Avaya Solution & Interoperability Test Lab

Application Notes for Virsae Service Management with Avaya Aura® Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R135 to interoperate with Avaya Aura® Application Enablement Services 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 monitored Application Enablement Services 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® Application Enablement Services (herein after referred to as AES). 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.

VSM uses Linux shell access connections to monitor AES statistics such as CPU, Memory and Disk Usage, License information and AE Services links status detail and SNMP for 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 connections to monitor and display system status from AES.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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.

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

- Verify that the server statistics information for AES is populated on VSM dashboard such as CPU, Memory and Disk Usage and list of Software/Processes.
- Verify proper display of AES server status and link information included SNMP Availability, Raised Alerts, Link Status, TSAPI Client Connections and DMCC Sessions.

- Verify that the list of AES links is visible in VSMs: ASAI Link, DLG CTI Link, TSAPI CTI Link and TSAPI TLink, along with utilization details.
- Verify License, DMCC and TSAPI Status were displayed correctly.

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 AES. In the compliance Communication Manager with a G430 Media Gateway connected to AES using the CTI link. The system has Avaya Workplace client for Windows and one-X® Communicator (SIP and H.323) softphone 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.

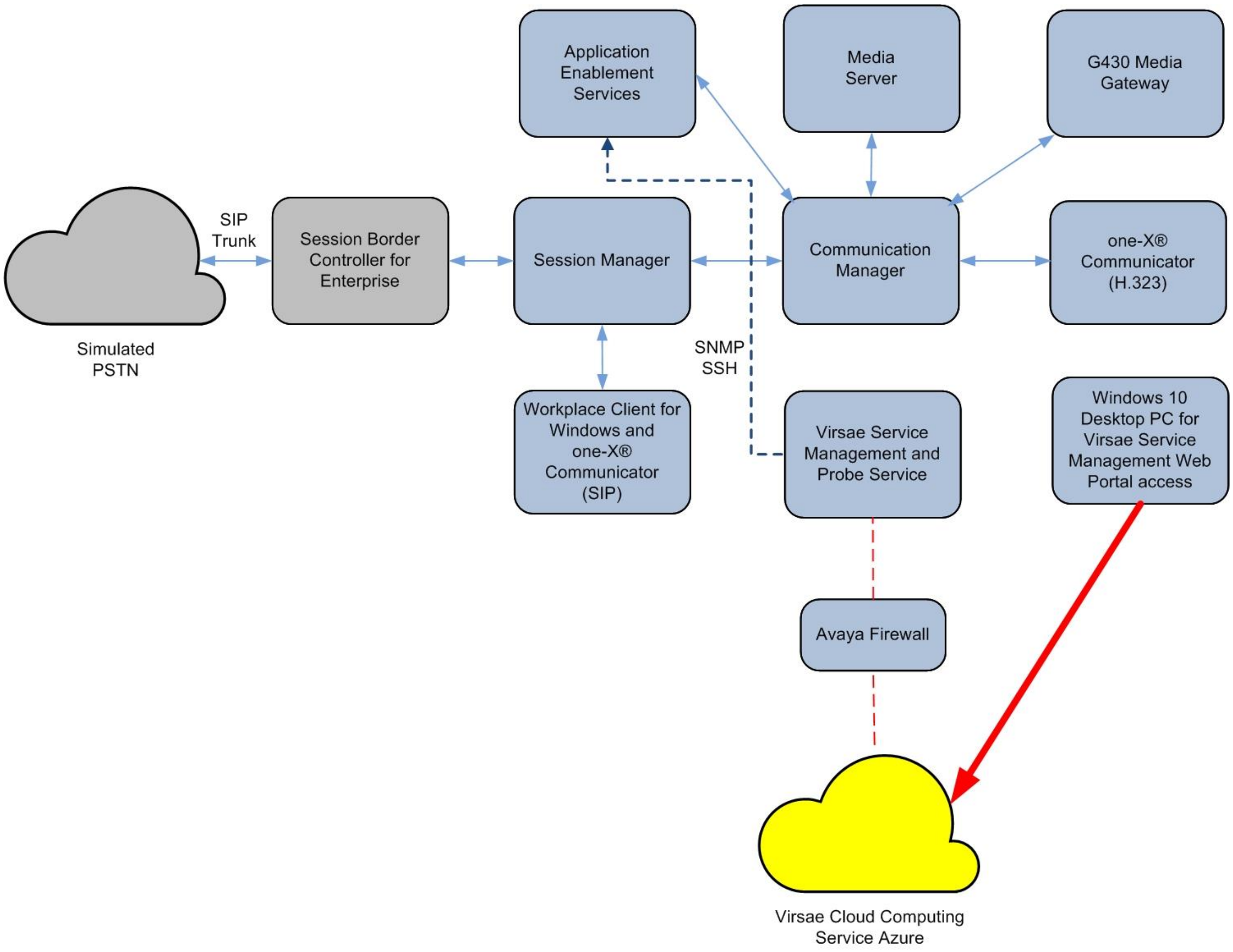

Application Enablement Services
Media Server
G430 Media Gateway
SIP Trunk
Session Border Controller for Enterprise
Session Manager
Communication Manager
one-X® Communicator (H.323)
Simulated PSTN
SNMP SSH
Workplace Client for Windows and one-X® Communicator (SIP)
Virsae Service Management and Probe Service
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® Application Enablement Services running on virtual server	8.1.2.1.0.6-0
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

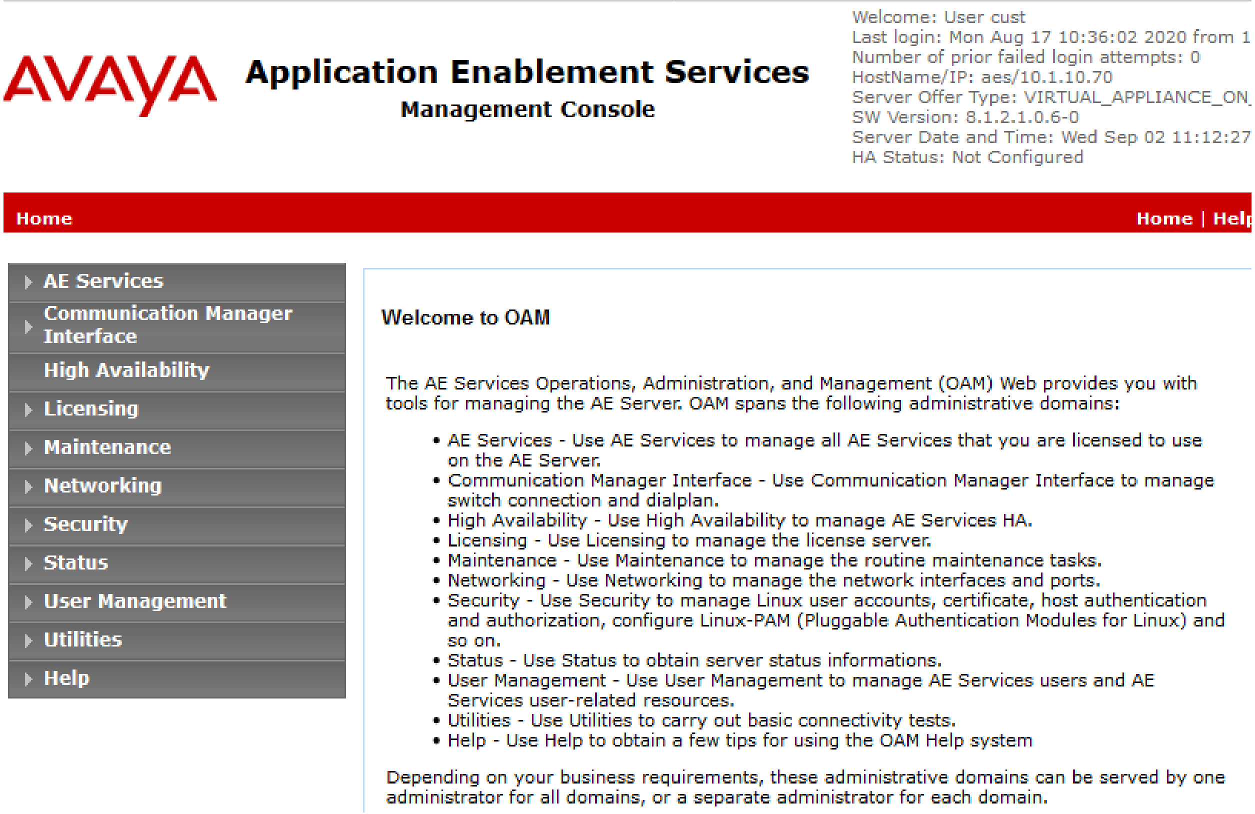
The configuration of Communication Manager and AES is assumed to be in place and will not be discussed in this document. For more information of how to configure Communication Manager and AES, please refer to **Section 10**.

6. Configure Avaya Aura® Application Enablement Services

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

AES is configured via the AES Management 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 AES. Log in using the appropriate login credential. The screen shown below is displayed.

Note: Not all screens in this section are shown after AES had been configured. Click **Save** button to save the screen parameters configured on AES if needed.



Welcome: User cust
Last login: Mon Aug 17 10:36:02 2020 from 1
Number of prior failed login attempts: 0
HostName/IP: aes/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_
SW Version: 8.1.2.1.0.6-0
Server Date and Time: Wed Sep 02 11:12:27
HA Status: Not Configured

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

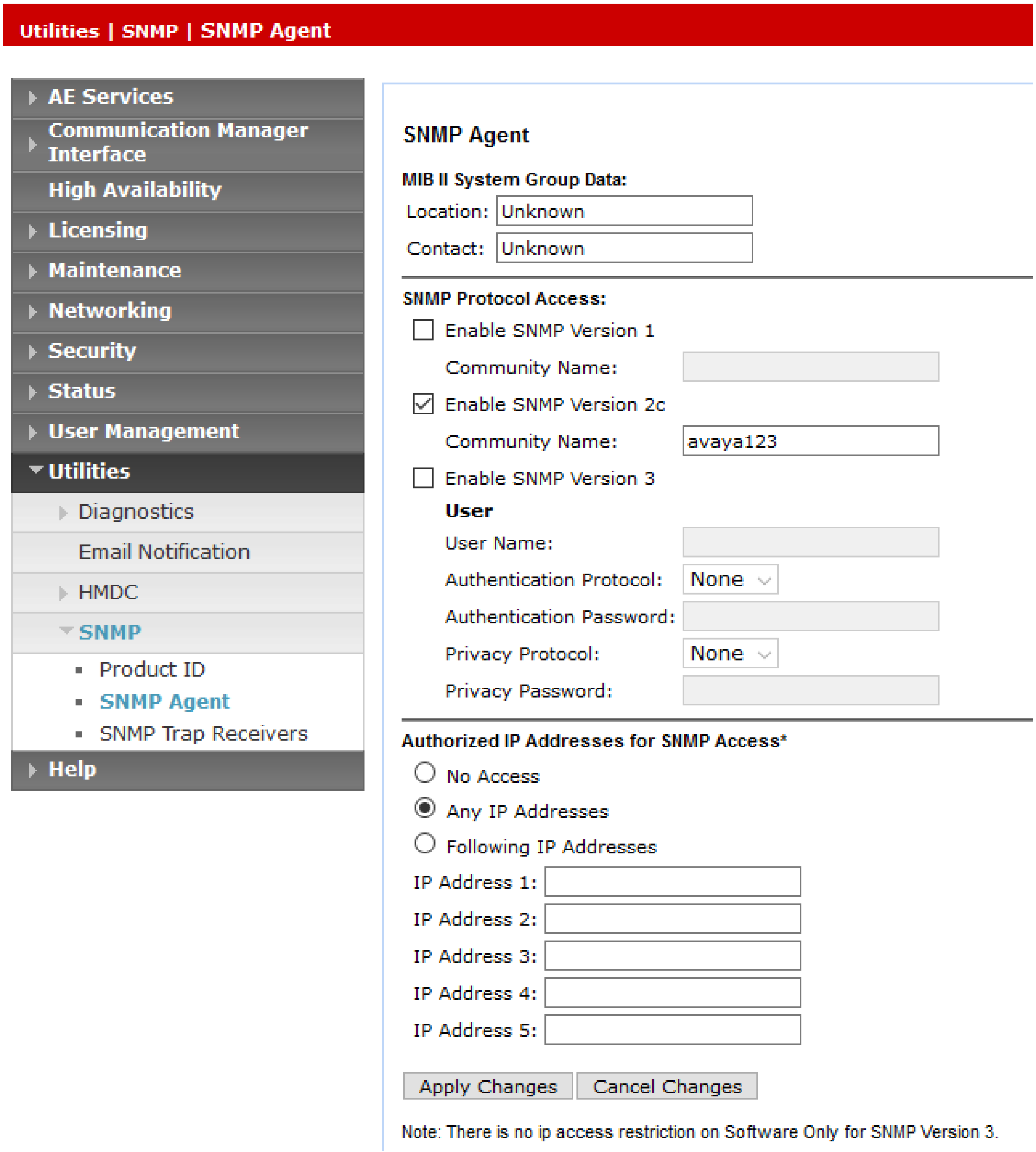
Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.1. Configure SNMP Connection

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

- Check the **Enable SNMP Version 2c** box.
- **Community Name:** Configured as **avaya123** during compliance testing.
- Select the radio button for **Any IP Addresses** to allow for connection. However, it would be more secure with using specific address.

Retain default values for all other fields and click on the **Apply Changes** button.



SNMP Agent

MIB II System Group Data:

Location: Unknown

Contact: Unknown

SNMP Protocol Access:

□ Enable SNMP Version 1

Community Name:

☑ Enable SNMP Version 2c

Community Name: avaya123

□ Enable SNMP Version 3

User

User Name:

Authentication Protocol: None

Authentication Password:

Privacy Protocol: None

Privacy Password:

Authorized IP Addresses for SNMP Access*

○ No Access

● Any IP Addresses

○ Following IP Addresses

IP Address 1:

IP Address 2:

IP Address 3:

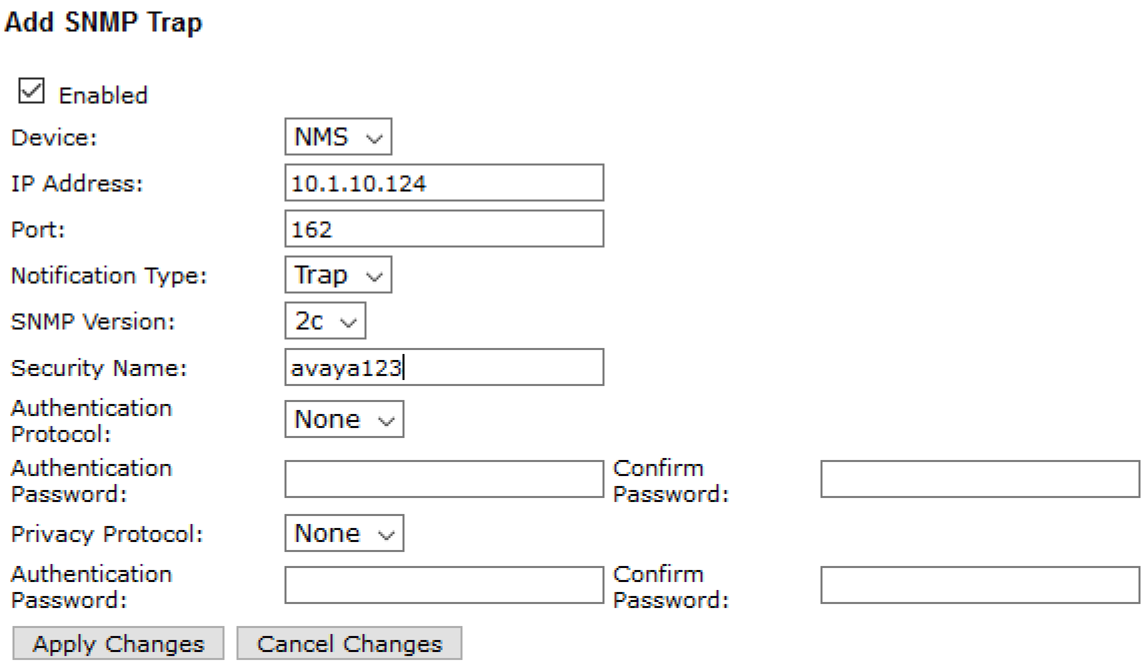
IP Address 4:

IP Address 5:

Note: There is no ip access restriction on Software Only for SNMP Version 3.

Navigate to **Utilities** → **SNMP** → **SNMP Trap Receivers**, then click **Add**. Configure the following and leave the rest as default. Click **Apply Changes** below.

- Tick the **Enabled** box.
- **Device**: Select **NMS**.
- **IP Address**: Enter the VSM server IP address.
- **Port**: Enter **162** for the default port of SNMP trap.
- **SNMP Version**: Select **2c**.
- **Security Name**: Enter security name desired.



Add SNMP Trap

☑ Enabled

Device:	NMS		
IP Address:	10.1.10.124		
Port:	162		
Notification Type:	Trap		
SNMP Version:	2c		
Security Name:	avaya123		
Authentication Protocol:	None		
Authentication Password:		Confirm Password:	
Privacy Protocol:	None		
Authentication Password:		Confirm Password:	

6.2. Configure Login Account

Create an Administrator account on AES since VSM requires access to AES with Administrative Rights. The new account should be like the default "**cust**" account. Log into AES 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
```

7. Configure Virsae Service Management

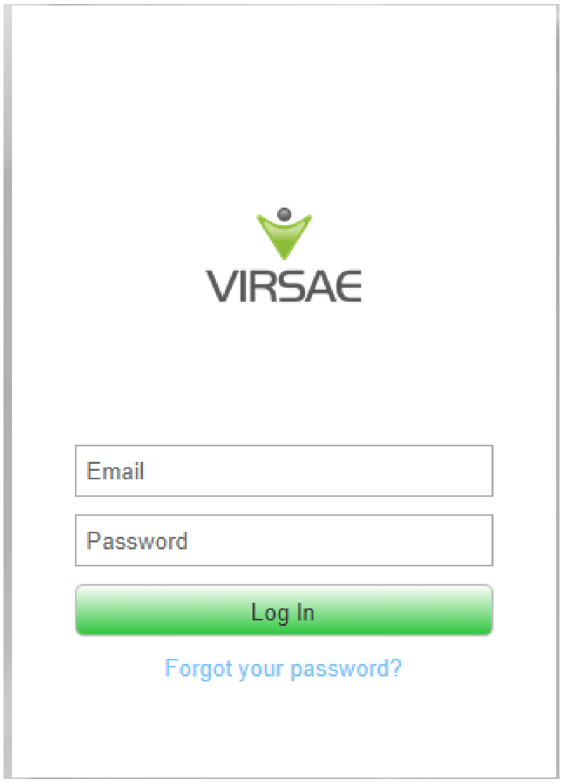
This section describes the configuration of VSM required to interoperate with AES.

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 these 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:

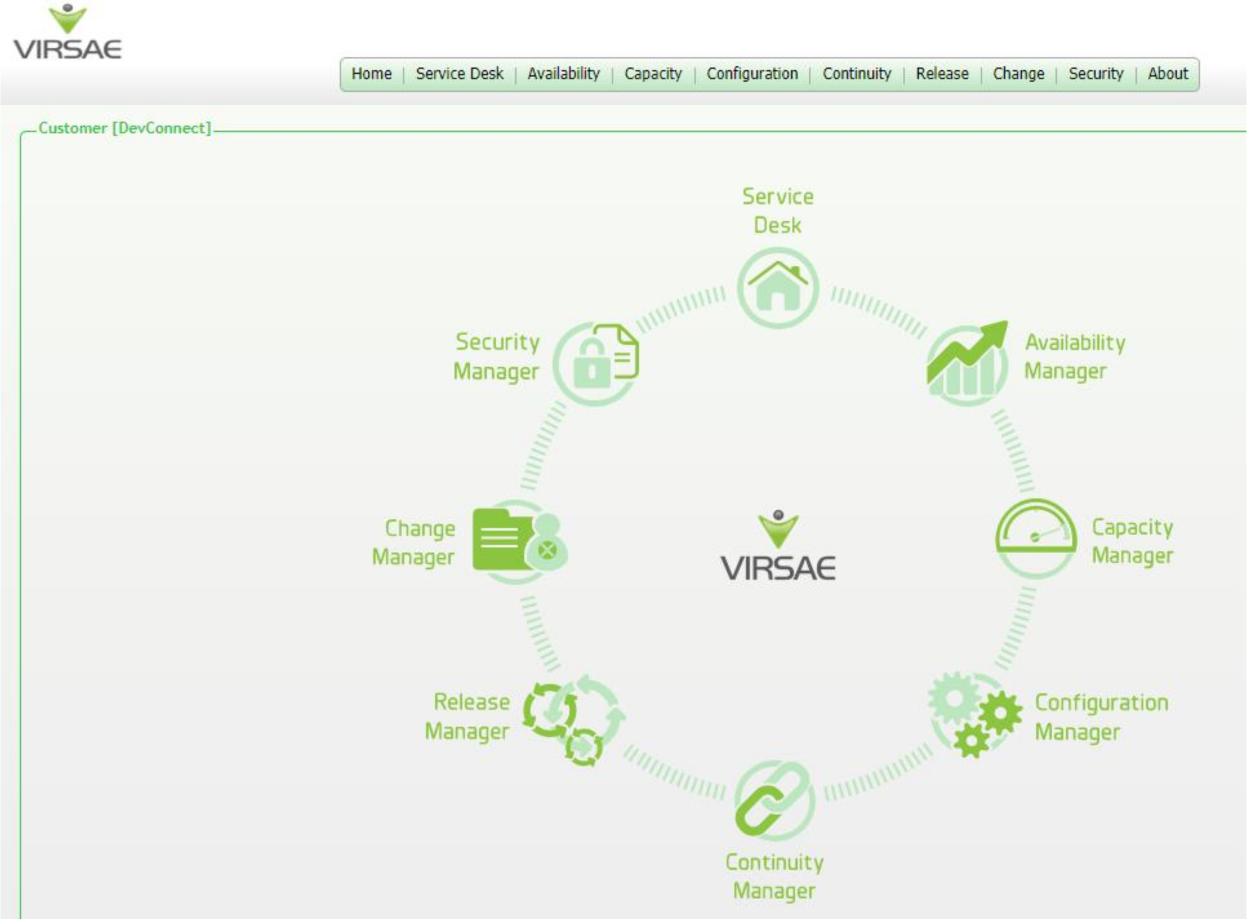
- Login to the Web Portal
- Configuring Avaya Aura® Application Enablement Services
- Configure Dashboard

7.1. Login to the Web Portal

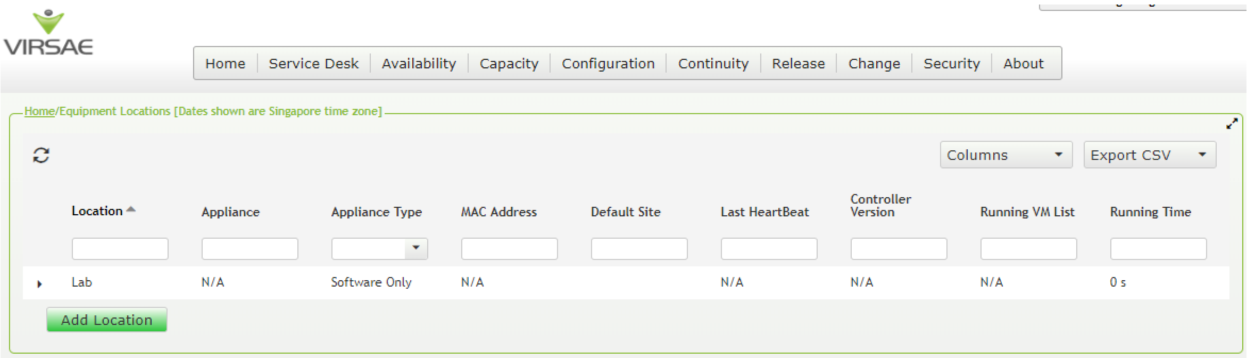
A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL <*business partner name*>.*virsae.com* in a web browser. During compliance testing the URL used was "*preview.virsae.com*". The Login screen is shown as below. Enter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

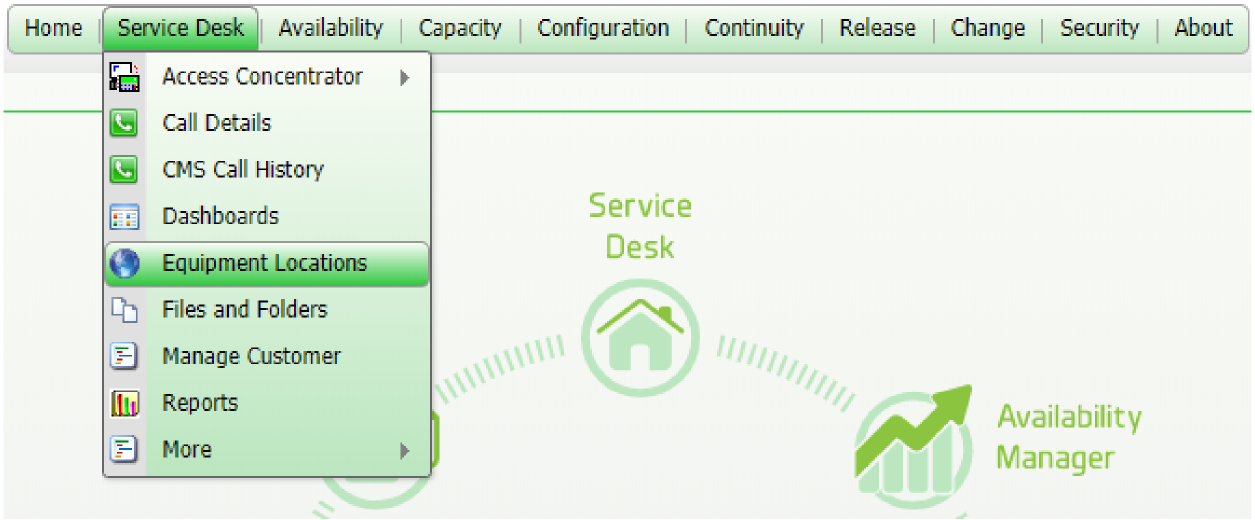


Navigate to **Service Desk → Equipment Locations** as shown below.

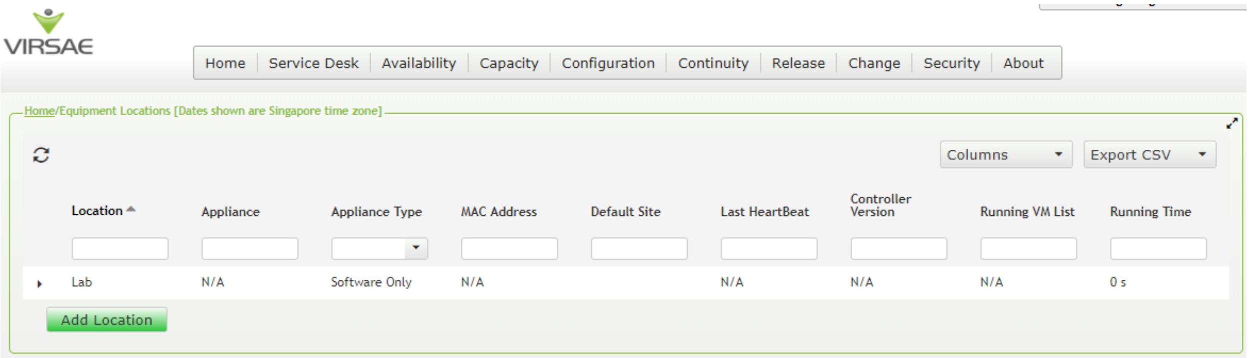

VIRSAE
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About
Columns
Export CSV
Add Location

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

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	0 s



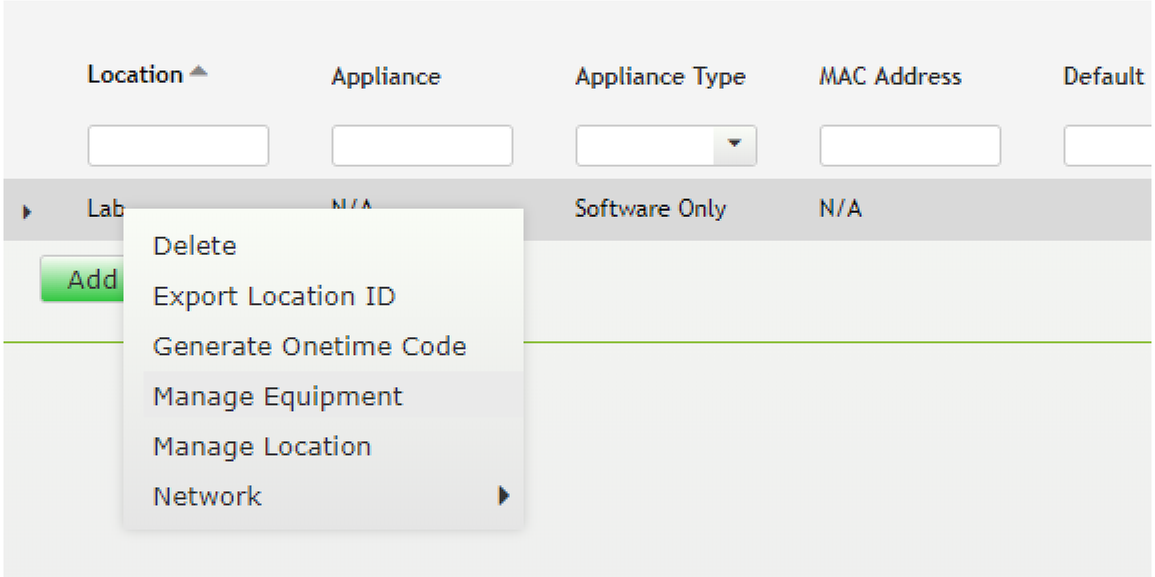
A **Location** called **Lab** is already configured as shown below.


VIRSAE
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About
Columns
Export CSV
Add Location

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

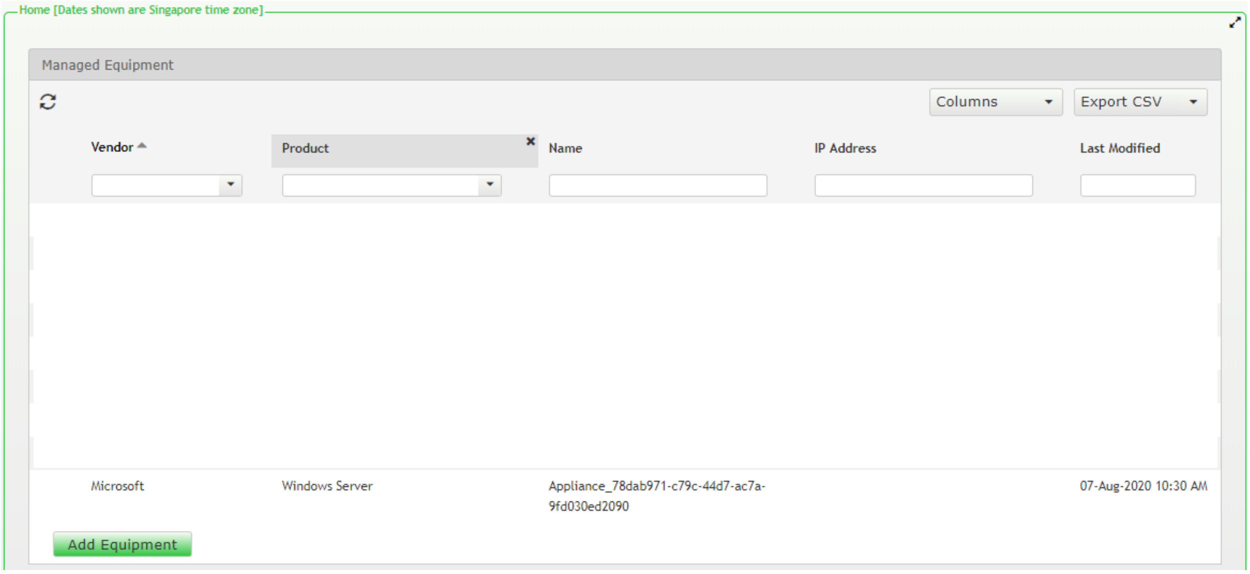
Location	Appliance	Appliance Type	MAC Address	Default Site	Last HeartBeat	Controller Version	Running VM List	Running Time
Lab	N/A	Software Only	N/A		N/A	N/A	N/A	0 s

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



Location	Appliance	Appliance Type	MAC Address	Default
Lab	N/A	Software Only	N/A	

Click **Add Equipment** below:



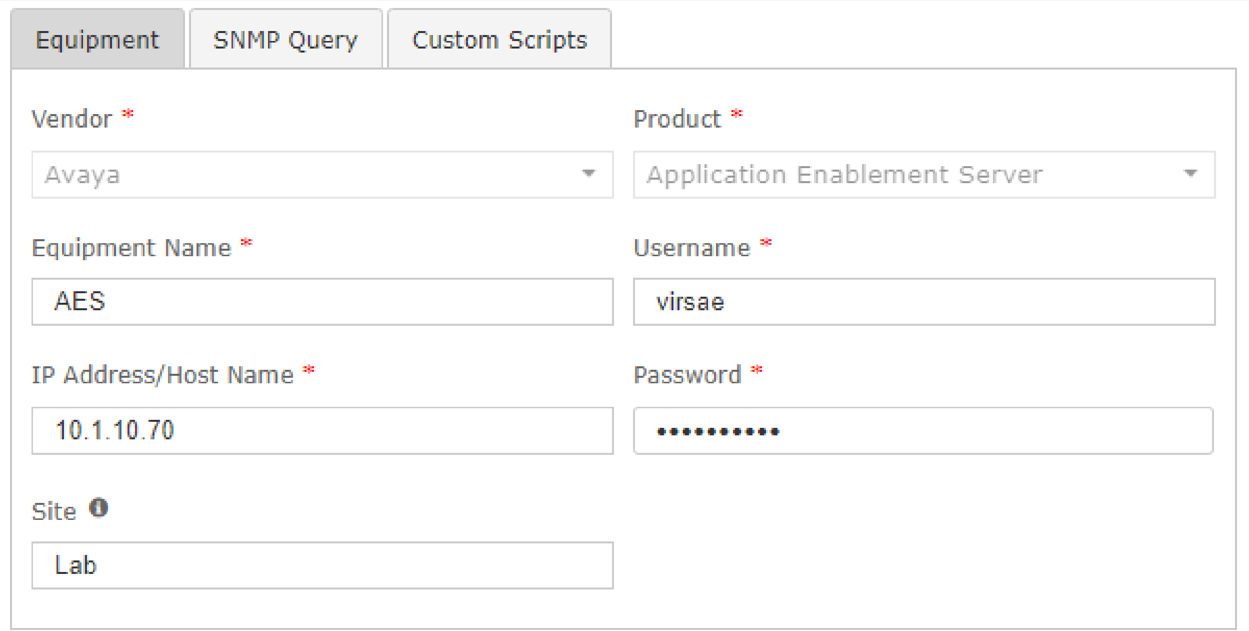
Vendor	Product	Name	IP Address	Last Modified
Microsoft	Windows Server	Appliance_78dab971-c79c-44d7-ac7a-9fd030ed2090		07-Aug-2020 10:30 AM

7.2. Configuring Avaya Aura® Application Enablement Services

From the **Add Equipment** window, add AES to the Location. Select **Avaya** from the **Vendor** list. Select **Application Enablement Server** from the **Product** list. Configure the following values.

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

Below are the configured values of the AES.

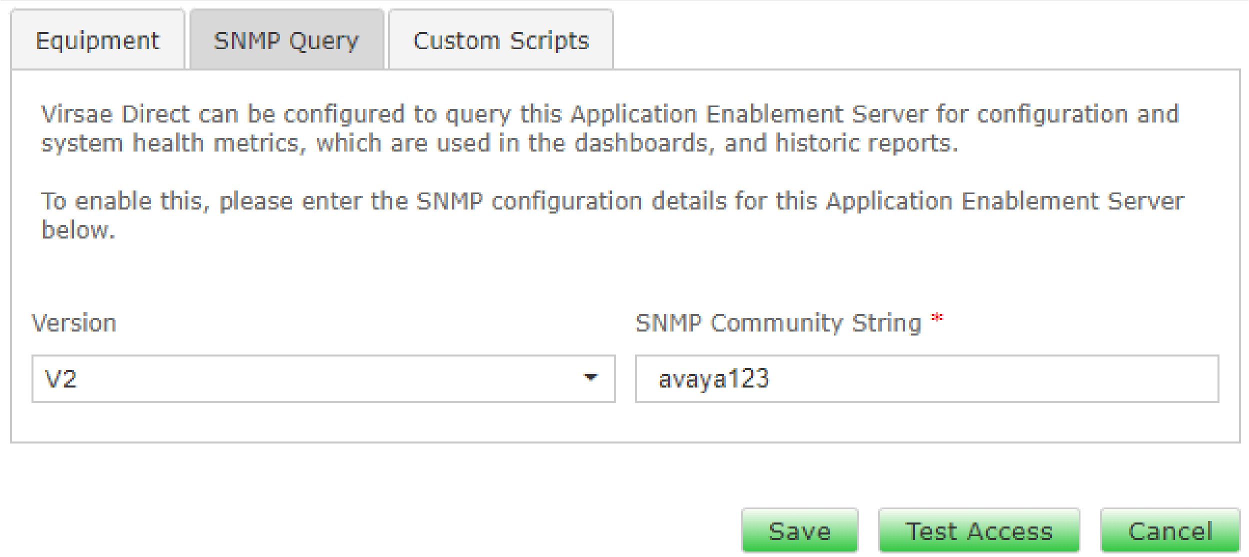


Vendor *	Product *
Avaya	Application Enablement Server
Equipment Name *	Username *
AES	virsae
IP Address/Host Name *	Password *
10.1.10.70	••••••••••
Site	
Lab	

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

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

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



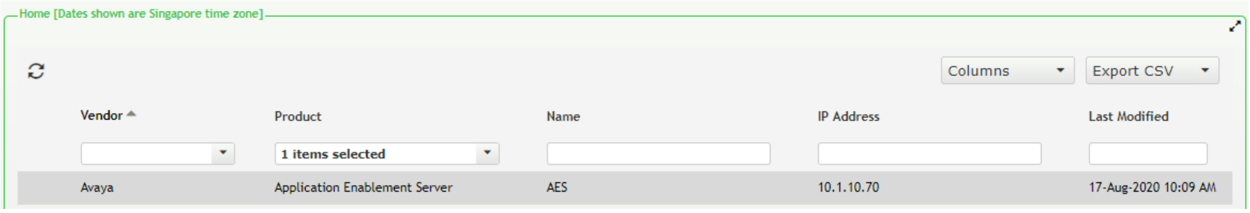
Virsae Direct can be configured to query this Application Enablement Server for configuration and system health metrics, which are used in the dashboards, and historic reports.

To enable this, please enter the SNMP configuration details for this Application Enablement Server below.

Version: V2

SNMP Community String *: avaya123

The screen below shows the added AES equipment.



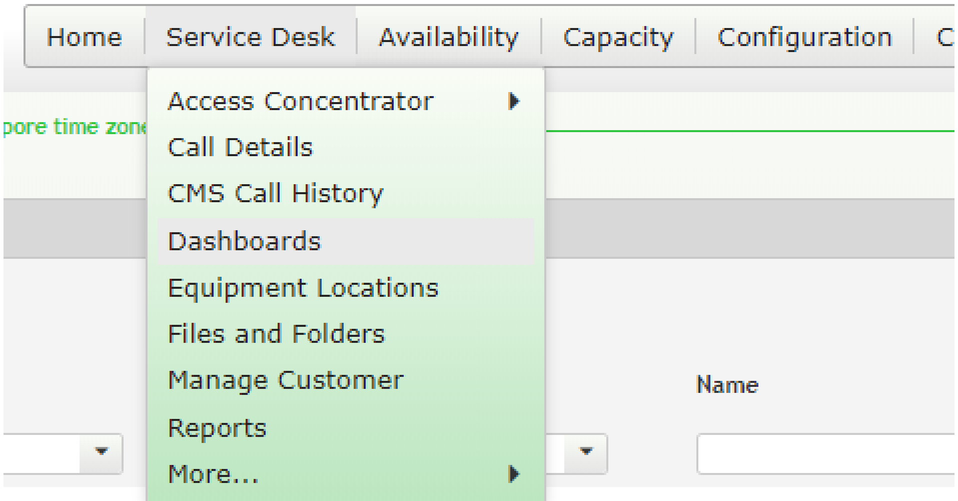
Home [Dates shown are Singapore time zone]

Vendor	Product	Name	IP Address	Last Modified
	1 items selected			
Avaya	Application Enablement Server	AES	10.1.10.70	17-Aug-2020 10:09 AM

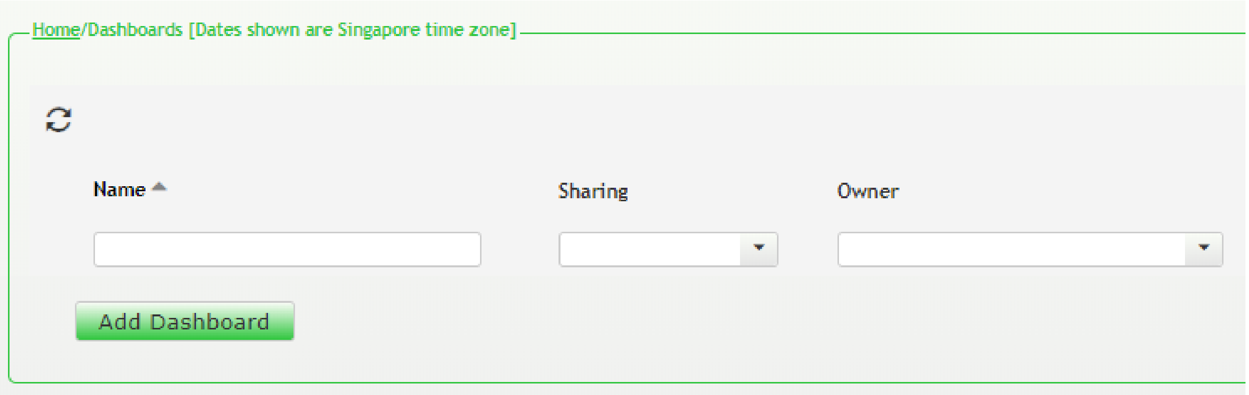
7.3. Configure Dashboard

This section shows the steps to configure AES on the dashboard.

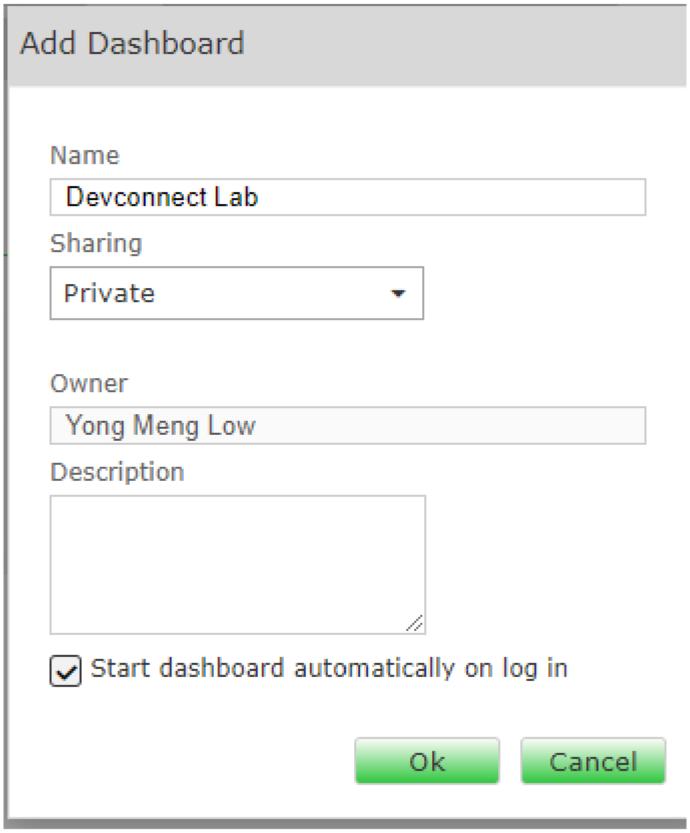
From the home screen, navigate to **Service Desk → Dashboards** as shown below.



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

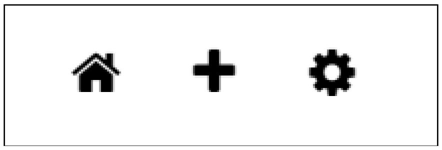
Sharing
Private

Owner
Yong Meng Low

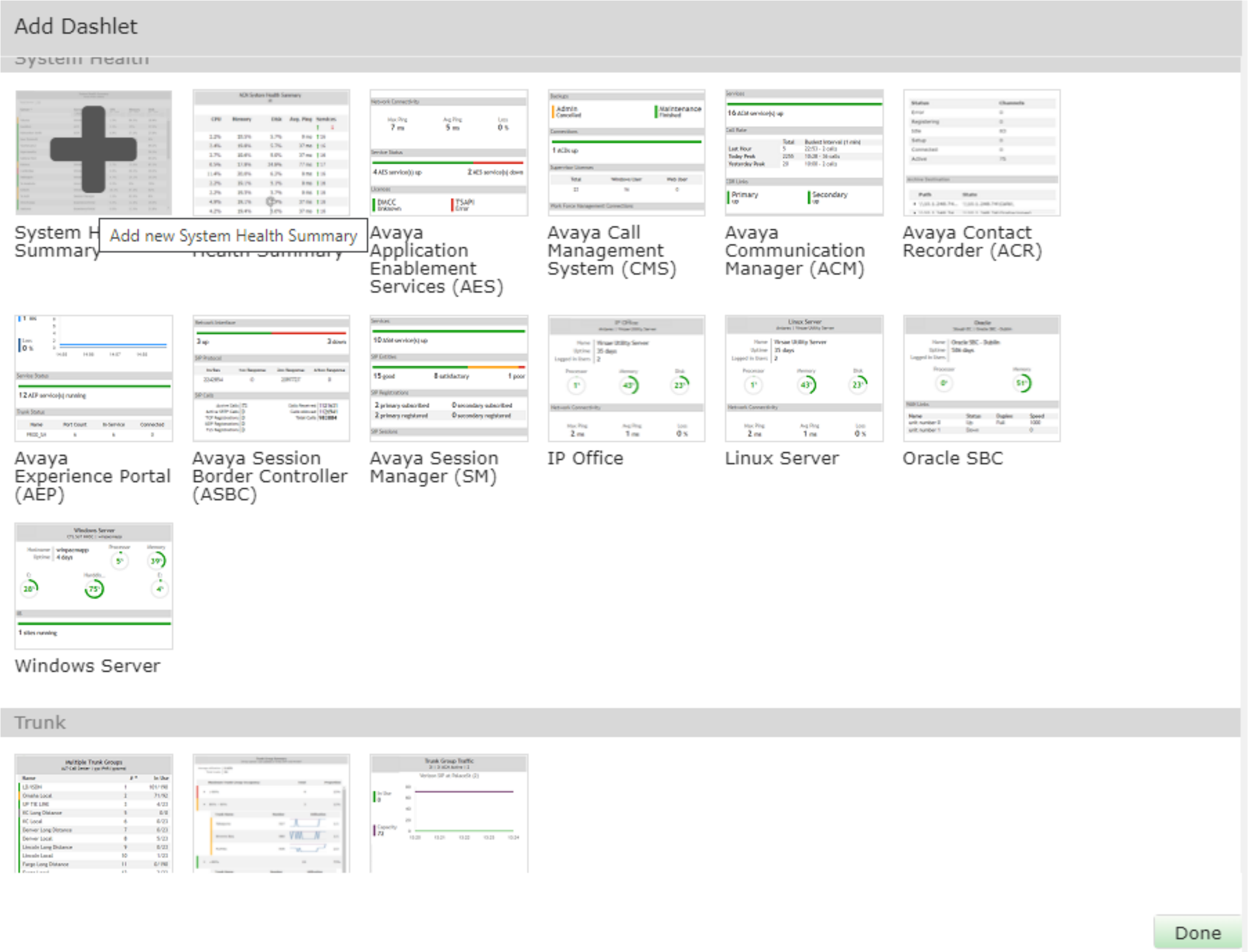
Description

☑ Start dashboard automatically on log in

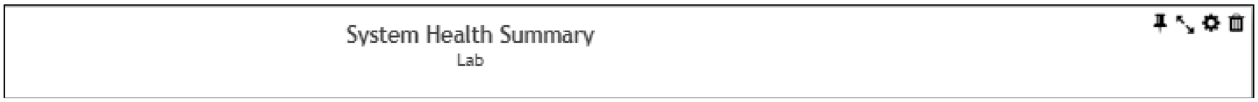
In the dashboard window bottom shown below, click on "+" sign at the bottom.



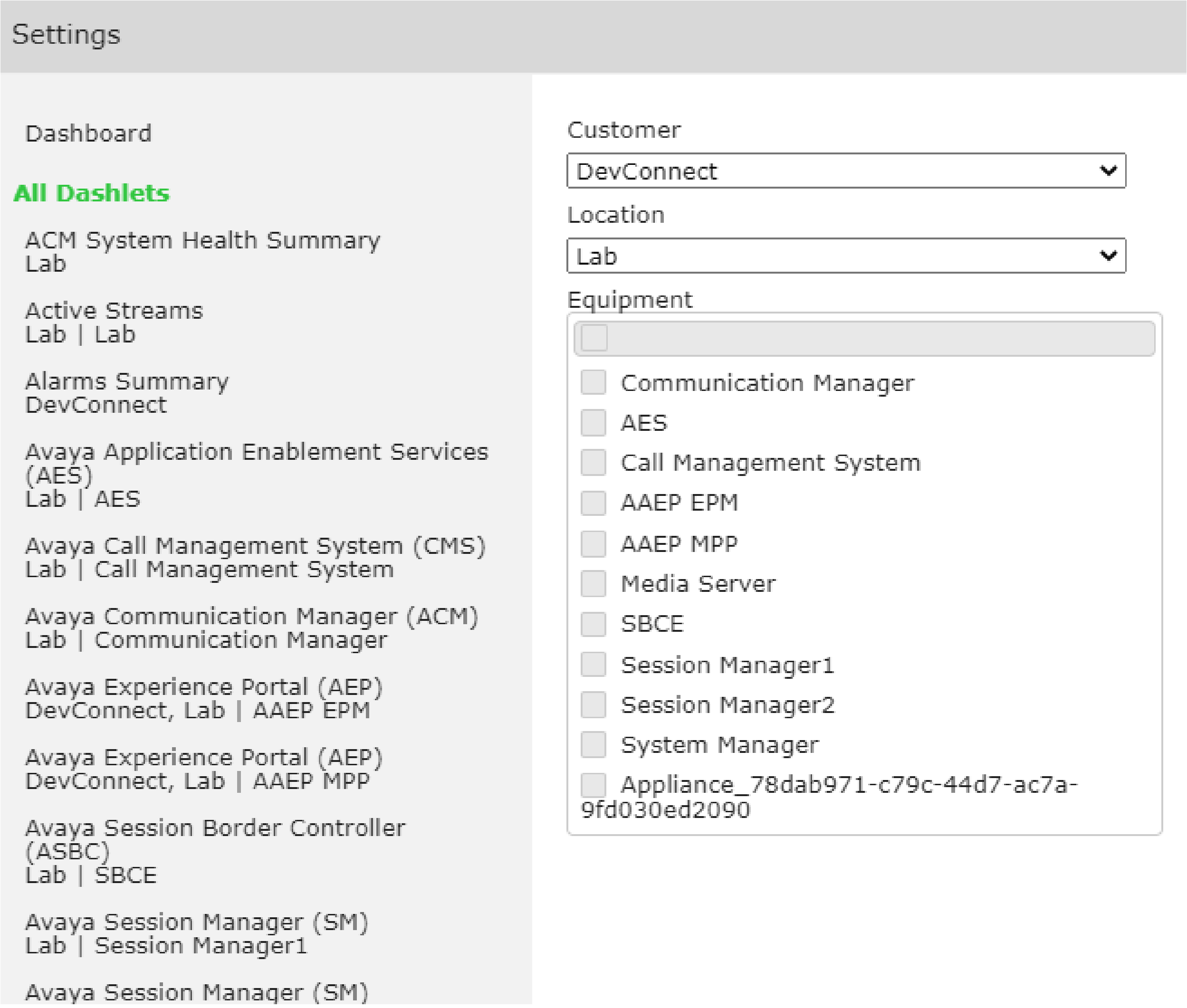
In the **Add Dashlet** window that pops up, select the **System Health Summary** from the available dashlet by hovering the "+" image over it and click **Done**.


Add Dashlet
System Health
System Health Summary
Add new System Health Summary
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
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., **AES** 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

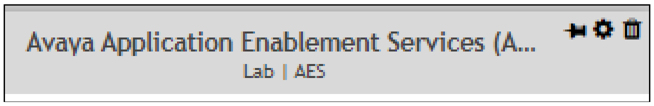
□ Session Manager1

□ Session Manager2

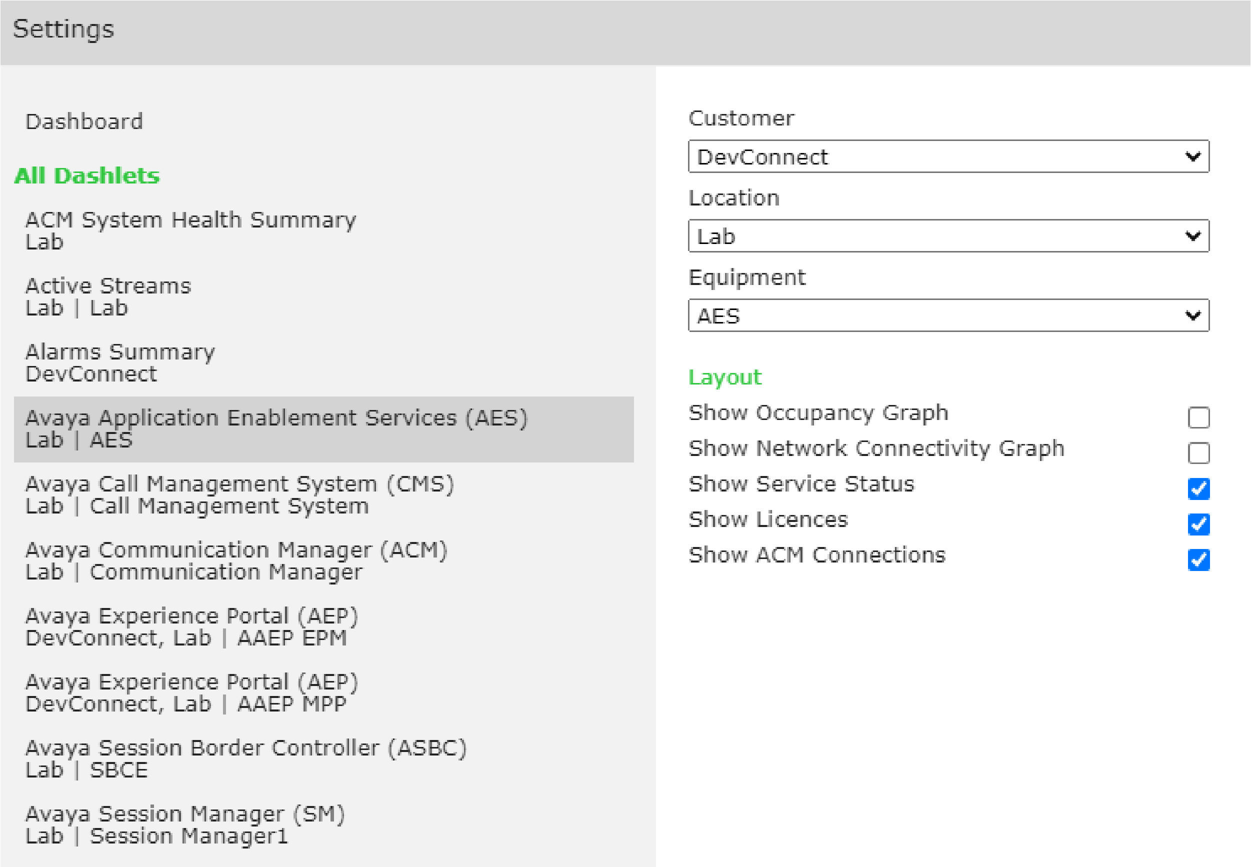
□ System Manager

□ Appliance_78dab971-c79c-44d7-ac7a-9fd030ed2090

Repeat the same for the **AES Server Health dashlet** and in addition select the desired **Layout**.



Avaya Application Enablement Services (A...
Lab | AES



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

Customer: DevConnect

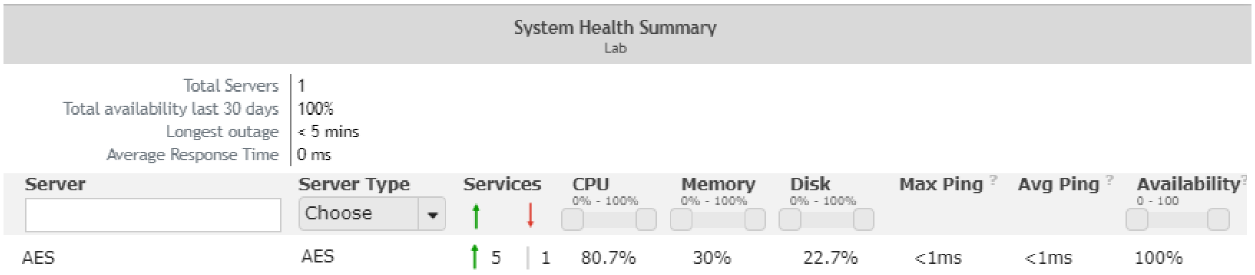
Location: Lab

Equipment: AES

Layout

- Show Occupancy Graph ☐
- Show Network Connectivity Graph ☐
- Show Service Status ☑
- Show Licences ☑
- Show ACM Connections ☑

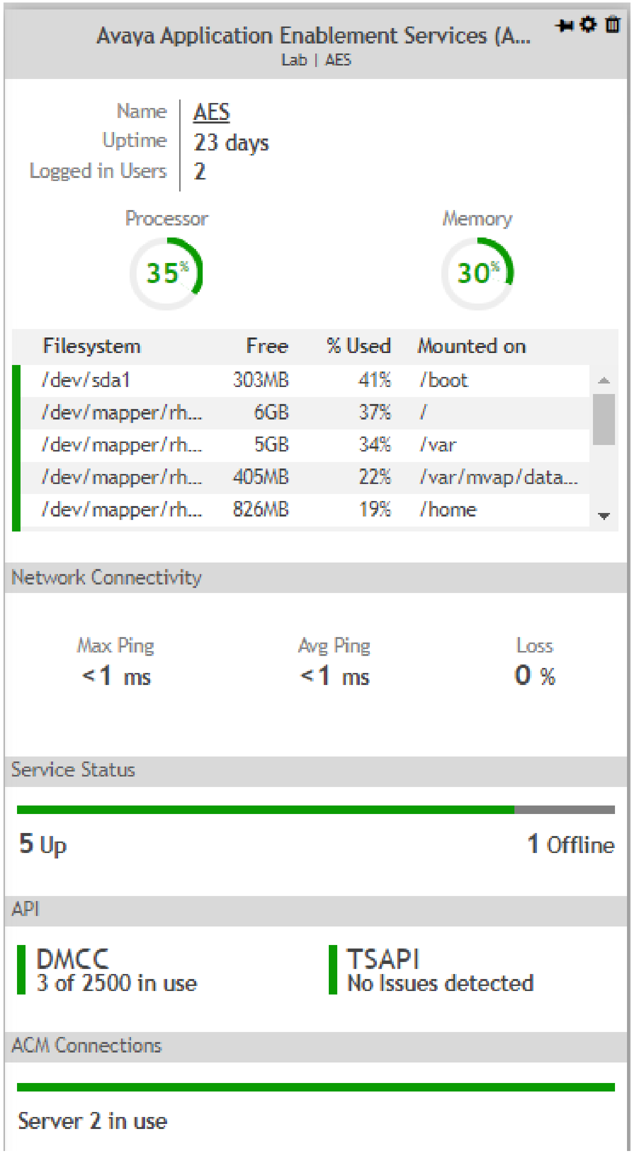
The dashboard with the configured equipment is shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.



System Health Summary
Lab

Total Servers	1
Total availability last 30 days	100%
Longest outage	< 5 mins
Average Response Time	0 ms

Server	Server Type	Services		CPU 0% - 100%	Memory 0% - 100%	Disk 0% - 100%	Max Ping ?	Avg Ping ?	Availability ? 0 - 100
	Choose	↑	↓						
AES	AES	↑ 5	1	80.7%	30%	22.7%	<1ms	<1ms	100%



Avaya Application Enablement Services (A...
Lab | AES

Name	AES
Uptime	23 days
Logged in Users	2

Processor 35%

Memory 30%

Filesystem	Free	% Used	Mounted on
/dev/sda1	303MB	41%	/boot
/dev/mapper/rh...	6GB	37%	/
/dev/mapper/rh...	5GB	34%	/var
/dev/mapper/rh...	405MB	22%	/var/mvap/data...
/dev/mapper/rh...	826MB	19%	/home

Network Connectivity

Max Ping <1 ms

Avg Ping <1 ms

Loss 0 %

Service Status

5 Up

1 Offline

API

DMCC
3 of 2500 in use

TSAPI
No Issues detected

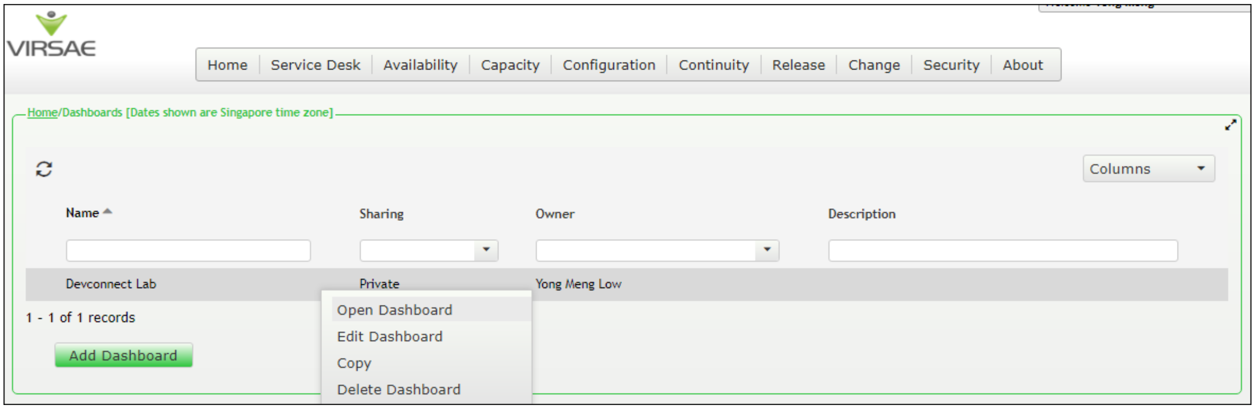
ACM Connections

Server 2 in use

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of AES 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".


VIRSAE
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About
Columns
Open Dashboard
Edit Dashboard
Copy
Delete Dashboard
Add Dashboard

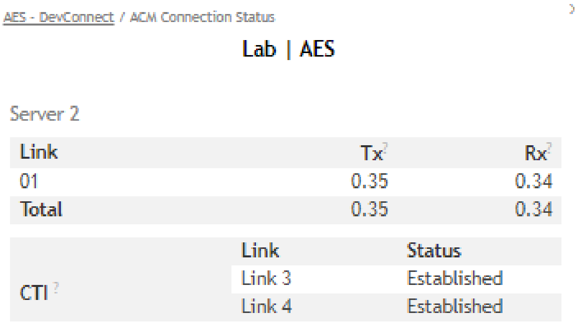
Home/Dashboards [Dates shown are Singapore time zone]

Name	Sharing	Owner	Description
Devconnect Lab	Private	Yong Meng 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 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 System Health of a configured AES for various parameters by drilling down from the Communication Manager Connections and API status (not shown).



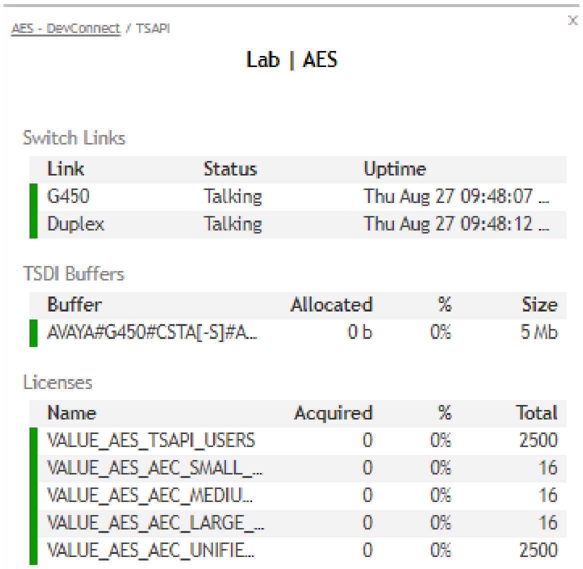
AES - DevConnect / ACM Connection Status

Lab | AES

Server 2

Link	Tx	Rx
01	0.35	0.34
Total	0.35	0.34

	Link	Status
CTI	Link 3	Established
	Link 4	Established



AES - DevConnect / TSAPI

Lab | AES

Switch Links

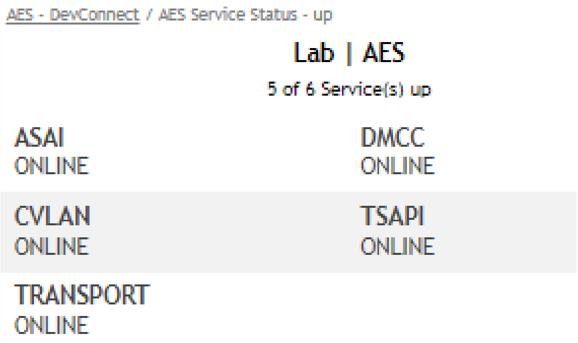
Link	Status	Uptime
G450	Talking	Thu Aug 27 09:48:07 ...
Duplex	Talking	Thu Aug 27 09:48:12 ...

TSDI Buffers

Buffer	Allocated	%	Size
AVAYA#G450#CSTA[-S]#A...	0 b	0%	5 Mb

Licenses

Name	Acquired	%	Total
VALUE_AES_TSAPI_USERS	0	0%	2500
VALUE_AES_AEC_SMALL_...	0	0%	16
VALUE_AES_AEC_MEDIU...	0	0%	16
VALUE_AES_AEC_LARGE_...	0	0%	16
VALUE_AES_AEC_UNIFIE...	0	0%	2500

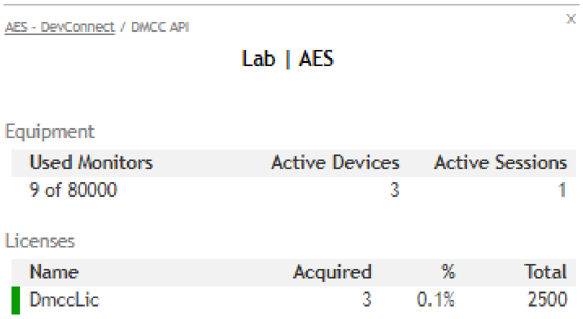


AES - DevConnect / AES Service Status - up

Lab | AES

5 of 6 Service(s) up

ASAI ONLINE	DMCC ONLINE
CVLAN ONLINE	TSAPI ONLINE
TRANSPORT ONLINE	



AES - DevConnect / DMCC API

Lab | AES

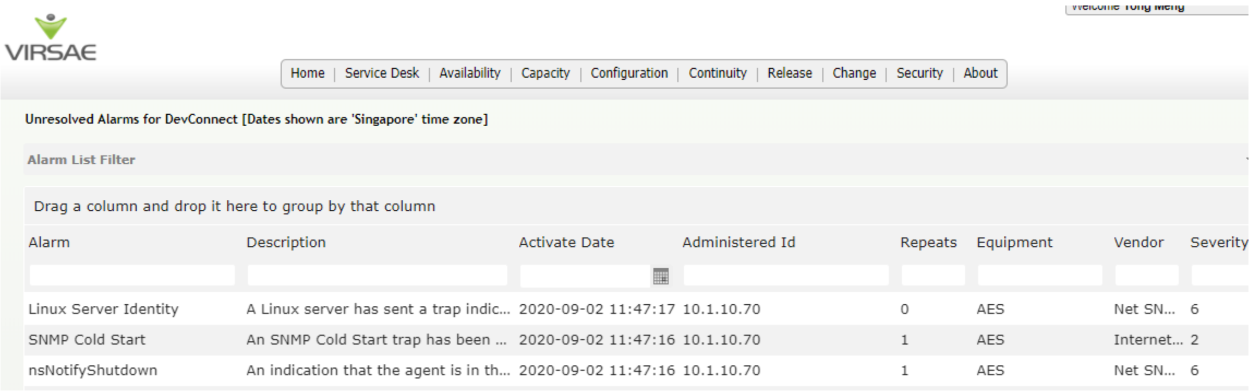
Equipment

Used Monitors	Active Devices	Active Sessions
9 of 80000	3	1

Licenses

Name	Acquired	%	Total
🟩 DmccLic	3	0.1%	2500

To view alarms using historical 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 AES equipment.



Welcome Tony Meng
VIRSAE
Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | About

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

Alarm List Filter

Drag a column and drop it here to group by that column

Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Vendor	Severity
Linux Server Identity	A Linux server has sent a trap indic...	2020-09-02 11:47:17	10.1.10.70	0	AES	Net SN...	6
SNMP Cold Start	An SNMP Cold Start trap has been ...	2020-09-02 11:47:16	10.1.10.70	1	AES	Internet...	2
nsNotifyShutdown	An indication that the agent is in th...	2020-09-02 11:47:16	10.1.10.70	1	AES	Net SN...	6

9. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R135 to interoperate with Avaya Aura® Application Enablement Services R8.1.2. 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. *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 5, Jun 2020.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1.x, Issue 8, May 2020.
3. *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment,* Release 8.1.x, Issue 4, Jul 2020.
4. *Administering and Maintaining Avaya Aura® Application Enablement Services,* Release 8.1.x, Issue 7, Jul 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*.

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.