Avaya Solution & Interoperability Test Lab

Application Notes for Virsae Service Management with Avaya Aura® Experience Portal - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R135 to interoperate with Avaya Aura® Experience Portal R7.2.3.

Virsae Service Management provides real-time monitoring and management solutions for IP telephony networks. Virsae Service Management 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.

Virsae Service Management monitored Experience Portal using SNMP and Linux shell access and displayed monitored data on a 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 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 Virsae Service Management (herein after referred to as VSM) with Avaya Aura® Experience Portal (herein after referred to as Experience Portal). VSM is a cloud-based service management platform that brings visibility, service transparency and cost savings to Unified Communications environments over the short, medium and long term.

In this compliance testing, Experience Portal setup comprise of an Experience Portal Manager (EPM) and a Media Processing Platform (MPP). VSM uses Linux shell access connection to monitor statistics such as CPU, Memory and Disk Usage and services status detail and SNMP to capture alarms, and display monitored data on web-based application.

2. General Test Approach and Test Results

The general test approach was to verify VSM using SNMP and Linux shell access connection to monitor and display system status from EPM and MPP.

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 VSM utilized enabled capabilities of encrypted SSH and non-encrypted SNMP as requested by Virsae.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third-party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager or the Telnet/SSH interface to interact with other Avaya products. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use of these interfaces as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the interfaces in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using these interfaces. Using these interfaces in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real-time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Avaya Product Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. For feature testing, VSM dashboard was used to view the configurations of both EPM and MPP such as the memory and CPU utilizations, disk usage and, Trunk and Application status from data collected via SSH.

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

2.2. Test Results

All test cases passed successfully

2.3. Support

For technical support on Virsae Service Management, contact the Virsae Support Team at:

- Tel: +1 800 248 7080 (Americas)
  +44 0808 234 2729 (UK and Europe)
  +64 9 477 0696 (Asia Pacific)
- Email: support@virsae.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify the VSM application with Experience Portal. In the compliance Communication Manager with a G430 Media Gateway connected to Experience Portal via SIP and H.323 Trunks. The system has Workplace Client for Windows and one-X® Communicator (SIP and H.323) softphones configured for making and receiving calls. VSM was installed on a server running Microsoft Windows Server 2016. Architecturally the VSM Service relies on an appliance being placed on a corporate LAN and being configured to connect to a Unified Communication platform as well as the Microsoft Azure cloud via the internet. The VSM appliance contains Probe Service use to collect service management data. The VSM appliance acts as a collector and compresses, encrypts then forwards data from all sources to the Virsae cloud computing service. A PC/Laptop is used to access the Virsae portal to manage VSM services, add additional users and view reporting data on the equipment being managed.

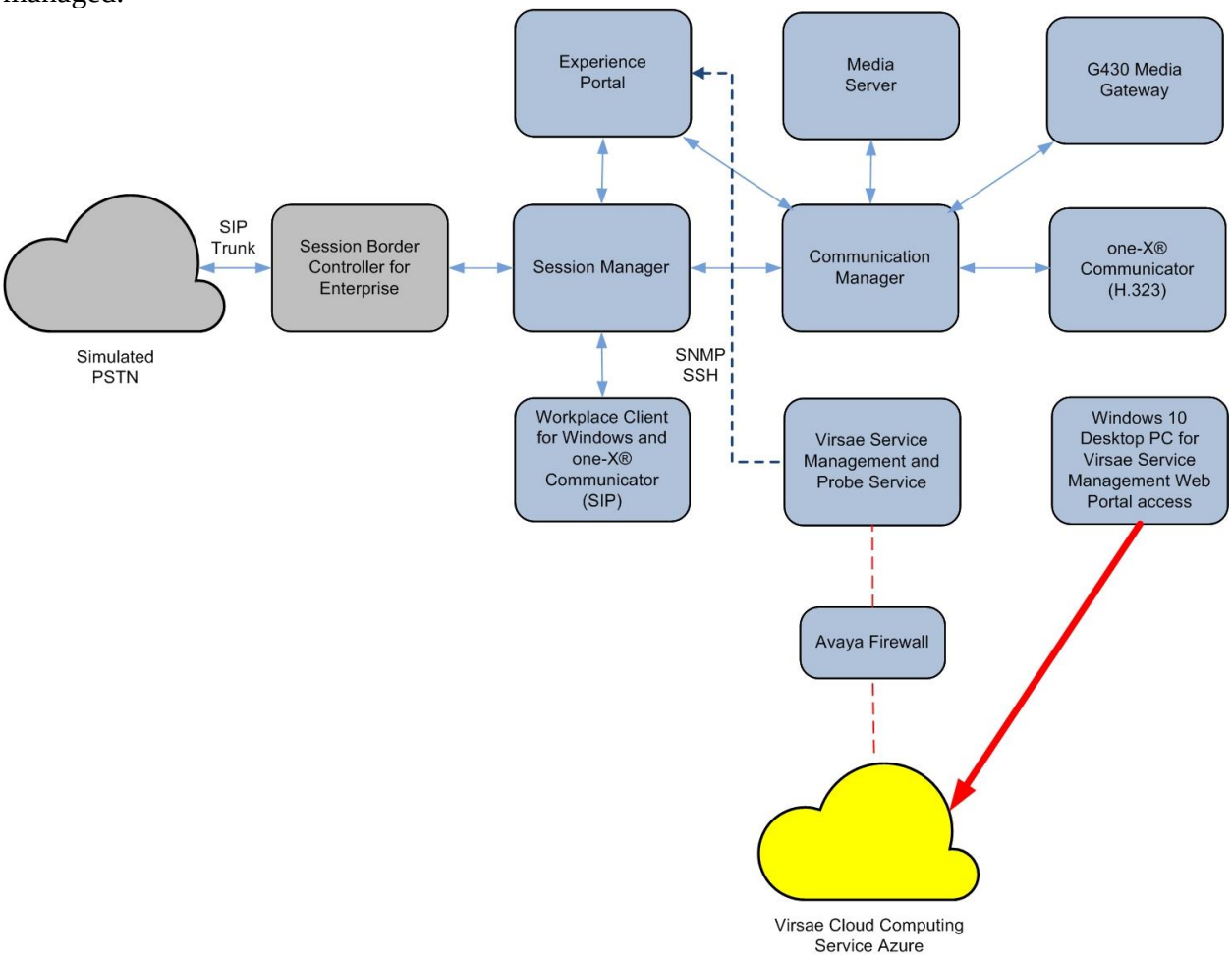


Figure 1: Test Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Experience Portal running on virtual server • EPM • MPP	 7.2.3.0.0494 7.2.3.0.0494
Avaya Aura® Session Manager running on virtual server	8.1.2.1.812101
Avaya Aura® System Manager running on virtual server	8.1.2.0.0611588
Avaya Aura® Communication Manager running on virtual server	8.1.2.0.0-FP2
Avaya G430 Media Gateway	41.16.0
Avaya Aura® Media Server running on virtual server	8.0.2.93
Avaya Workplace Client for Windows	3.9.0.84.8
Avaya one-X® Communicator (SIP and H.323)	6.2.12.04-FP14
Virsae Service Management and Probe Service running on Windows 2016	R135

5. Configure Avaya Aura® Communication Manager

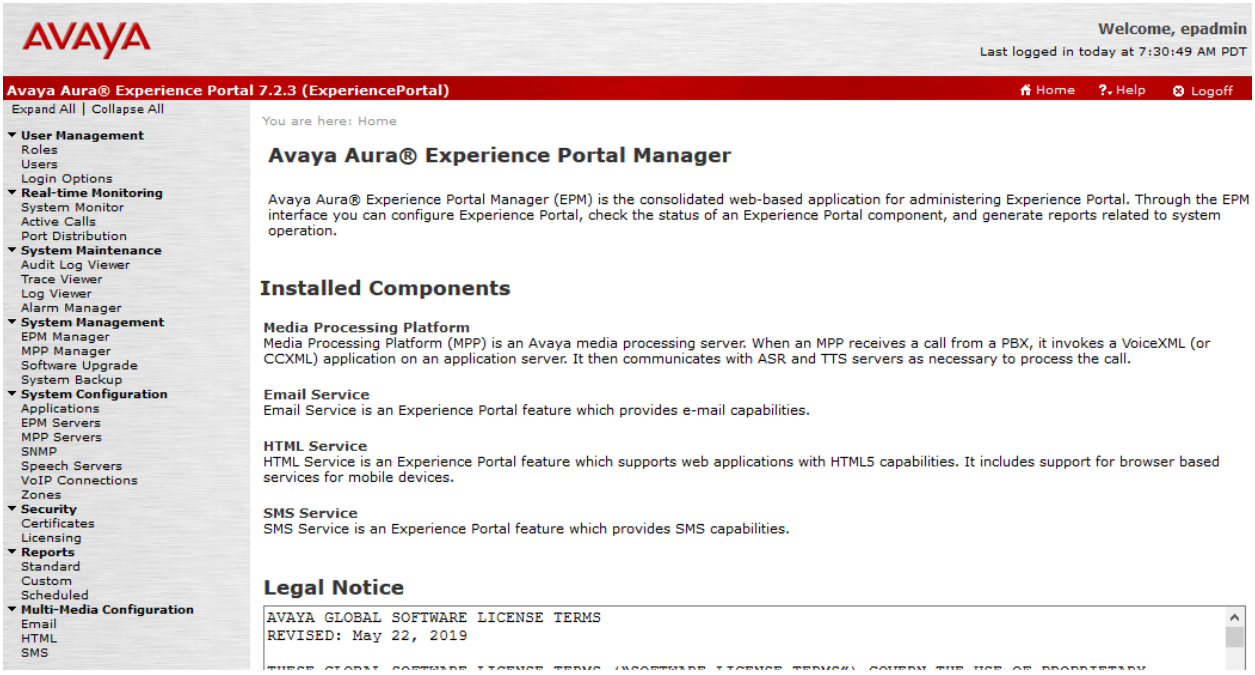
The configuration of Communication Manager and Experience Portal is assumed to be in place and will not be discussed in this document. For more information of how to configure Communication Manager and Experience Portal, please refer to **Section 10**.

6. Configure Avaya Aura® Experience Portal

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

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

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

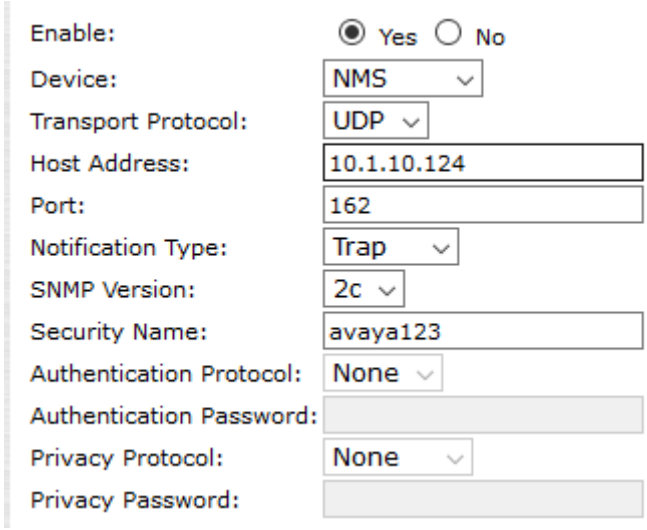


6.1. Configure SNMP Connection

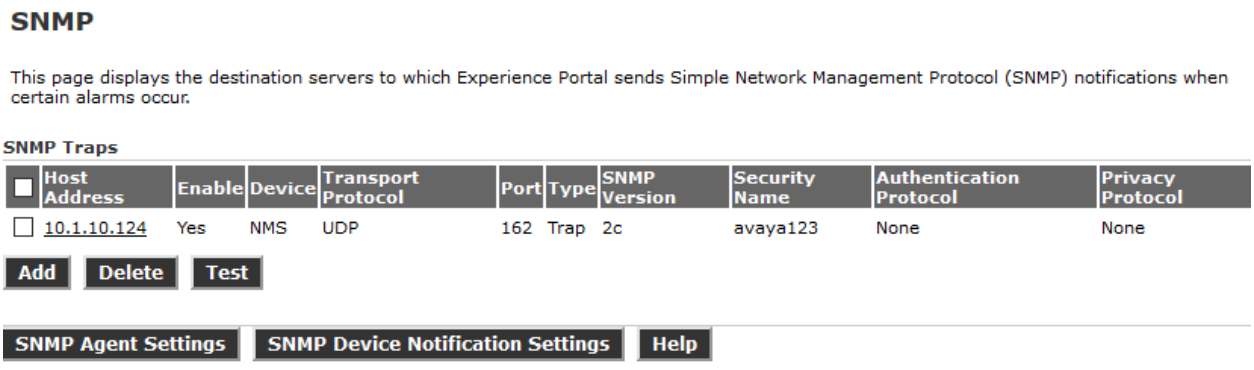
From the home page, navigate to **System Configuration → SNMP** and click **Add**. Configure the following for SNMP Traps:

- Select the **Enable** dot.
- **Device**: Select the **NMS**.
- **Transport Protocol**: Select **UDP**.
- **Host Address**: Enter the VSM server IP address.
- **Notification Type**: Select **Trap**.
- **SNMP Version**: Select **2c**.
- **Security Name**: Enter a desired name.

Leave the rest as default. A screen shot of the configuration is shown below.



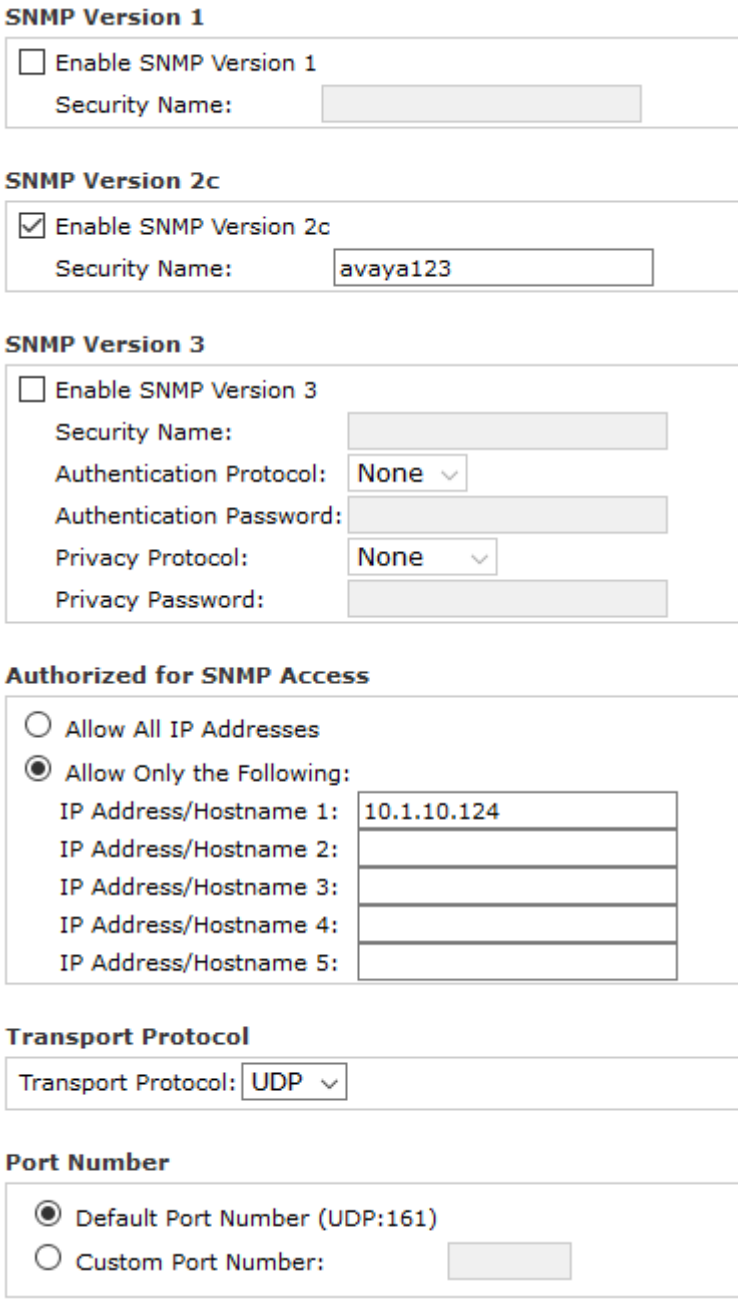
The result screen is shown below. Click on **SNMP Agent Settings**.



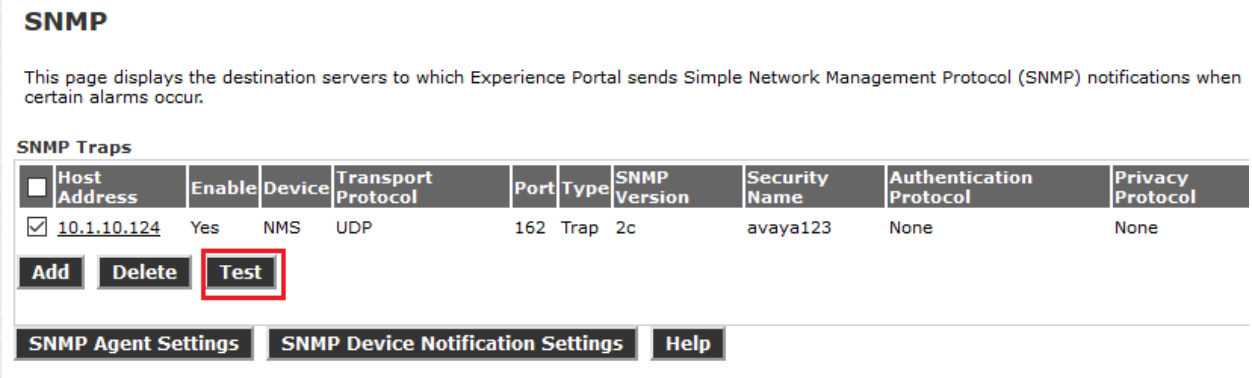
Configure the SNMP query settings for the following:

- Tick **Enable SNMP Version 2c**.
- **Security Name**: Enter a desired name. The same name was used for the SNMP trap in this compliance testing.
- Select **Allow Only the Following** and enter **IP Address/Hostname 1** as the VSM server IP address.
- **Transport Protocol**: Select **UDP**.
- **Port Number**: Select **Default Port Number (UDP:161)**.

Below is a screen shot of the above configuration.



To generate a test alrm, select the **SNMP Traps** destination created earlier and click the **Test** button.



6.2. Configure Login Group

Create an administrator account on Experience Portal since VSM requires access to EPM with Administrative Rights. The new account should be like the default administrator account. Login to EPM console with root access and run the following command.

```
useradd <NAME>            ;Add User
id <NAME>                 ;Check User group
usermod -g 497 <NAME>     ;Modify User group to avayaavpgroup
passwd <NAME>             ;Enter password twice
chage -M 99999 <NAME>     ;Lengthen the expiry date of account
```

Repeat the creation of an administrator account above with MPP.

7. Configure Virsae Service Management

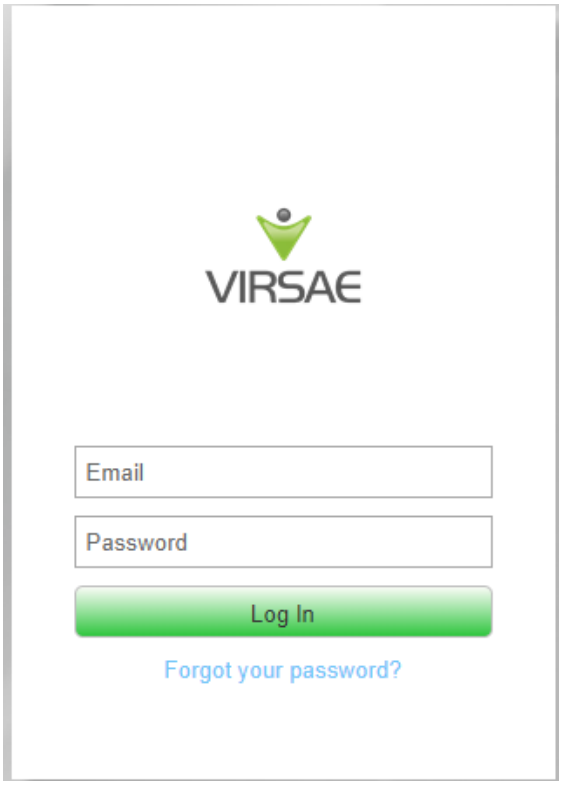
This section describes the configuration of VSM required to interoperate with Experience Portal.

This section provides a "snapshot" of VSM configuration used during compliance testing. Virsae creates the Business partner portal in the cloud environment and is beyond the scope of this Application Notes. The screen shots and partial configuration shown below, are provided only for reference. These represent only an example of the configuration GUI of VSM, available through the web Portal. Contact Virsae for details on how to configure VSM. The configuration operations described in this section can be summarized as follows:

- Login to the Web Portal
- Configuring Avaya Aura® Experience Portal
- Configure Dashboard

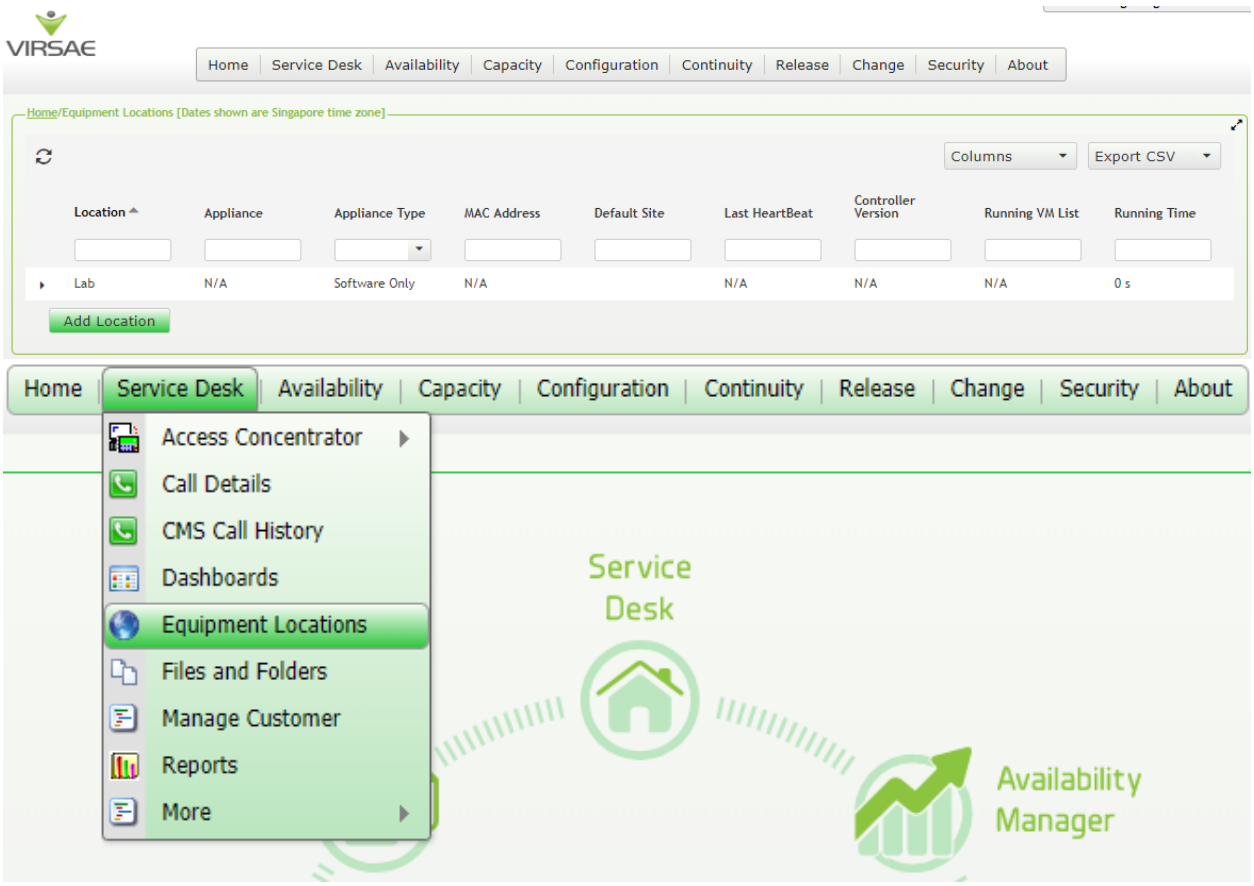
7.1. Login to the Web Portal

A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL *<business partner name>.virsae.com* in a web browser. During compliance testing the URL used was "*preview.virsae.com*". The Login screen is shown as below. Enter the **Email** and **Password** and click on the **Log In** button.

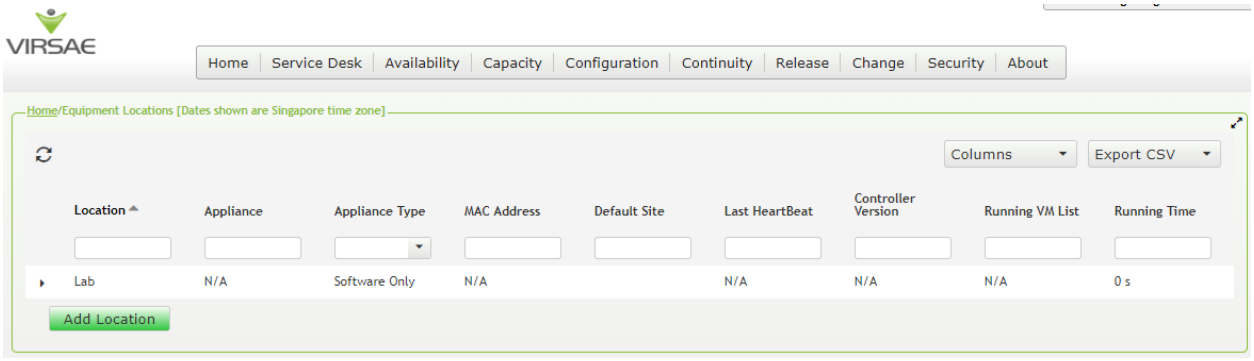


The customer screen is shown. During compliance testing the customer created by Virsae is **Devconnect** as can be seen near the top left corner.

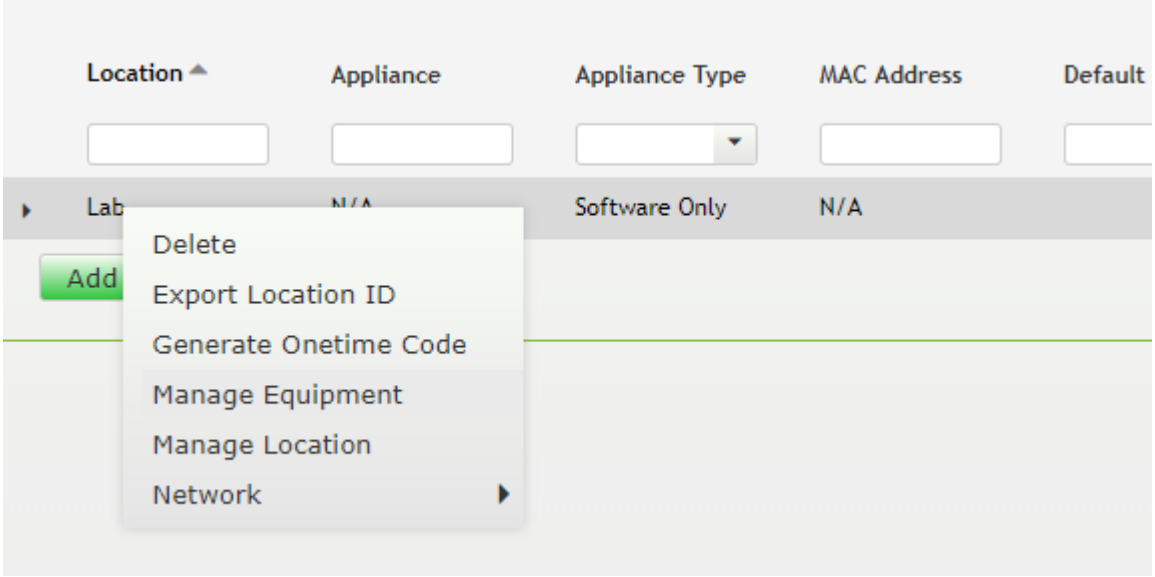
Navigate to **Service Desk → Equipment Locations** as shown below.



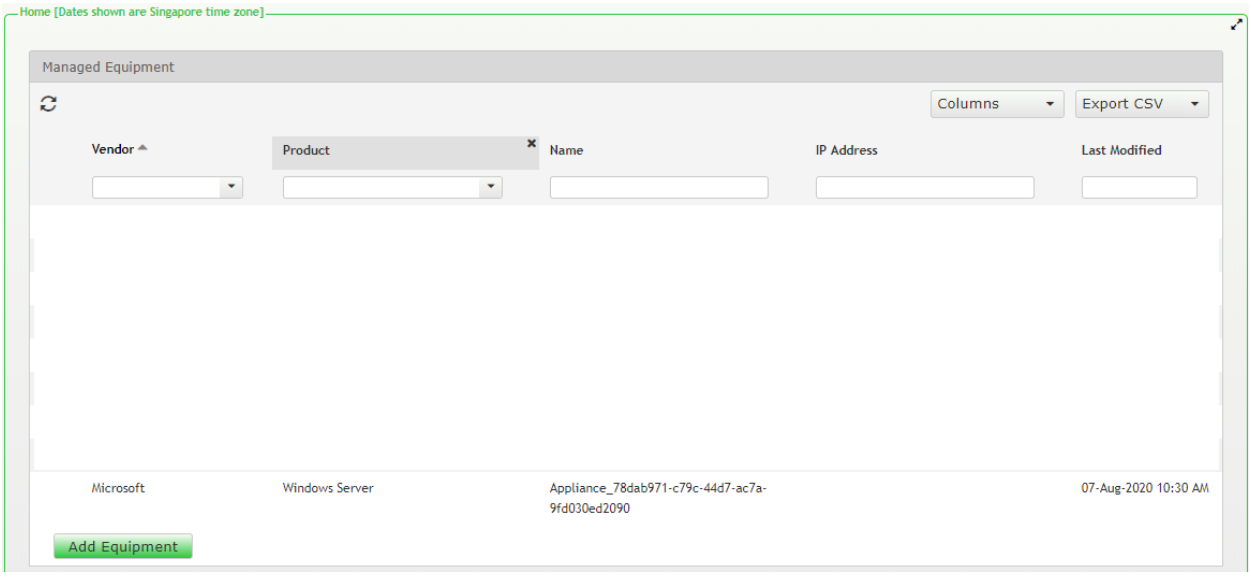
A **Location** called **Lab** is already configured as shown below.



Right click on the **Lab** and select **Manage Equipment**.



Click **Add Equipment** below:

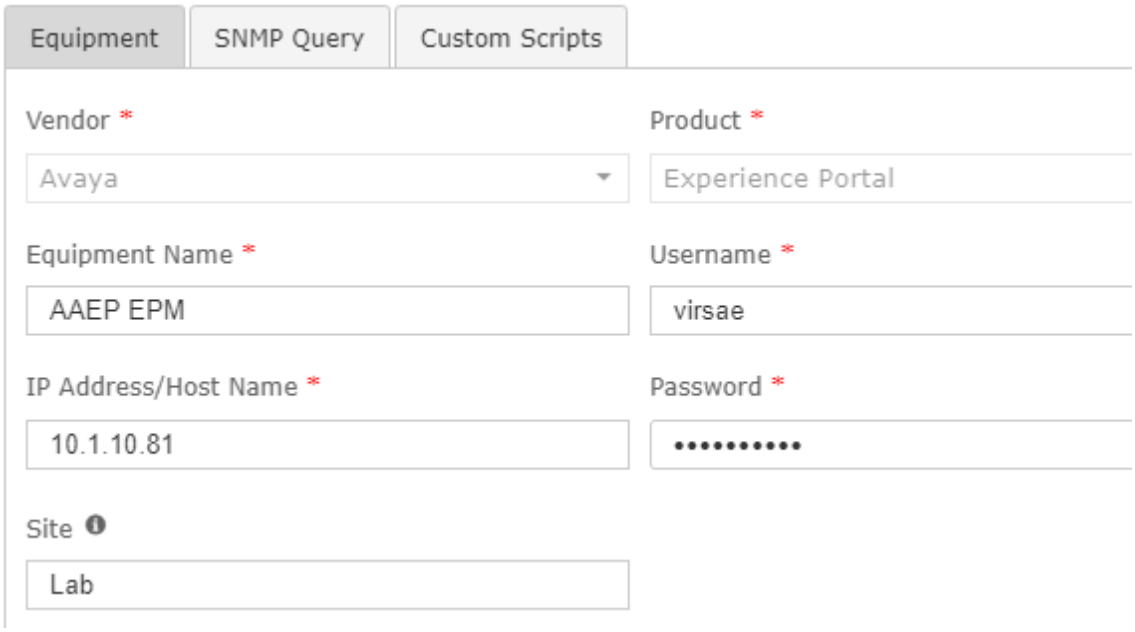


7.2. Configuring Avaya Aura® Experience Portal

From the **Add Equipment** window, add Experience Portal EPM to the Location. Select **Avaya** from the **Vendor** list. Select **Experience Portal** from the **Product** list. Configure the following values.

- **Equipment Name:** A descriptive name say **AAEP EPM**.
- **Username**: The username configured in **Section 6.2**.
- **Password:** The password configured in **Section 6.2**.
- **IP Address/Host Name:** IP address of EPM.
- **Site:** A descriptive site name.

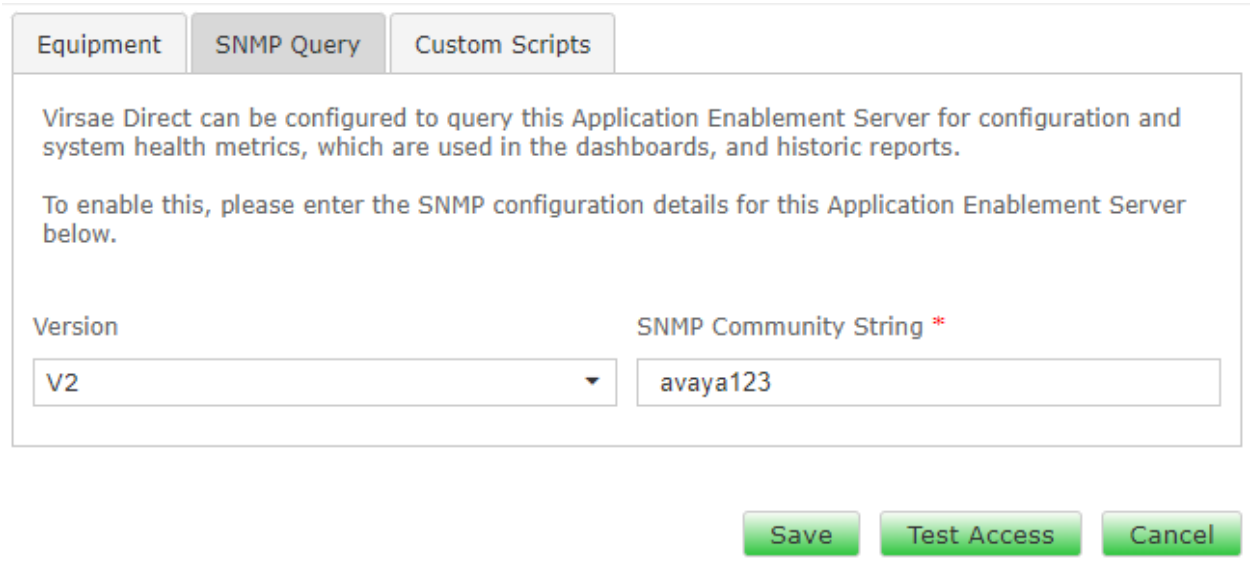
Below are the configured values of the Experience Portal EPM.



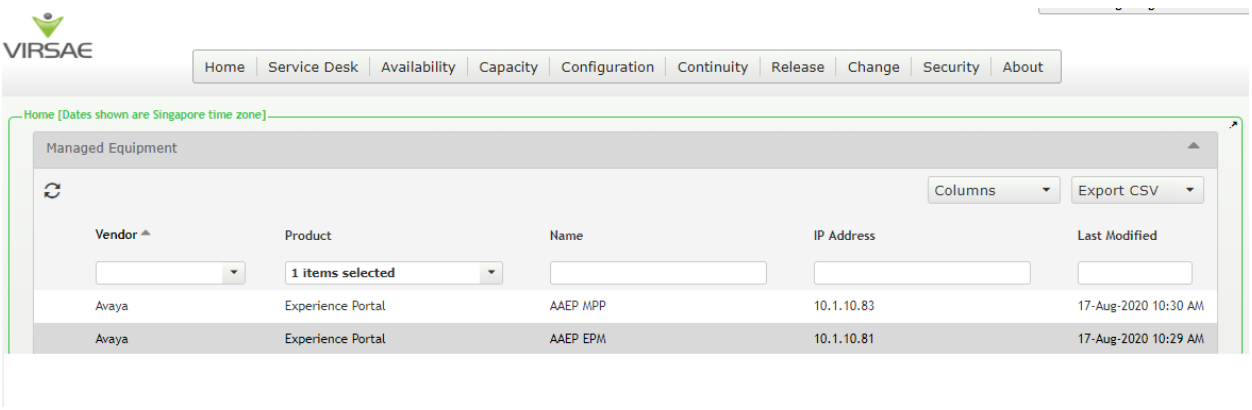
In the **SNMP Query** tab, configure the following values.

- **Version:** Select **V2** from the drop-down menu.
- **SNMP Community String**: Enter the value of the Security Name configured in **Section 6.1**.

Click on the **Save** button to complete the configuration.



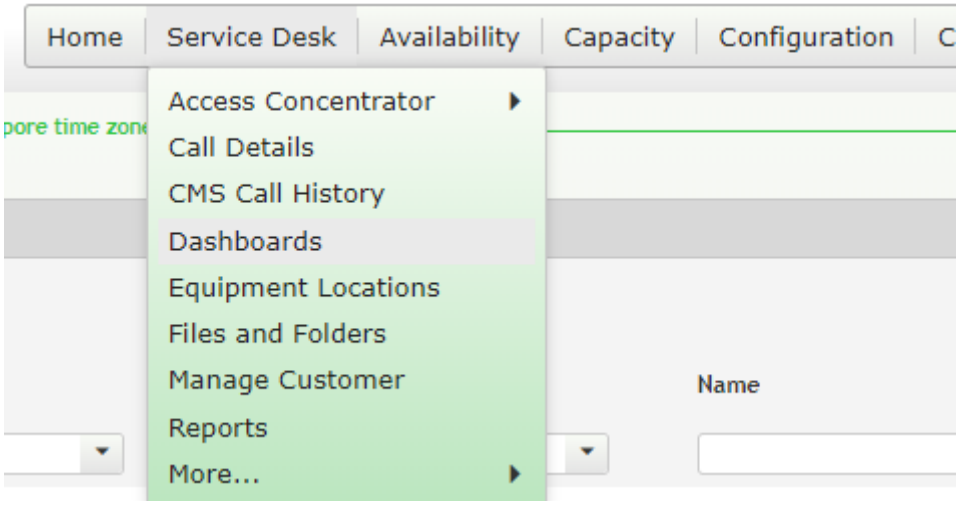
Repeat the steps above for the Experience Portal MPP. The screen below shows the added Experience Portal equipment for EPM and MPP.



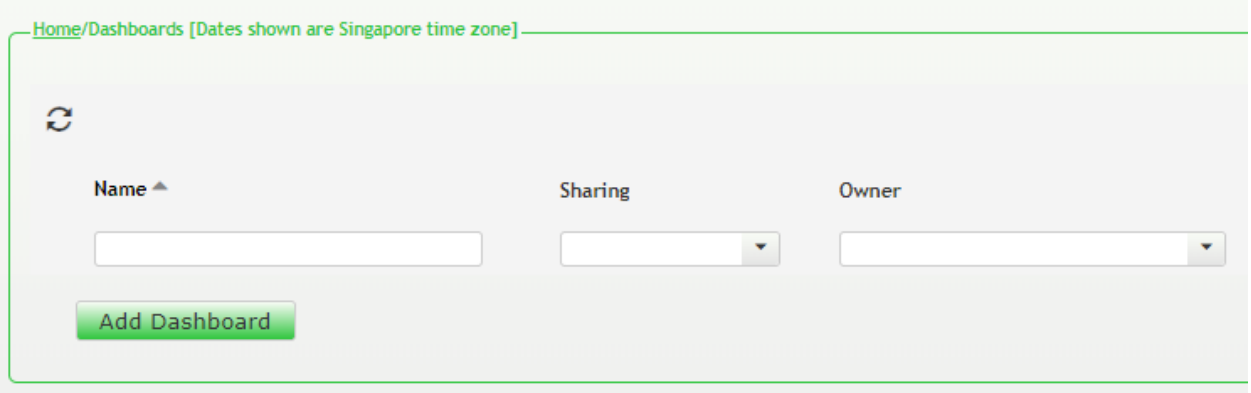
7.3. Configure Dashboard

This section shows the steps to configure Experience Portal on the dashboard.

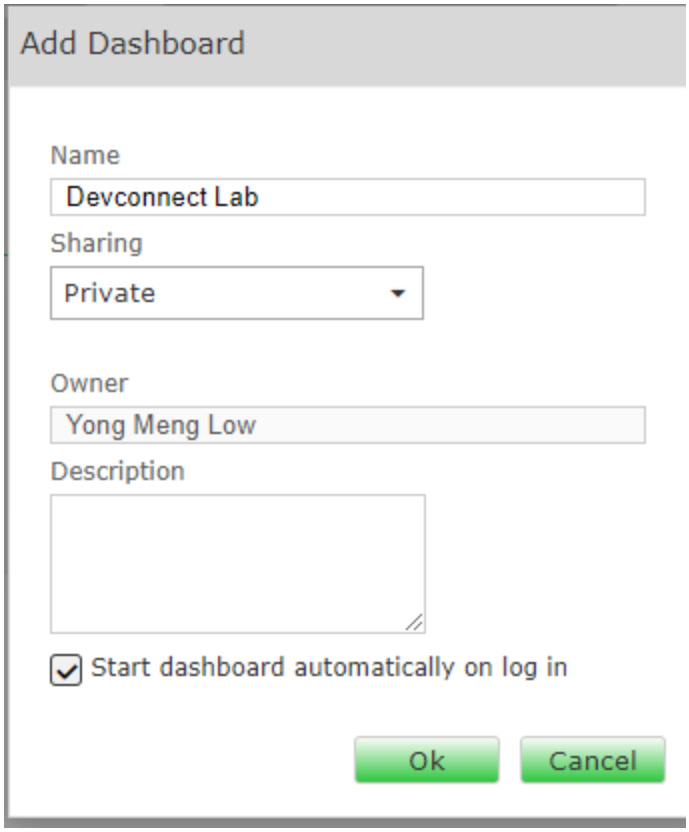
From the home screen, navigate to **Service Desk → Dashboards** as shown below.



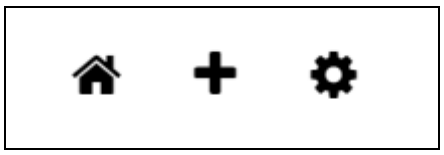
From the **Available Dashboards** window, click on the **Add Dashboard** button.



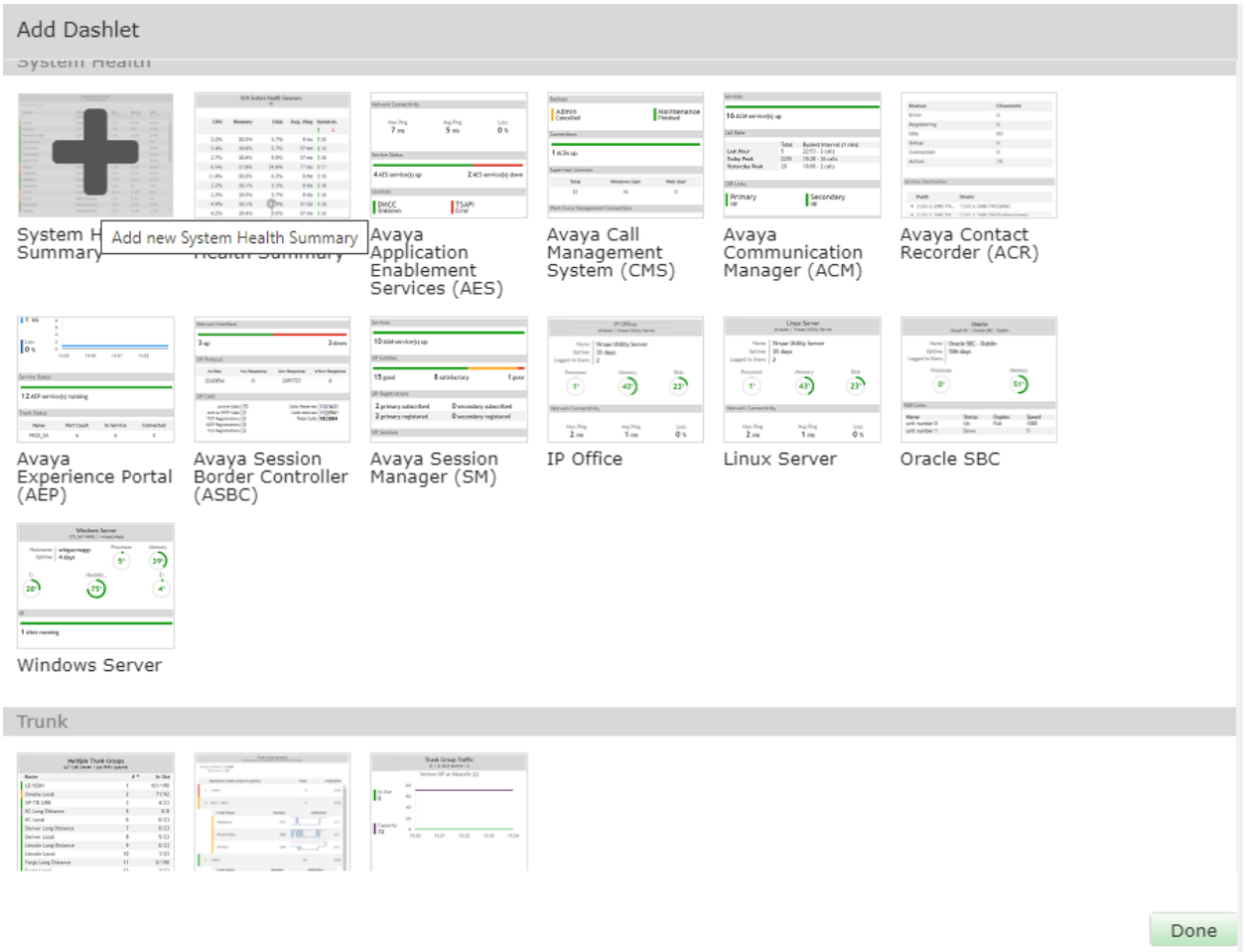
In the **Add Dashboard** window, type a descriptive name for **Name** field as shown below. Retain default values for all other fields. Click on **Start dashboard automatically…** box and then click on **Ok** to submit**.**



In the dashboard window bottom shown below, click on **"+"** sign at the bottom.

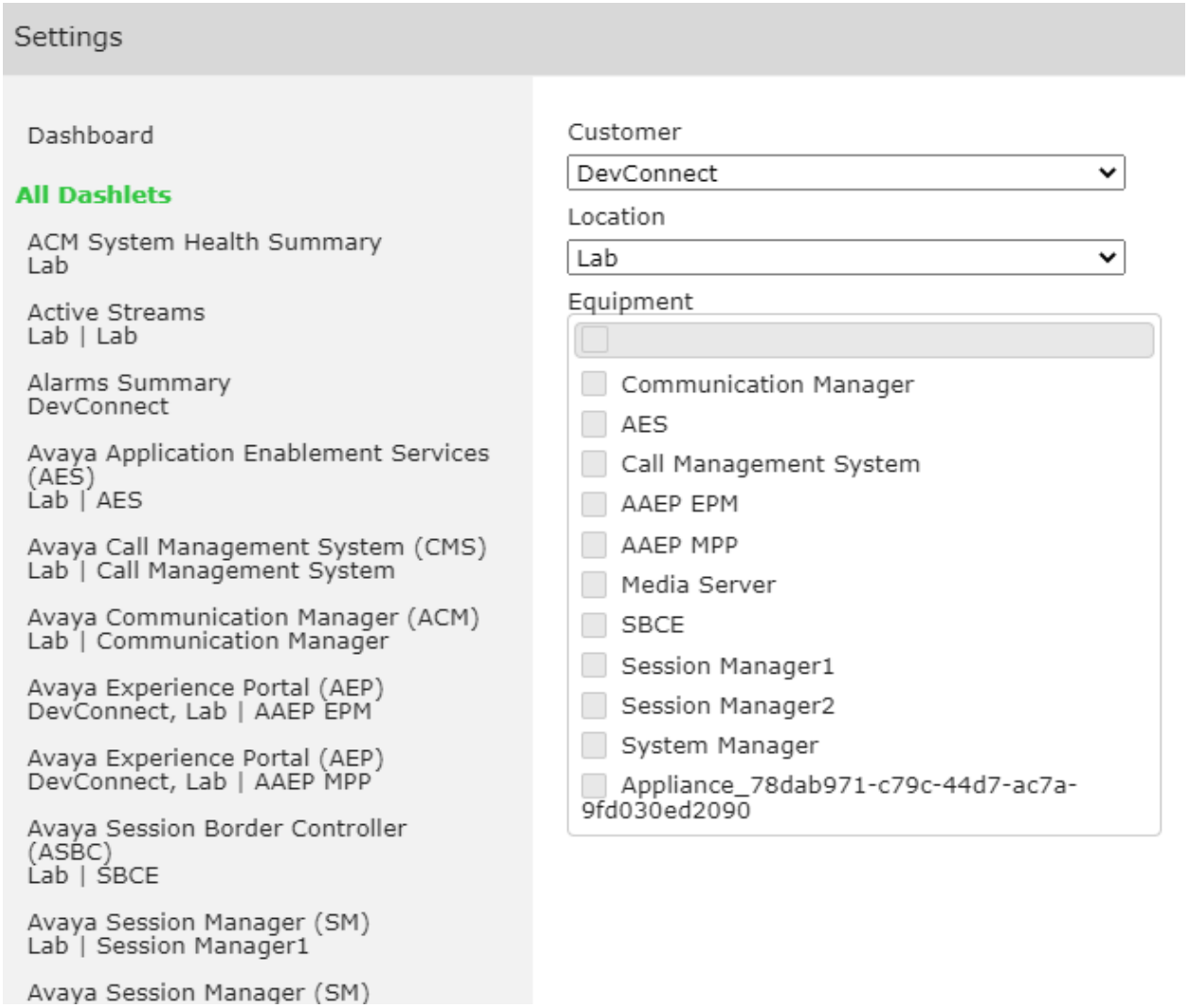


In the **Add Dashlet** window that pops up, select the **System Health Summary** from the available dashlet by hovering the "+" image over it and click **Done**.

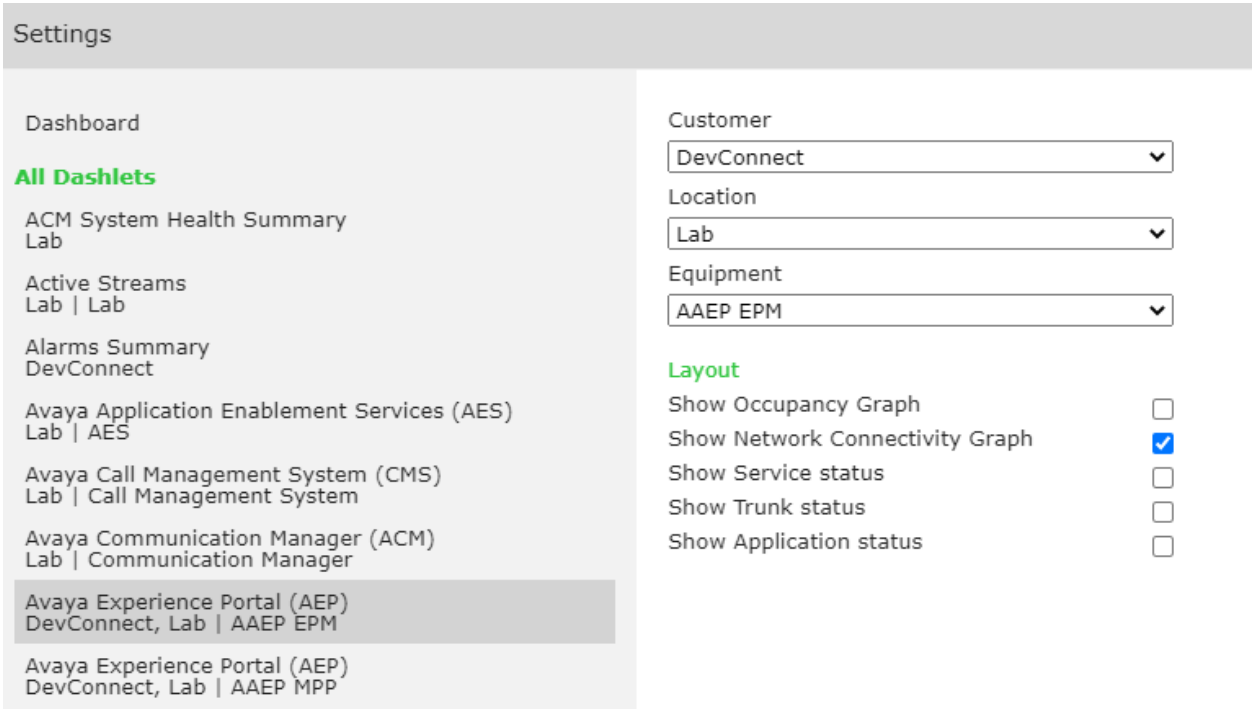


From the **System Health Summary** window, select the **setup wheel** on the top right corner of the box.

Select “Lab” for the **Location** drop-down menu, the appropriate **Equipment** i.e., **AAEP EPM** and **AAEP MPP**. Click **Done** (not shown).



Repeat the same for the **Avaya Experience Portal (AEP)** dashlet by selecting **AAEP EPM** and **AAEP MPP** as equipment.

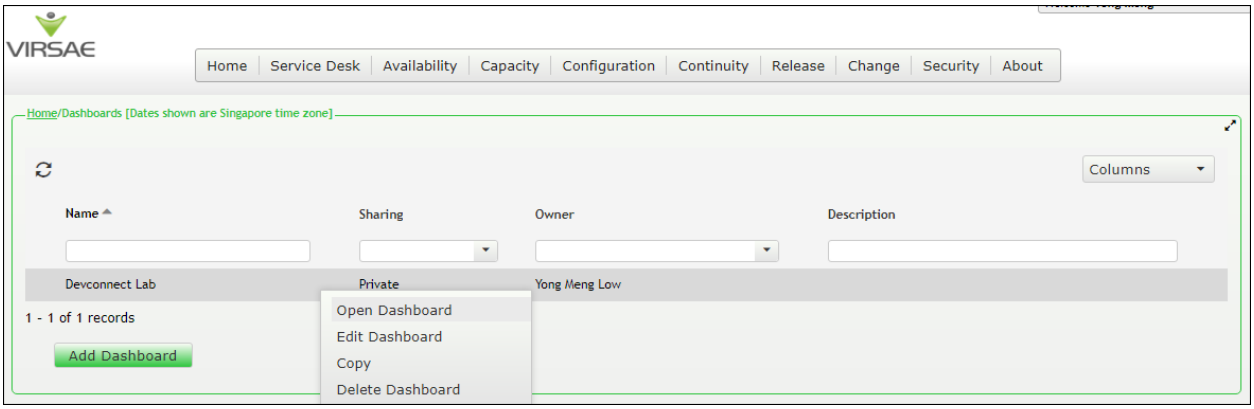


The dashboard with the configured equipment is shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.

8. Verification Steps

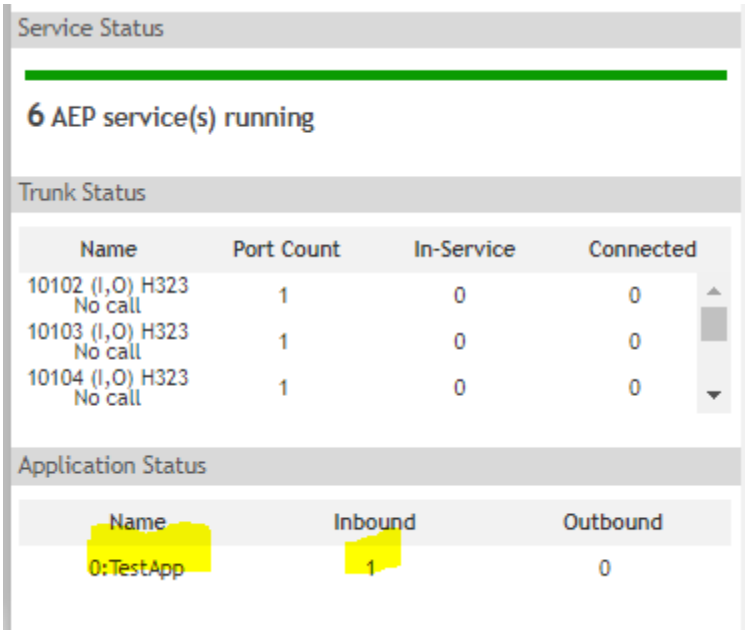
This section provides the tests that can be performed to verify proper configuration of Experience Portal and VSM. The following steps are done by accessing the VSM web portal for the Business partner.

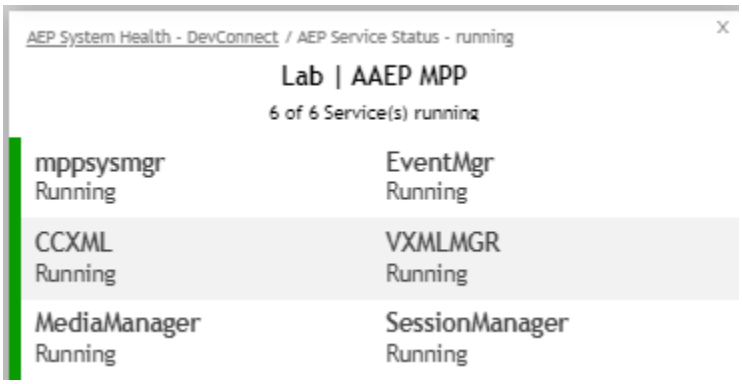
After login to the web portal, navigate to **Service Desk → Dashboard** (not shown) and the screen is shown as below. Right click "Devconnect lab" and select "Open Dashboard".



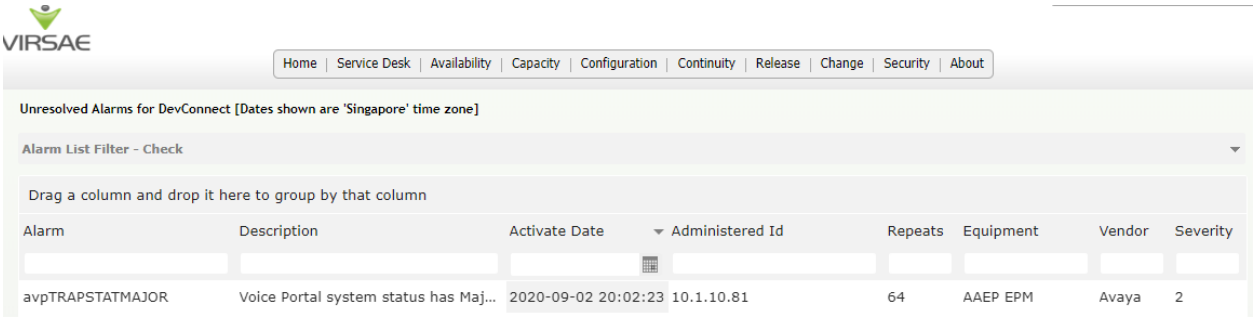
Whatever is configured during setup will be shown here. However, if the dashboard is configured to open automatically on startup in **Section 7.3**, once logged in, all the dashboards last configured at the end of **Section 7.3** will be populated in a new tab on the browser.

The screens below show the Experience Portal (AEP) of the already configured MPP for various parameters including services running under **Application Status**.





To view alarms using reporting, navigate to **Availability → Manage Alarms** (not shown). A list of all unresolved alarms for all equipment is shown. Screen below shows the alarm for **AAEP EPM** equipment.



9. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R135 to interoperate with Avaya Aura® Experience Portal R7.2.3. During compliance testing, all test cases were completed successfully.

10. Additional References

This section references the product documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at http://support.avaya.com.

1. *Administering Avaya Aura® Experience Portal*, Release 7.2.3, Issue 1, Sep 2019.
2. *Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment*, Release 7.2.3, Issue 1, Sep 2019.
3. *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 5, Jun 2020.
4. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1.x, Issue 8, May 2020.

Product documentation for Virsae products can be obtained directly from Virsae.

1. *Virsae Service Management – Adding Avaya Aura Applications and Servers*.
2. *Virsae Service Management – Service Definition, May 2020*.