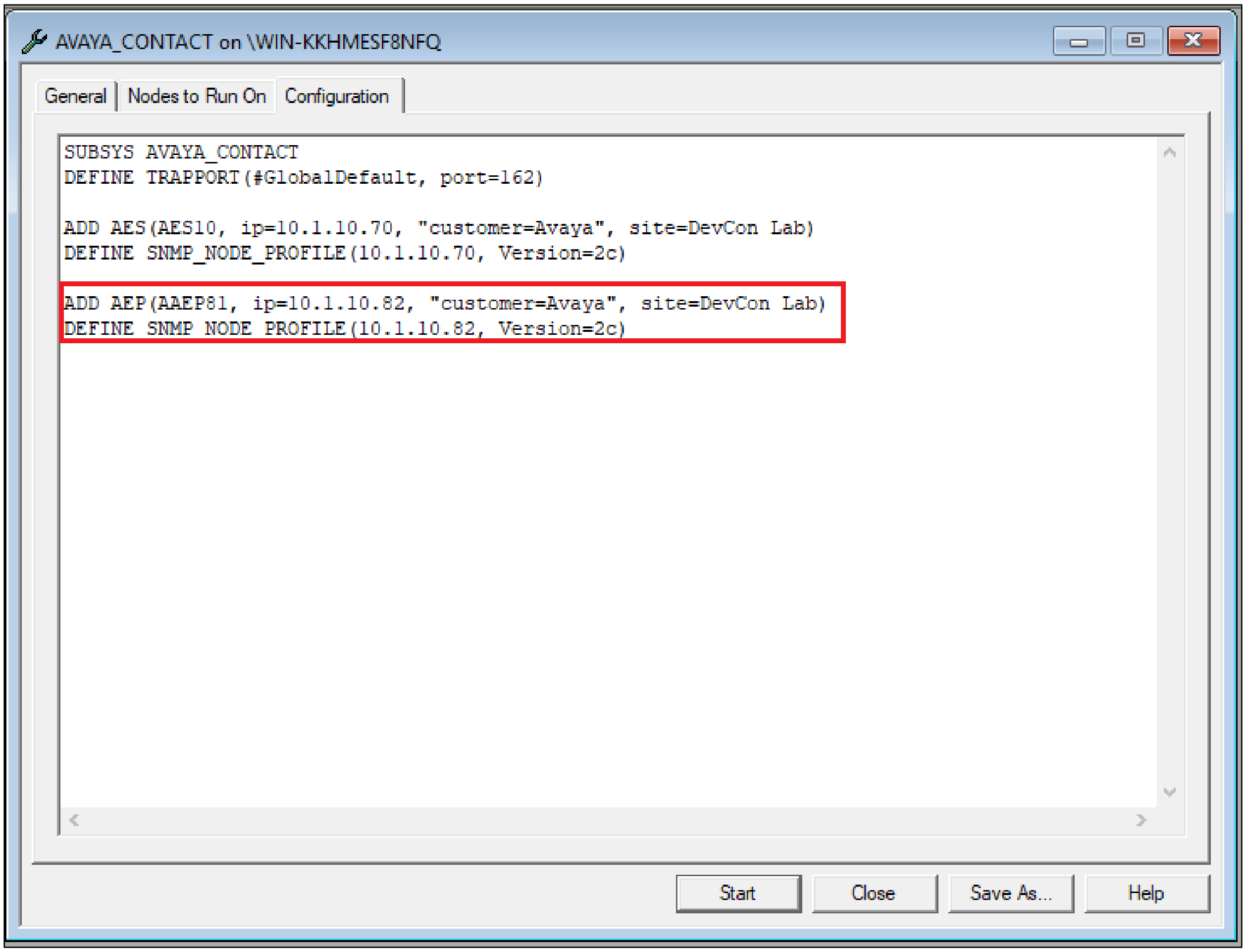
Password:

Connected to \\WIN-KKHMESF8NFQ.

To check the configurations of the Experience Portal to be monitored, expand **Configurations** of the Monitoring Node on the left pane, right-click on **AVAYA_CONTACT** and select **Properties**.

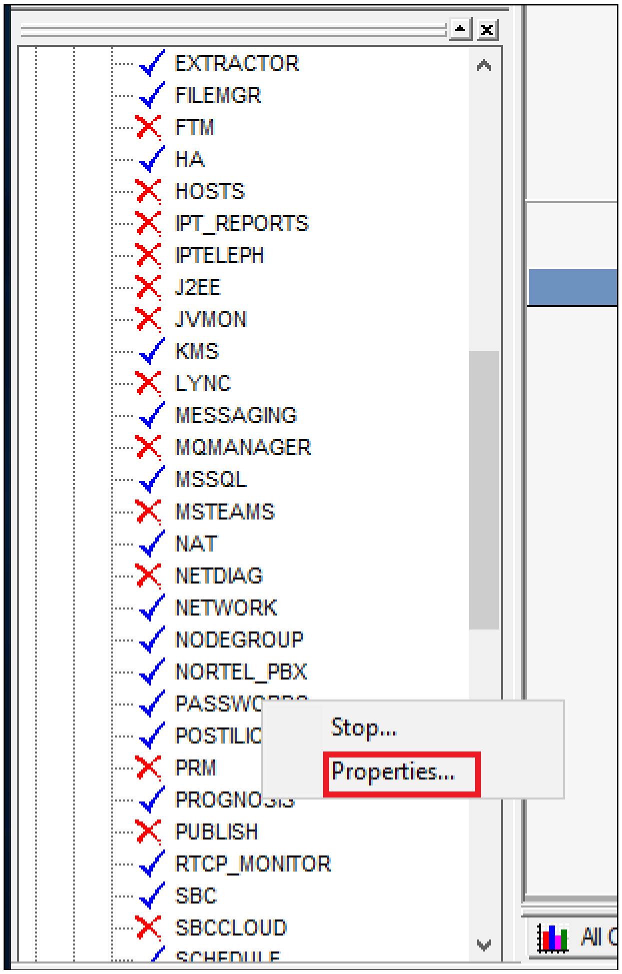


The **AEP** entry configured earlier is displayed below:

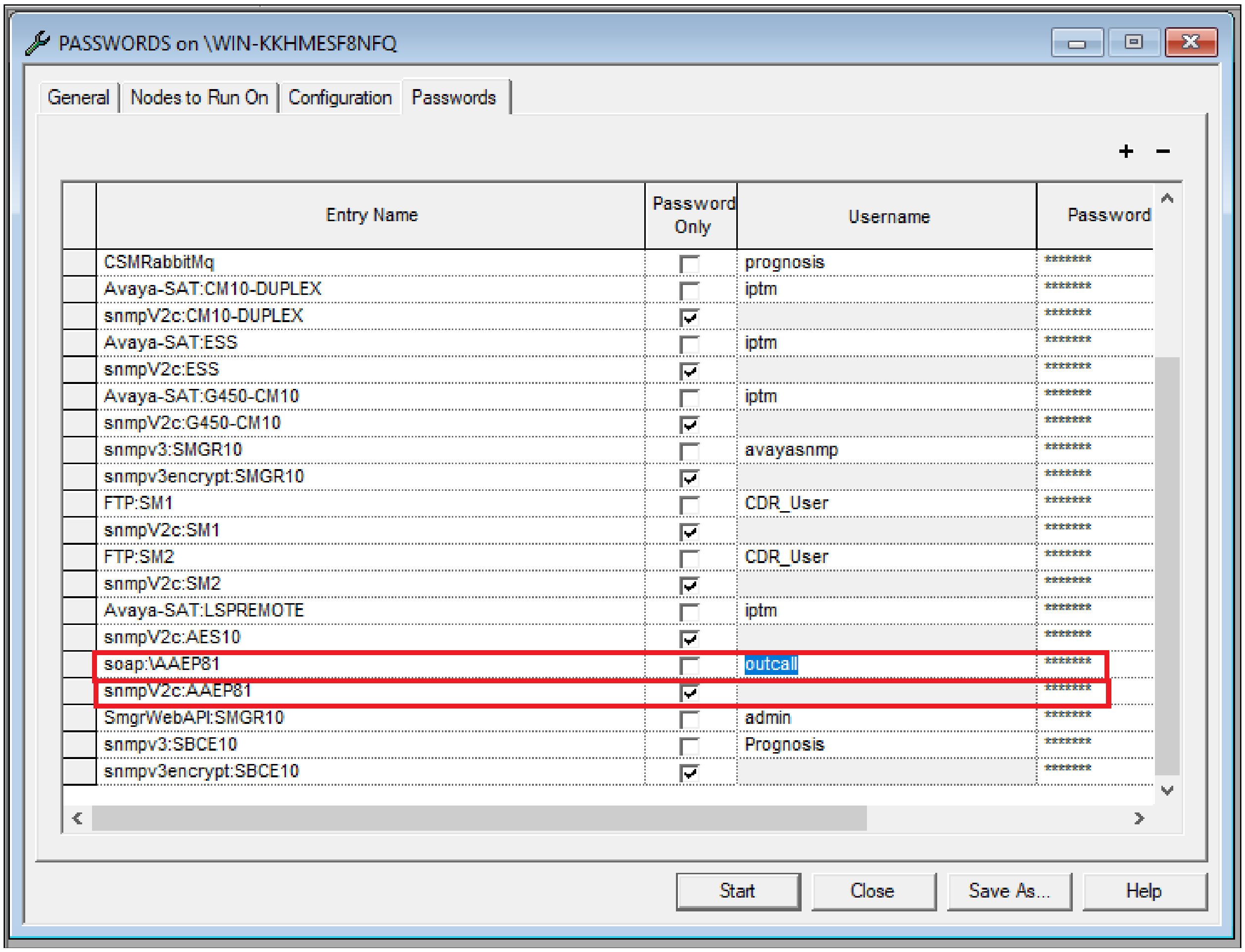


```
SUBSYS AVAYA_CONTACT
DEFINE TRAPPORT(#GlobalDefault, port=162)

ADD AES(AES10, ip=10.1.10.70, "customer=Avaya", site=DevCon Lab)
DEFINE SNMP_NODE_PROFILE(10.1.10.70, Version=2c)

ADD AEP(AAEP81, ip=10.1.10.82, "customer=Avaya", site=DevCon Lab)
DEFINE SNMP_NODE_PROFILE(10.1.10.82, Version=2c)
```

To check the configurations of the password to be monitored, expand Configurations of the Monitoring Node on the left pane, right-click on **PASSWORDS** and select **Properties**.



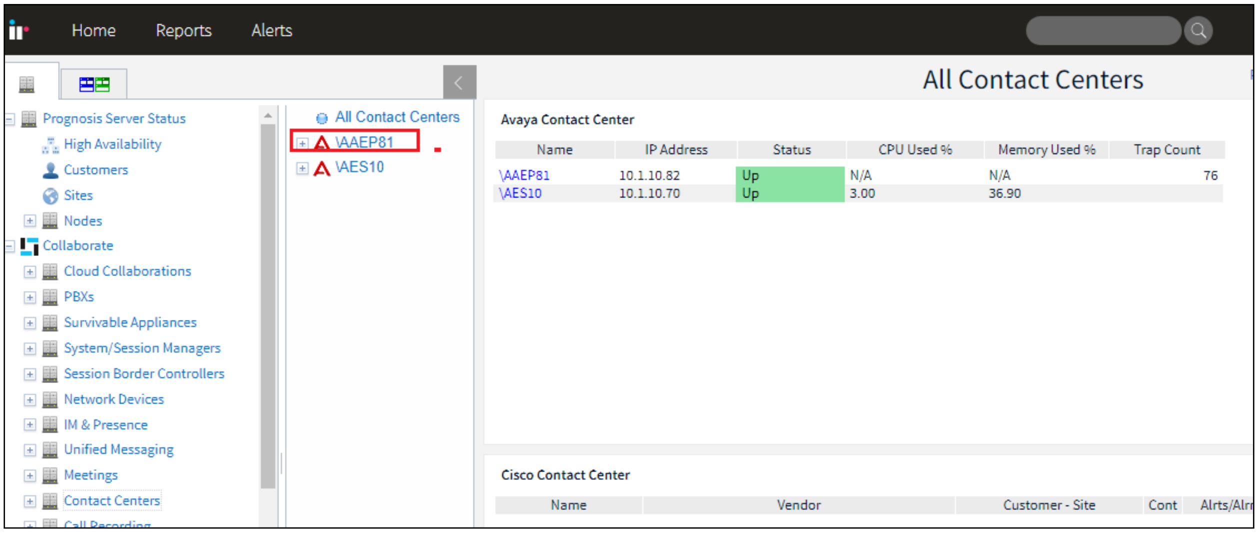
The password entries are displayed. In the compliance test, the first entry of AAEP was added **snmpv2c:AAEP81** with the password and **soap:\AAEP81** with username and the password (Community String) as configured in **Section 8.1**.



Entry Name	Password Only	Username	Password
CSMRabbitMq	□	prognosis	*******
Avaya-SAT:CM10-DUPLEX	□	iptm	*******
snmpV2c:CM10-DUPLEX	☑		*******
Avaya-SAT:ESS	□	iptm	*******
snmpV2c:ESS	☑		*******
Avaya-SAT:G450-CM10	□	iptm	*******
snmpV2c:G450-CM10	☑		*******
snmpv3:SMGR10	□	avayasnmp	*******
snmpv3encrypt:SMGR10	☑		*******
FTP:SM1	□	CDR_User	*******
snmpV2c:SM1	☑		*******
FTP:SM2	□	CDR_User	*******
snmpV2c:SM2	☑		*******
Avaya-SAT:LSPREMOTE	□	iptm	*******
snmpV2c:AES10	☑		*******
soap:\AAEP81	□	outcall	*******
snmpV2c:AAEP81	☑		*******
SmgrWebAPI:SMGR10	□	admin	*******
snmpv3:SBCE10	□	Prognosis	*******
snmpv3encrypt:SBCE10	☑		*******

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of AAEP and Prognosis. Log in to the Prognosis with administrative privileges as in **Section 8**. Then select **View Systems** on the top right icon (not shown). Select **Collaborate → Contract Centers** on the left pane and verify that the **AAEP81** is listed in the middle pane as below and the **Status** shows **Up**.



All Contact Centers

Avaya Contact Center

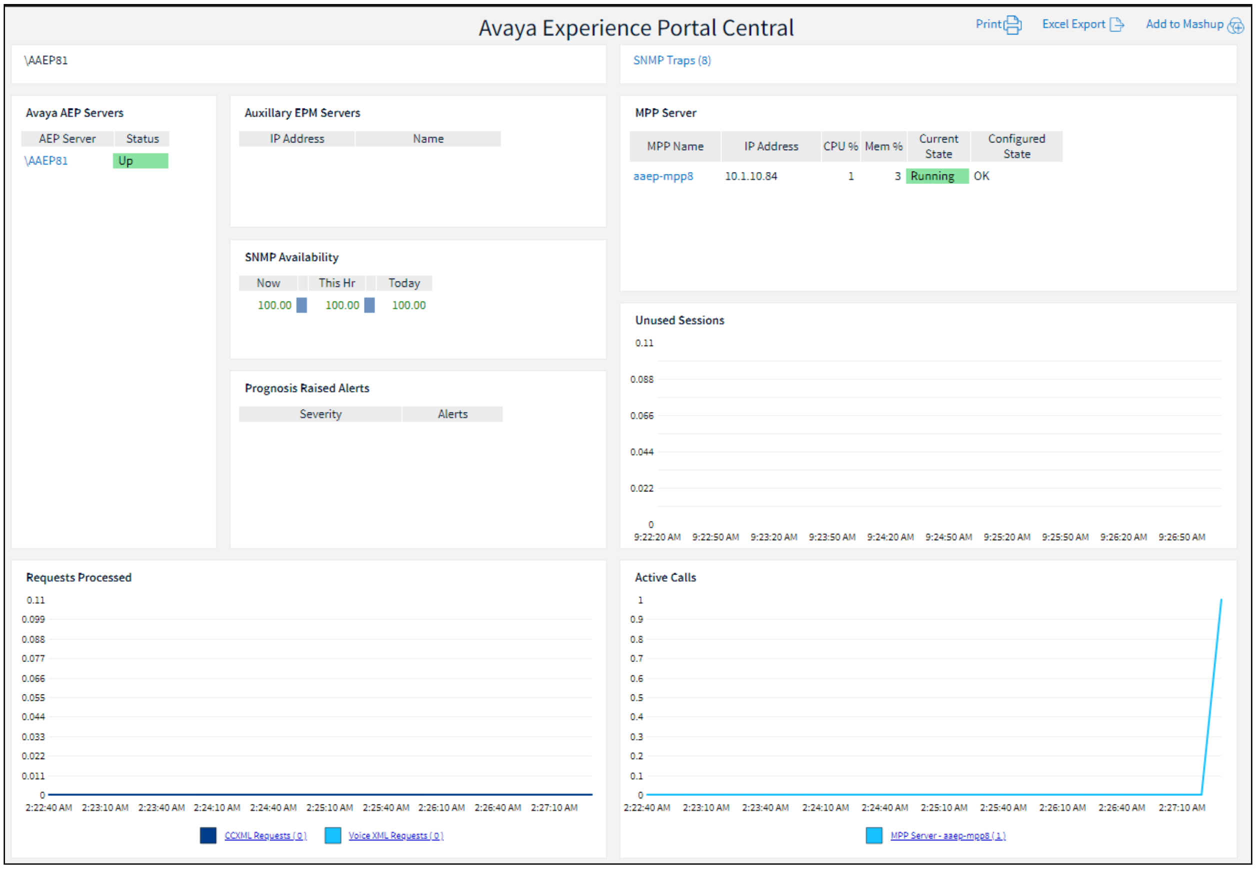
Name	IP Address	Status	CPU Used %	Memory Used %	Trap Count
\AAEP81	10.1.10.82	Up	N/A	N/A	76
\AES10	10.1.10.70	Up	3.00	36.90	

Cisco Contact Center

Name	Vendor	Customer - Site	Cont	Alrts/Alr

Click the **AAEP81** on the middle and a new page shows **Avaya Experience Portal Central** general status such as Avaya AEP (EPM) Servers, Status, SNMP Availability, MPP Server, Active Calls, Sessions etc., ... as shown below. Further details like Applications and SNMP Traps can be displayed by clicking the respective information.

Place multiple calls to Experience portal, verify the Active Calls shows correct ongoing calls and the other statistic of Experience Portal in the interface.



Avaya Experience Portal Central

\AAEP81

SNMP Traps (8)

Avaya AEP Servers

AEP Server	Status
\AAEP81	Up

Auxillary EPM Servers

IP Address	Name

SNMP Availability

Now	This Hr	Today
100.00	100.00	100.00

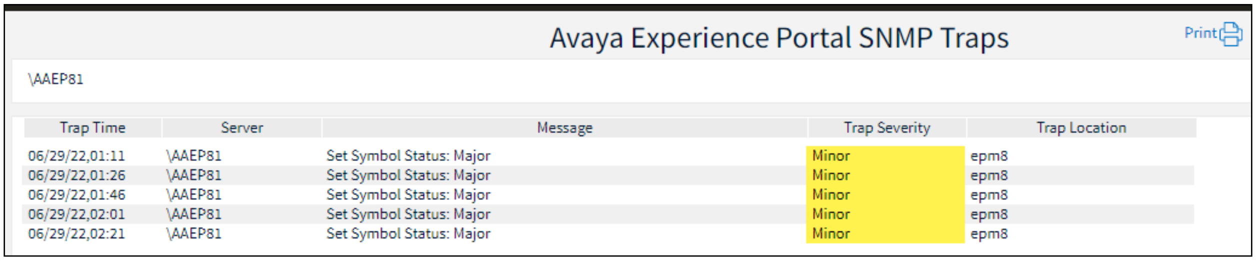
Prognosis Raised Alerts

Severity	Alerts

MPP Server

MPP Name	IP Address	CPU %	Mem %	Current State	Configured State
aaep-mpp8	10.1.10.84	1	3	Running	OK

To verify whether the Prognosis can receive and display the SNMP traps sent from the Experience Portal, select **SNMP Traps** on the top right from the previous screen to open **Avaya Experience Portal SNMP Traps** window.



Avaya Experience Portal SNMP Traps

\AAEP81

Trap Time	Server	Message	Trap Severity	Trap Location
06/29/22,01:11	\AAEP81	Set Symbol Status: Major	Minor	epm8
06/29/22,01:26	\AAEP81	Set Symbol Status: Major	Minor	epm8
06/29/22,01:46	\AAEP81	Set Symbol Status: Major	Minor	epm8
06/29/22,02:01	\AAEP81	Set Symbol Status: Major	Minor	epm8
06/29/22,02:21	\AAEP81	Set Symbol Status: Major	Minor	epm8

10. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research's Collaborate - Prognosis Server R12.1 to interoperate with Avaya Aura® Experience Portal R8.1.1. During compliance testing, all test cases were completed successfully with observations in **Section 2.2**.

11. 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® Session Manager*, Release 10.1, Issue 1, Dec 2021.
[3] *Administering Avaya Aura® Application Experience Portal*, Release 8.1.1, Issue 1, Dec 2021.

Prognosis documentations are provided in the online help that comes with the software package.

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.