Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis Unified Communication 10 with Avaya Aura® Application Enablement Services 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis Unified Communication 10 to interoperate with Avaya Aura® Application Enablement Services 6.3. Prognosis monitored Application Enablement Services using SNMP and displayed monitored data on web-based application.

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 Integrated Research Prognosis Unified Communication 10 (herein after referred to as Prognosis) with Avaya Aura® Application Enablement Services (AES) 6.3. Prognosis used SNMP connection to monitor AES statistics such as CPU, Memory and Disk Usage, License information and AE Services links status detail and display monitored data on web-based application.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying proper display of AES monitored data on Prognosis.

- Verify that the server statistics information for AES is populated on Prognosis display such as CPU, Memory and Disk Usage and list of Software/Processes.
- Verify proper display of AES server status and link information included SNMP Availability, Raised Alerts, Link Status, TSAPI Client Connections and DMCC Sessions.
- Verify that the list of AES links is visible in Prognosis: ASAI Link, DLG CTI Link, TSAPI CTI Link and TSAPI TLink, along with utilization details.
- Verify License, SNMP Status were displayed correctly.

The serviceability testing focused on verifying the ability of Prognosis to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Prognosis server.

2.2. Test Results

All test cases were passed and met the requirements as shown in **Section 2.1** with the following observation: It takes about 10-20 seconds for Prognosis to start displaying AES data in the web user interface.

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 the Prognosis application with AES. In the compliance Avaya S8800 Server running Communication Manager with an Avaya G650 Media Gateway providing CTI link to AES.

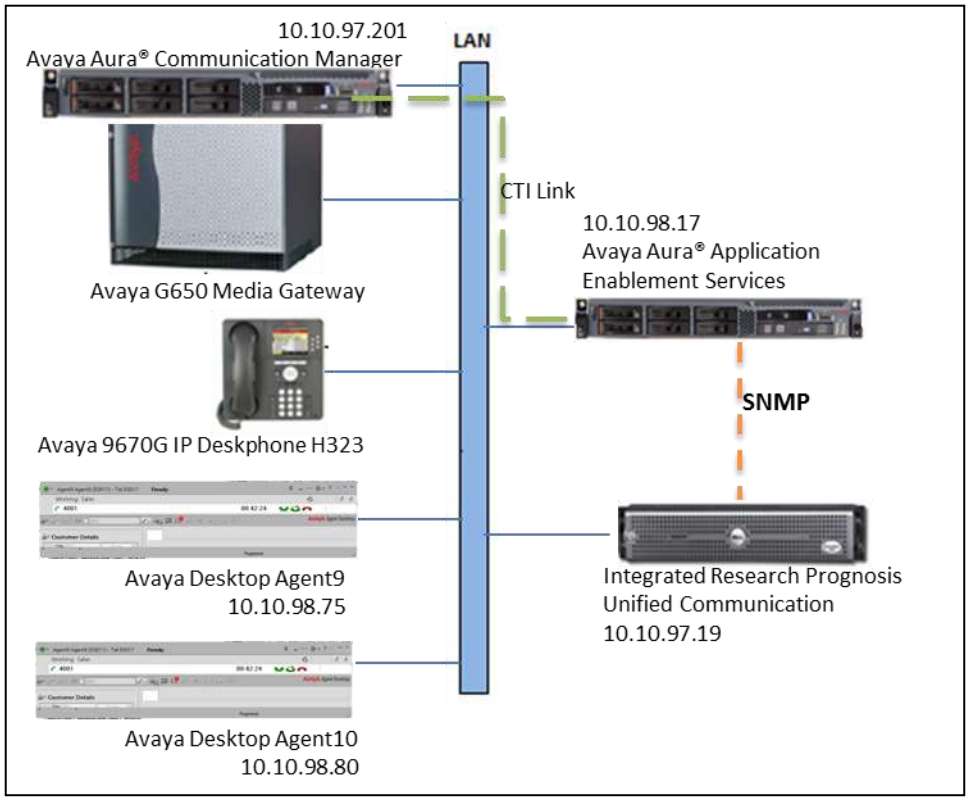


Figure 1: Test Configuration Diagram

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 running on Avaya S8800 Server	6.3 SP 8 (R016x.03.0.124.0 w/Patch 21588)
Avaya G650 Media Gateway (TN2312BP)	Vintage HW06 FW043
Avaya Aura® Application Enablement Services	6.3.3
Avaya Aura® Contact Center CCMS/CCMA/CCT/MAS Co-Resident system running on S8800 Server	6.4 SP13 Window 64-bit 2008 R2 Service Pack 1
Avaya 9670G IP Deskphone (H323)	3.2.4
Avaya Agent Desktop 6.4	Release 6.4 Version 8.4.0.419
Integrated Research Prognosis Unified Communication running on Window 64 bit 2008	Version 10 Window 64-bit 2008 R2 SP1

5. Configure Avaya Aura® Communication Manager

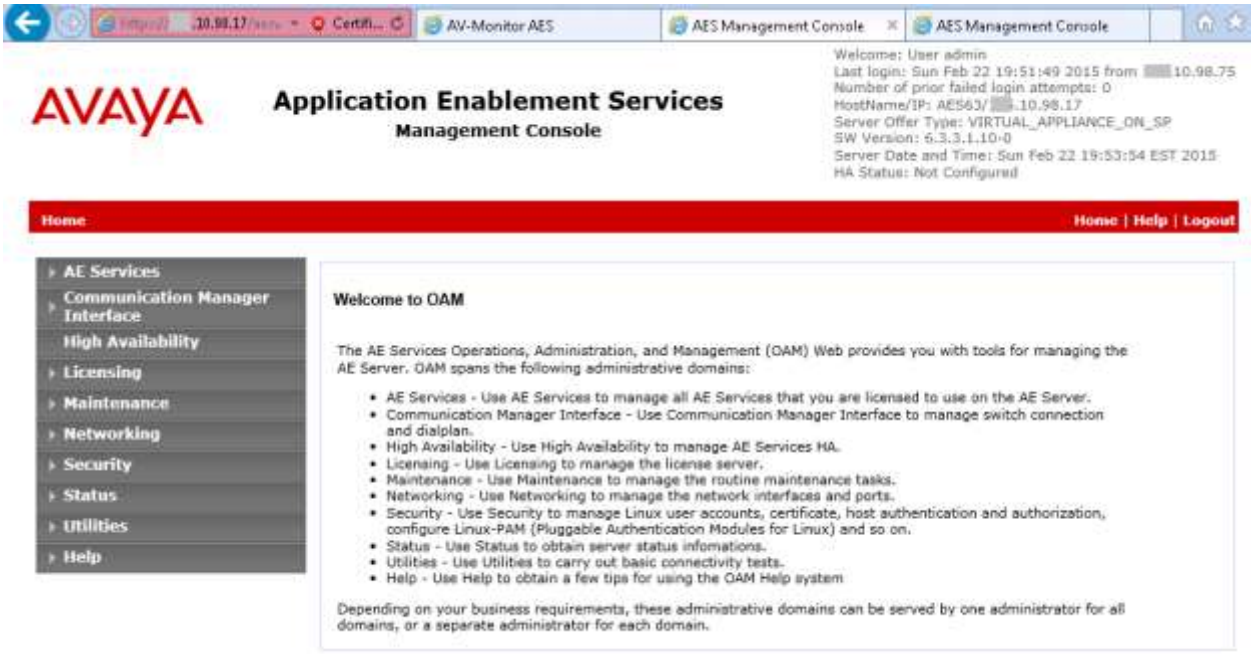
The configuration of Communication Manager and AES is assumed to be in place and will not be discussed in this document. For more information of how to configure Communication Manager and AES, please refer to **Section 10**.

6. Configure Avaya Aura® Application Enablement Services

The initial administration of AES and the connection to Communication Manager is assumed to be in place and will not be covered here. This section covers the configuration of SNMP that is required for integration with Prognosis.

AES is configured via the AES Management web interface. In order to access the web interface, enter http://<ip-addr>/ as the URL in an internet browser, where<ip-addr> is the IP address of AES. Log in using the appropriate login credential. The screen shown below is displayed.

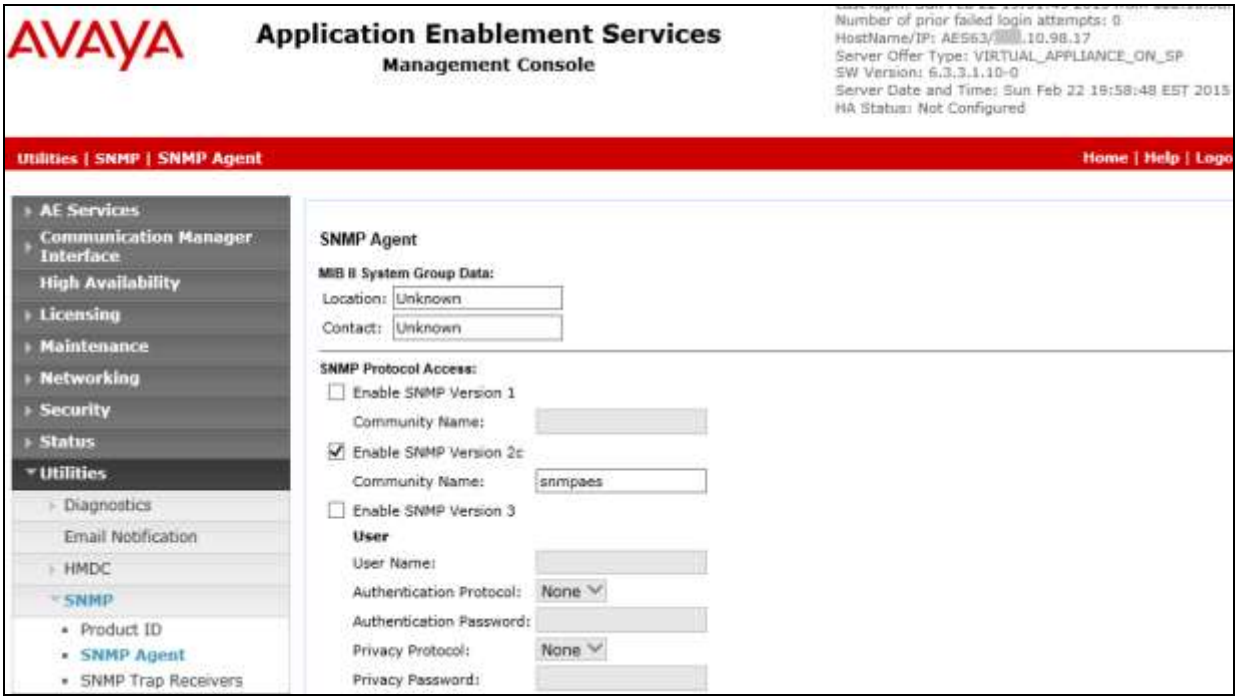
Note: All screens in this section are shown after AES had been configured. Click **Save** button to save the screen parameters configured on AES if needed.



6.1. Configure SNMP Connection

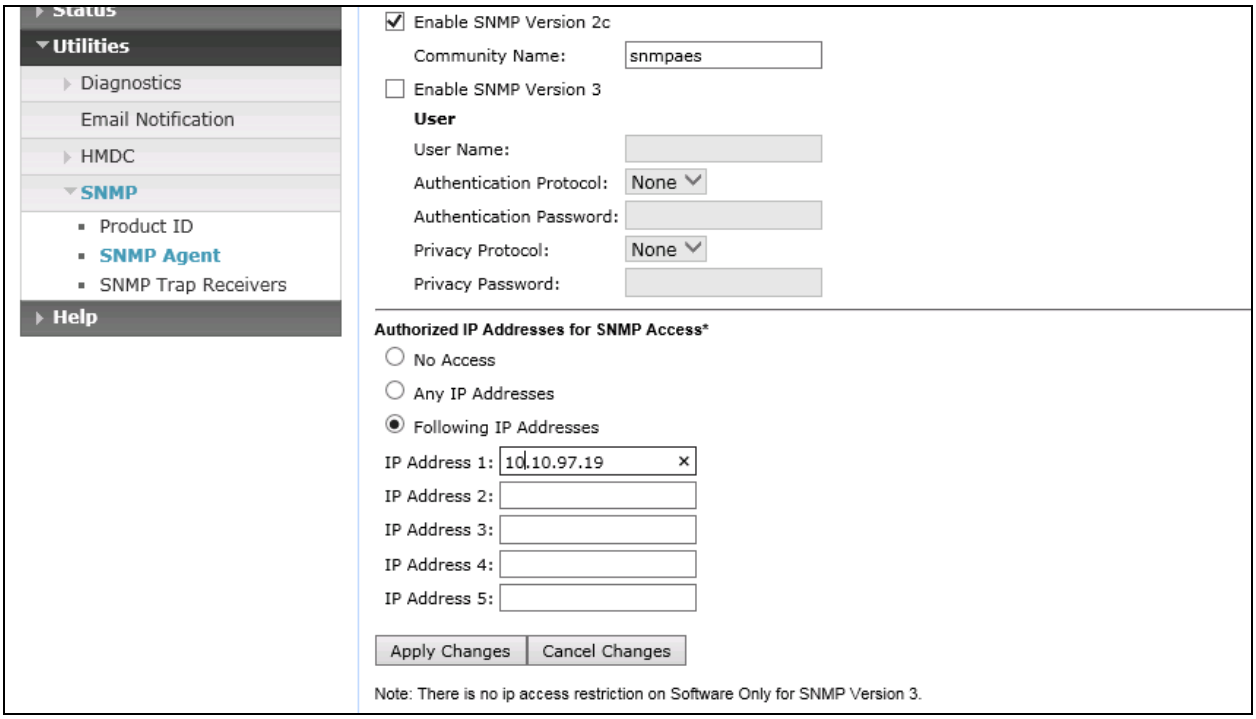
To configure SNMP Connection, navigate to **Utilities → SNMP → SNMP Agent**. The SNMP Agent page is displayed in the right. Configure the following parameters as shown below.

- Enable **SNMP Version 2c** and enter any descriptive security name such as **snmpaes**, this security name will be used in the Prognosis configuration.



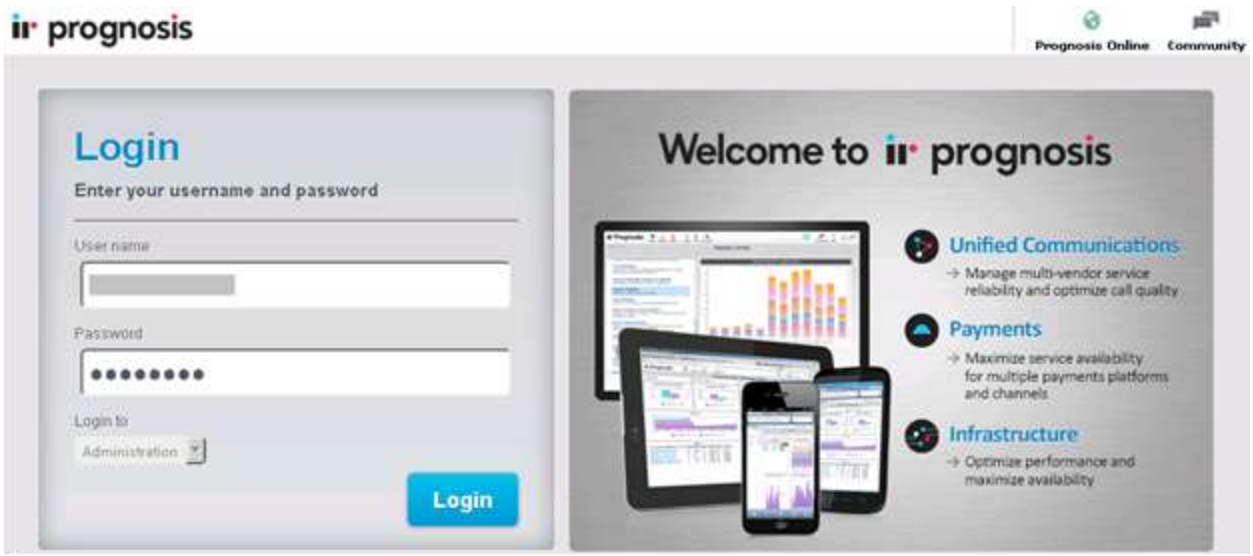
Navigate to **Authorized IP Addresses for SNMP Access**. Enter IP address of the Prognosis server. This will allow the Prognosis server to access the AES server via SNMP.

- Select **Following IP Addresses**.
- **IP Address 1**: enter Prognosis IP address, example: 10.10.97.19.

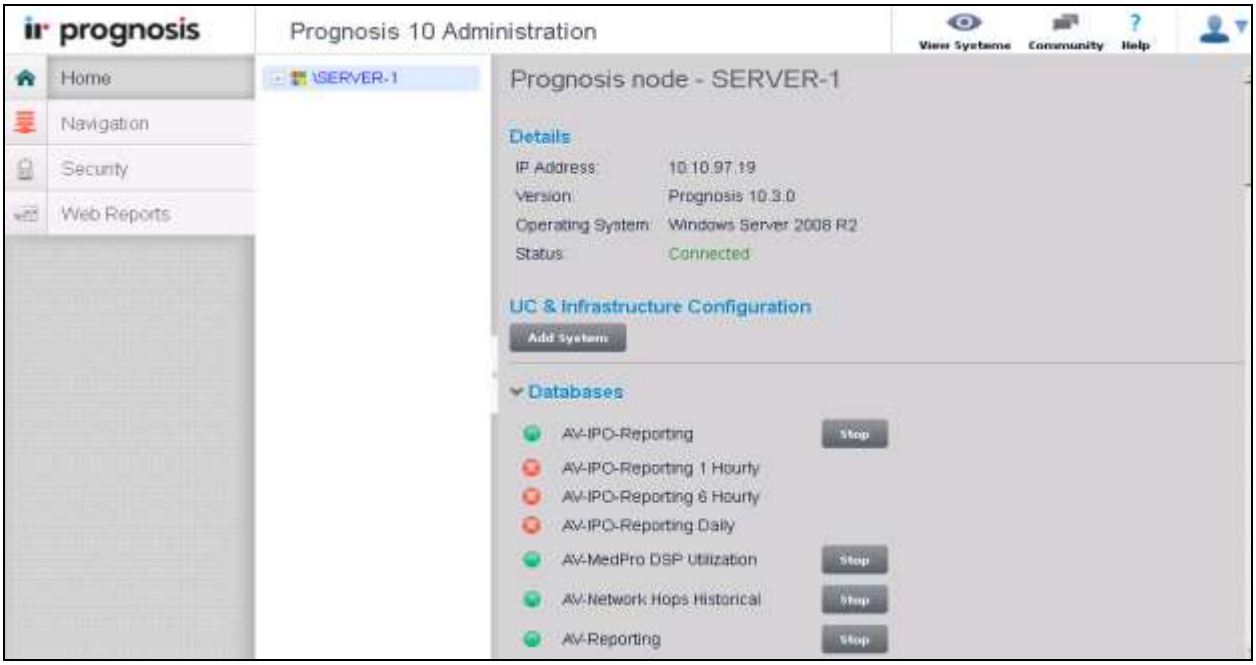


7. Configure Integrated Research Prognosis Unified Communication

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

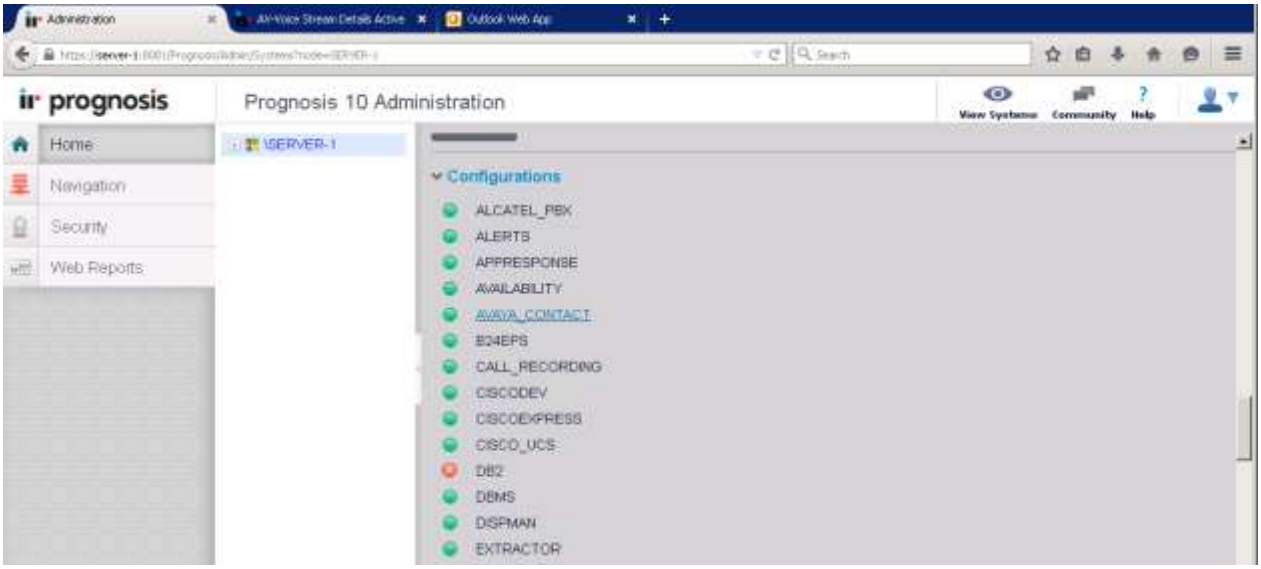


The **Prognosis 10 Administration** homepage is displayed as shown below.



7.1. Administer AVAYA_CONTACT Static Configuration

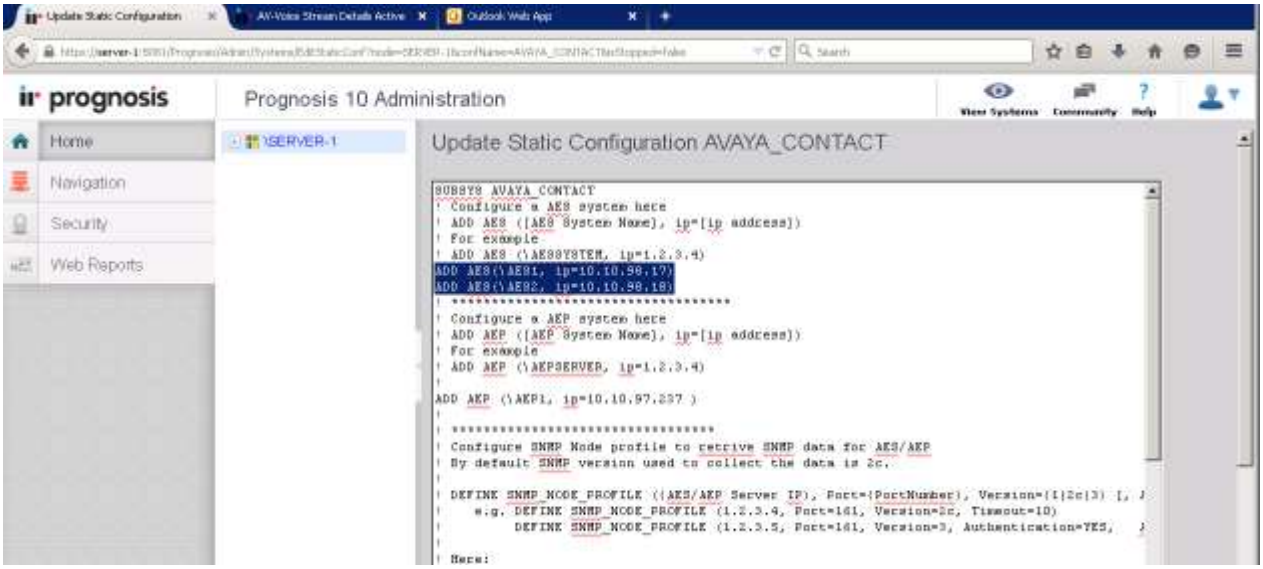
This section describes steps to add AES into AVAYA_CONTACT static configuration. In the Prognosis home screen, scroll down to **Configurations** and click on **AVAYA_CONTACT** hyperlink (shown below) to open **Update Static Configuration AVAYA_CONTACT** page.



In the **Update Static Configuration AVAYA_CONTACT** page, add an entry for AES using the following format **ADD AES (\any_name, ip=<ip-address-of-AES-server>)**, during compliance test although 2 entries were added only **AES1** was used for testing purpose.

- **ADD AES (\AES1, 10.10.98.17)**
- **ADD AES (\AES2, 10.10.98.18)**

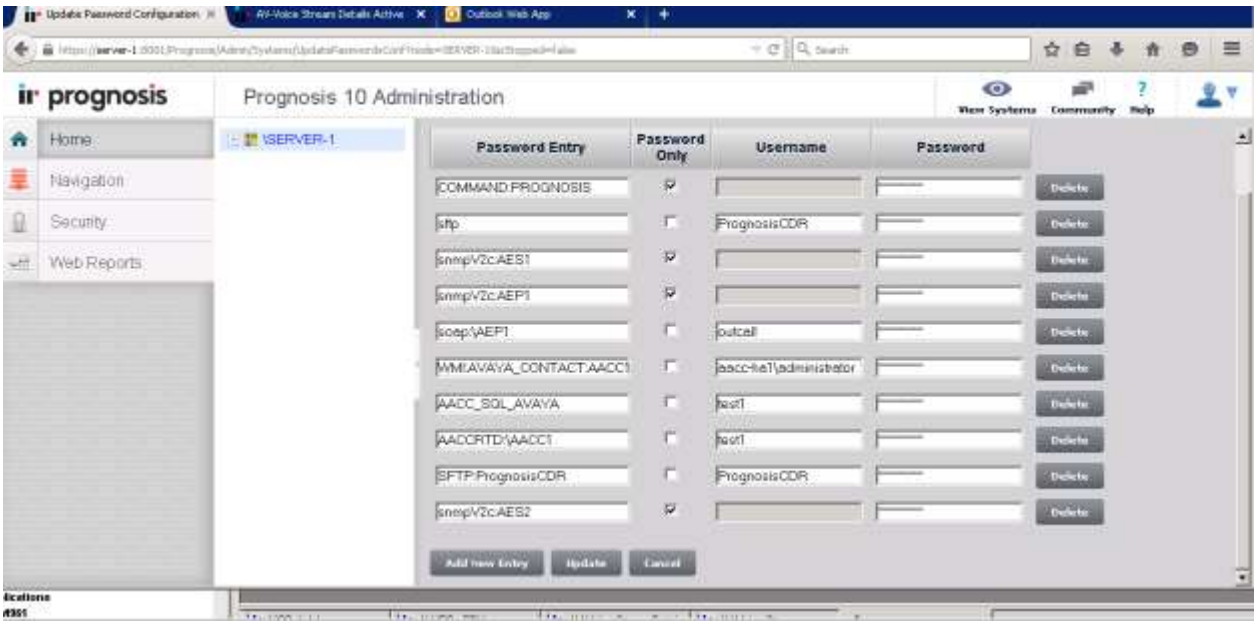
Click on **Start** button (not shown) to save changes and return to the home page.



7.2. Administer Password

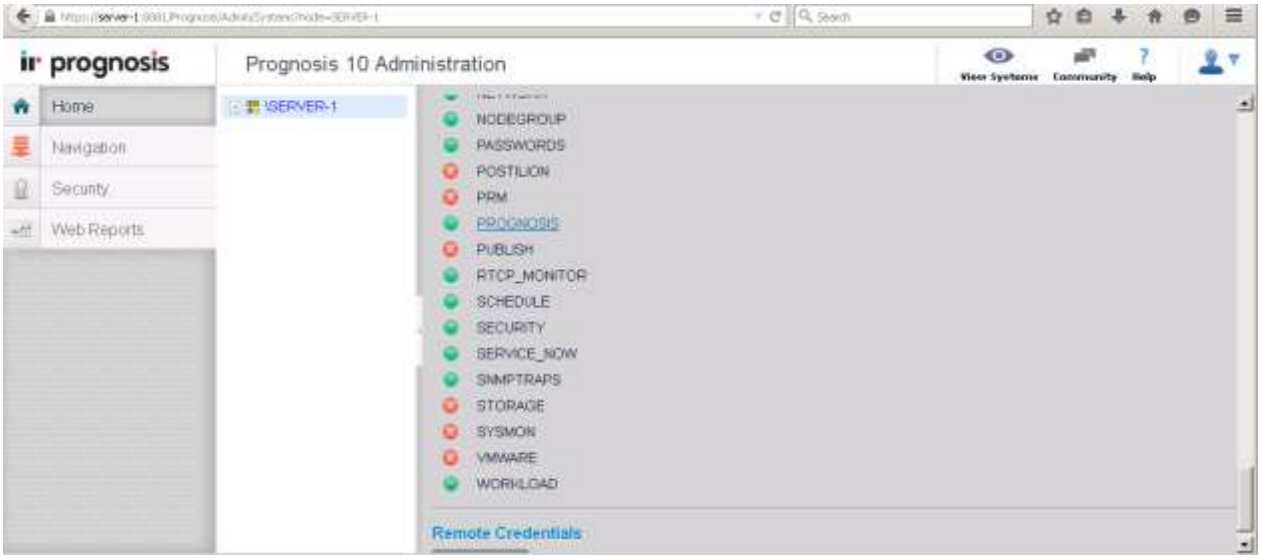
On the home page, scroll down to **Configuration** section and click on **PASSWORDS**.

A list of password entries is displayed. In the compliance test, an entry for **AES1** was added **snmpv2c:AES1** with **Password** of **snmpaes** as configured in **Section 6.1.** Click **Update** to save changes and to return to the home page.

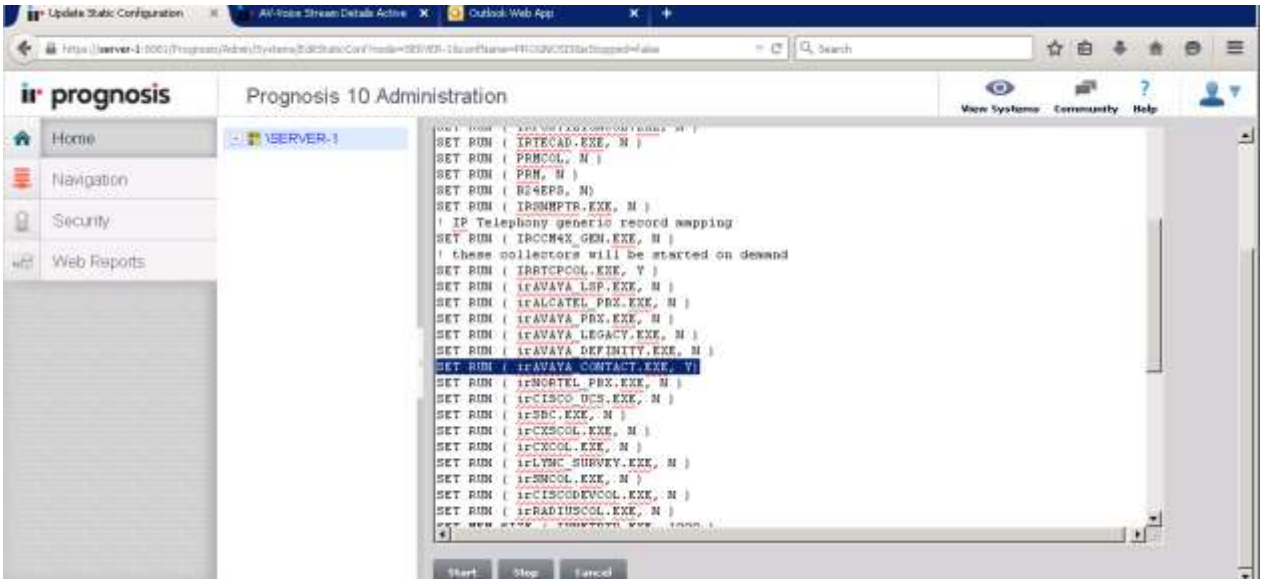


7.3. Start irAVAYA_CONTACT

On the home page, scroll down to the **Configuration** section and click on **PROGNOSIS**.



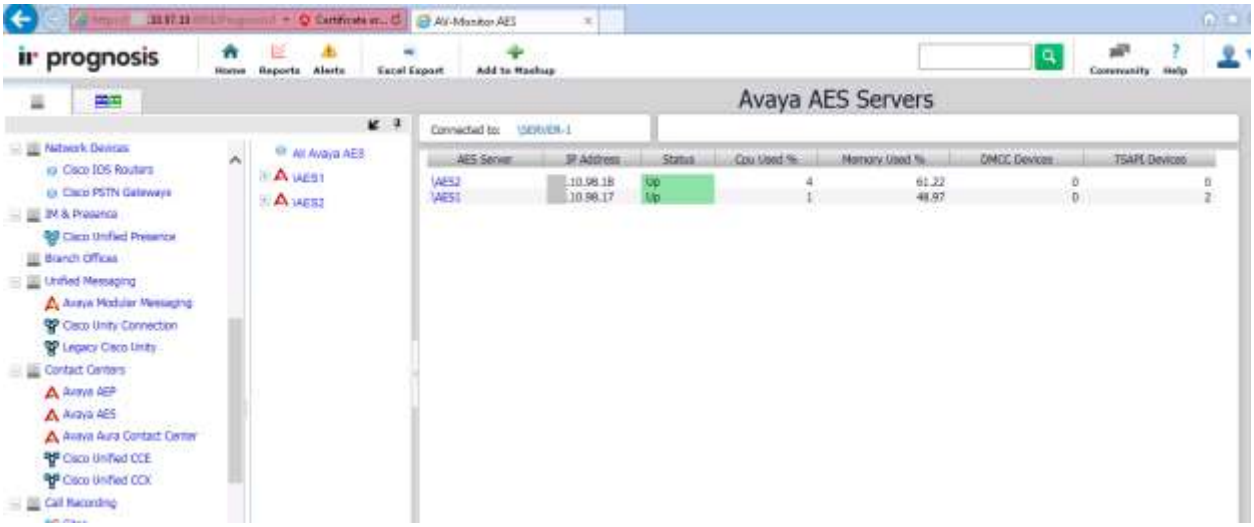
In the updated page, make certain that **irAVAYA_CONTACT.EXE** is set to **Y** as shown below. Click **Start** to save change and start the module.



8. Verification Steps

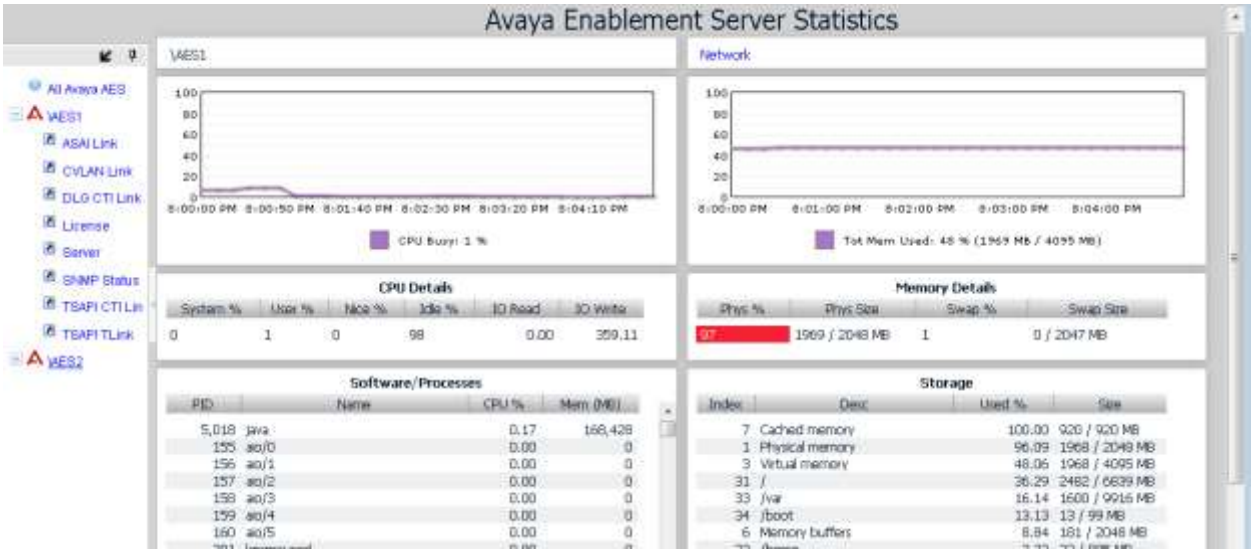
This section provides the tests that can be performed to verify proper configuration of AES and Prognosis. Launch the Prognosis View System web user interface, by entering https://ip-address:8081 in browser address bar where ip-address is Prognosis IP address, and enter appropriate login credential.

Browse to **Contact Centers → Avaya AES** in the left navigation pane. The AES server instances are displayed in the middle pane. The Avaya AES Servers page show general status of monitored AES as shown below.



Click on **AES1** link to verify AES server status and configured links status information.

Click on **AES1→ Server** link to view statistics information for AES1.



9. Conclusion

These Application Notes describe the procedures for configuring Integrated Research Prognosis Unified Communications 10 to interoperate with Avaya Aura® Application Enablement Services 6.3. During compliance testing, all test cases were completed successfully.

10. Additional References

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

[1] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3 02-300357 June 2014.

[2] *Avaya Aura® Application Enablement Services Overview and Specification*, Release 6.3 02-300360 June 2014

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

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.