



Avaya Solution & Interoperability Test Lab

Application Notes for Virsae Service Management with Avaya Aura® System Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R135 to interoperate with Avaya Aura® System Manager R8.1.2.

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 integrates directly to System Manager using Secure Shell (SSH) or Telnet and uses Simple Network Management Protocol (SNMP) to query System Manager.

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® System Manager (herein after referred to as System Manager). 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.

The Virsae product uses SNMP, SFTP and Linux shell access integration method to monitor System Manager.

- SNMP collection –Virsae uses SNMP to collect alarm and status information from System Manager.
- SSH – Virsae establishes a Linux Shell connection to run the “sar” command and obtain system information. This command typically collects, reports and saves CPU, Memory, I/O usage in the Linux operating system.
- SFTP – Virsae provides a SFTP access to System Manager for backup of data.

2. General Test Approach and Test Results

The general test approach was to verify VSM using SNMP and SSH connection to monitor and display system status from System Manager. SFTP was also verified for backup of System Manager data to VSM.

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 encrypted capabilities of SSH, SFTP and 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

For feature testing, VSM dashboard was used to view the configurations of System Manager such as the memory and CPU utilizations, disk usage and status from data collected via SSH and alarms via SNMP. SFTP backup of System Manager data to VSM was also verified.

For serviceability testing, reboots were applied to the VSM and System Managers to simulate system unavailability. Loss of network connectivity to both VSM and System Managers were also performed during testing.

2.2. Test Results

All test cases passed successfully with the following observation.

- The “sar” command cannot be executed in the System Manager version used during this compliance testing since the “Sysstat” directory is not used in this version of Linux platform. By not being able to execute this command, only the CPU occupancy information could not be obtained.
- System Manager SNMP trap for this release is not sent for alarms to be detected by VSM. Avaya are investigating this.

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 VSM interoperability with System Manager. The configuration consists of a Communication Manager system with an Avaya G430 Media Gateway. The system has Workplace Client for Windows and one-X® Communicator (SIP and H.323) softphones configured for making and receiving calls. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. 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.

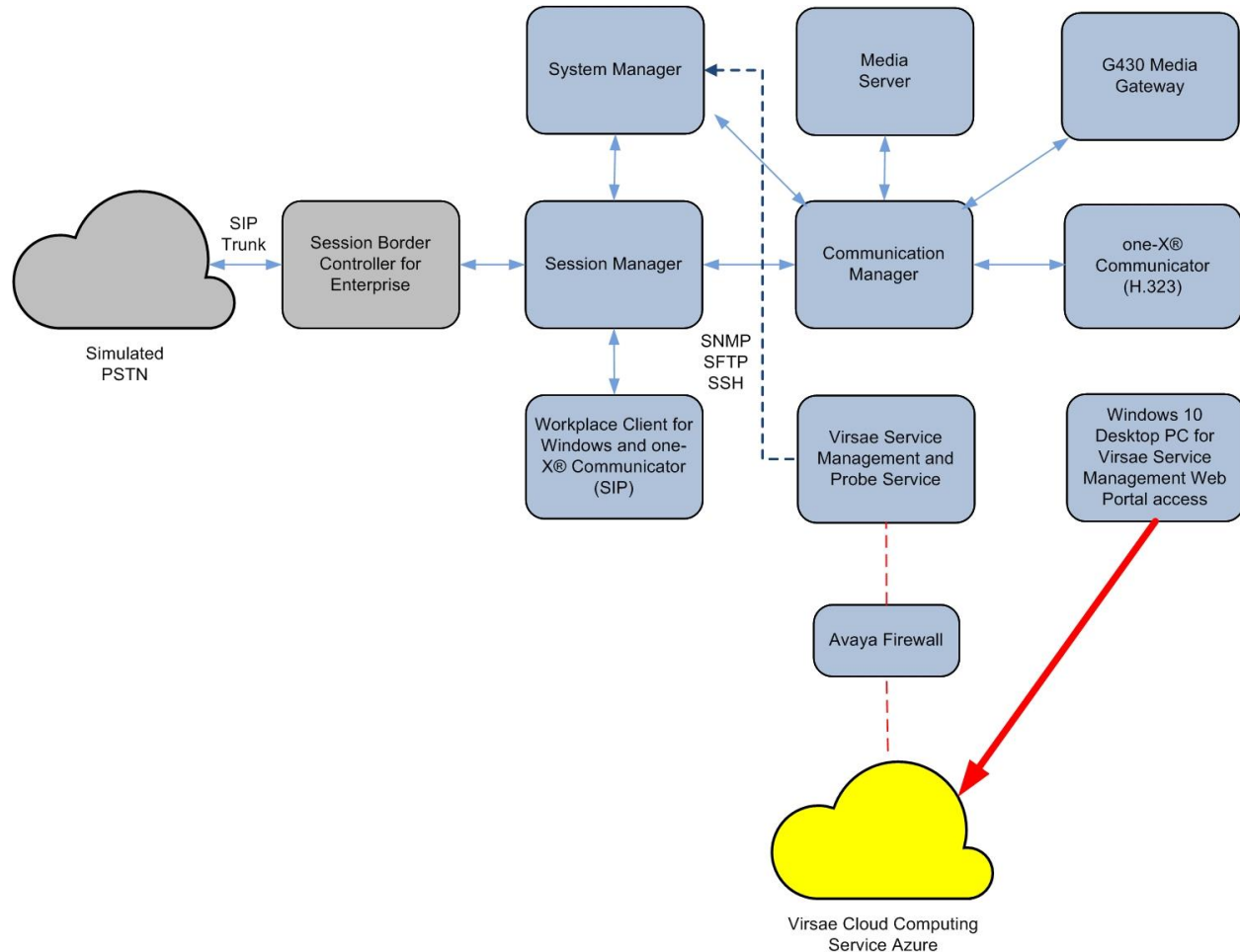


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® 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
Virsa Service Management and Probe Service running on Windows 2016	R135

5. Configure Avaya Aura® System Manager

This section describes the steps needed to configure System Manager to interoperate with VSM. This includes creating a login account for VSM to access System Manager and enabling SNMP.

5.1. Configure Login Account

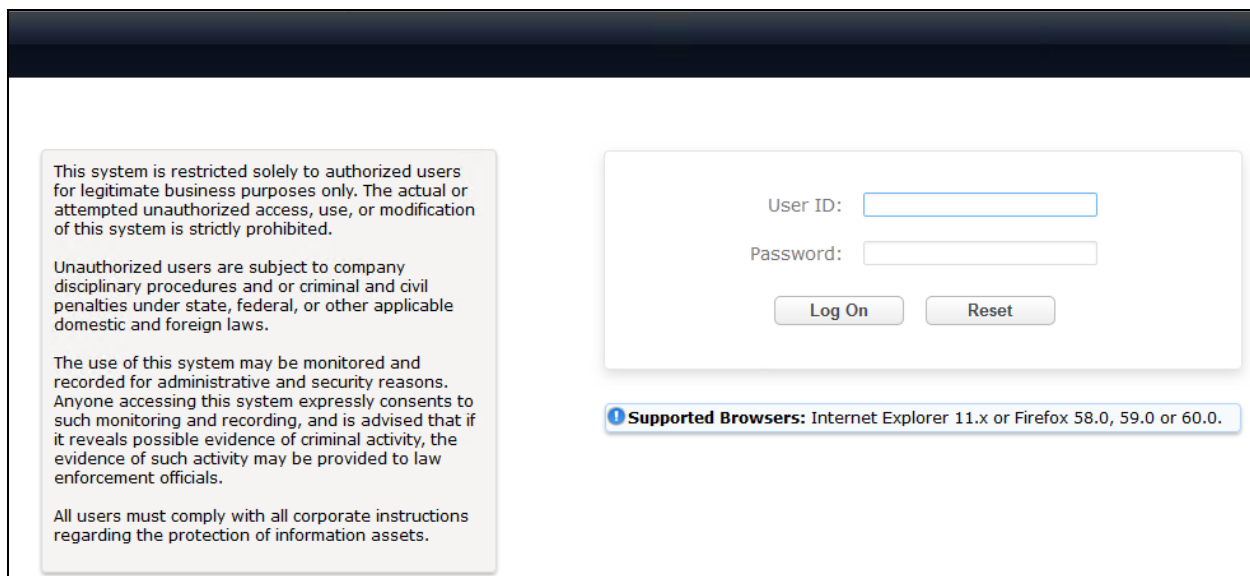
Create an Administrator account on System Manager since the VSM Probe requires access to System Manager with Administrative Rights. The new account should be like the default administrator account. Login to System Manager console with root access and run the following command.

```
useradd <NAME>           ;Add User
passwd <NAME>             ;Enter password twice
chage -M 99999 <NAME>    ;Lengthen the expiry date of account
```

5.2. Configure SNMP

SNMP is used to capture alarms raised by Session Manager. All configurations are done via Avaya Aura® System Manager (System Manager).

Using a web browser, enter **https://<IP address of System Manager>** to connect to the System Manager server and log in using appropriate credentials as shown below.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

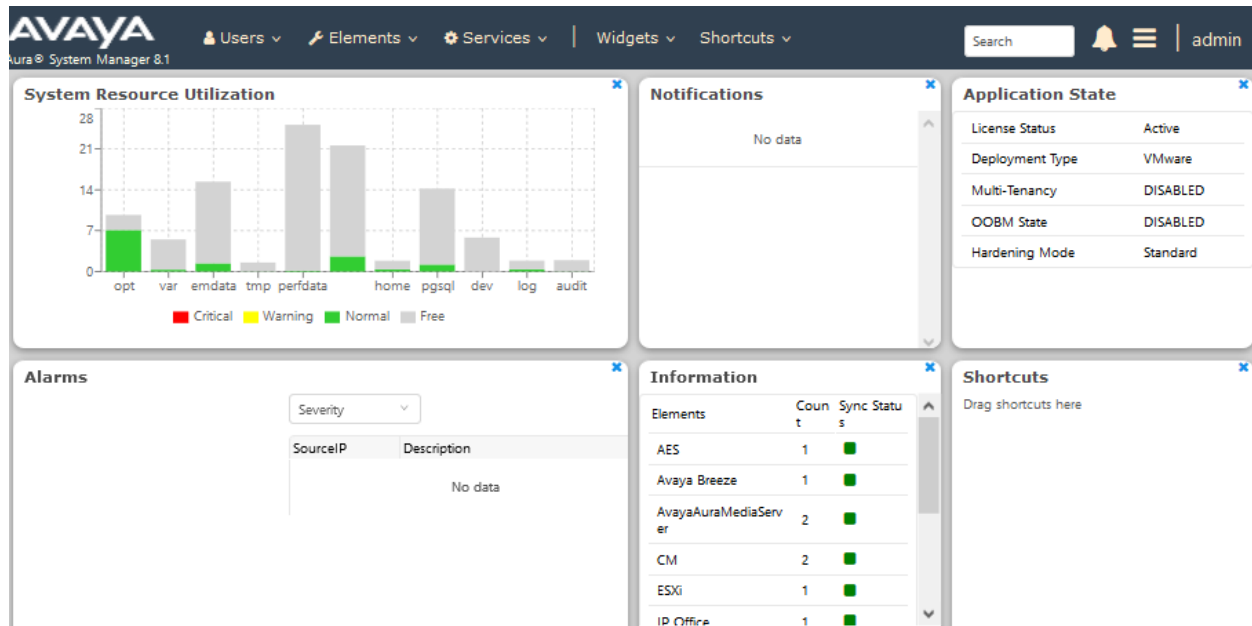
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

Supported Browsers: Internet Explorer 11.x or Firefox 58.0, 59.0 or 60.0.

The main System Manager dashboard page is shown below.



Then navigate to **Manage Servicability Agents** → **SNMPv3 User Profiles** and click **New** (not shown). Configure the following:

- **User Name:** Descriptive name for SNMPv3.
- **Authentication Protocol:** Select “MD5 or SHA”.
- **Authentication Password and Confirm Authentication Password:** Enter password.
- **Privacy Protocol:** Select “AES, DES or none”.
- **Privacy Password and Confirm Privacy Password:** Enter password.

New User Profile

User Details

* User Name: VirsaeV3

* Authentication Protocol: MD5

* Authentication Password:

* Confirm Authentication Password:

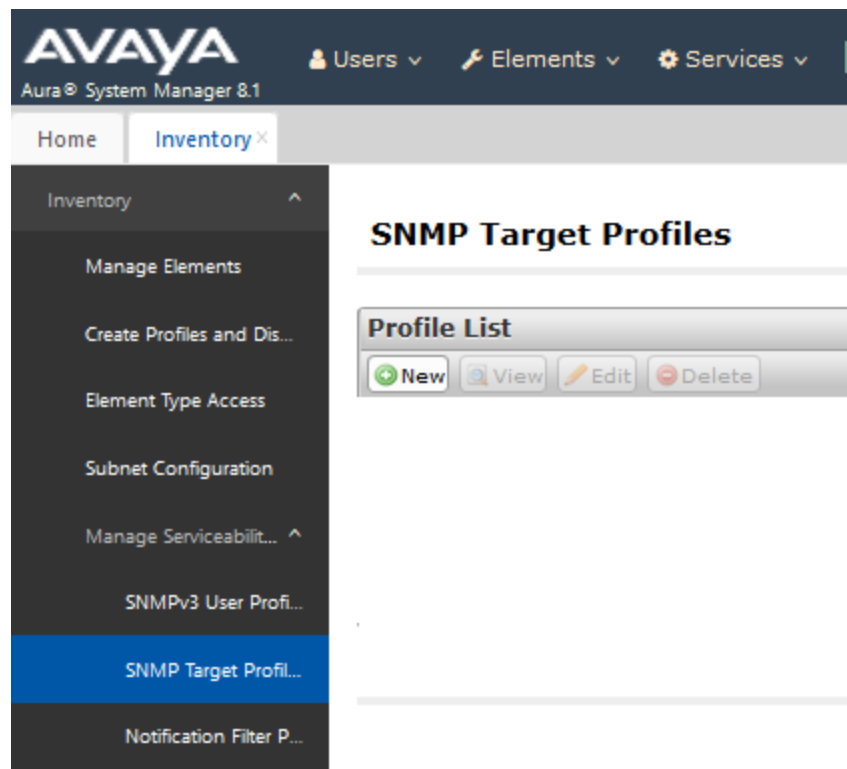
* Privacy Protocol: AES

* Privacy Password:

* Confirm Privacy Password:

* Privileges: Read

Navigate to **Services** → **Inventory** → **Manage Servicability Agents** → **SNMP Target Profiles** as shown in the screen below. Click on **New**.



From the **New Target Profile** window, under the **Target Details** tab, configure the following.

- **Name:** A descriptive name.
- **IP Address:** The VSM IP address.
- **Notification Type:** Select “Trap” from the drop-down menu.
- **Protocol:** Select **V3** from the drop-down menu.

Retain default values for all other fields and click on the **Attach/Detach User Profile**.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home Inventory

Inventory ▾

- Manage Elements
- Create Profiles and Dis...
- Element Type Access
- Subnet Configuration
- Manage Serviceabilit...
- SNMPv3 User Profi...
- SNMP Target Profil...**
- Notification Filter P...
- Serviceability Agents

Status

New Target Profile

Target Details * Attach/Detach User Profile

Target Details ▾

* Name: Virsaev3

Description:

* IP Address: 10.1.10.124

* Port: 162

* Notification Type: Trap ▾

* Protocol: V3 ▾

Select the **Virsaev3** user profile created earlier and click **Assign**.

New Target Profile

Commit Back

Target Details * Attach/Detach User Profile

Assignable Profiles ▾

Assign

1 Item

	User Name	Authentication Protocol	Privacy Protocol	Privileges
<input type="radio"/>	Virsaev3	MD5	AES	R

Select : None

Removable Profiles ▸

The **Virsaev3** user profile is shown below as assigned to the Target.

New Target Profile

[Commit](#) [Back](#)

Target Details *
Attach/Detach User Profile

Assignable Profiles

Assign

0 Items

User Name	Authentication Protocol	Privacy Protocol	Privileges
No records to display			

Removable Profiles

Remove

1 Item

User Name	Authentication Protocol	Privacy Protocol	Privileges
<input type="radio"/> Virsaev3	MD5	AES	R

Select : [None](#)

Then navigate to **Manage Servicability Agents** → **Servicability Agents** as shown in the screen below. Select System Manager agent from the **Agent List** window, in this case the System Manager and click on the **Manage Profiles** button.

AVAYA
 Aura® System Manager 8.1

[Users](#)
[Elements](#)
[Services](#)
[Widgets](#)
[Shortcuts](#)

[Home](#)
[Inventory](#)

Inventory
Manage Elements
Create Profiles and Dis...
Element Type Access
Subnet Configuration
Manage Serviceability...
SNMPv3 User Profi...
SNMP Target Profil...
Notification Filter P...
Serviceability Agents

Status

Serviceability Agents

Agent List

[Activate](#)
[Manage Profiles](#)
[Generate Test Alarm](#)
[Repair Serviceability Agent](#)
[Manage Profile Job Status](#)

8 Items
Show All

	Hostname	IP Address	System Name	System OID
<input type="checkbox"/>	g450-US	127.0.0.1	g450-US	
<input type="checkbox"/>	Utility-Services	10.1.40.14	Utility-Services	
<input type="checkbox"/>	sm1.sglab.com	10.1.10.60	sm1.sglab.com	
<input type="checkbox"/>	sm1.sglab.com	10.1.10.59	Session Manager	.1.3.6.1.4.1.6889.1.36
<input type="checkbox"/>	sm3.sglab.com	10.1.10.47	sm3.sglab.com	
<input checked="" type="checkbox"/>	smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35

From the **Manage Profile** window, under the **SNMP Target Profiles** tab, select the **Virsaev3** profile, click on **Assign** and do the same for **SNMPv3 User Profiles** tab. Then click the **Commit** button.

Manage Profile

[Commit](#) [Back](#)

Selected Agents
SNMP Target Profiles
SNMPv3 User Profiles

Assignable Profiles

Assign

1 Item

<input type="checkbox"/>	Name	Domain Type	IP Address	Port	SNMP Version
Select : All, None					

Removable Profiles

Remove Assign/Remove Filter Profiles

1 Item

<input type="checkbox"/>	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
<input type="checkbox"/>	Virsaev3	UDP	10.1.10.124	162	V3	
Select : All, None						

Manage Profile

[Commit](#) [Back](#)

Selected Agents
SNMP Target Profiles
SNMPv3 User Profiles

Assignable Profiles

Assign

0 Items

<input type="checkbox"/>	User Name	Authentication Protocol	Privacy Protocol	Privileges
No records to display				

Removable Profiles

Remove

1 Item

<input type="checkbox"/>	User Name	Authentication Protocol	Privacy Protocol	Privileges
<input type="checkbox"/>	Virsaev3	MD5	AES	R
Select : All, None				

6. Configure Virsae Service Management

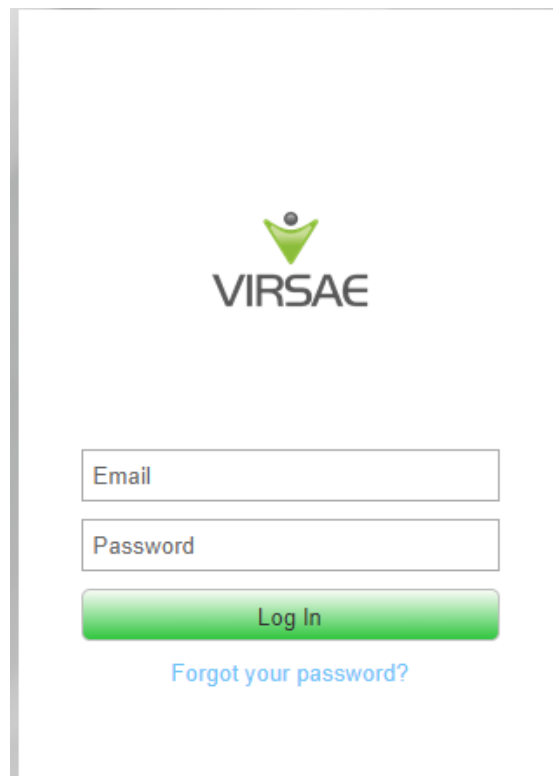
This section describes the configuration of VSM required to interoperate with System Manager.

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® System Manager
- Configure Dashboard

6.1. 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 image shows a login screen for the Virsae web portal. At the top center is the Virsae logo, which consists of a green stylized figure with arms raised above the word "VIRSAE" in a bold, sans-serif font. Below the logo are two input fields: the first is labeled "Email" and the second is labeled "Password". Both labels are in a small, light blue font. Below these fields is a green button with the text "Log In" in white. At the bottom of the login area is a blue link that says "Forgot your password?". The entire login form is enclosed in a thin grey border.

The customers 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.

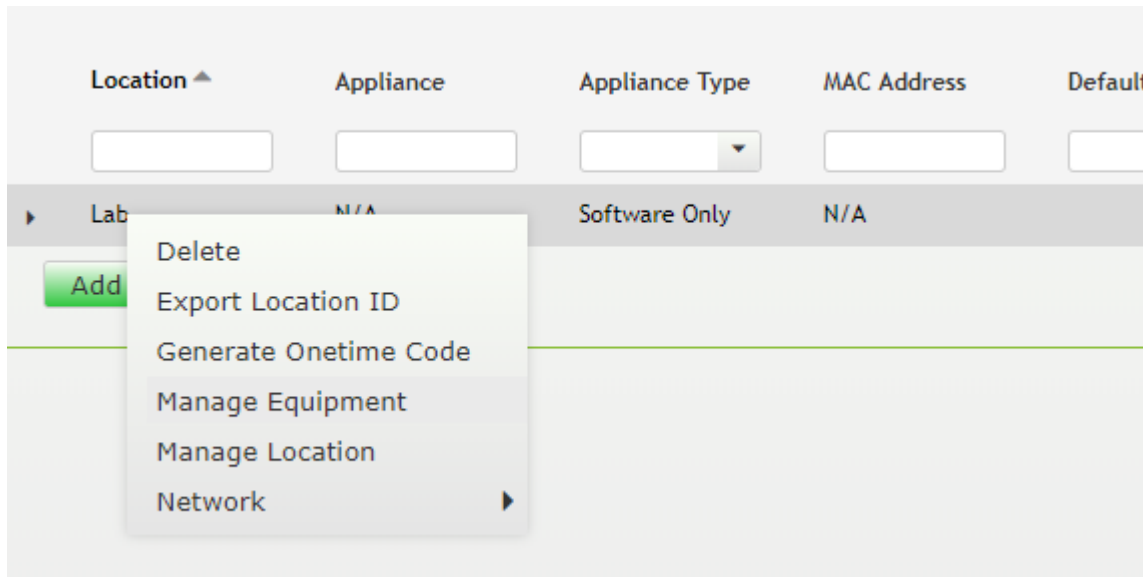
The screenshot shows the VIRSAE web application interface. The top navigation bar includes links for Home, Service Desk, Availability, Capacity, Configuration, Continuity, Release, Change, Security, and About. The 'Service Desk' tab is selected. A dropdown menu is open from the 'Service Desk' tab, showing options: Access Concentrator, Call Details, CMS Call History, Dashboards, **Equipment Locations** (highlighted), Files and Folders, Manage Customer, Reports, and More. The background of the page features a large graphic with a house icon labeled 'Service Desk' and a bar chart icon labeled 'Availability Manager'.

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

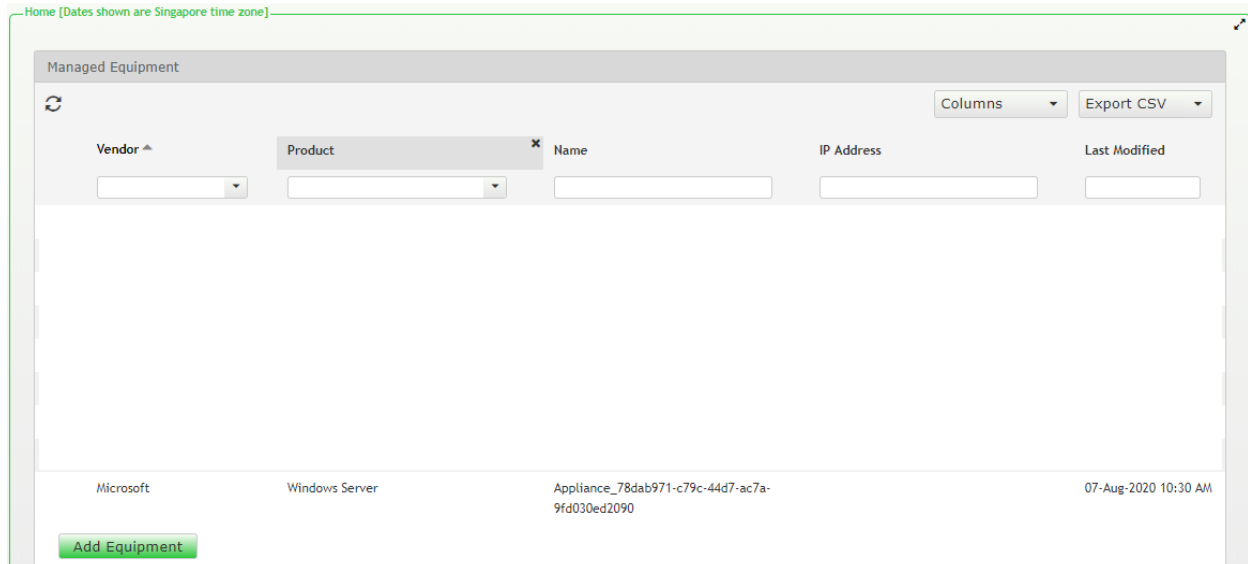
The screenshot shows the VIRSAE web application interface with the 'Equipment Locations' page selected. The top navigation bar is the same as in the previous screenshot. The page title is 'Home/Equipment Locations [Dates shown are Singapore time zone]'. Below the title is a table with the following columns: Location, Appliance, Appliance Type, MAC Address, Default Site, Last HeartBeat, Controller Version, Running VM List, and Running Time. The table contains one row for a location named 'Lab' with the following values: Appliance: N/A, Appliance Type: Software Only, MAC Address: N/A, Default Site: N/A, Last HeartBeat: N/A, Controller Version: N/A, Running VM List: N/A, and Running Time: 0 s. There is an 'Add Location' button below the table.

Location	Appliance	Appliance Type	MAC Address	Default Site	Last HeartBeat	Controller Version	Running VM List	Running Time
Lab	N/A	Software Only	N/A	N/A	N/A	N/A	N/A	0 s

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



Click **Add Equipment** below:



6.2. Configuring Avaya Aura® System Manager

From the **Add Equipment** window, add a System Manager to the Location. Select **Avaya** from the **Vendor** list. Select **System Manager** from the **Product** list. Configure the following values.

- **Equipment Name:** A descriptive name.
- **Username:** The username configured in **Section 5.1**.
- **Password:** The password configured in **Section 5.1**.
- **IP Address/Host Name:** IP address of System Manager.
- **Site:** A descriptive site name.

Equipment	SNMP Query	Custom Scripts
<hr/>		
Vendor *		Product *
<div>Avaya ▼</div>		<div>System Manager ▼</div>
Equipment Name *		Username *
<div>System Manager</div>		<div>virsa</div>
IP Address/Host Name *		Password *
<div>10.1.10.46</div>		<div>.....</div>
Site ⓘ		
<div>Lab</div>		

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

- **Version:** Select **V3** from the drop-down menu.
- **Username:** Enter username configured in **Section 5.2**.
- **Authentication Protocol:** Protocol configured in **Section 5.2**.
- **Authentication Password:** Password configured in **Section 5.2**.
- **Privacy Protocol:** Protocol configured in **Section 5.2**.
- **Privacy Password:** Password configured in **Section 5.2**.

Click on the **Save** (not shown) button to complete the configuration.

Equipment

SNMP Query

Custom Scripts

Virsa Direct can be configured to query this System Manager for configuration and system health metrics, which are used in the dashboards, and historic reports.

To enable this, please enter the SNMP configuration details for this System Manager below.

Version

V3

Username *

VirsaV3

Authentication Protocol *

MD5

Authentication Password

.....

Privacy Protocol *

AES128

Privacy Password *

.....

Save

Test Access

Cancel

The screen below shows the added System Manager equipment.

Home [Dates shown are Singapore time zone]

Vendor ▲

Product

1 items selected

Name

IP Address

Avaya

System Manager

System Manager

10.1.10.46

Add Equipment

Import

Navigate to **Service Desk → Equipment Locations**, right click on the **Lab** and select **Manage Locations** (not shown). Check **Enable SFTP** is turn on i.e., tick and configure the SFTP user accounts for System Manager backup.

- **User Name and Password:** Enter the name and password to be used by System Manager.
- **Protocol:** Select **SFTP/SCP** from the drop-down menu.
- **Upload Type:** Select **Backup** from the drop-down menu.

Details	Appliance	SNMP Traps	File Transfer	VQM
---------	-----------	------------	---------------	-----

VSM provides various methods for uploading data, which can be configured below. Data uploads can be used as an offsite back-up, and for collecting voice quality information, syslog and other data from unified communication servers and adjuncts.

☐ Enable TFTP

☐ Enable FTP

☐ Enable UUCP



SFTP and SCP Configuration

☒ Enable SFTP ☐ Enable SCP

Port

22

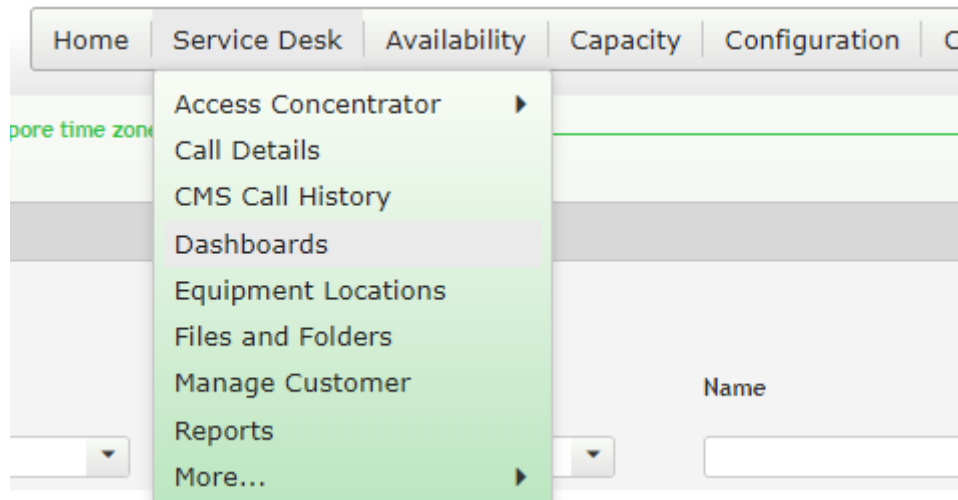
SFTP and FTP user accounts

User Name *	Password *	Protocol	Upload Type	Public Key	
devconnect	SFTP/SCP	Backup		 

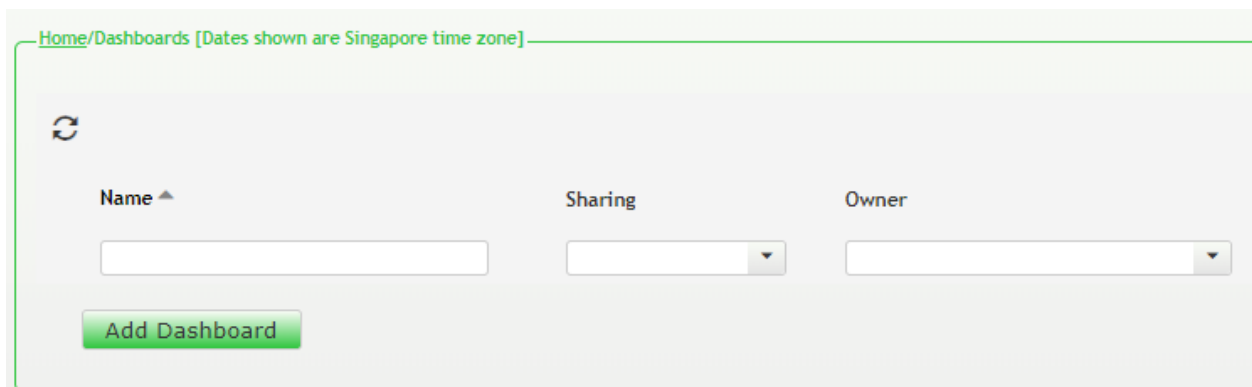
6.3. Configure Dashboard

This section shows the steps to configure Communication Manager on the dashboard.

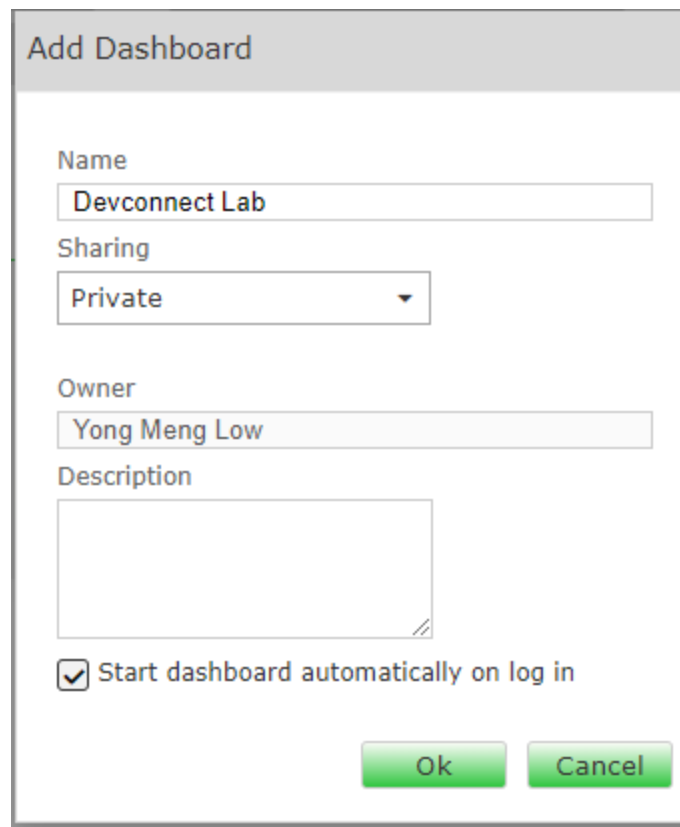
From the home screen, navigate to **Service Desk → Dashboards** as shown below.



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.



Add Dashboard

Name
Devconnect Lab

Sharing
Private ▼

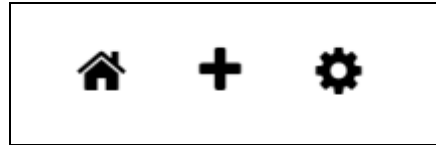
Owner
Yong Meng Low

Description

☒ Start dashboard automatically on log in

Ok Cancel

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**.

Add Dashlet

system health

System Health Summary

Add new System Health Summary

Avaya Application Enablement Services (AES)

Avaya Call Management System (CMS)

Avaya Communication Manager (ACM)

Avaya Contact Recorder (ACR)

Avaya Experience Portal (AEP)

Avaya Session Border Controller (ASBC)

Avaya Session Manager (SM)

IP Office

Linux Server

Oracle SBC

Windows Server

Trunk

Multiple Trunk Groups

Trunk Group Traffic

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., **System Manager** and click **Done** (not shown).

Settings

Dashboard

All Dashlets

ACM System Health Summary
Lab

Active Streams
Lab | Lab

Alarms Summary
DevConnect

Avaya Application Enablement Services (AES)
Lab | AES

Avaya Call Management System (CMS)
Lab | Call Management System

Avaya Communication Manager (ACM)
Lab | Communication Manager

Avaya Experience Portal (AEP)
DevConnect, Lab | AAEP EPM

Avaya Experience Portal (AEP)
DevConnect, Lab | AAEP MPP

Avaya Session Border Controller (ASBC)
Lab | SBCE

Avaya Session Manager (SM)
Lab | Session Manager1

Avaya Session Manager (SM)

Customer
DevConnect

Location
Lab

Equipment

Communication Manager

AES

Call Management System

AAEP EPM

AAEP MPP

Media Server

SBCE

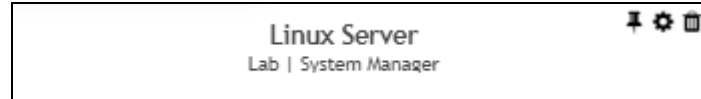
Session Manager1

Session Manager2

System Manager

Appliance_78dab971-c79c-44d7-ac7a-9fd030ed2090

Repeat the same for the **Linux Server** dashboard and in addition select the desired **Layout**.



Settings

Dashboard

All Dashlets

ACM System Health Summary
Lab

Active Streams
Lab | Lab

Alarms Summary
DevConnect

Avaya Application Enablement Services (AES)
Lab | AES

Avaya Call Management System (CMS)
Lab | Call Management System

Avaya Communication Manager (ACM)
Lab | Communication Manager

Avaya Experience Portal (AEP)
DevConnect, Lab | AAEP EPM

Avaya Experience Portal (AEP)
DevConnect, Lab | AAEP MPP

Avaya Session Border Controller (ASBC)
Lab | SBCE

Avaya Session Manager (SM)
Lab | Session Manager1

Avaya Session Manager (SM)
Lab | Session Manager2

Calls In Progress
Lab | Lab

Linux Server
Lab | Media Server

Customer
DevConnect

Location
Lab

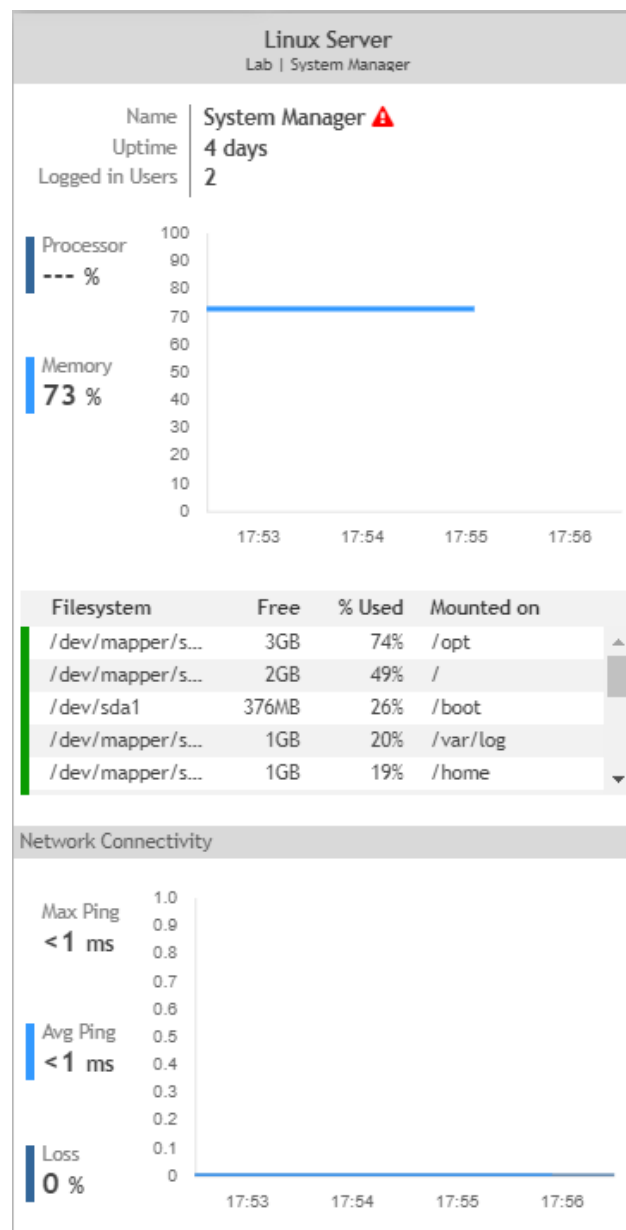
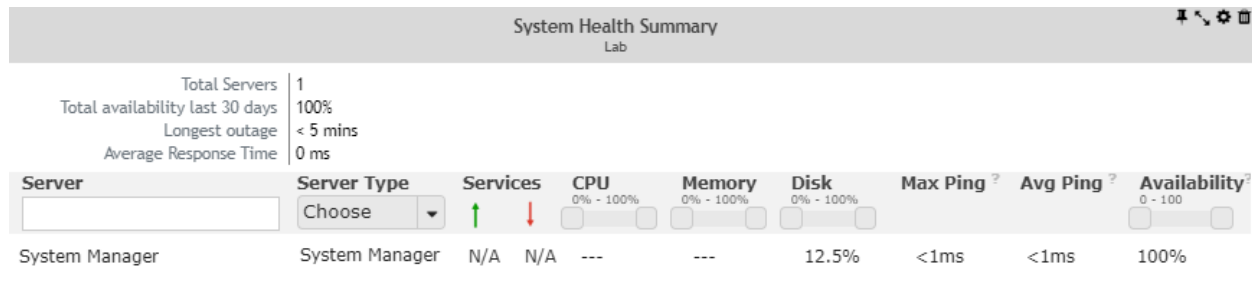
Equipment
System Manager

Layout

Show Occupancy Graph☒

Show Network Connectivity Graph☒

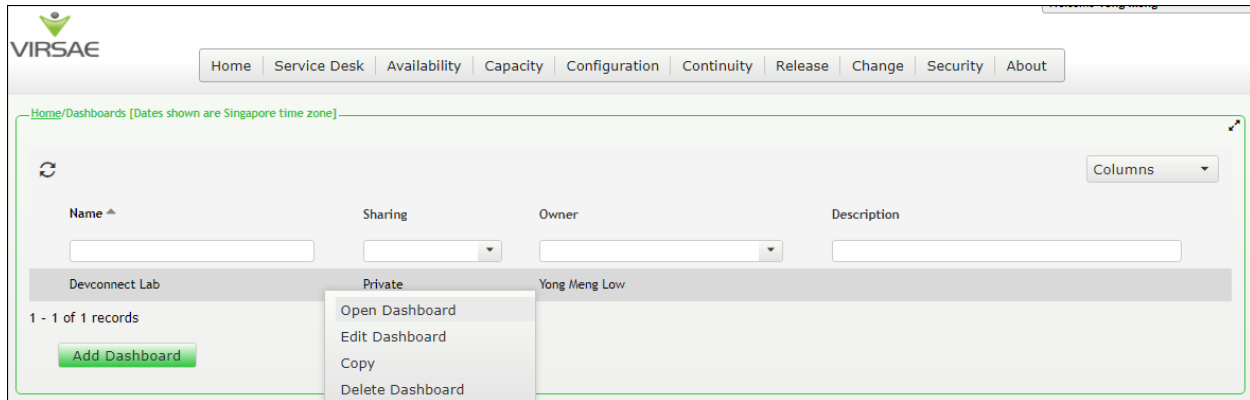
The two dashboards with the configured equipment are shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.



7. Verification Steps

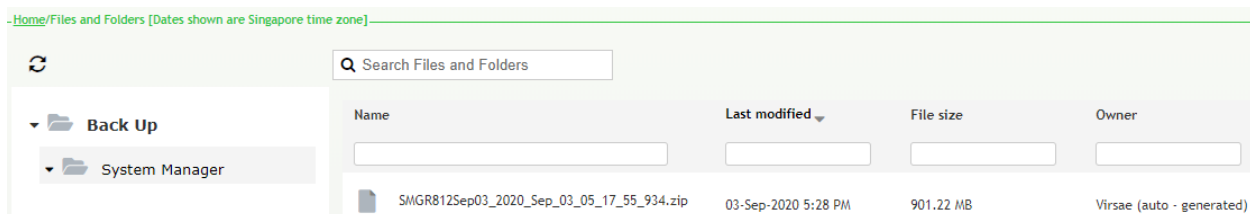
This section provides the tests that can be performed to verify proper configuration of System Manager and VSM. The following steps are done by accessing the VSM web portal for the business partner.

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 6.3**, once login, all the dashboards last configured at the end of **Section 6.3** will be populated in a new tab on the browser.

Perform a backup of the SMGR to VSM. Refer to reference [4] for details of how to backup SMGR. To view the off-site backups on VSM, navigate to **Continuity → Browse Backups** (not shown). Screen below shows an example of backups for System Manager.



To view alarms using reporting, navigate to **Availability → Manage Alarms** (not shown). A list of all unresolved alarms for all equipment is shown. As observed in **Section 2.2**, alarms couldn't be picked up by VSM. In the **Alarm List Filter**, create a rule set for **Equipment** as **System Manager** equipment as shown below and apply the rule.

The screenshot displays the Virsae web application interface. At the top right, a user greeting "Welcome Yong Meng" is visible. Below the Virsae logo, a navigation bar contains links: Home, Service Desk, Availability, Capacity, Configuration, Continuity, Release, Change, Security, and About. The main content area is titled "Unresolved Alarms for DevConnect [Dates shown are 'Singapore' time zone]". Below this, the "Alarm List Filter" section is expanded, showing a "Rule Sets:" dropdown menu with "Check" selected. Underneath, the "Expression (condition)" section is visible, containing a table with a single row: "Equipment equal System Manager". To the right of this row are "+" and "-" icons. At the bottom right of the filter section are three buttons: "Save", "Save All", and "Apply".

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R135 to interoperate with Avaya Aura® System Manager R8.1.2. During compliance testing, all test cases were completed successfully with observations noted in **Section 2.2**.

9. 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. *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtual Appliance*, Release 8.1.x, Issue 3, Mar 2020.
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 6, Aug 2020.
3. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 5, May 2020.
4. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 6, Apr 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.

©2020 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.