



Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research's Collaborate - Prognosis Server R12.1 with Avaya Aura® Application Enablement Services 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® Application Enablement Services 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. Prognosis monitors directly to Application Enablement Services 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® Application Enablement Services (AES) R10.1. Prognosis uses Simple Network Management Protocol (SNMP) to monitor AES server, link availability and utilization.

2. General Test Approach and Test Results

The general test approach was to verify Prognosis using SNMP connection to monitor and display system status from AES.

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 interface to display correct information of AES.

- Verify that the server statistics information for the AES is populated on Prognosis display: SNMP Availability, Prognosis Raised Alerts, Link Status, TSAPI Client Connections and DMCC Sessions.
- Verify that the list of AES links is visible in Prognosis: ASAI Link, CVLAN Link, DLG CTI Link, License, Server, SNMP Status, TSAPI CTI Link and TSAPI TLink.
- For each of the links, click on the links to view utilization details.

2.2. Test Results

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

- The following links were not tested along with its detail since there is no available connection or device exists: CVLAN Link and DLG CTI Link.

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® Application Enablement Services. The configuration consists of a duplex Avaya Aura® Communication Manager (System A) with an Avaya G430 Media Gateway, and Avaya Aura® Media Server. Another simplex Avaya Aura Communication Manager (System B) was configured with an Avaya G450 Media Gateway. Both provides CTI links to Avaya Aura® Application Enablement Services. Avaya Aura® Session Manager was configured via Avaya Aura® System Manager to provide SIP Deskphones. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to the Enterprise solution.

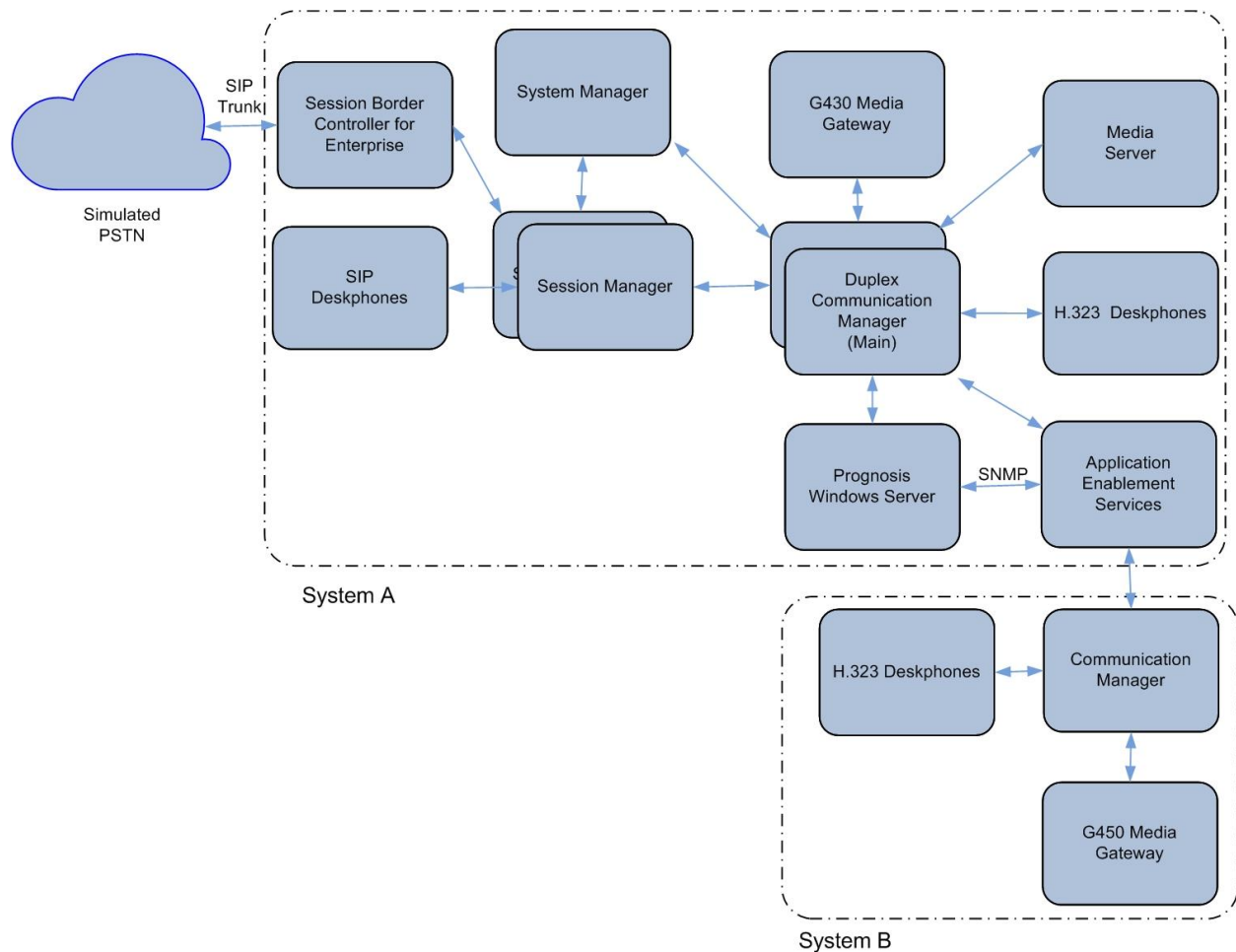


Figure 1: Test Configuration Diagram

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 (System A)	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 Aura® Communication Manager (System B)	10.1 (10.1.0.0.0.974.27293)
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
Avaya Aura® Session Manager	10.1 (10.1.0.0.1010019)
Avaya J100 Series IP Telephones - J179 - J129	4.0.11.0
Avaya 96x1 Series IP Telephones - 9641G - 9611G	9.8511
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® Communication Manager

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

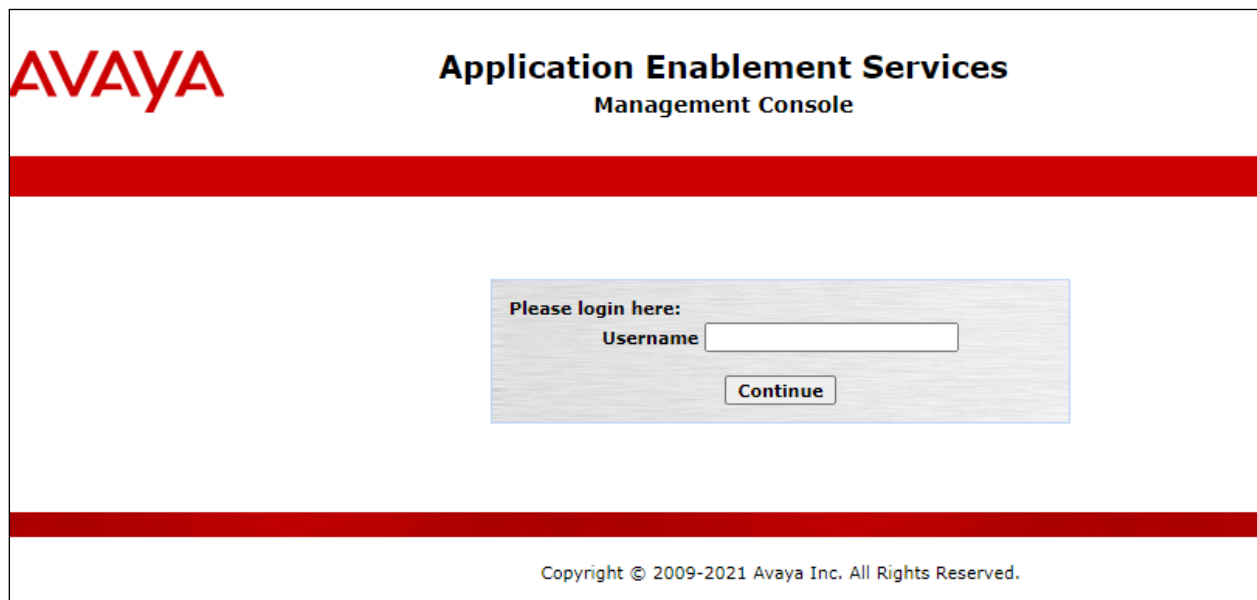
6. Configure Avaya Aura® Session Manager

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

7. Configure Avaya Aura® Application Enablement Services

The initial administration of Application Enablement Services and the connection to Communication Manager is assumed to be in place and will not be covered here. This section only covers the configuration of SNMP connection of Application Enablement Services that is required for the purpose of administering Prognosis.

AES is configured via the AES Management 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 AES. Log in using the appropriated login credential.



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo in red. To its right, the text "Application Enablement Services Management Console" is displayed in black. Below this is a thick red horizontal bar. In the center of the page is a light blue rectangular box containing the login prompt "Please login here:" followed by a "Username" label and an empty text input field. Below the input field is a "Continue" button. At the bottom of the page, another thick red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2021 Avaya Inc. All Rights Reserved." is displayed in small black text.

Note: All the screens in this section are shown after the AES had been configured. Click **Save** button to save the screen parameters configured on Application Enablement Services if needed.

7.1. Configure SNMP Connection

To configure SNMP Connection, navigate to **Utilities** → **SNMP** → **SNMP Agent**. The SNMP Agent page is displayed in the right. In the **SNMP Agent**, configure the following parameters as shown below.

- Tick **Enable SNMP Version 2c** and enter the desired security name, in this case **avaya123**. This security name will be used in Prognosis configuration.

The screenshot shows a web interface for configuring the SNMP Agent. The breadcrumb path is **Utilities | SNMP | SNMP Agent**. On the left is a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, and Utilities. Under Utilities, there are sub-items: Diagnostics, Email Notification, HMDC, and SNMP. The SNMP sub-item is expanded to show Product ID, **SNMP Agent**, and SNMP Trap Receivers. The main content area is titled **SNMP Agent** and contains the following configuration sections:

- MIB II System Group Data:**
 - Location:
 - Contact:
- SNMP Protocol Access:**
 - Enable SNMP Version 1
 - Community Name:
 - Enable SNMP Version 2c
 - Community Name:
 - Enable SNMP Version 3
- User:**
 - User Name:
 - Authentication Protocol:
 - Authentication Password:
 - Privacy Protocol:
 - Privacy Password:

At the bottom, there is a section for **Authorized IP Addresses for SNMP Access***.

Navigate to **Authorized IP Addresses for SNMP Access** from the same **SNMP Agent** settings. Enter IP address of the Prognosis monitoring server. This will allow the Prognosis server to access the AE server via SNMP.

- Select **Following IP Addresses**.
- **IP Address 1:** Enter Prognosis IP address, e.g., 10.1.10.125.

Authorized IP Addresses for SNMP Access*

No Access

Any IP Addresses

Following IP Addresses

IP Address 1:

IP Address 2:

IP Address 3:

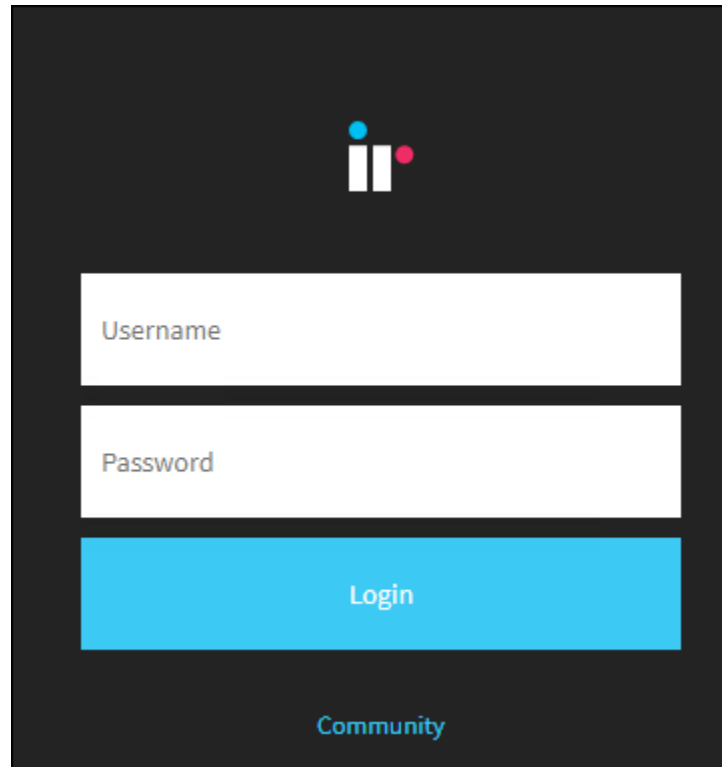
IP Address 4:

IP Address 5:

Note: There is no ip access restriction on Software Only for SNMP Version 3.

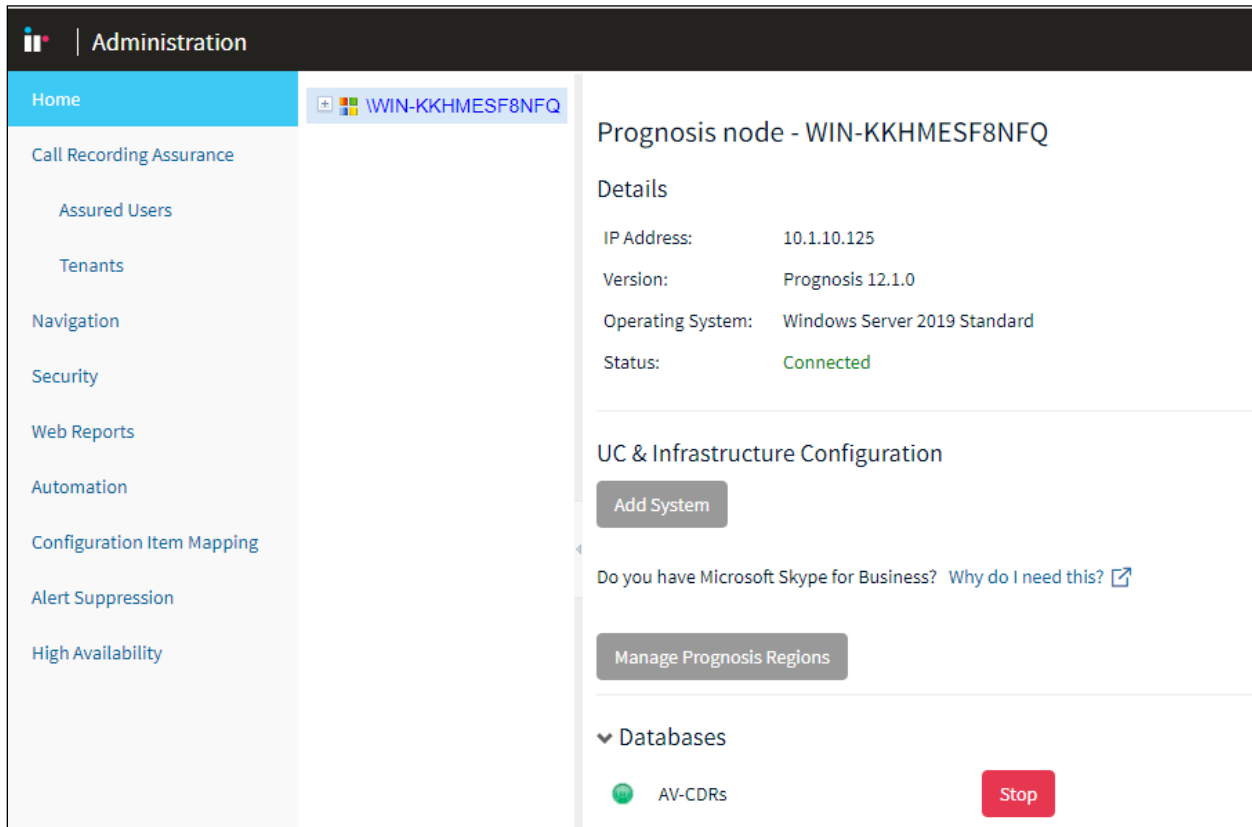
8. Configure Prognosis

This section describes the configuration of Prognosis required to interoperate with Application Enablement Services. Log in to the Prognosis with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Administration** and log in with the appropriate password.



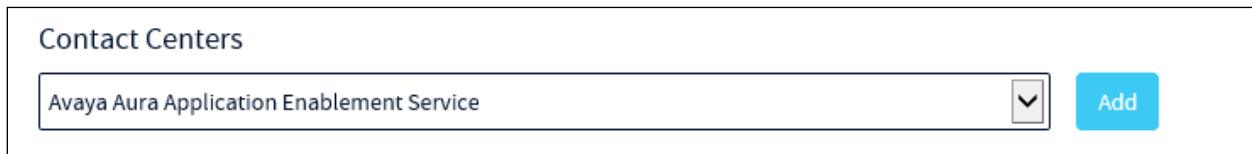
The screenshot shows a login interface with a dark background. At the top center is a logo consisting of three vertical bars of varying heights, with a blue dot above the left bar and a red dot above the right bar. Below the logo are three white input fields: the first is labeled 'Username', the second is labeled 'Password', and the third is a blue button labeled 'Login'. At the bottom center, the word 'Community' is written in a light blue font.

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



8.1. Administer Avaya Aura® Enablement Service Configuration

Click **Add System** and scroll below to **Contact Centers**.



Select **Avaya Aura Application Enablement Service** from drop-down menu. Click **Add** to add a new AES. In this test configuration, the following entries are added for AES with display name of **AES10** and with IP addresses of **10.1.10.70**.

The following settings were used during the compliance test.

Basic Details:

- **Display Name: AES10**
- **IP address: 10.1.10.70**
- **Customer Name: Avaya**
- **Site Name: DevCon Lab**

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 configured settings.

Update Avaya Aura Application Enablement Services

Basic Details

Display Name: AES10

IP Address: *

Customer Name:

Site Name:

SNMP Connection Details

Use SNMP Version 1

Use SNMP Version 2c

Use SNMP Version 3

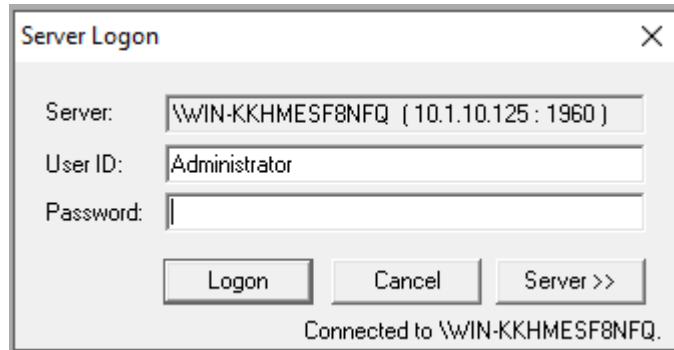
Community String:

Databases and Thresholds

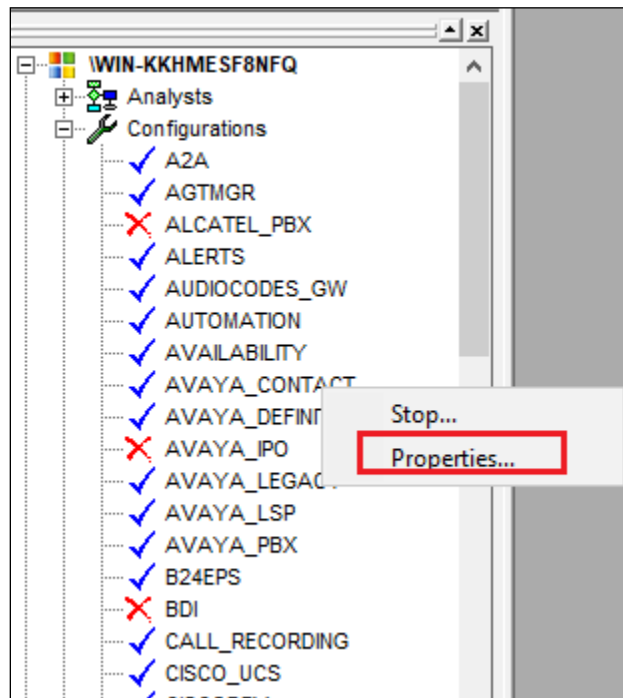
Start standard databases and thresholds

8.2. Verifying Configurations with Prognosis Client

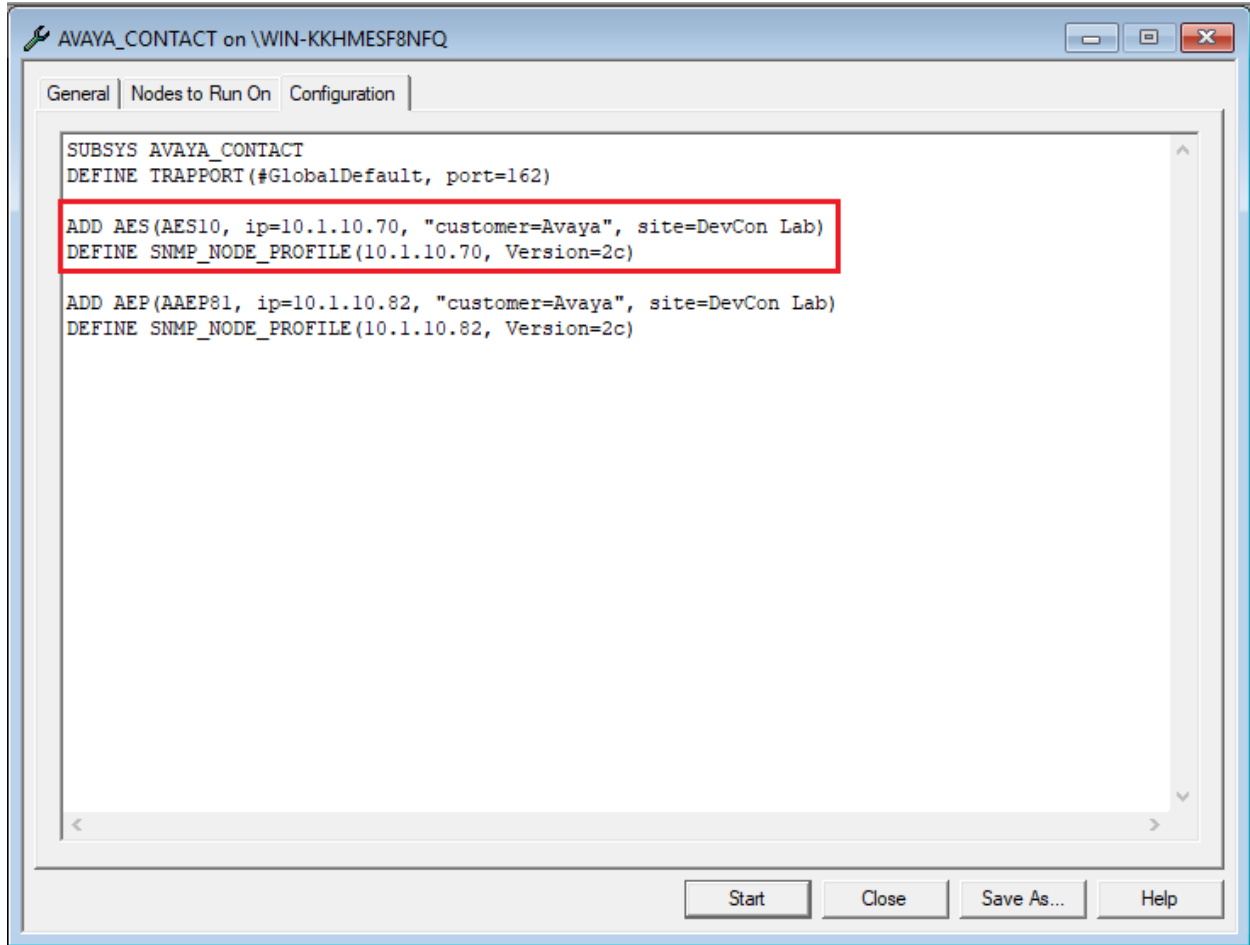
On Prognosis server, click **Start** → **All Programs** → **Prognosis** → **Prognosis Client** to start the Windows Client application. Log in with the appropriate credentials.



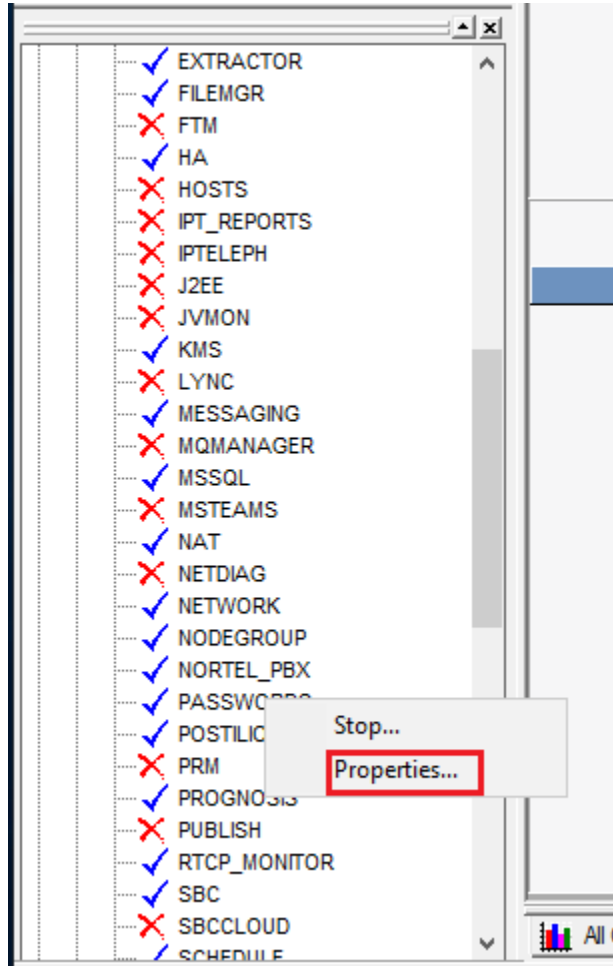
To check the configurations of the AES to be monitored, expand **Configurations** of the Monitoring Node on the left pane, right-click on **AVAYA_CONTACT** and select **Properties**.



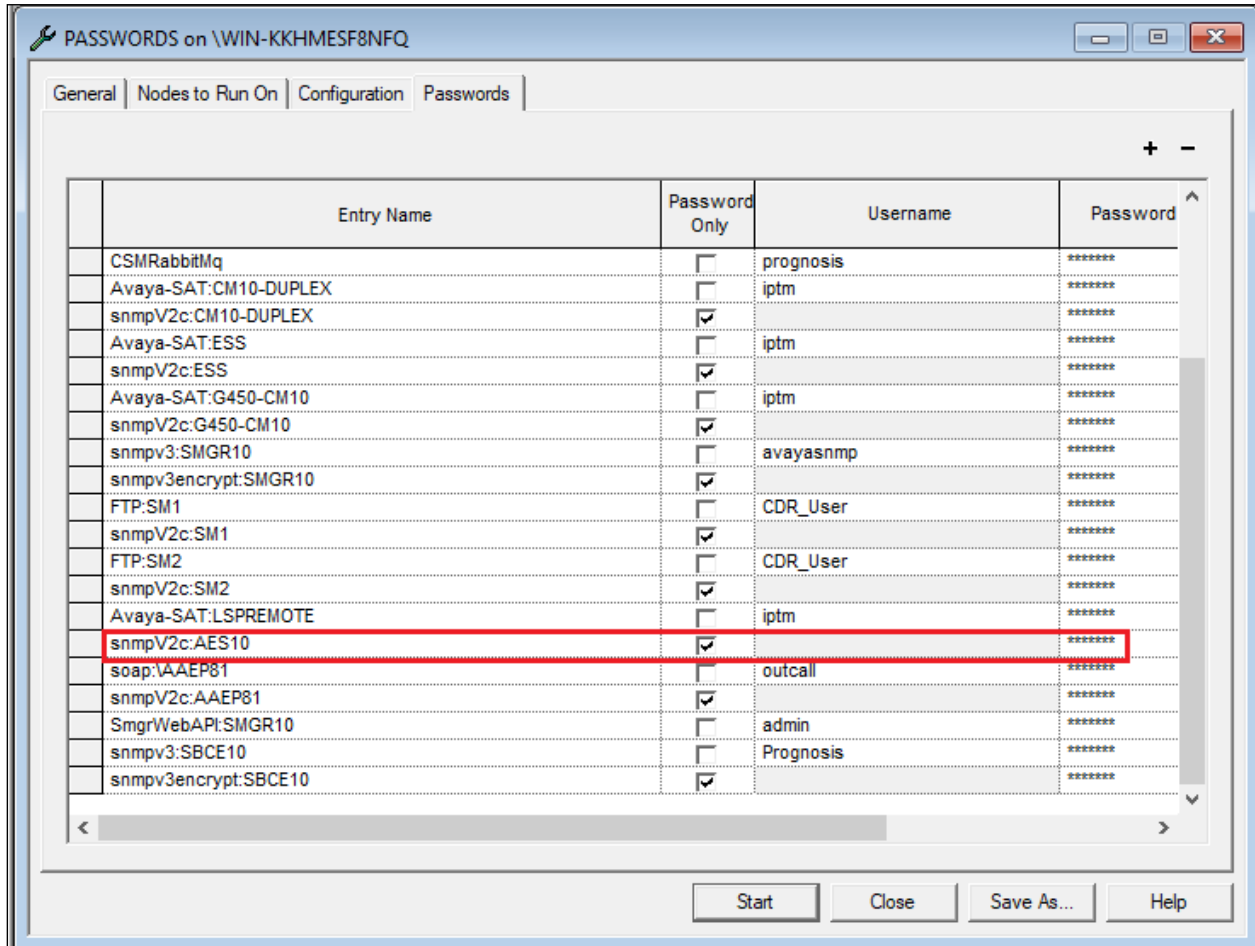
The **AES** entry configured earlier is displayed below:



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 AES was added **snmpv2c: AES10** with the password (Community String) as configured in **Section 8.1**.



9. Verification Steps

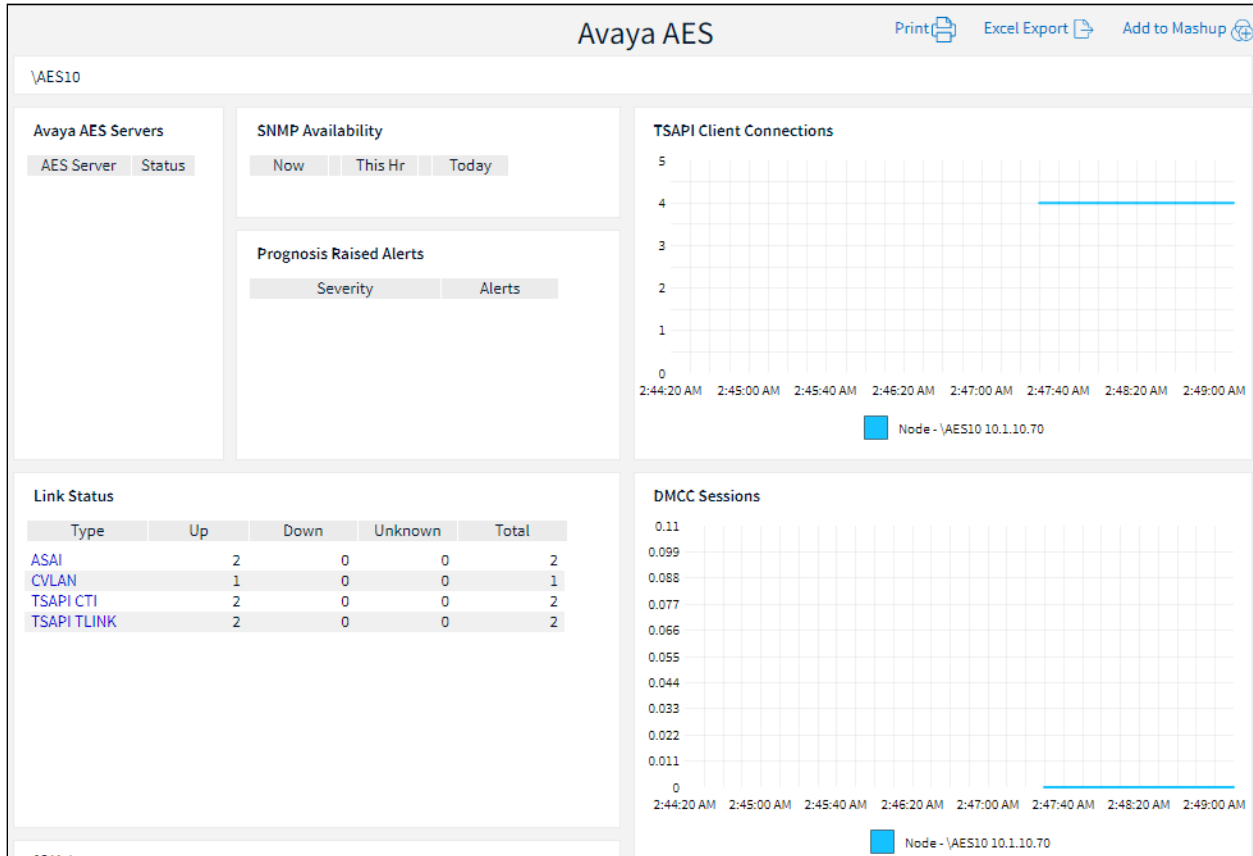
This section provides the tests that can be performed to verify proper configuration of AES and Prognosis. Log in to the Prognosis with administrative privileges as in **Section 8**. Then select **View Systems** on the top right icon (not shown). Select **Collaborate** → **Contract Centers** on the left pane and verify that the **AES10** is listed in the middle pane and **Status** shows **Up**.

The screenshot shows the Prognosis interface with the following data:

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 **AES10** on the right pane below. A new page shows **Avaya AES** general status of the monitored AES such as AES Server, Status, SNMP Availability, Link Status, DMCC sessions etc., ... as shown below. Details of the **Link Status** can be viewed by clicking the individual CTI link **Type**.



The screenshot below shows the TSAPI CTI links administered and their **Status**.

The screenshot displays the 'Avaya AES TSAPI CTI Links' table for node \AES10. The table contains the following data:

Switch Name	Link Id	Associations	Message Period	Message Received	Message Sent	Status	Last Status Changed
G450	1	1	30	15	15	Up (talking)	Wed Jun 29 14:36:26 2022
Duplex	3	0	30	15	15	Up (talking)	Wed Jun 29 14:35:52 2022

10. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research's Collaborate - Prognosis Server R12.1 to interoperate with Avaya Aura® Application Enablement Services R10.1. During compliance testing, all test cases were completed successfully with observation noted 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 Enablement Services*, Release 10.1, Issue 1, Dec 2021.

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.