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 R174 to interoperate with Avaya Aura® System Manager R10.1.

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) 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.

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 to simulate system unavailability. Loss of network connectivity to VSM was 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.

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 H.323/SIP Deskphones and 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.

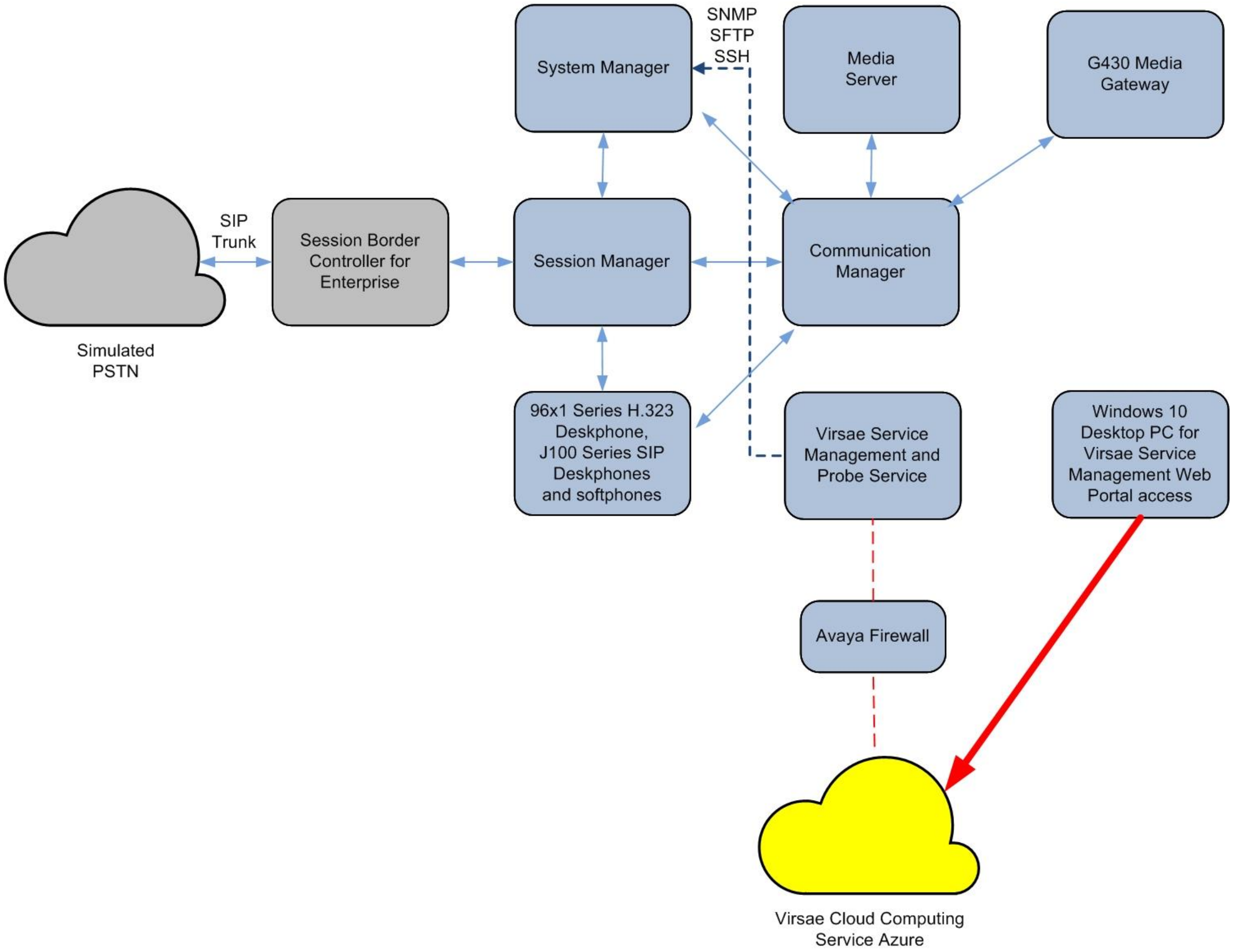

SNMP
SFTP
SSH
System Manager
Media Server
G430 Media Gateway
SIP Trunk
Session Border Controller for Enterprise
Session Manager
Communication Manager
Simulated PSTN
96x1 Series H.323 Deskphone, J100 Series SIP Deskphones and softphones
Virsae Service Management and Probe Service
Windows 10 Desktop PC for Virsae Service Management Web Portal access
Avaya Firewall
Virsae Cloud Computing Service Azure

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® Communication Manager running on Virtual Server	10.1 (10.1.0.0.0.974.27293)
Avaya G430 Media Gateway	42.4.0
Avaya Aura® Media Server running on Virtual Server	10.1.0.77
Avaya Aura® Session Manager running on Virtual Server	10.1 (10.1.0.0.1010019)
Avaya Aura® System Manager running on Virtual Server	10.1 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya 96x1 Series (H.323)	6.8523
Avaya J100 Series (SIP)	4.0.11.0
Avaya Workplace Client for Windows (SIP)	3.27
Avaya Agent for Desktop (H.323)	2.0.6.22.3003
Virsae Service Management and Probe Service running on Windows 2016	174.1.2.268

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

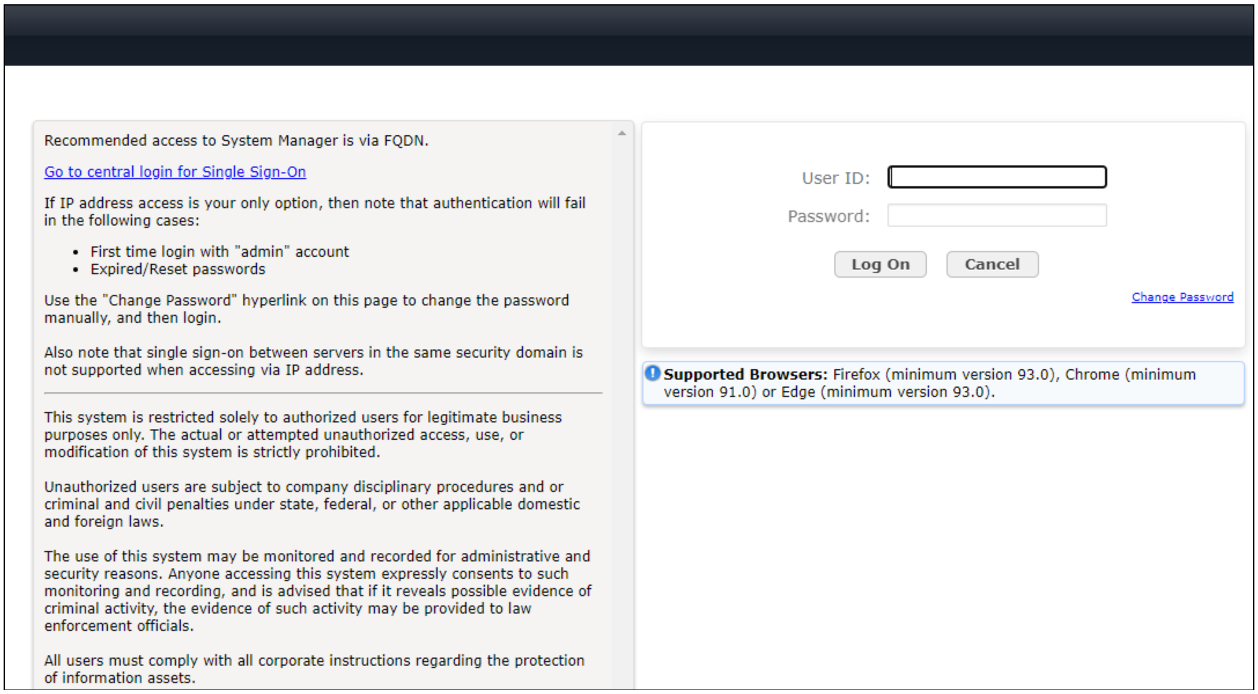
Create an Administrator account on System Manager since the VSM Probe requires access to System Manager with Administrative Rights. The new account should be like the default administrator account. Login to System Manager console with root access and run the following command.

```
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.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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.

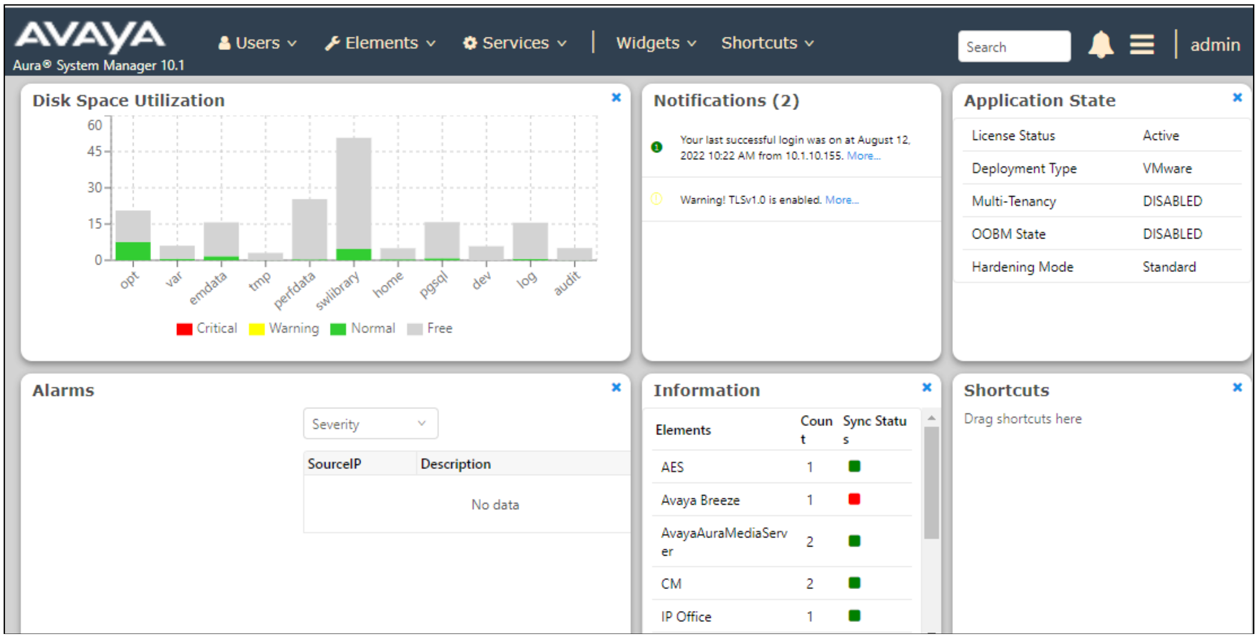
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

The main System Manager dashboard page is shown below.



Notifications (2)

Your last successful login was on at August 12, 2022 10:22 AM from 10.1.10.155. More...

Warning! TLSv1.0 is enabled. More...

Application State

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

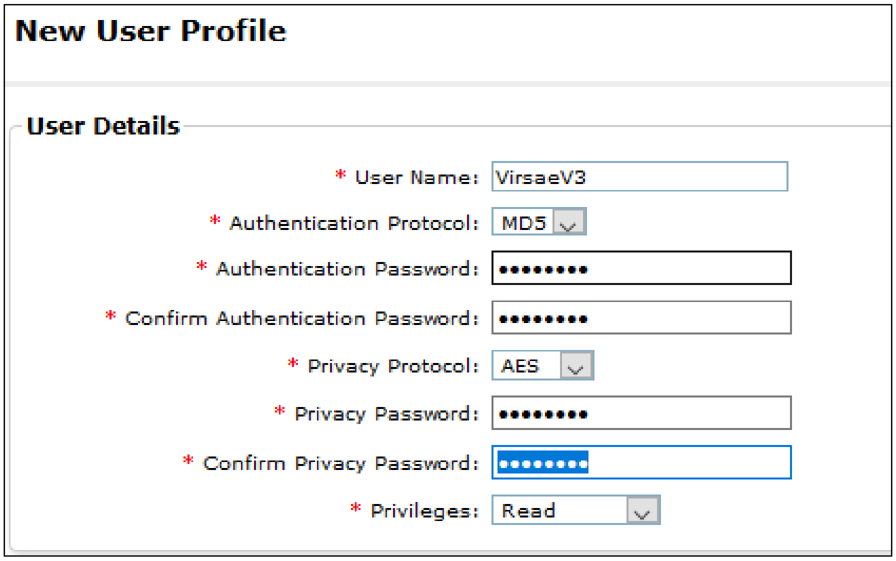
SourceIP	Description
	No data

Information

Elements	Count	Sync Status
AES	1	🟩
Avaya Breeze	1	🟥
AvayaAuraMediaServer	2	🟩
CM	2	🟩
IP Office	1	🟩

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.

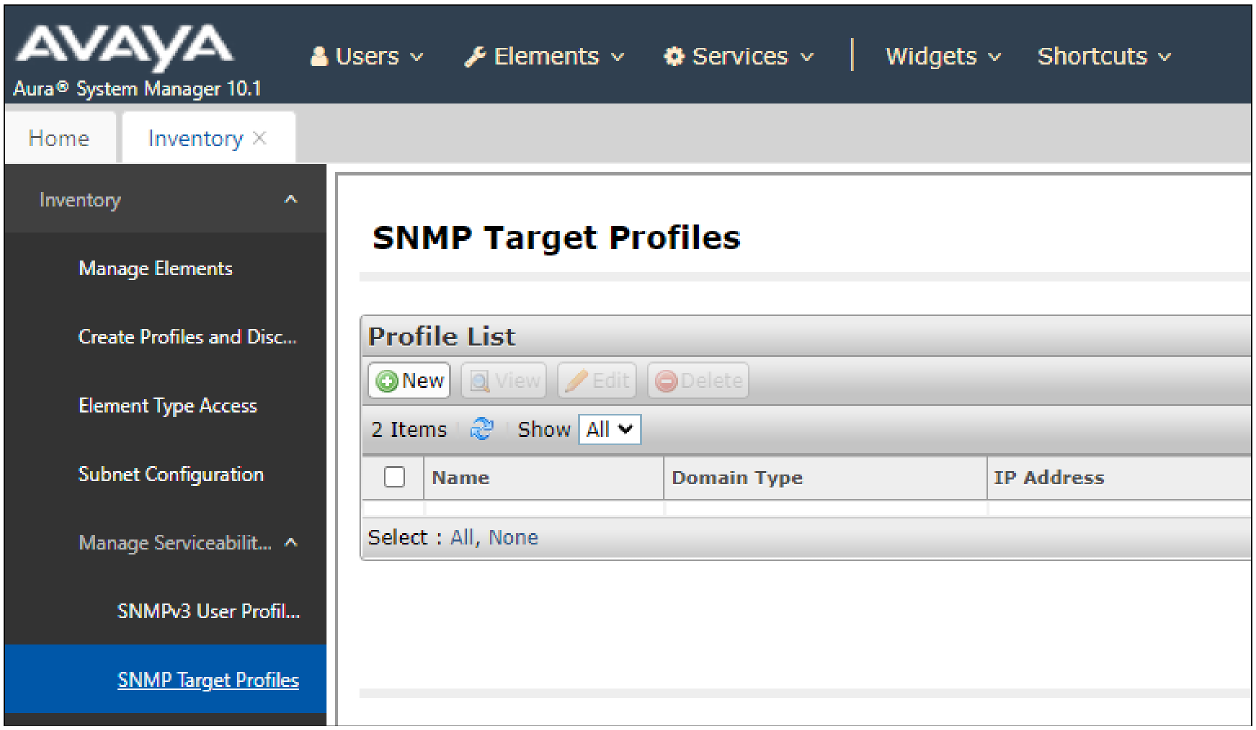


New User Profile

User Details

* User Name:	VirsaeV3
* Authentication Protocol:	MD5
* Authentication Password:	••••••••
* Confirm Authentication Password:	••••••••
* Privacy Protocol:	AES
* Privacy Password:	••••••••
* Confirm Privacy Password:	••••••••
* Privileges:	Read

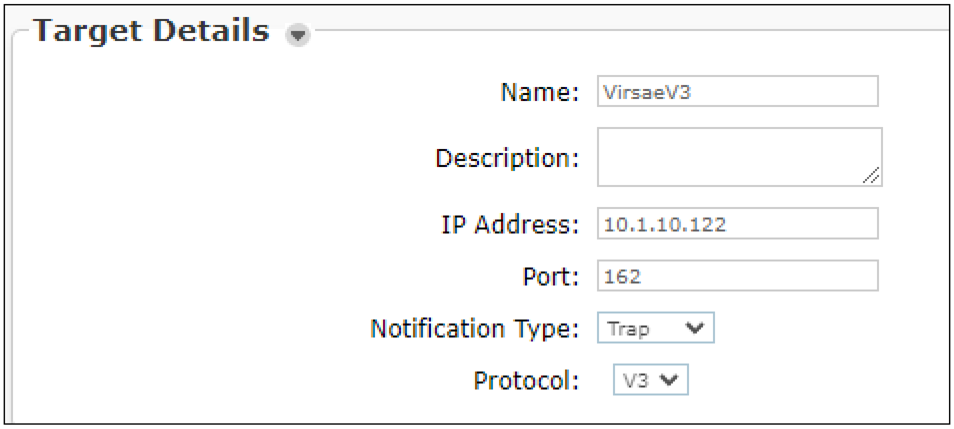
Navigate to **Services → Inventory → Manage Servicability Agents → SNMP Target Profiles** as shown in the screen below. Click on **New**.



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** (not shown).



Target Details

Name: VirsaeV3

Description:

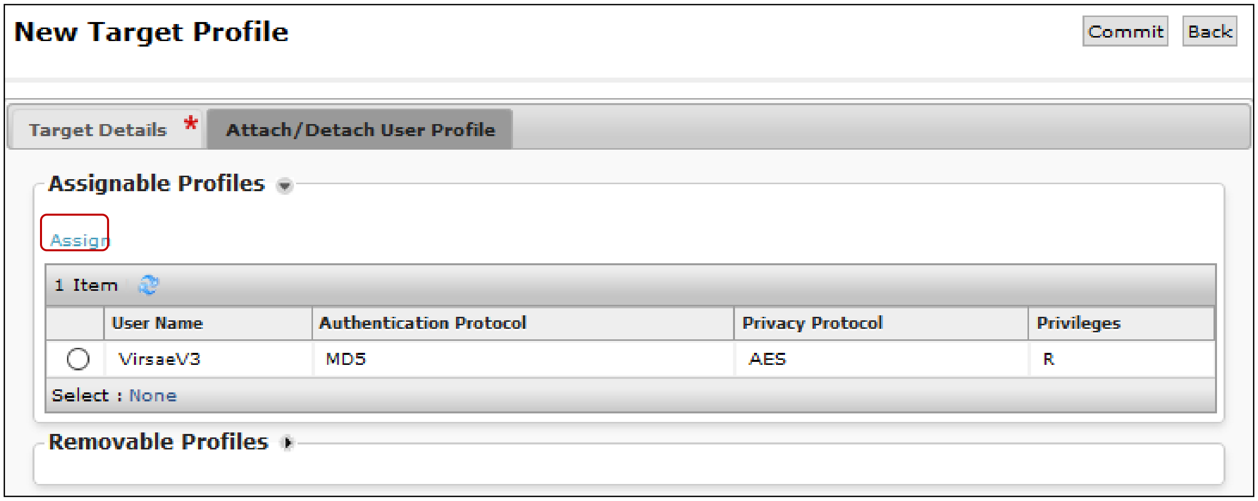
IP Address: 10.1.10.122

Port: 162

Notification Type: Trap

Protocol: V3

Select the **VirsaeV3** user profile created earlier and click **Assign**.



New Target Profile

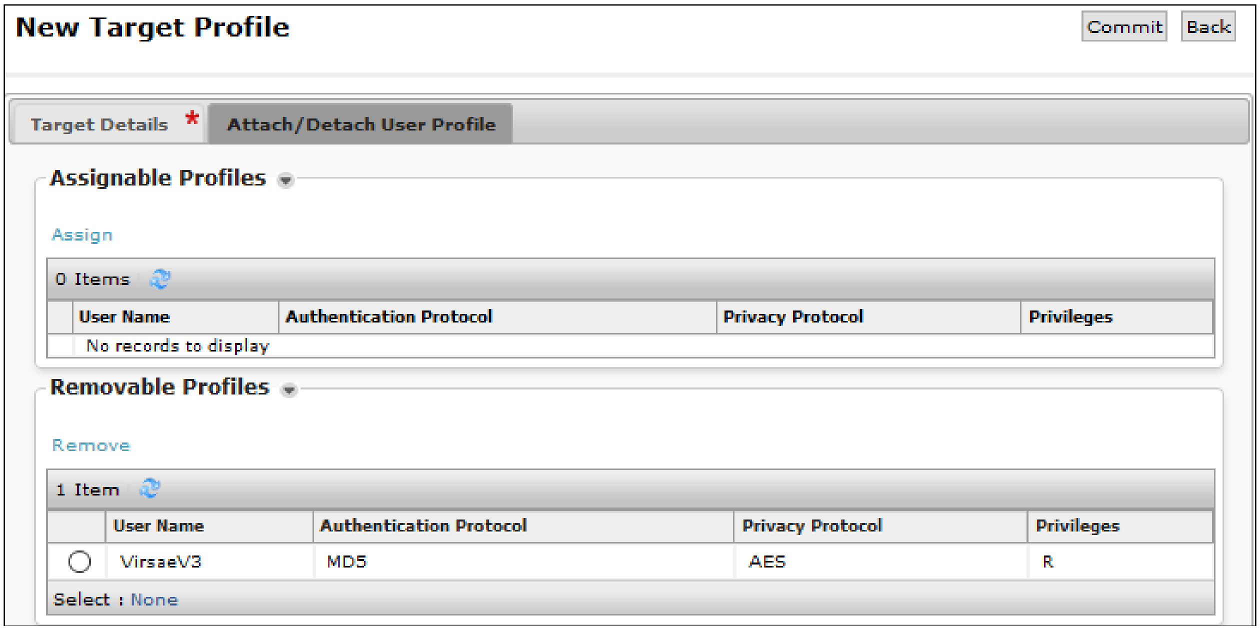
Assignable Profiles

	User Name	Authentication Protocol	Privacy Protocol	Privileges
○	VirsaeV3	MD5	AES	R

Select : None

Removable Profiles

The **VirsaeV3** user profile is shown below as assigned to the Target.

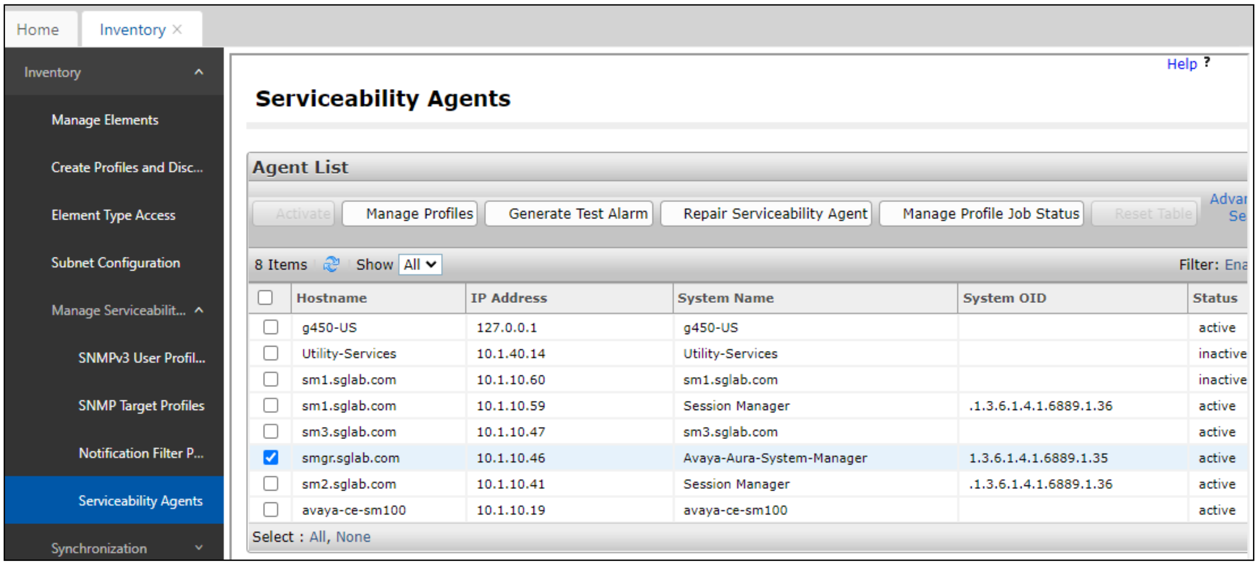


	User Name	Authentication Protocol	Privacy Protocol	Privileges
	No records to display			

	User Name	Authentication Protocol	Privacy Protocol	Privileges
○	VirsaeV3	MD5	AES	R

Select : None

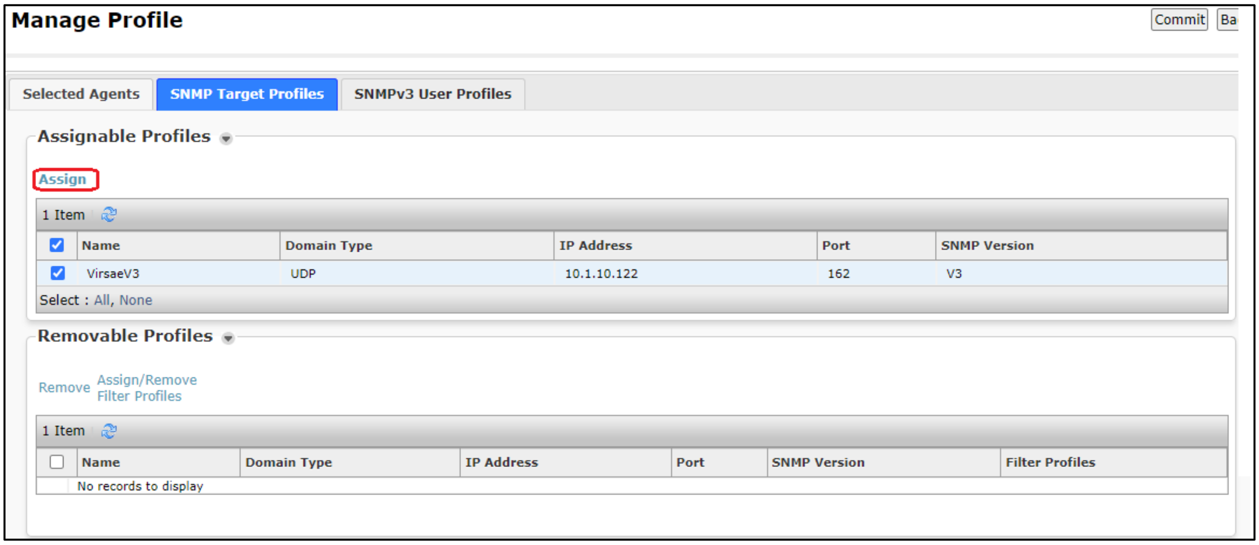
Then navigate to **Manage Servicability Agents → Servicability Agents** as shown in the screen below. Select System Manager agent from the **Agent List** window, in this case the **Avaya-Aura-System-Manager** and click on the **Manage Profiles** button.



□	Hostname	IP Address	System Name	System OID	Status
□	g450-US	127.0.0.1	g450-US		active
□	Utility-Services	10.1.40.14	Utility-Services		inactive
□	sm1.sglab.com	10.1.10.60	sm1.sglab.com		inactive
□	sm1.sglab.com	10.1.10.59	Session Manager	.1.3.6.1.4.1.6889.1.36	active
□	sm3.sglab.com	10.1.10.47	sm3.sglab.com		active
☑	smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
□	sm2.sglab.com	10.1.10.41	Session Manager	.1.3.6.1.4.1.6889.1.36	active
□	avaya-ce-sm100	10.1.10.19	avaya-ce-sm100		active

Select : All, None

From the **Manage Profile** window, under the **SNMP Target Profiles** tab, select the **VirsaeV3** profile, click on **Assign**. Then click the **Commit** button. Do the same for **SNMPv3 User Profiles** tab.



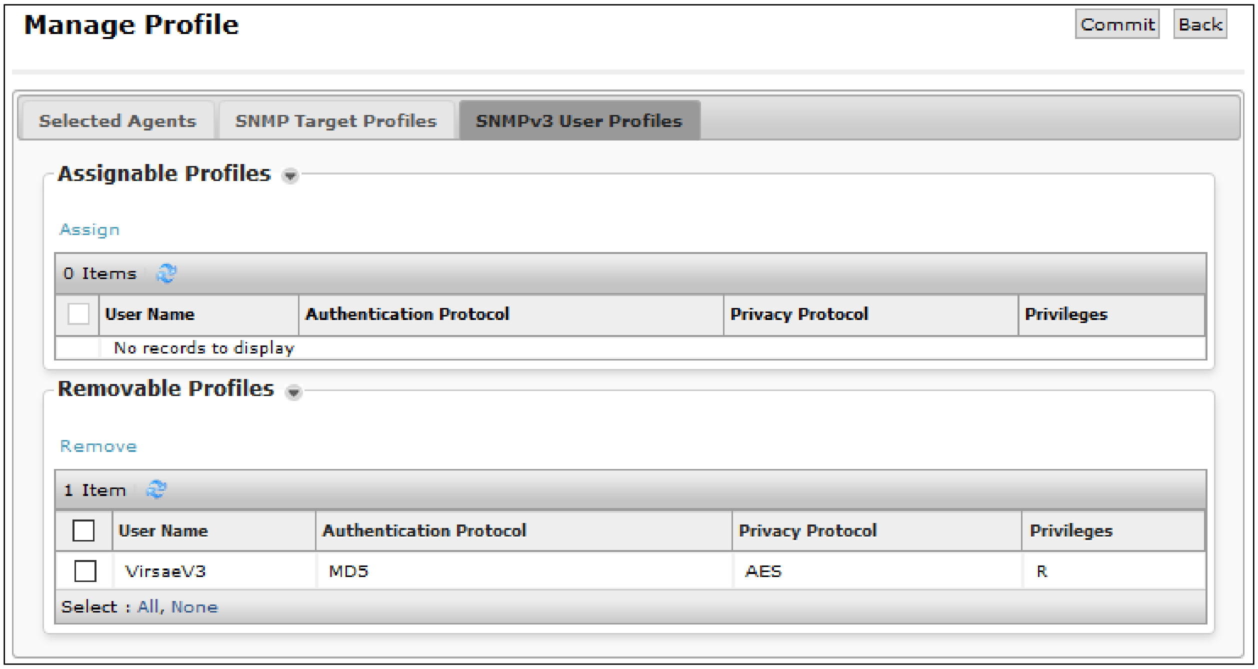
1 Item

☑	Name	Domain Type	IP Address	Port	SNMP Version
☑	VirsaeV3	UDP	10.1.10.122	162	V3

Select : All, None

1 Item

□	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
	No records to display					



0 Items

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
	No records to display			

1 Item

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
□	VirsaeV3	MD5	AES	R

Select : All, None

6. Configure Virsae Service Management

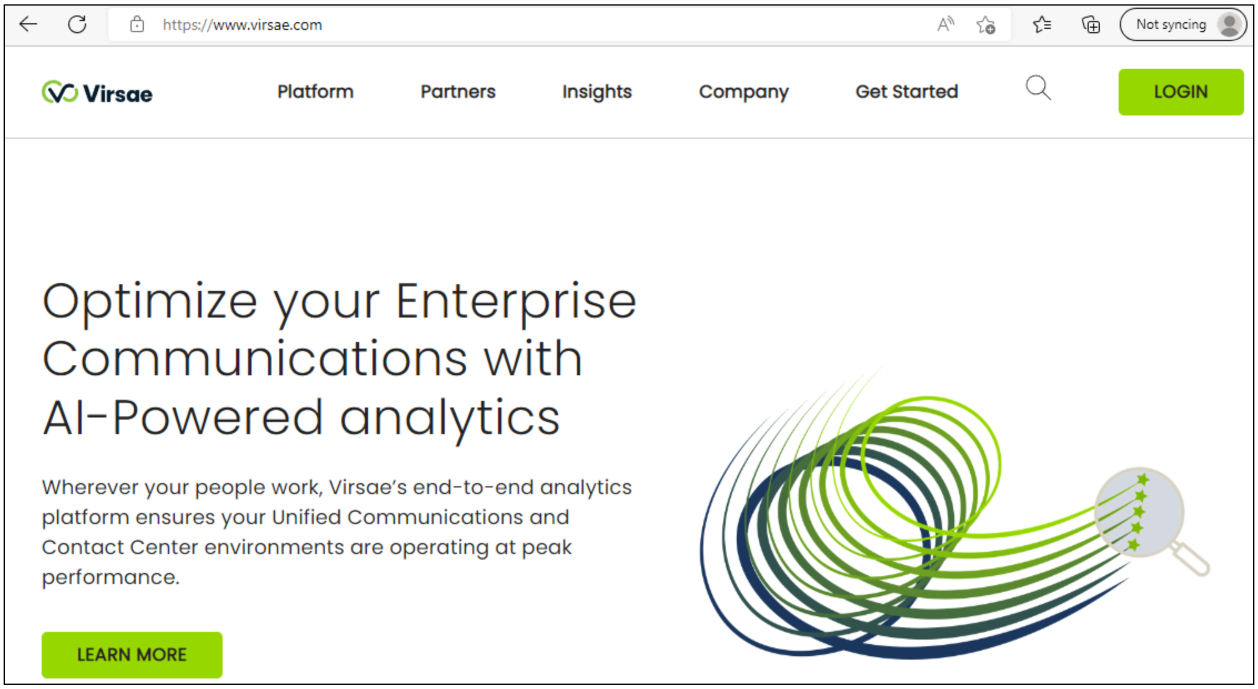
This section describes the configuration of VSM required to interoperate with System Manager.

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

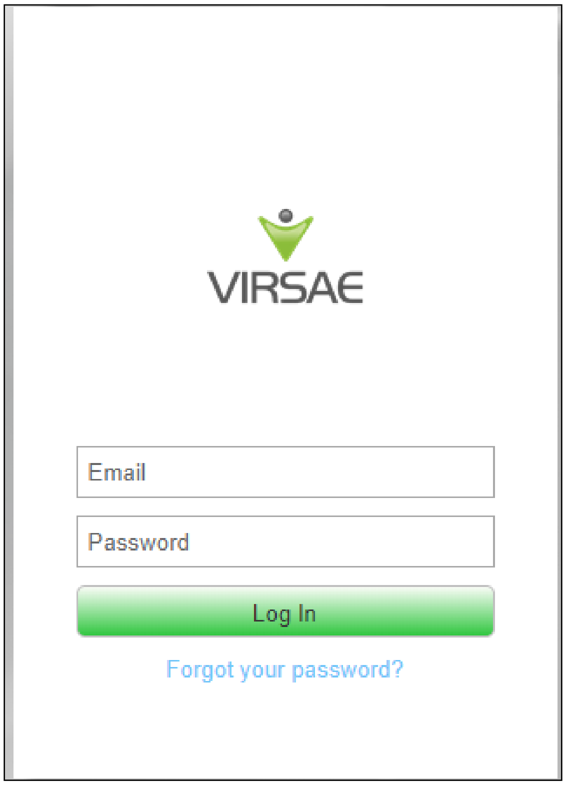
A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL *www.virsae.com* in a web browser. During compliance testing the same URL used. Click on the **LOGIN** shown on the top right below.



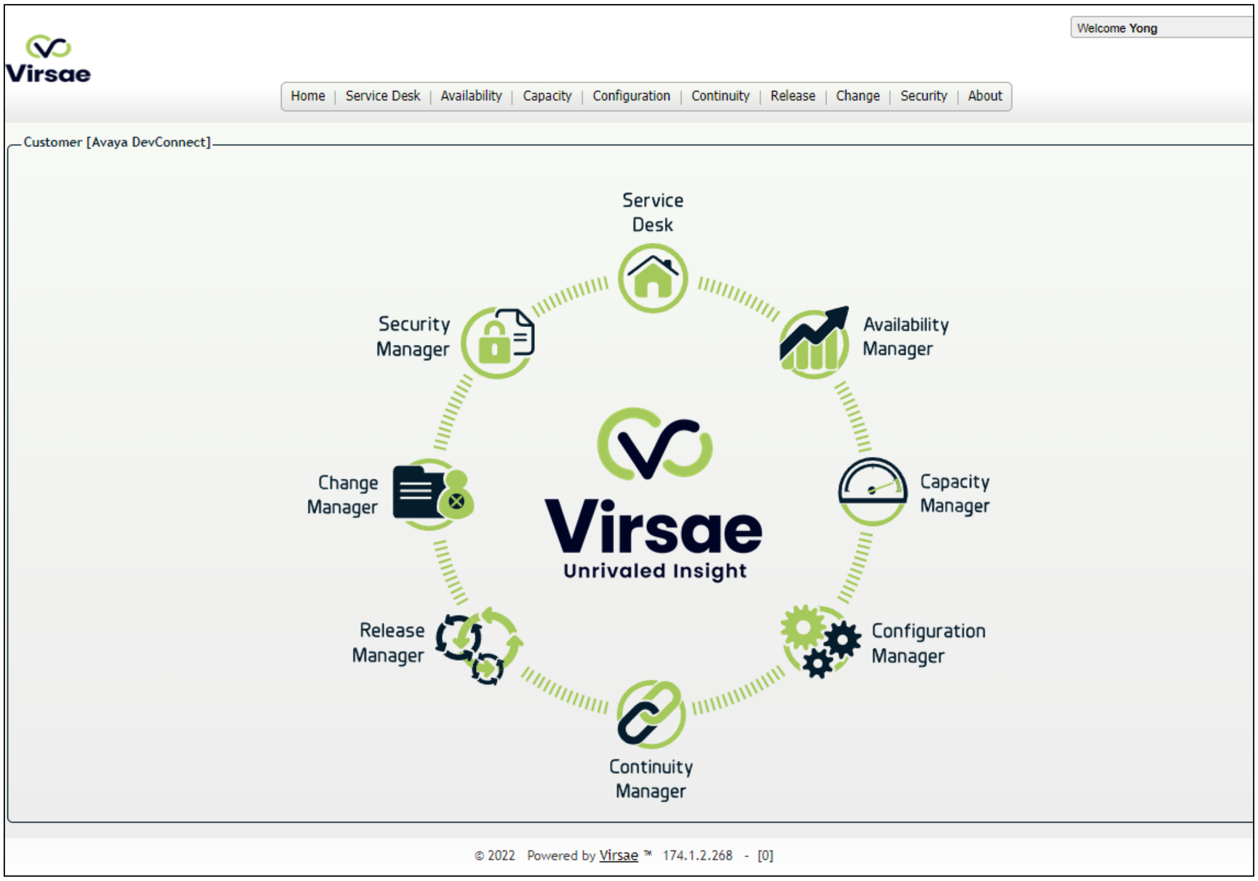
Optimize your Enterprise Communications with AI-Powered analytics

Wherever your people work, Virsae's end-to-end analytics platform ensures your Unified Communications and Contact Center environments are operating at peak performance.

Enter the **Email** and **Password** and click on the **Log In** button.

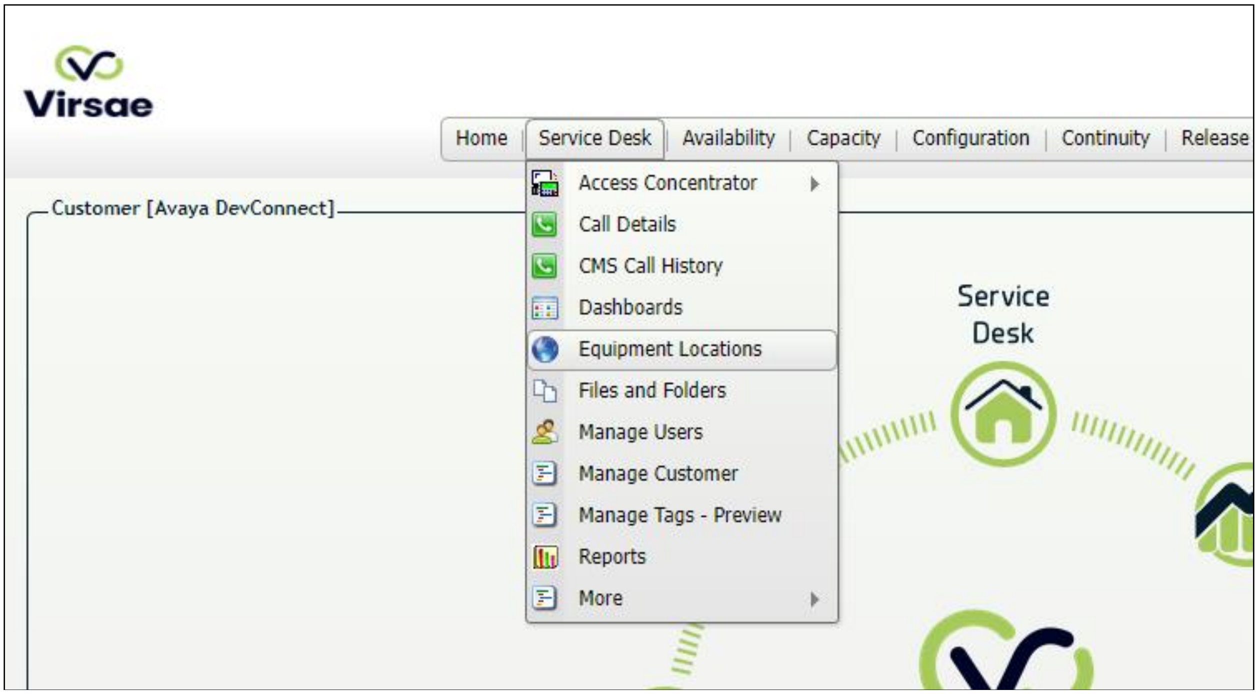


The customer screen is shown. During compliance testing the customer created by Virsae can be seen near the top right corner. Note the version running is shown at the bottom i.e., **174.1.2.268**.

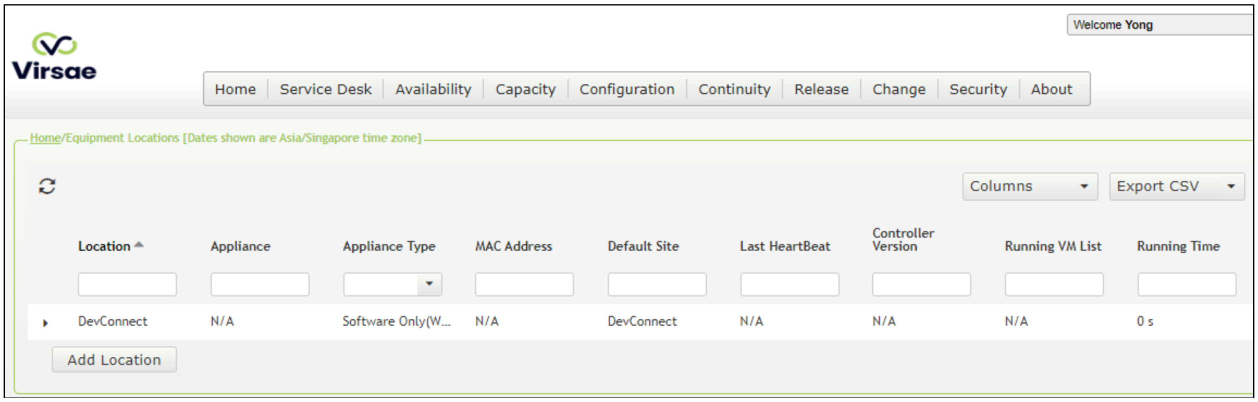


Welcome Yong
Virsae
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About
Customer [Avaya DevConnect]
Service Desk
Availability Manager
Capacity Manager
Configuration Manager
Continuity Manager
Release Manager
Change Manager
Security Manager
Virsae
Unrivaled Insight
© 2022 Powered by Virsae ™ 174.1.2.268 - [0]

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



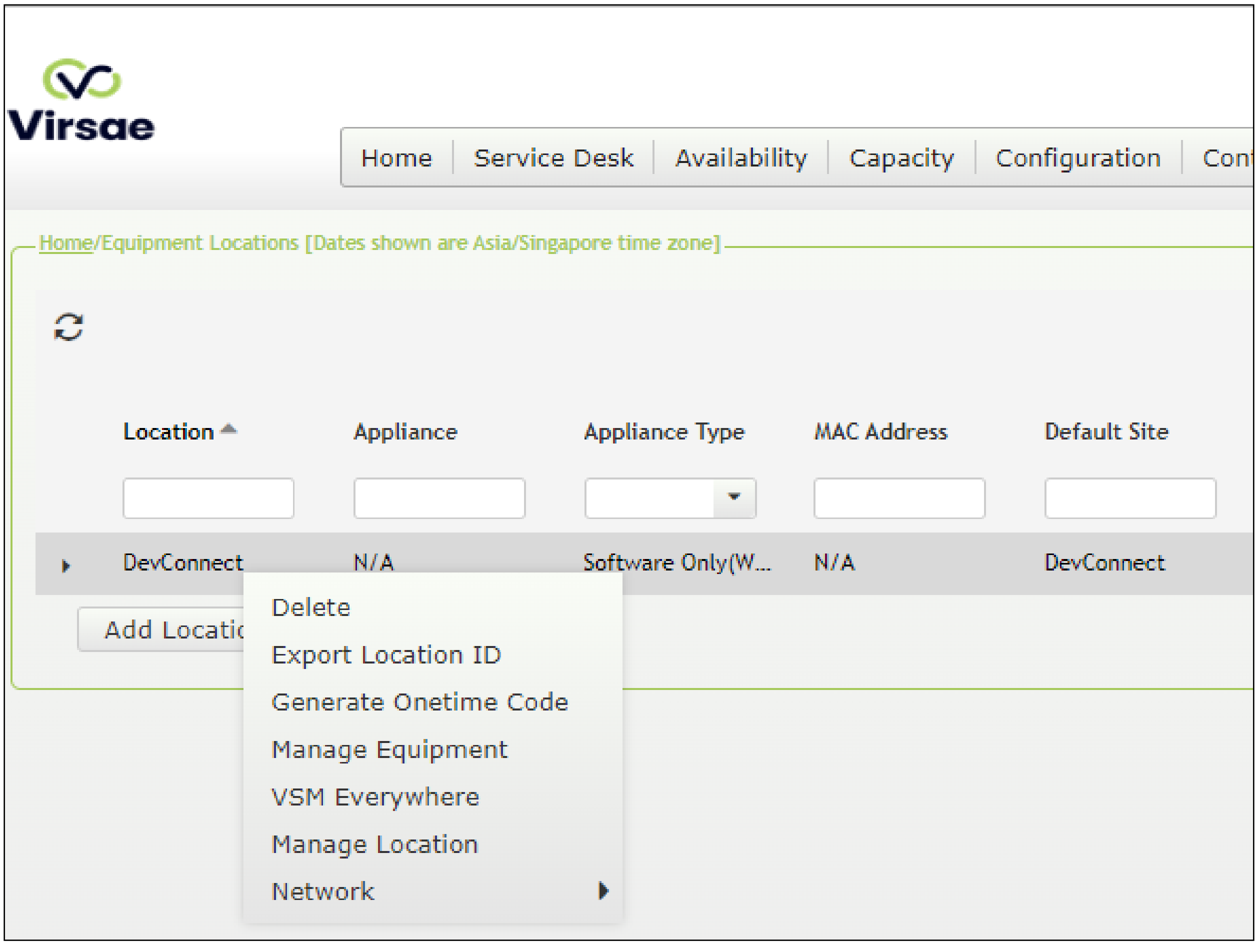
A **Location** called **DevConnect** is already configured as shown below.



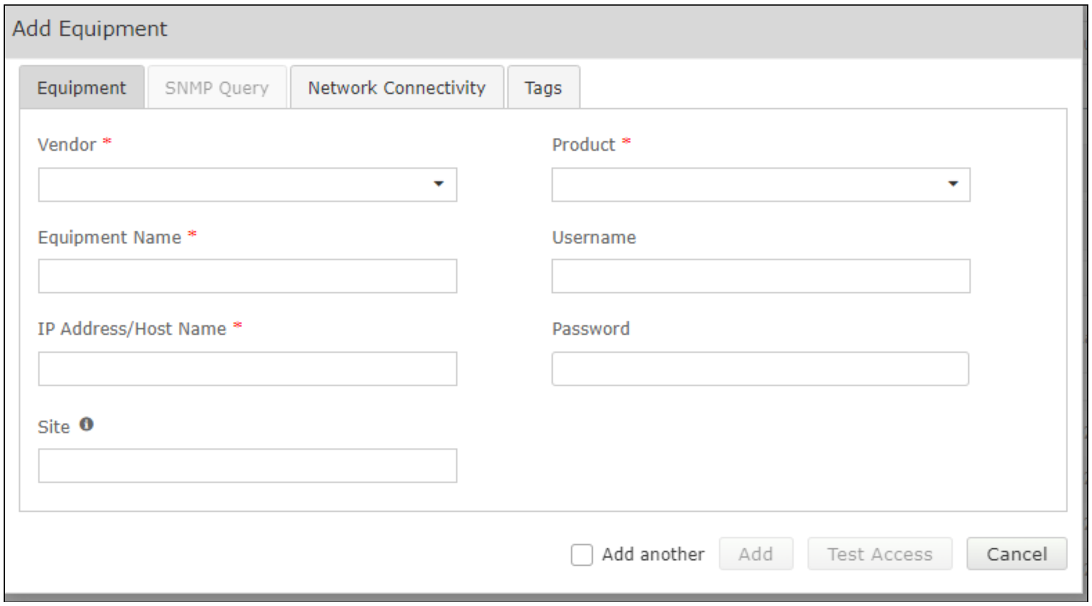
Home/Equipment Locations [Dates shown are Asia/Singapore time zone]

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

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



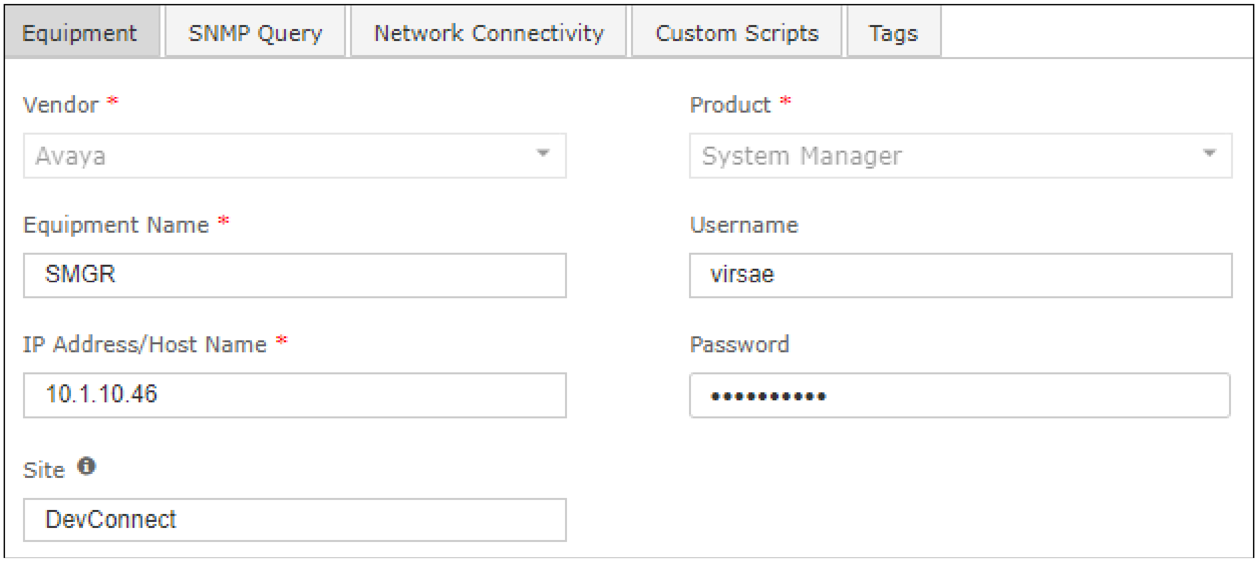
Click **Add Equipment** (not shown) and the screen below pops up:



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.



Vendor * Avaya

Product * System Manager

Equipment Name * SMGR

Username virsae

IP Address/Host Name * 10.1.10.46

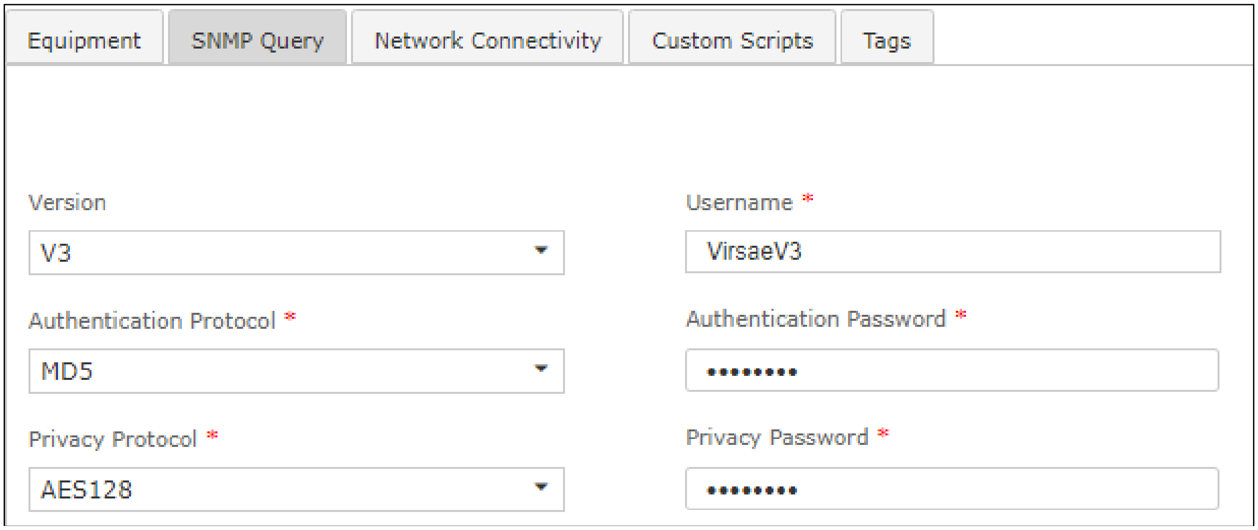
Password ••••••••••••

Site DevConnect

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

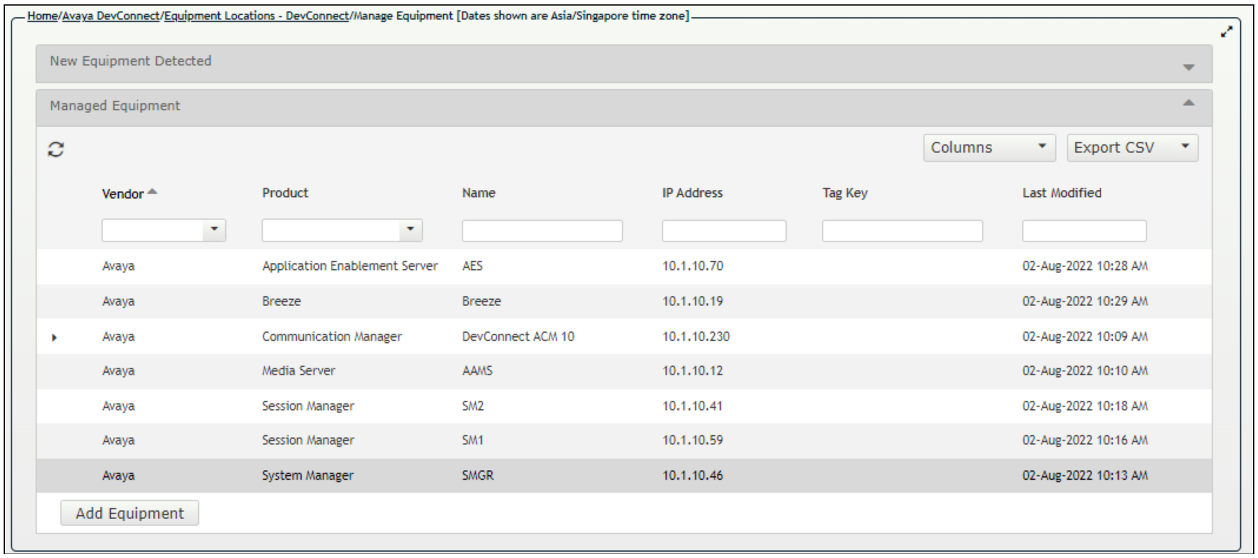
- **Version:** Select **V3** from the drop-down menu.
- **Username:** Enter username configured in **Section 5.2.**
- **Authentication Protocol**: Protocol configured in **Section 5.2**.
- **Authentication Password**: Password configured in **Section 5.2**.
- **Privacy Protocol**: Protocol configured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

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



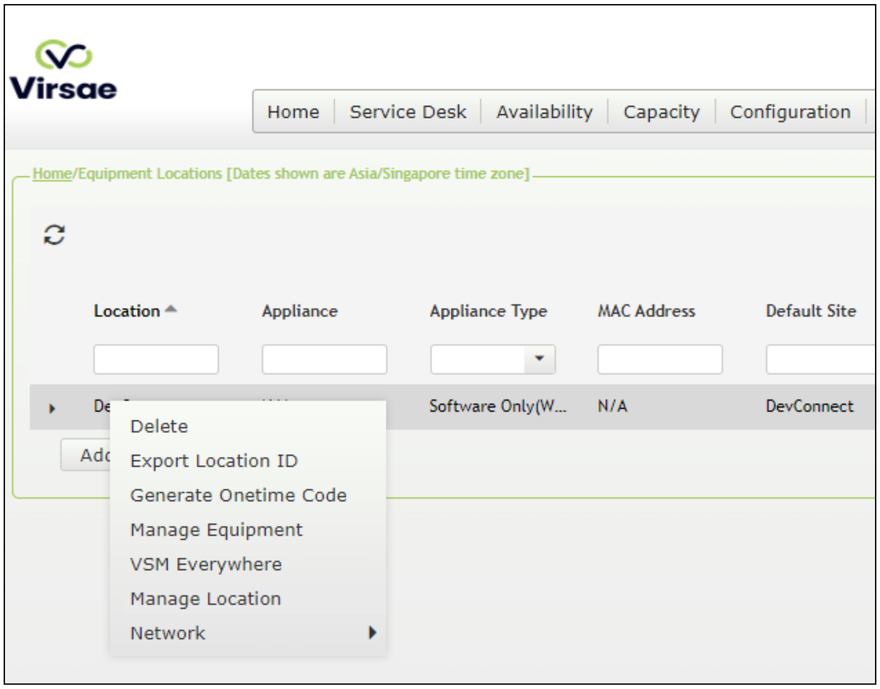
Version	Username *
V3	VirsaeV3
Authentication Protocol *	Authentication Password *
MD5	••••••••
Privacy Protocol *	Privacy Password *
AES128	••••••••

The screen below shows the added System Manager equipment.


Home/Avaya DevConnect/Equipment Locations - DevConnect/Manage Equipment [Dates shown are Asia/Singapore time zone]

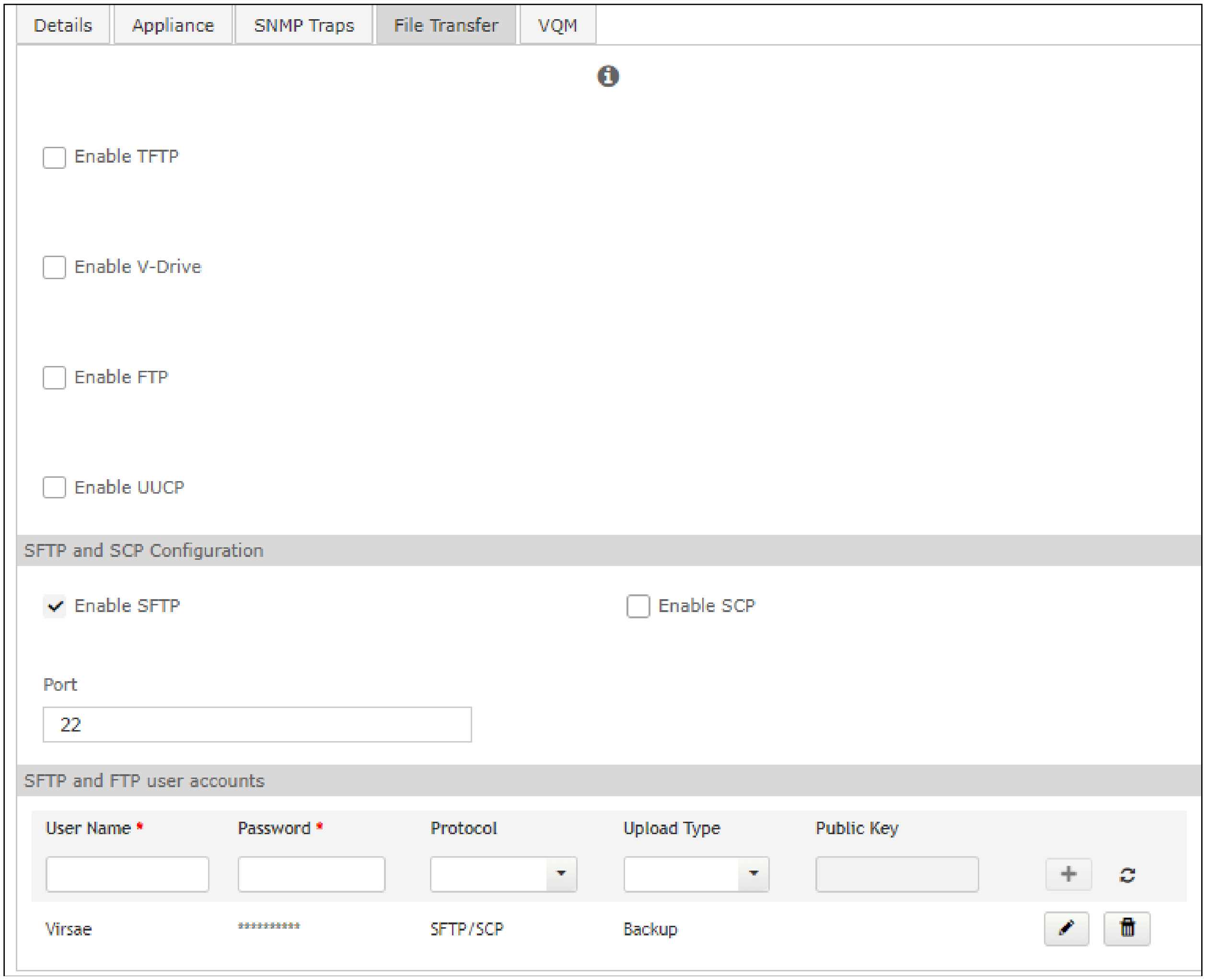
Vendor	Product	Name	IP Address	Tag Key	Last Modified
Avaya	Application Enablement Server	AES	10.1.10.70		02-Aug-2022 10:28 AM
Avaya	Breeze	Breeze	10.1.10.19		02-Aug-2022 10:29 AM
Avaya	Communication Manager	DevConnect ACM 10	10.1.10.230		02-Aug-2022 10:09 AM
Avaya	Media Server	AAMS	10.1.10.12		02-Aug-2022 10:10 AM
Avaya	Session Manager	SM2	10.1.10.41		02-Aug-2022 10:18 AM
Avaya	Session Manager	SM1	10.1.10.59		02-Aug-2022 10:16 AM
Avaya	System Manager	SMGR	10.1.10.46		02-Aug-2022 10:13 AM

Navigate to **Service Desk → Equipment Locations** (not shown), right click on the **DevConnect** and select **Manage Location**.



From the screen that pops up below, click on the **File Transfer** tab. 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.



□ Enable TFTP

□ Enable V-Drive

□ Enable FTP

□ Enable UUCP

SFTP and SCP Configuration

☑ Enable SFTP □ Enable SCP

Port

22

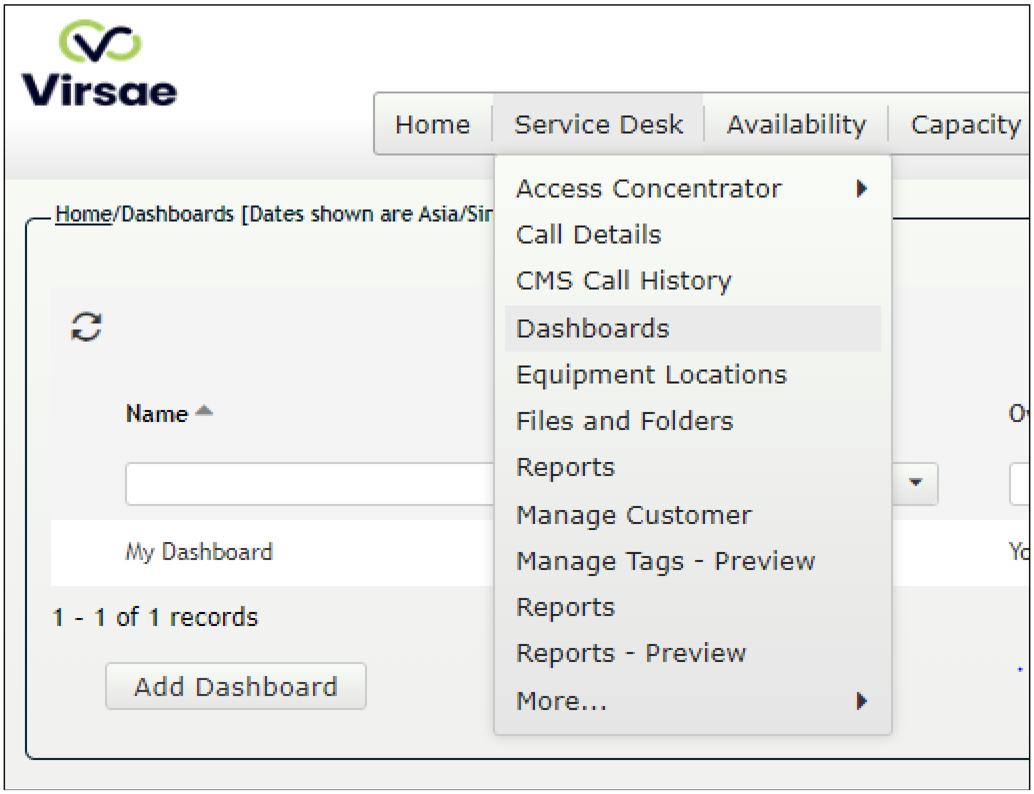
SFTP and FTP user accounts

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

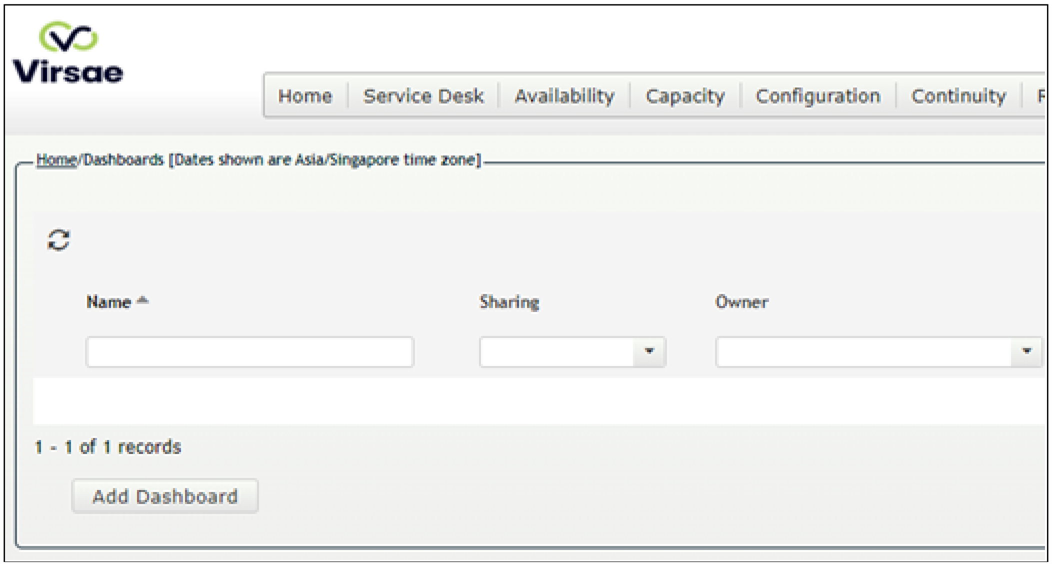
6.3. Configure Dashboard

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

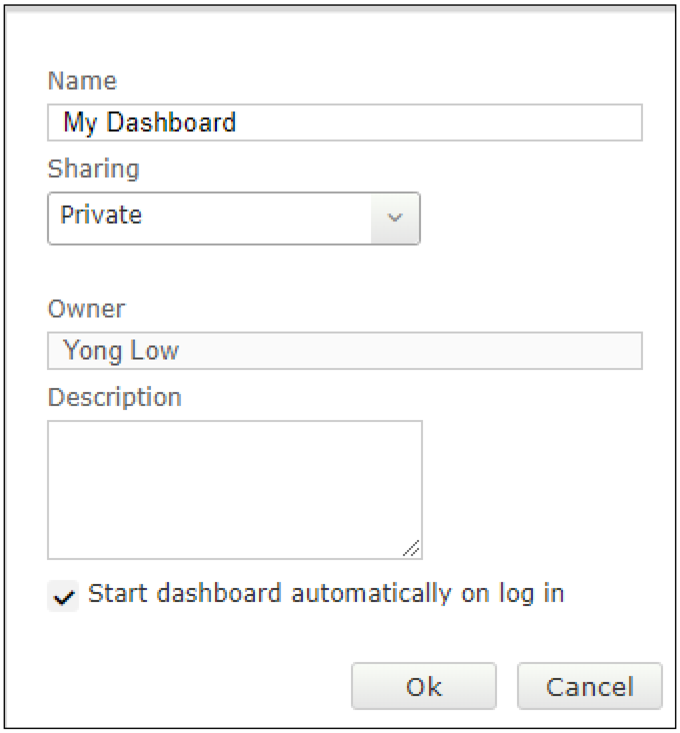
From the home screen, navigate to **Service Desk → Dashboards** as shown below.



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



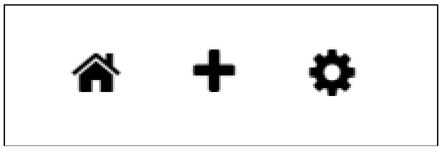
In the **Add Dashboard** window, type a descriptive name for **Name** field as shown below. Retain default values for all other fields. Click on **Start dashboard automatically on log in** box and then click on **Ok** to submit**.**



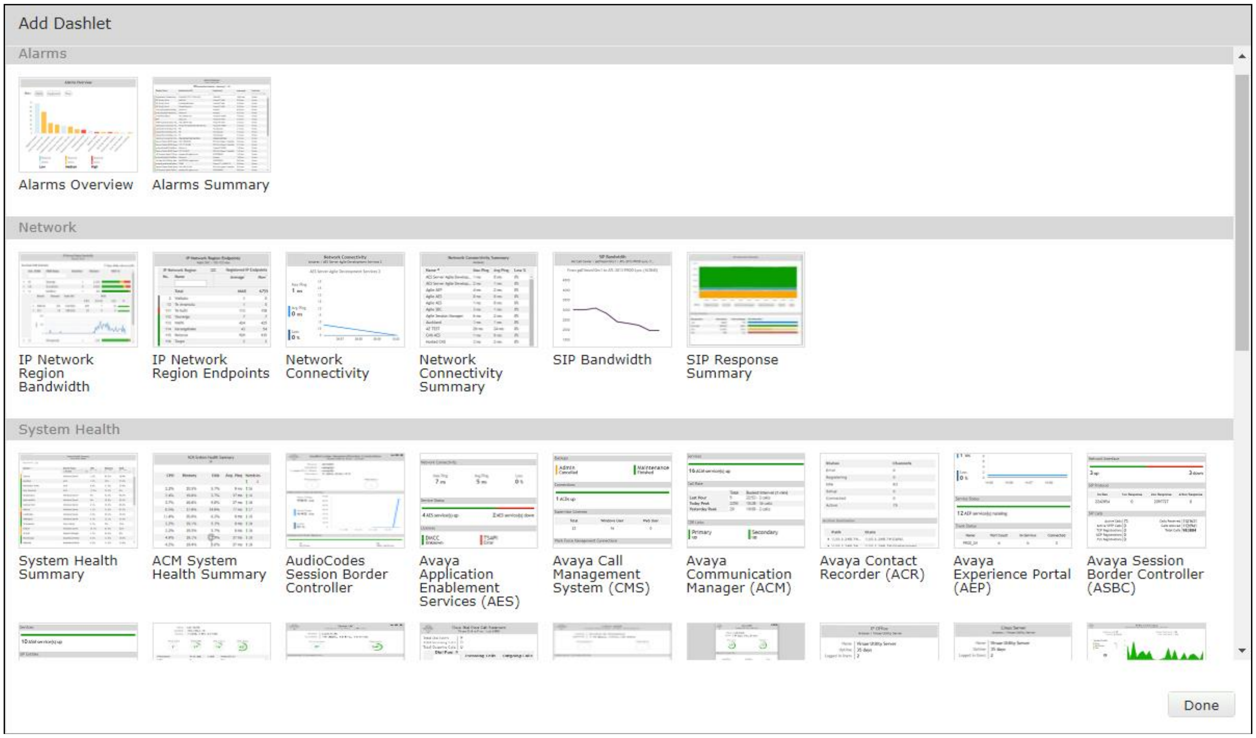
Name
My Dashboard
Sharing
Private
Owner
Yong Low
Description

☑ Start dashboard automatically on log in

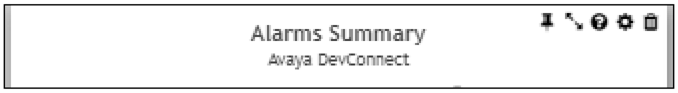
In the dashboard window bottom shown below, click on **"+"** sign at the bottom.



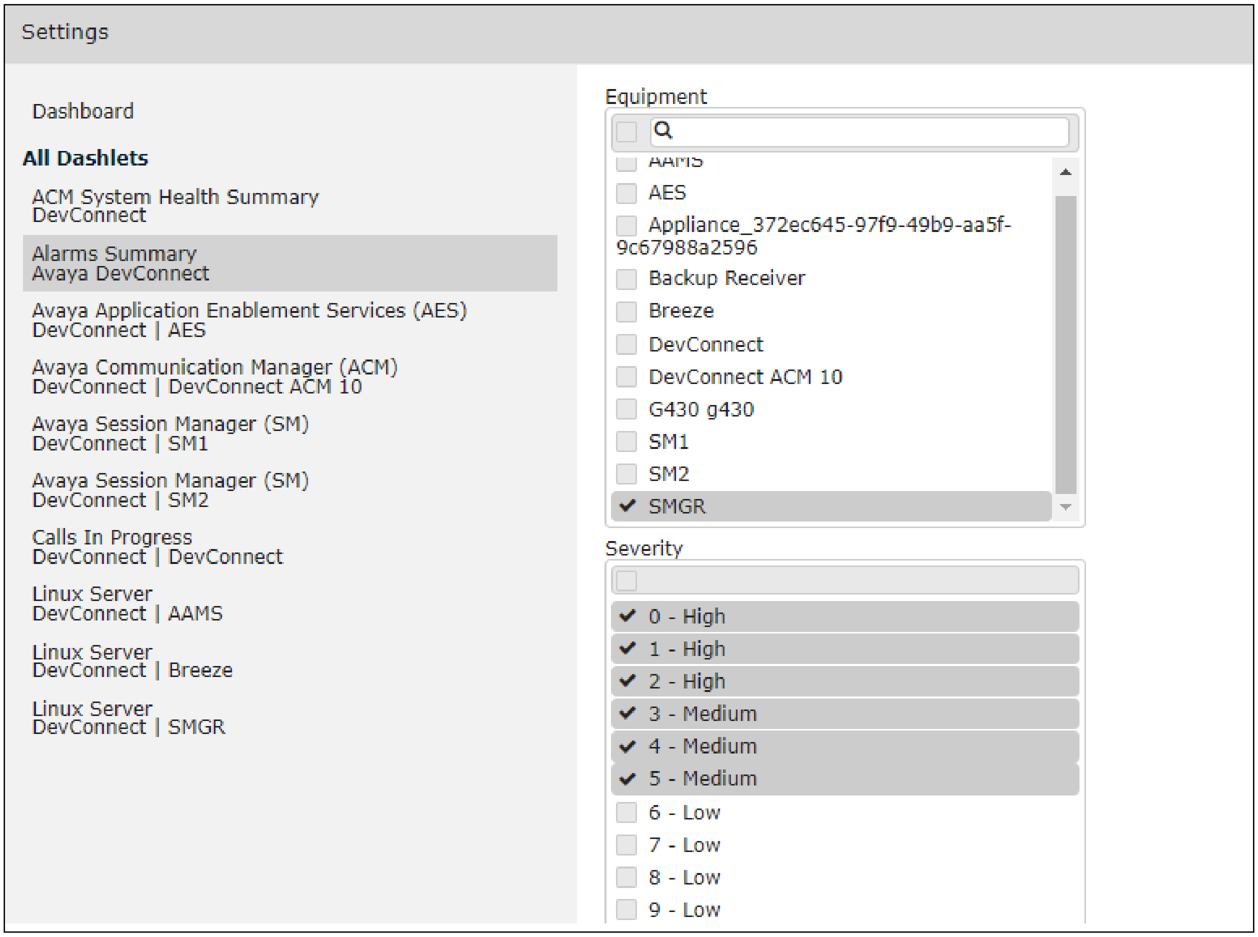
In the **Add Dashlet** window that pops up, select the **Alarms Summary** from the available dashlet by hovering the "+" image over it and click **Done**.


Add Dashlet
Alarms
Alarms Overview
Alarms Summary
Network
IP Network Region Bandwidth
IP Network Region Endpoints
Network Connectivity
Network Connectivity Summary
SIP Bandwidth
SIP Response Summary
System Health
System Health Summary
ACM System Health Summary
AudioCodes Session Border Controller
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)
Done

From the **Alarms Summary** window, select the **setup cog** on the top right corner of the box.



Select the appropriate **Equipment** i.e., **SMGR** for System Manager and the Severity of alarms desired to be shown. Click **Done** (not shown) to complete.



Settings

Dashboard

All Dashlets

ACM System Health Summary
DevConnect

Alarms Summary
Avaya DevConnect

Avaya Application Enablement Services (AES)
DevConnect | AES

Avaya Communication Manager (ACM)
DevConnect | DevConnect ACM 10

Avaya Session Manager (SM)
DevConnect | SM1

Avaya Session Manager (SM)
DevConnect | SM2

Calls In Progress
DevConnect | DevConnect

Linux Server
DevConnect | AAMS

Linux Server
DevConnect | Breeze

Linux Server
DevConnect | SMGR

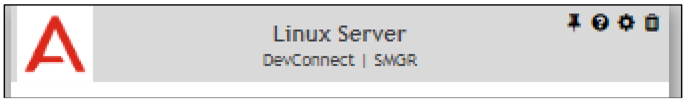
Equipment

- □ AAMS
- □ AES
- □ Appliance_372ec645-97f9-49b9-aa5f-9c67988a2596
- □ Backup Receiver
- □ Breeze
- □ DevConnect
- □ DevConnect ACM 10
- □ G430 g430
- □ SM1
- □ SM2
- ☑ SMGR

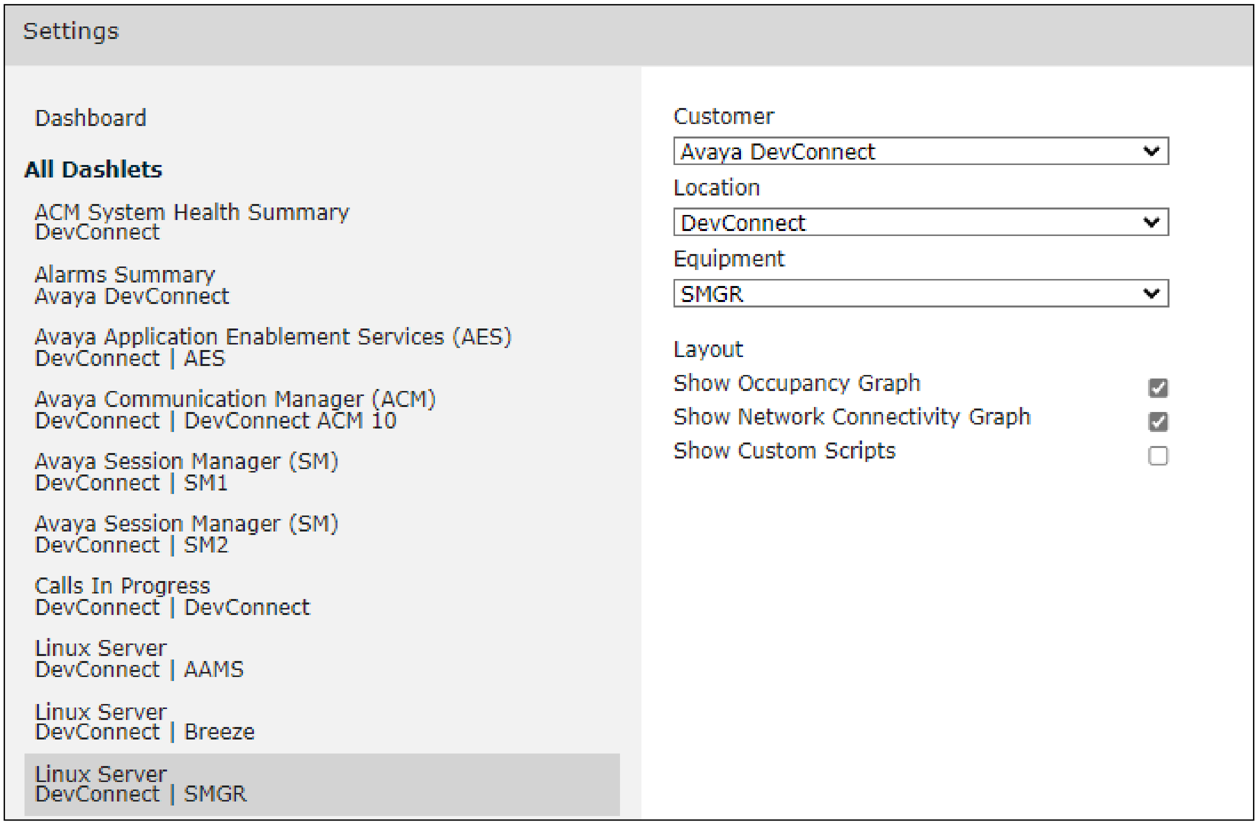
Severity

- ☑ 0 - High
- ☑ 1 - High
- ☑ 2 - High
- ☑ 3 - Medium
- ☑ 4 - Medium
- ☑ 5 - Medium
- □ 6 - Low
- □ 7 - Low
- □ 8 - Low
- □ 9 - Low

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



Linux Server
DevConnect | SMGR



Settings

Dashboard

All Dashlets

ACM System Health Summary
DevConnect

Alarms Summary
Avaya DevConnect

Avaya Application Enablement Services (AES)
DevConnect | AES

Avaya Communication Manager (ACM)
DevConnect | DevConnect ACM 10

Avaya Session Manager (SM)
DevConnect | SM1

Avaya Session Manager (SM)
DevConnect | SM2

Calls In Progress
DevConnect | DevConnect

Linux Server
DevConnect | AAMS

Linux Server
DevConnect | Breeze

Linux Server
DevConnect | SMGR

Customer: Avaya DevConnect

Location: DevConnect

Equipment: SMGR

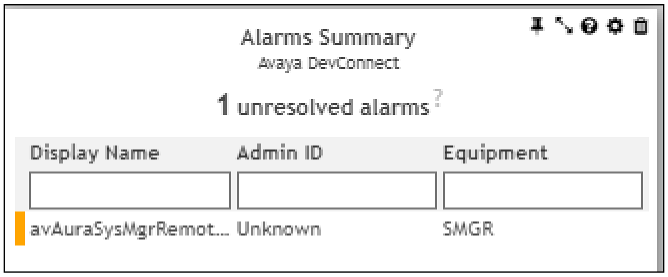
Layout

Show Occupancy Graph ☑

Show Network Connectivity Graph ☑

Show Custom Scripts □

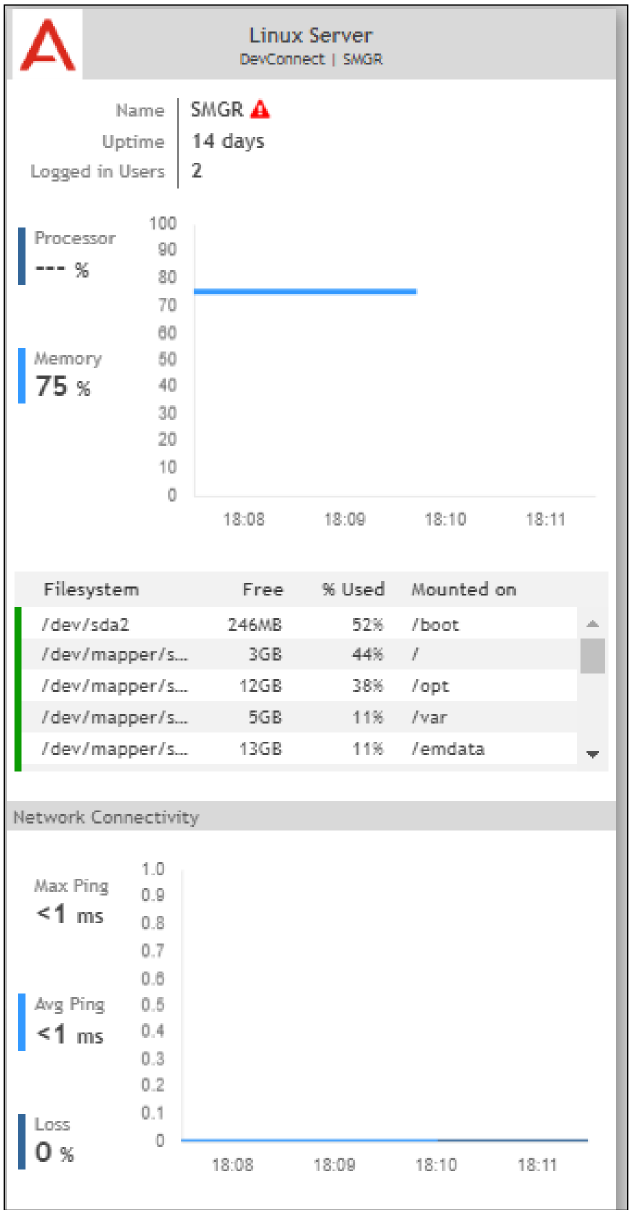
The two dashboards with the configured equipment are shown below. The above steps can be repeated to configure other equipment and/or dashboard parameters.



Alarms Summary
Avaya DevConnect

1 unresolved alarms ?

Display Name	Admin ID	Equipment
avAuraSysMgrRemot...	Unknown	SMGR



Linux Server
DevConnect | SMGR

Name	SMGR
Uptime	14 days
Logged in Users	2

Processor
--- %

Memory
75 %

Filesystem	Free	% Used	Mounted on
/dev/sda2	246MB	52%	/boot
/dev/mapper/s...	3GB	44%	/
/dev/mapper/s...	12GB	38%	/opt
/dev/mapper/s...	5GB	11%	/var
/dev/mapper/s...	13GB	11%	/emdata

Network Connectivity

Max Ping
<1 ms

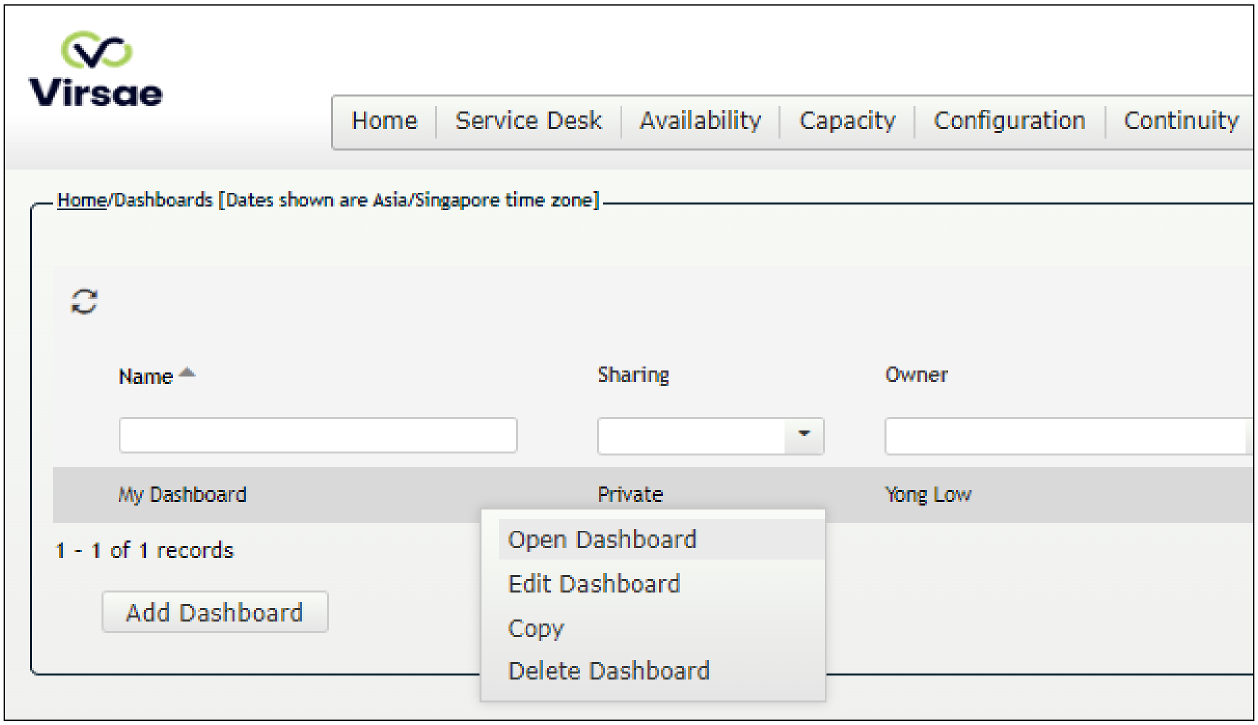
Avg Ping
<1 ms

Loss
0 %

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 → Dashboards** (not shown) and the screen is shown as below. Right click "My Dashboard" and select "Open Dashboard".



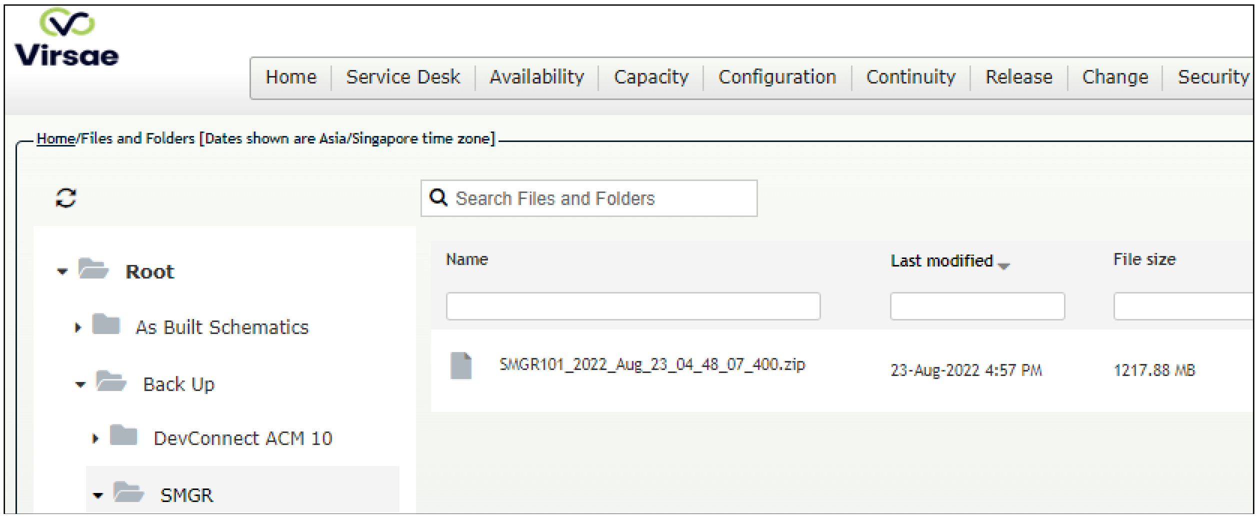
Home/Dashboards [Dates shown are Asia/Singapore time zone]

Name	Sharing	Owner
My Dashboard	Private	Yong Low

1 - 1 of 1 records

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.

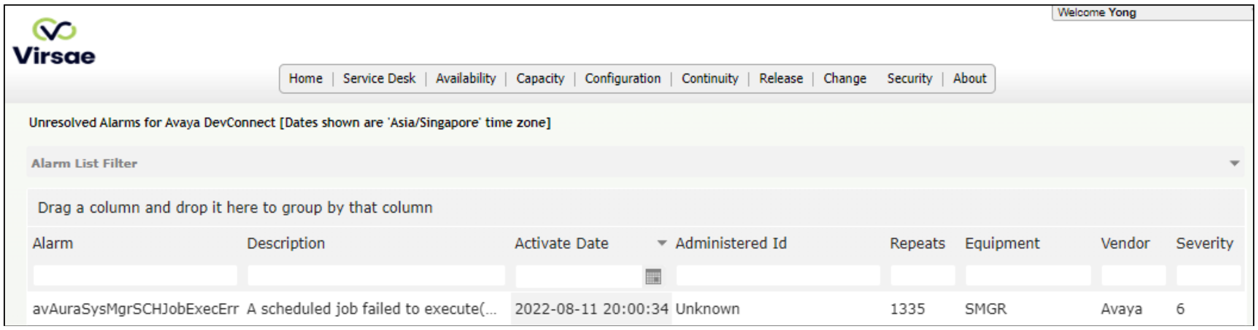
Perform a backup of the System Manager to VSM. Refer to reference **[2]** for details of how to backup SMGR. To view the off-site backups on VSM, navigate to **Continuity → Browse Backups** (not shown). Screen below shows an example of backups for System Manager.


Virsae
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security
Search Files and Folders
Root
As Built Schematics
Back Up
DevConnect ACM 10
SMGR

Home/Files and Folders [Dates shown are Asia/Singapore time zone]

Name	Last modified	File size
SMGR101_2022_Aug_23_04_48_07_400.zip	23-Aug-2022 4:57 PM	1217.88 MB

To view alarms using reporting, navigate to **Availability → Manage Alarms** (not shown). A list of all unresolved alarms for all equipment is shown. In the **Equipment** column, look for SMGR and the related alarms.


Welcome Yong
Virsae
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About
Alarm List Filter
Drag a column and drop it here to group by that column

Unresolved Alarms for Avaya DevConnect [Dates shown are 'Asia/Singapore' time zone]

Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Vendor	Severity
avAuraSysMgrSCHJobExecErr	A scheduled job failed to execute(...	2022-08-11 20:00:34	Unknown	1335	SMGR	Avaya	6

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R174 to interoperate with Avaya Aura® System Manager R10.1. 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® System Manager in Virtualized Environment*, Release 10.1, Issue 2, Mar 2022.
2. *Administering Avaya Aura® System Manager*, Release 10.1, Issue 3, Feb 2022.

Product documentation for Virsae products may be found at https://documentation.virsae.com.

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.