



Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis Unified Communication Version 10 with Avaya Aura® Experience Portal Release 7.0 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis Unified Communication 10 to interoperate with Avaya Aura® Experience Portal. 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.

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 Communication10 (herein after referred to as Prognosis) with Avaya Aura® Experience Portal.

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 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.

2.1. Interoperability Compliance Testing

The feature test of the interoperability compliance testing was to verify Prognosis using Web Services and SNMP Traps to display real-time information and to monitor status of operation on Experience Portal. There are 4 kinds of information of 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**. There were some observations made below:

- The Prognosis Call Load, MPP and Application take 10-20 seconds to start displaying real-time ongoing call of Experience Portal in the web user interface.
- The Prognosis Application shows all VXML and CCXML applications configured in the Experience Portal rather than specific application used for individual call.

2.3. Support

For technical support on Integrated Research 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 Avaya Aura® Experience Portal. The configuration consists of an Avaya S8800 Server running Avaya Aura® Communication Manager with an Avaya G450 Media Gateway providing H.323 trunk 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.

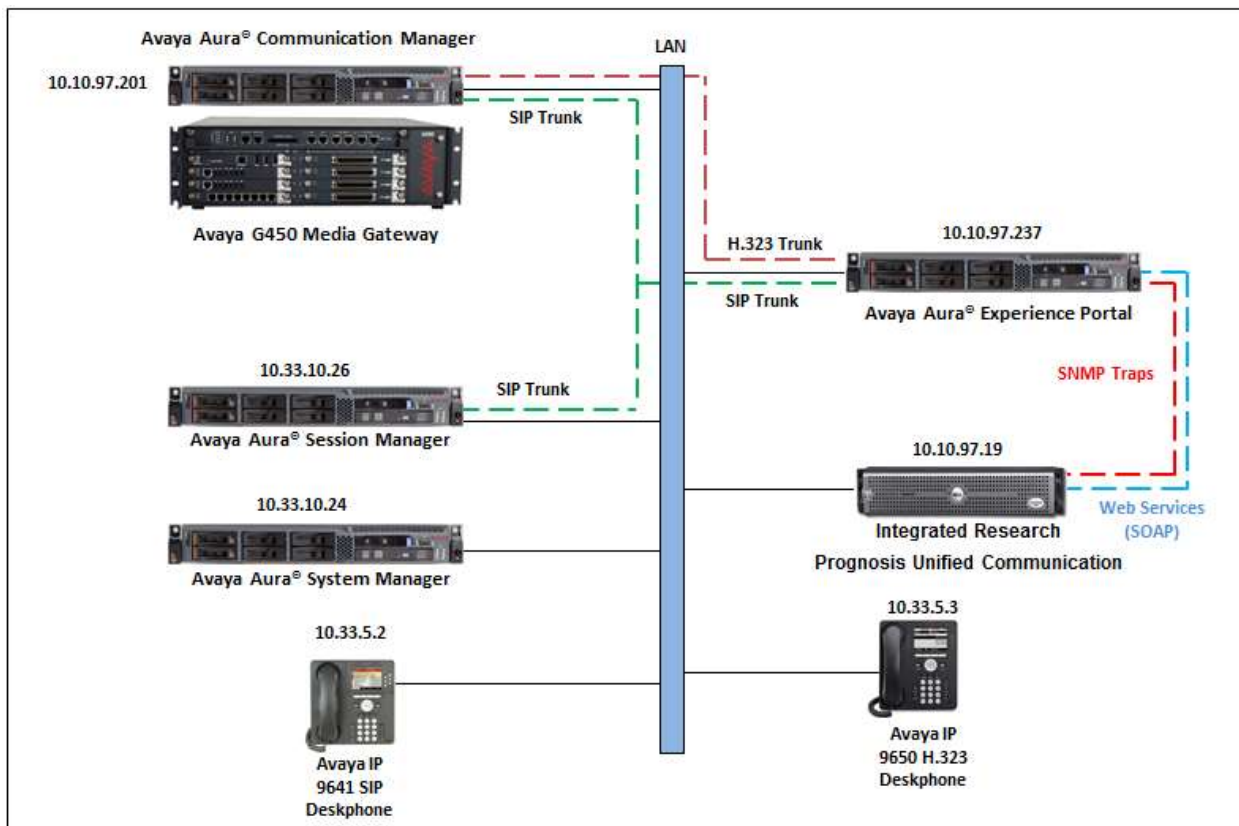


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communicaiton Manager running on Avaya S8800 Server	6.3 SP 8 (R016x.03.0.124.0 w/Patch 21588)
Avaya Media Gateway G450	35.8.0
Avaya Aura® Session Manager	6.3 SP 10 (6.3.10.0.637008)
Avaya Aura® System Manager	6.3.10 Build No. – 6.3.0.8.5682-6.3.8.3204 Software Update Revision No: 6.3.10.7.2275
Avaya Aura® Experience Portal	7.0.1
Avaya 964G1 SIP IP Deskphone	6.4.1.25 (SIP)
Avaya 9650 H.323 IP Deskphone	S3.230A (H.323)
Integrated Search Prognosis Unified Communication	Version 10

5. Configure Avaya Aura® Communication Manager

The configuration of the H323 Trunks between Communication Manager and Experience Portal, and the routing of calls to Experience Portal are 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 the SIP Trunks between Session Manager and Experience Portal, and the routing of calls to Experience Portal are 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.

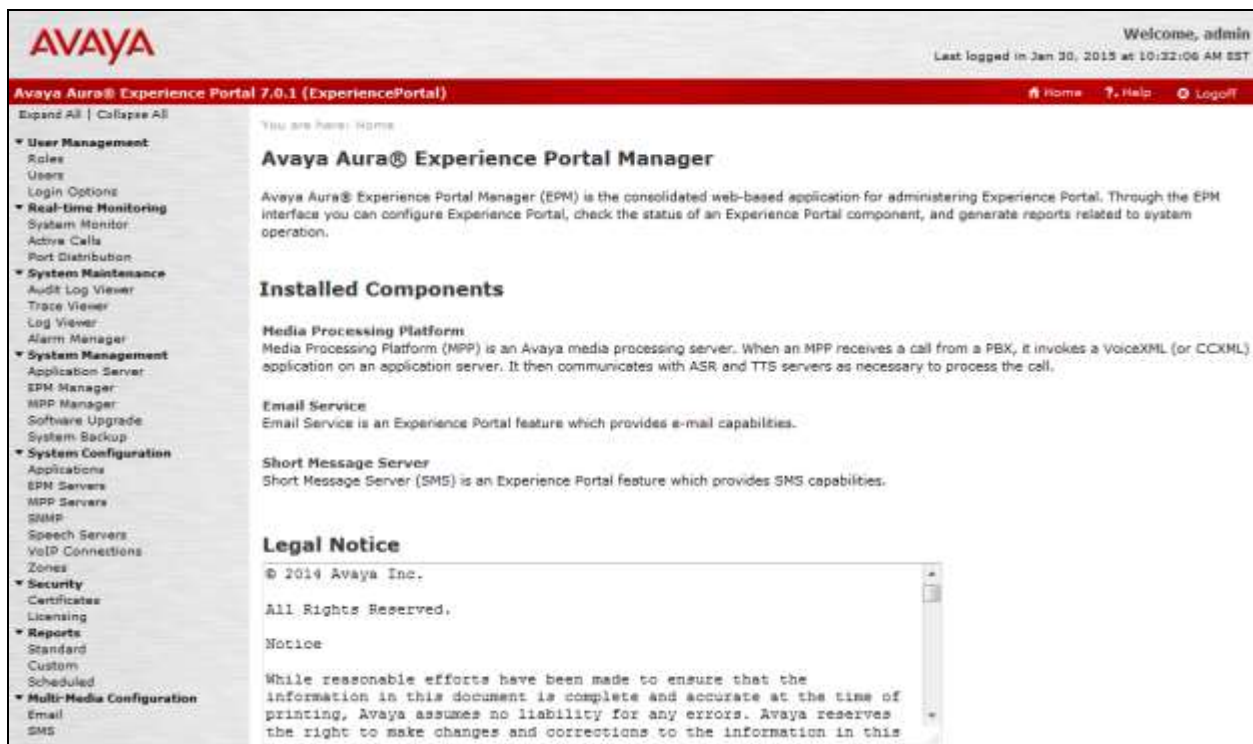
7. Configure Avaya Aura® Experience Portal

The initial administration of Experience Portal and the configuration of the H323 VoIP Connection to Communication Manager and the SIP VoIP Connection to Session Manager are assumed to be in place and will not be discussed here. This section covers the additional procedures 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. 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 the EPM. Log in using the appropriate credentials. The screen shown below is displayed.

Note: All of the screens in this section are shown after the Experience Portal had been configured. Don't forget to save the screen parameters after configuring Experience Portal.



The screenshot displays the Avaya Aura® Experience Portal Manager web interface. At the top left is the Avaya logo. The top right corner shows the user 'Welcome, admin' and the last login time 'Last logged in Jan 30, 2015 at 10:32:06 AM EST'. Below the header is a red navigation bar with 'Avaya Aura® Experience Portal 7.0.1 (ExperiencePortal)', 'Home', 'Help', and 'Logout' links. A left-hand navigation menu is expanded to show categories like 'User Management', 'Real-time Monitoring', 'System Maintenance', 'System Management', 'System Configuration', 'Security', 'Reports', and 'Multi-Media Configuration'. The main content area is titled 'Avaya Aura® Experience Portal Manager' and includes a description of the EPM interface. It also features sections for 'Installed Components' (Media Processing Platform, Email Service, Short Message Server) and a 'Legal Notice' section with copyright information for Avaya Inc. and a disclaimer.

7.1. Configure SNMP Connection

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

- Check on the **Enable SNMP Version 2c** and enter the **Security Name** as “snmpaep”, this security name can be any name and it will be used in Prognosis configuration.
- **Authorized for SNMP Access** – select **Allow All IP Addresses**.
- **Transport Protocol** – Select **UDP**.
- **Port Number** – Select **Default Port Number (UDP: 161)**.

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

The screenshot displays the 'SNMP Agent Settings' page in the Avaya Aura Experience Portal. The page title is 'SNMP Agent Settings' and it includes a breadcrumb trail: 'Home > System Configuration > SNMP > SNMP Agent Settings'. The main content area is divided into several sections:

- SNMP Version 1:** Contains a checkbox for 'Enable SNMP Version 1' (unchecked) and a text input field for 'Security Name'.
- SNMP Version 2c:** Contains a checked checkbox for 'Enable SNMP Version 2c' and a text input field for 'Security Name' containing the value 'snmpaep'.
- SNMP Version 3:** Contains a checkbox for 'Enable SNMP Version 3' (unchecked) and three text input fields for 'Security Name', 'Authentication Password', and 'Privacy Password'.
- Authorized for SNMP Access:** Contains two radio button options: 'Allow All IP Addresses' (selected) and 'Allow Only the Following:'. Below this are five text input fields for 'IP Address/Hostname 1' through 'IP Address/Hostname 5'.
- Transport Protocol:** A dropdown menu showing 'UDP'.
- Port Number:** Two radio button options: 'Default Port Number (UDP: 161)' (selected) and 'Custom Port Number:' with an empty text input field.

At the bottom of the page, there are four buttons: 'Save', 'Apply', 'Cancel', and 'Help'.

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 for the **Add SNMP Trap Configuration**.

- **Enable** – Select **Yes**.
- **Device** – Select **NMS**.
- **Transport Protocol** – Select **UDP**.
- **Host Address** – Enter the IP address of Prognosis server **10.10.97.19**.
- **Port** – Use the port **162**.
- **Notification Type** – Select **Trap**.
- **SNMP Version** – Select version **2c**.
- **Security Name** – Obtain this name from Prognosis, in this case the security name is **Prognosis**.

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

The screenshot displays the Avaya Aura Experience Portal 7.0.1 interface. The top navigation bar shows the Avaya logo, the user name 'admin', and the last login time '10:27:05 AM EST'. The main navigation menu on the left includes sections for User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The 'System Configuration' section is expanded, showing 'SNMP' as the selected option. The main content area displays the 'Add SNMP Trap Configuration' page, which includes a breadcrumb trail: 'Home > System Configuration > SNMP > Add SNMP Trap Configuration'. The page contains a form with the following fields and values: 'Enable' (radio buttons for Yes and No, with 'Yes' selected), 'Device' (dropdown menu set to 'NMS'), 'Transport Protocol' (dropdown menu set to 'UDP'), 'Host Address' (text input field containing '10.10.97.19'), 'Port' (text input field containing '162'), 'Notification Type' (dropdown menu set to 'Trap'), 'SNMP Version' (dropdown menu set to '2c'), 'Security Name' (text input field containing 'Prognosis'), 'Authentication Protocol' (dropdown menu set to 'None'), 'Authentication Password' (empty text input field), 'Privacy Protocol' (dropdown menu set to 'None'), and 'Privacy Password' (empty text input field). At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Help'.

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 Settings** button the **EPM Settings** page is displayed. In the **Outcall** subsection of the **Web Service Authentication** section, enter username **outcall** in the **User Name** field and its password e.g. **outcall123** in the **Password** field, keep other fields at default values. Note that the outcall authentication username and password can be any desired values that are accepted by Experience Portal.

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

The screenshot shows the Avaya Aura Experience Portal 7.0.1 configuration interface. The top navigation bar includes the Avaya logo, the user name 'admin', and the last login time '11:13:46 AM EST'. The main navigation menu on the left lists various system management options, with 'System Configuration' expanded to show 'EPM Servers'. The main content area is titled 'EPM Settings' and contains several configuration sections:

- System Parameters:** Experience Portal Name (ExperiencePortal), Number of Application Server Failover Logs (10), and Commands to Retain in Configuration History (50).
- Resource Alerting Thresholds (%):** High Water (90) and Low Water (80).
- Web Service Authentication:**
 - Application Reporting:** User Name (<Default>), Password (masked), and Verify Password (empty).
 - Outcall:** User Name (outcall), Password (masked), and Verify Password (empty).
- Miscellaneous:** A section with a right-pointing arrow.

At the bottom of the page, there are four buttons: **Save**, **Apply**, **Cancel**, and **Help**.

7.3. Configure Applications

Speech application is a central operation of Experience Portal. When a caller dials in to the system, the Media Processing Platform (MPP) accesses appropriate speech application to control the call based on DNIS. From that point on, the speech application directs the flow of the call until the caller hangs up or the application is finished. To configure speech application, navigate to **System Configuration → Applications**. The **Applications** page is displayed in the right.

The screen below shows a list of pre-configured speech applications on Experience Portal. In the compliance test, these applications were used to verify appropriate display of the applications on the Prognosis console.

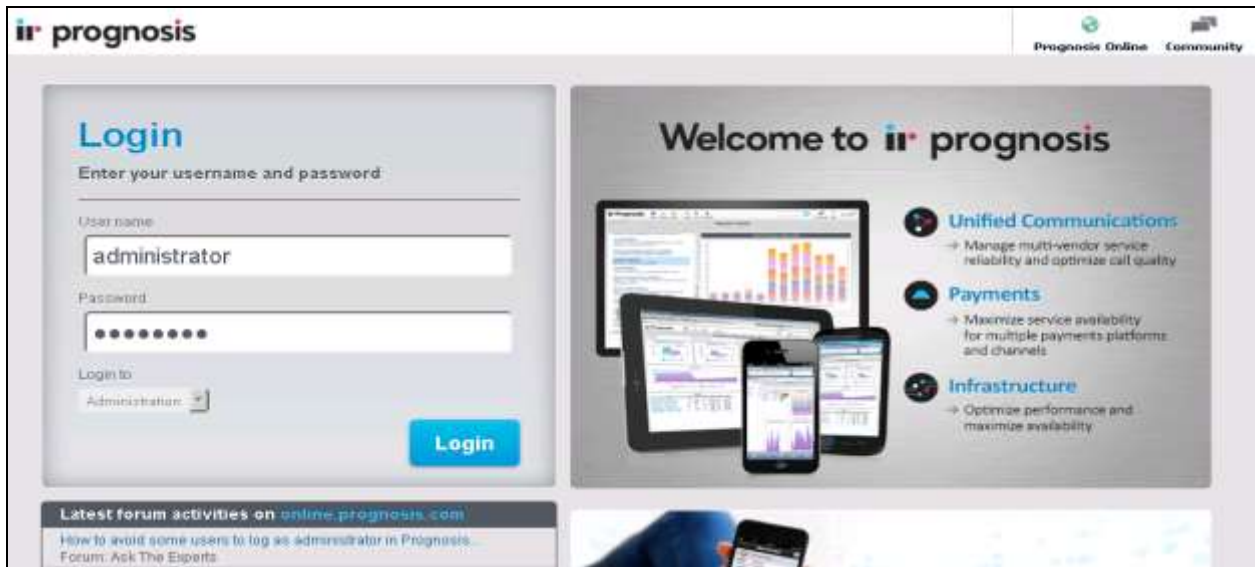
The screenshot shows the Avaya Aura Experience Portal 7.0.1 interface. The top navigation bar includes the Avaya logo, the user name 'admin', and the login time 'Last logged in today at 11:13:46 AM EST'. The main header indicates the current page is 'Applications' under 'System Configuration'. A left-hand navigation menu lists various system management and configuration options. The main content area displays a table of applications with the following data:

Name	Enable	Type	URI	Launch	ASR	TTS	Requested SIP Calls	Configurable Application Variables
test1	Yes	VoiceXML	http://10.97.237/mpp/misc/avptestapp/intro.vxml	Outbound	No ASR	No TTS	None	
test2	Yes	CCXML	http://10.97.237/mpp/misc/avptestapp/root.ccxml	Outbound	No ASR	No TTS	None	
Test_App	Yes	VoiceXML	http://10.97.237/mpp/misc/avptestapp/intro.vxml	4001	No ASR	No TTS	None	
Test_App_CCXML	Yes	CCXML	http://10.97.237/mpp/misc/avptestapp/root.ccxml	4002	No ASR	No TTS	None	
Test_vxml_H323	Yes	VoiceXML	http://10.97.237/mpp/misc/avptestapp/intro.vxml	60343, 60380-60384	No ASR	No TTS	None	

At the bottom of the table, there are buttons for 'Add', 'Delete', 'Clear MPP Cache', and 'Help'. A 'Launch Order' link is also present in the top right of the table area.

8. Configure Integrated Research Prognosis Unified Communication

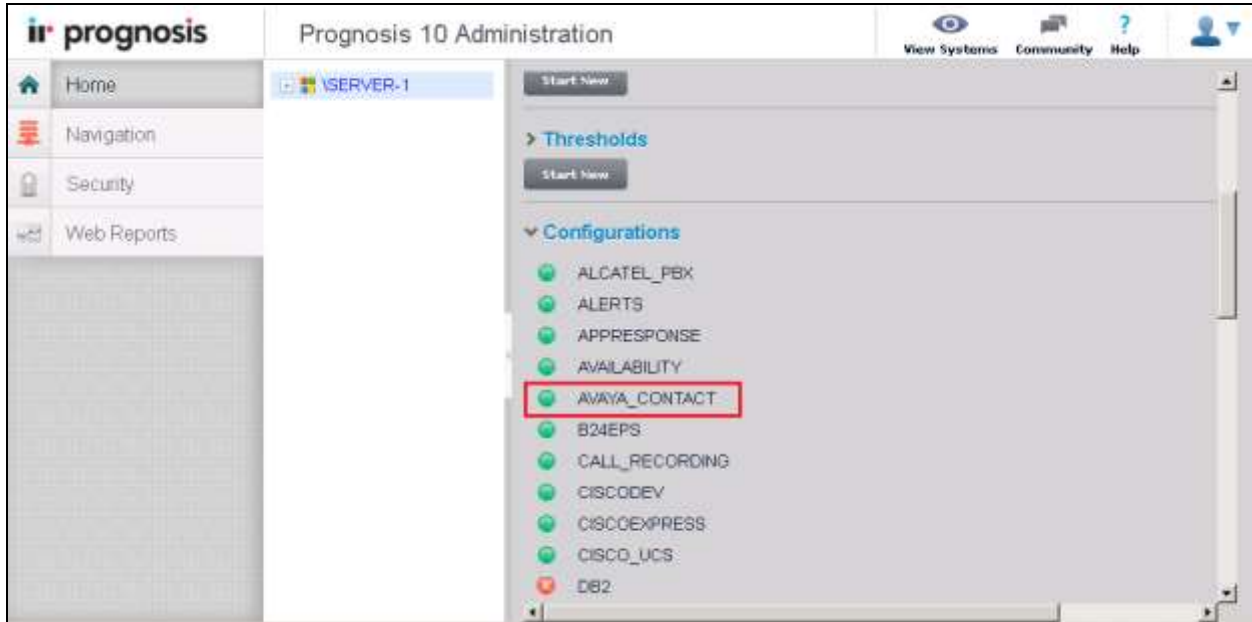
This section describes the configuration of Prognosis required to interoperate with Experience Portal. Log in to the Prognosis server with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Administration** and log in with the appropriate password.



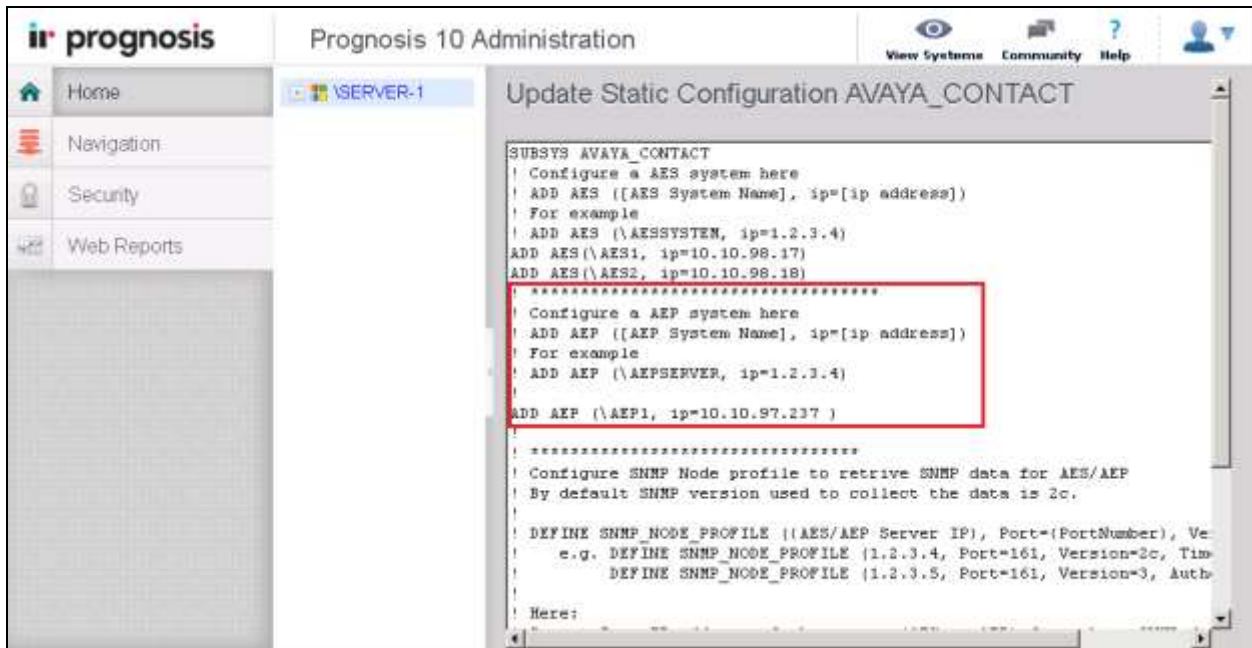
The **Prognosis 10 Administration** homepage is displayed as shown below.



Scroll down to **Configuration** section and click on **AVAYA_CONTACT** entry as shown in the screen below to configure for Experience Portal system.



The **Update Static Configuration AVAYA_CONTACT** window is displayed in the right. Enter the entry “**ADD AEP (\AEP1, ip=10.10.97.237)**” for the Experience Portal system in the AVAYA_CONTACT configuration file, in which **10.10.97.237** is IP address of Experience Portal and this IP will be assigned to the name “**AEP1**”, the name “**AEP1**” can be any desired name. Click on **Start** button in the bottom (not shown) to save the configuration.



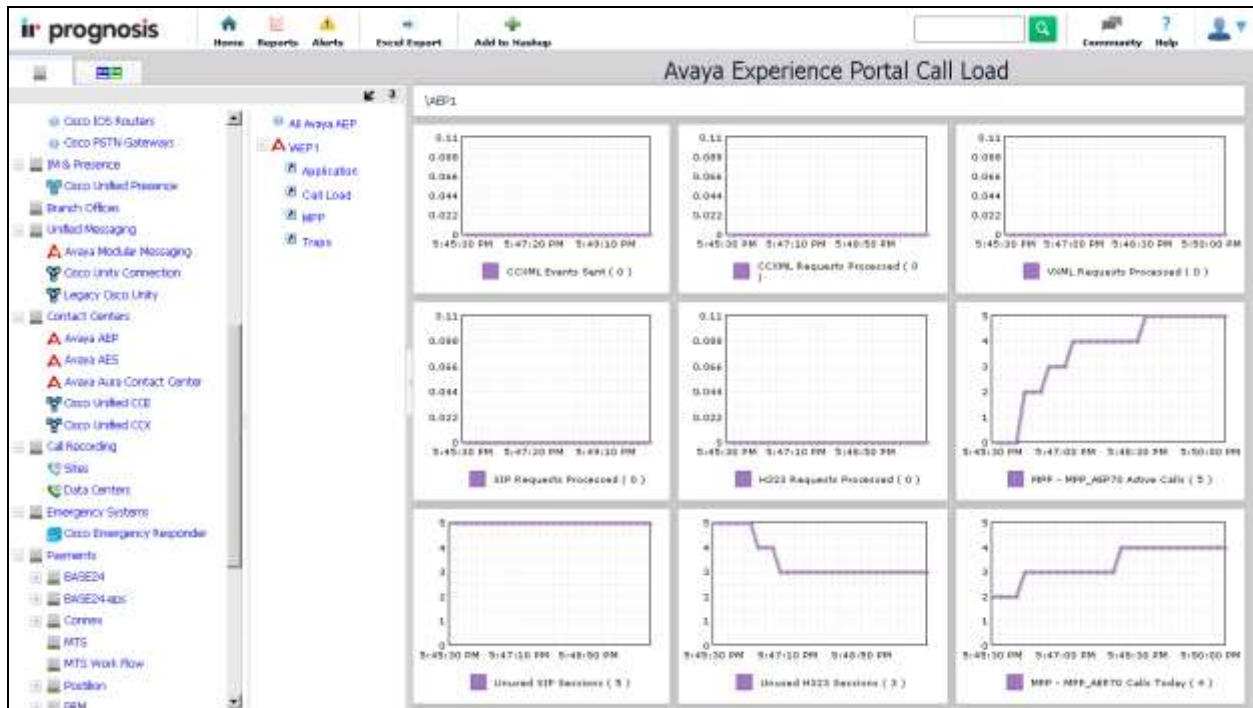
Continue s navigating to **Configuration** → **Password** (not shown). The **Update Password Entries window** is displayed. In the compliance test, two entries of Experience Portal were added. The first entry was **snmpV2c:AEP1** with the password **snmpaep** as configured in **Section 7.1**, the second entry was **soap:\AEP1** using the **outcall** username and its password as configured in **Section 7.2**.



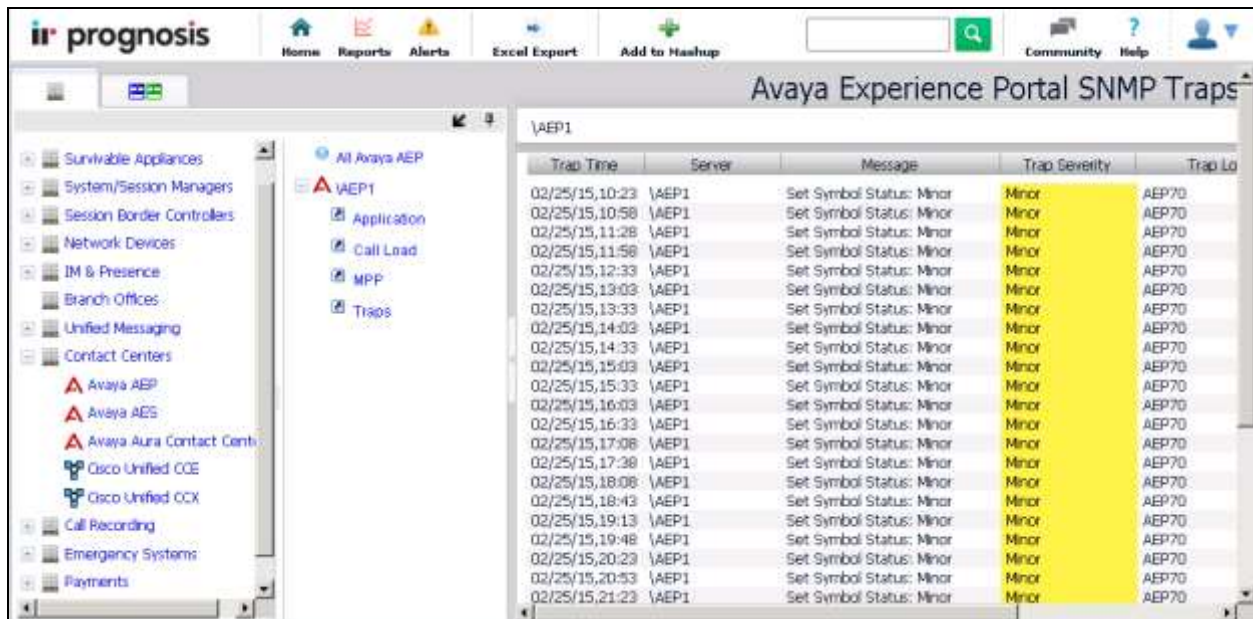
9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Experience Portal and Prognosis.

- From the Prognosis server, launch Prognosis View System to open the Prognosis web user interface, select the Avaya AEP instance in the left navigation pane. The Experience Portal server instance is displayed in the medium column. There are four types of information that Prognosis collect and monitor from Experience Portal: SNMP Traps, MPP, Call Load and Application.
- Place multiple calls to Experience portal, select Call Load to open the Avaya Experience Call Load in the right hand side. Verify the Call Load shows correct ongoing calls and statistic of Experience Portal in the web user interface.



- To verify whether the Prognosis UC application is able to receive and display the SNMP traps sent from the Experience Portal, select **Traps** to open **Avaya Experience Portal SNMP Traps** window in the right hand side.



10. Conclusion

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

11. Additional References

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

- [1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, Issue 14.0, December 2014, Document Number 555-245-205.
- [2] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 10.0, June 2014, Document Number 03-300509.
- [3] *Administering Avaya Aura® Experience Portal, Release 7.0, Issue 1, Dec 2013*.
- [4] *Troubleshooting Avaya Aura® Experience Portal, Release 7.0, Issue 1, Dec 2013*.
- [5] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 7, September 2014*.

The following Prognosis documentations are provided by Integrated Research. Documents are also provided in the online help that comes with the software Package.

- [6] *Prognosis 10 Deployment and Installation Guide*, 31st October 2013

©2015 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.