



## **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 R174 to interoperate with Avaya Aura® Application Enablement Services 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 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.

## **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.

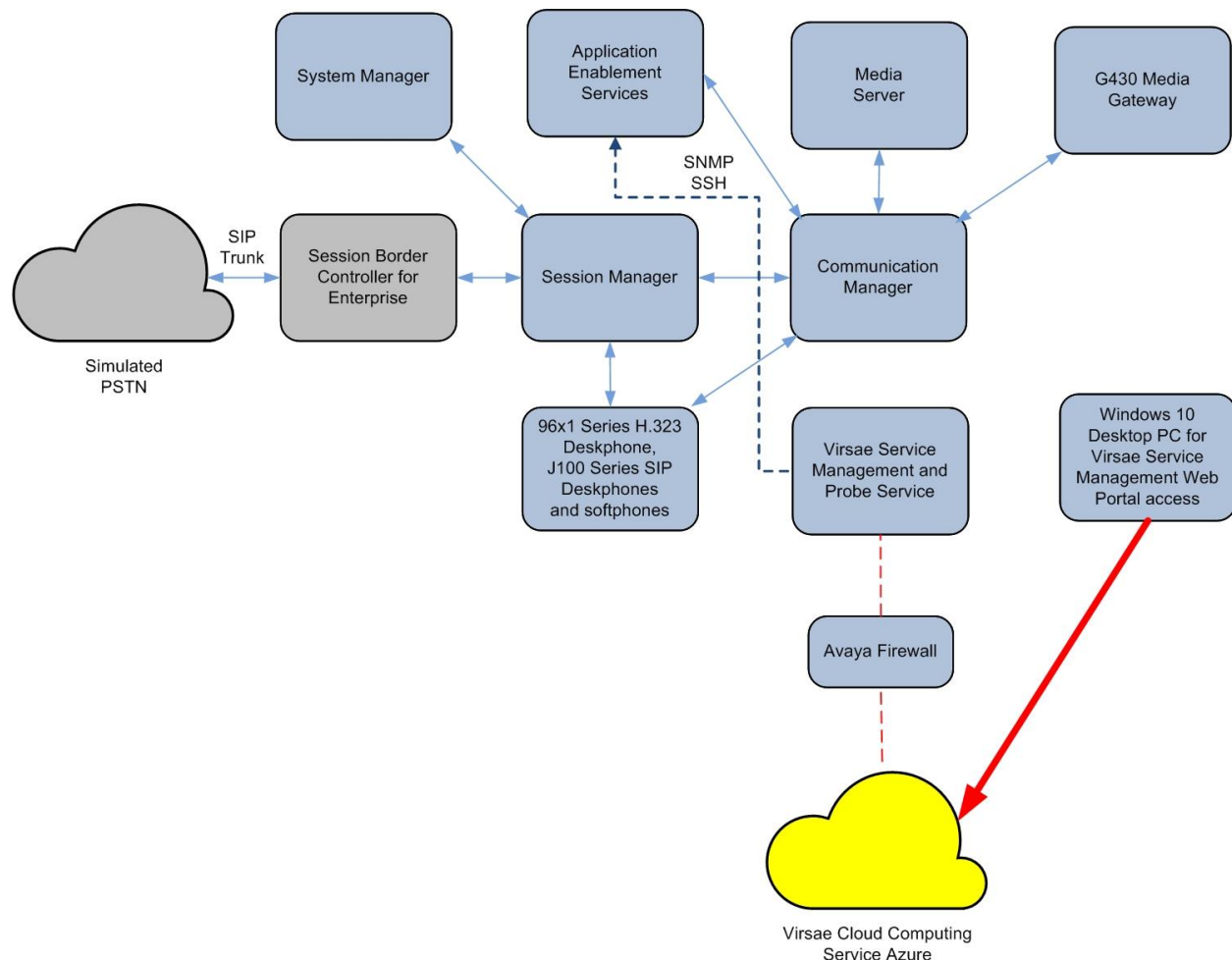
## 2.3. Support

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](mailto:support@virsae.com)

### 3. Reference Configuration

**Figure 1** illustrates the test configuration used to verify the VSM application with AES. In this compliance testing, Communication Manager with a G430 Media Gateway connected to AES using the CTI link. 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.



**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 Application Enablement Services running on virtual server	10.1 (10.1.0.0.2.11-0)
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
Virsa Service Management and Probe Service running on Windows 2016	174.1.2.268

## 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 **Error! Hyperlink reference not valid.** 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.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". In the top right corner, a welcome message is shown: "Welcome: User cust", "Last login: Wed Aug 10 18:07:30 2022 from 10.1.10.155", "Number of prior failed login attempts: 0", "HostName/IP: aes.sglab.com/10.1.10.70", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 10.1.0.0.2.11-0", "Server Date and Time: Wed Aug 17 15:49:27 SGT 2022", and "HA Status: Not Configured". Below this is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. On the left side of the main content area is a dark grey sidebar menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area has a light blue header "Welcome to OAM". Below this, it states: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list: "• 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.", and "• Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom of the main content area, it says: "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 **Following IP Addresses** to allow for connection of VSM IP Address.

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

The screenshot shows a web interface for configuring the SNMP Agent. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities (expanded), Diagnostics, Email Notification, HMDC, SNMP (expanded), Product ID, SNMP Agent (selected), SNMP Trap Receivers, and Help. The main content area is titled 'SNMP Agent' and contains the following sections:

- MIB II System Group Data:** Location: Unknown, Contact: Unknown.
- SNMP Protocol Access:**
  - ☐ Enable SNMP Version 1
  - ☒ Enable SNMP Version 2c: Community Name: avaya123
  - ☐ Enable SNMP Version 3
- User:**
  - User Name: [text box]
  - Authentication Protocol: None (dropdown)
  - Authentication Password: [text box]
  - Privacy Protocol: None (dropdown)
  - Privacy Password: [text box]
- Authorized IP Addresses for SNMP Access\***
  - ☐ No Access
  - ☐ Any IP Addresses
  - ☒ Following IP Addresses
    - IP Address 1: 10.1.10.122
    - IP Address 2: [text box]
    - IP Address 3: [text box]
    - IP Address 4: [text box]
    - IP Address 5: [text box]

At the bottom of the main content area are two buttons: 'Apply Changes' and 'Cancel Changes'. A note at the very bottom states: '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.

**Edit SNMP Trap**

☒ Enabled

Device: NMS ▾

IP Address: 10.1.10.122

Port: 162

Notification Type: Trap ▾

SNMP Version: 2c ▾

Security Name: avaya123

Authentication Protocol: None ▾

Authentication Password:  Confirm Password:

Privacy Protocol: None ▾

Privacy 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

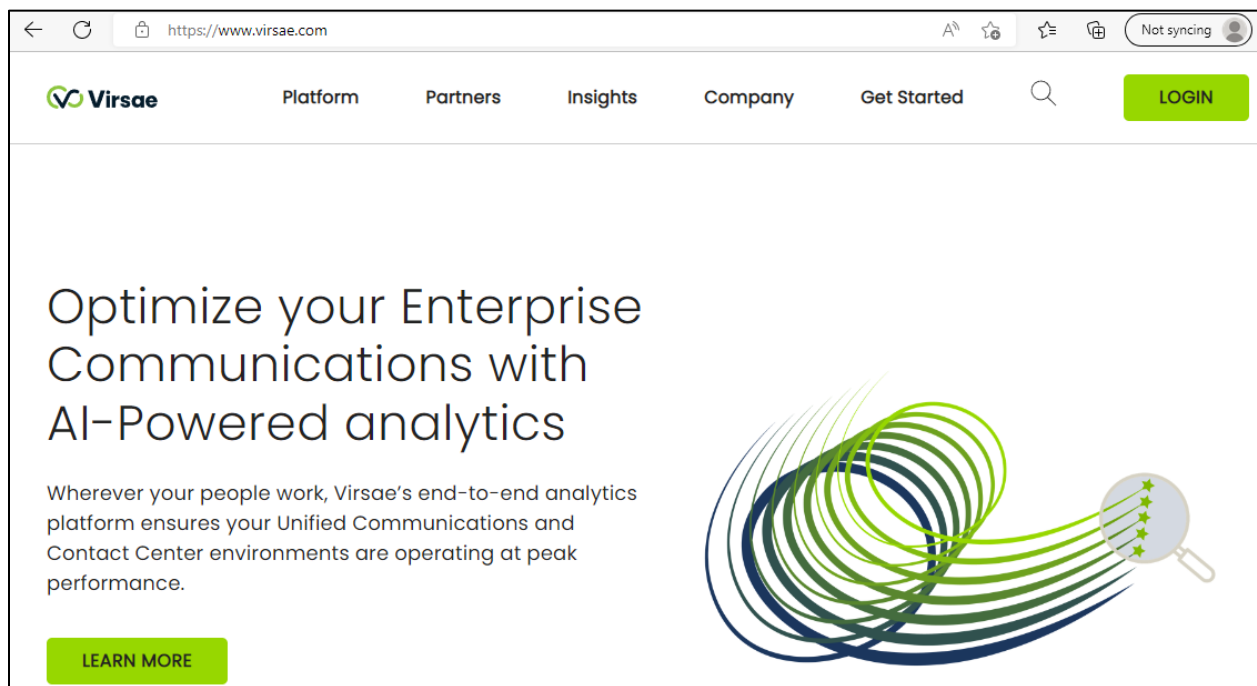
This section describes the configuration of VSM required to interoperate with AES.

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 *www.virsae.com* in a web browser. During compliance testing the same URL was used. Click on the **LOGIN** shown on the top right below.



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



The logo consists of a green stylized figure with arms raised, positioned above the word "VIRSAE" in a bold, sans-serif font.

Email

Password

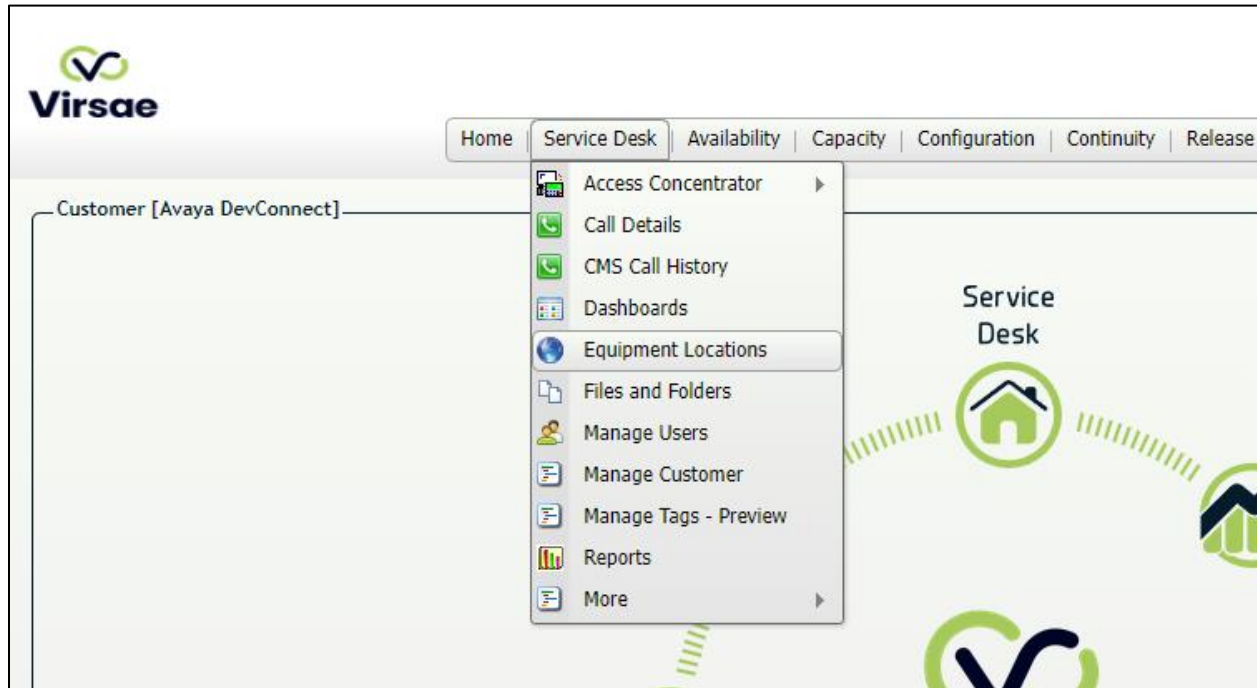
Log In

[Forgot your password?](#)

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**.



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



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

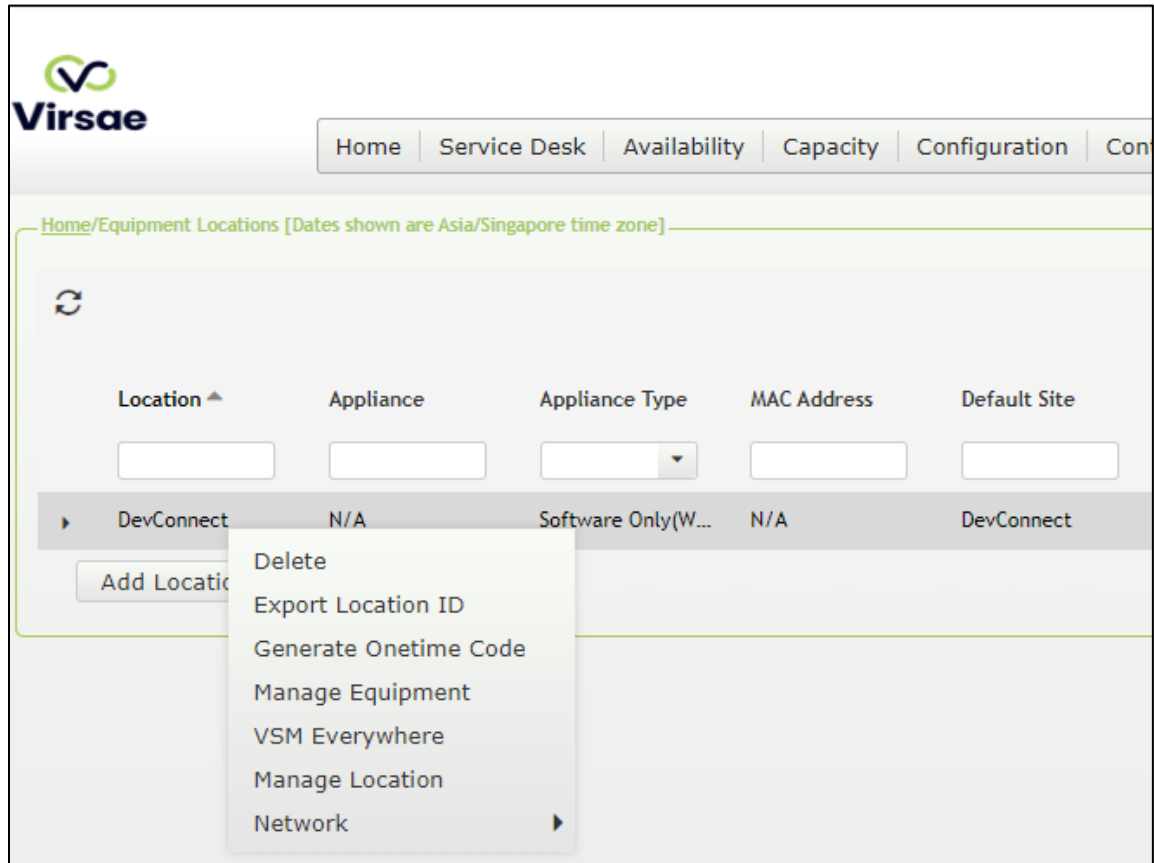
Home/Equipment Locations [Dates shown are Asia/Singapore time zone]

Columns Export CSV

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

Add Location

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



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

The 'Add Equipment' dialog box is shown. It has tabs for 'Equipment', 'SNMP Query', 'Network Connectivity', and 'Tags'. The 'Equipment' tab is active. It contains the following fields: 'Vendor \*' (dropdown), 'Product \*' (dropdown), 'Equipment Name \*' (text input), 'Username' (text input), 'IP Address/Host Name \*' (text input), 'Password' (text input), and 'Site' (text input with an information icon). At the bottom, there is a checkbox 'Add another', and three buttons: 'Add', 'Test Access', and 'Cancel'.

## 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 **AES** 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.

Equipment	SNMP Query	Network Connectivity	Custom Scripts	Tags
Vendor *		Product *		
<input type="text" value="Avaya"/>		<input type="text" value="AES"/>		
Equipment Name *		Username		
<input type="text" value="AES"/>		<input type="text" value="virsae"/>		
IP Address/Host Name *		Password		
<input type="text" value="10.1.10.70"/>		<input type="password" value="....."/>		
Site ⓘ				
<input type="text" value="DevConnect"/>				

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.

The screenshot shows the 'SNMP Query' tab selected in a navigation bar. Below the tabs, there are two input fields. The first field is labeled 'Version' and has a dropdown menu with 'V2' selected. The second field is labeled 'SNMP Community String \*' and contains the text 'avaya123'.

The screen below shows the added AES equipment.

The screenshot shows the 'Managed Equipment' table in the Avaya DevConnect interface. The table has columns for Vendor, Product, Name, IP Address, Tag Key, and Last Modified. The table contains three rows of equipment data.

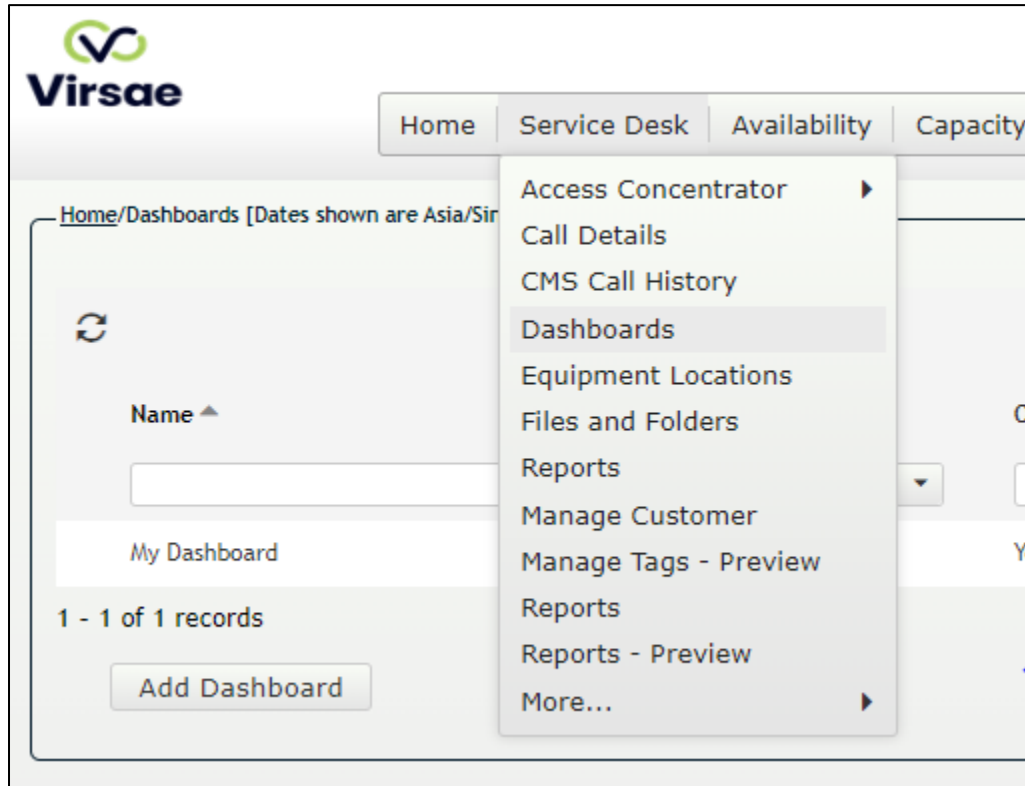
Vendor	Product	Name	IP Address	Tag Key	Last Modified
Avaya	Application Enablement Server	AES	10.1.10.70		02-Aug-2022 10:28 AM
Avaya	Breeze	Breeze	10.1.10.19		02-Aug-2022 10:29 AM
Avaya	Communication Manager	DevConnect ACM 10	10.1.10.230		02-Aug-2022 10:09 AM



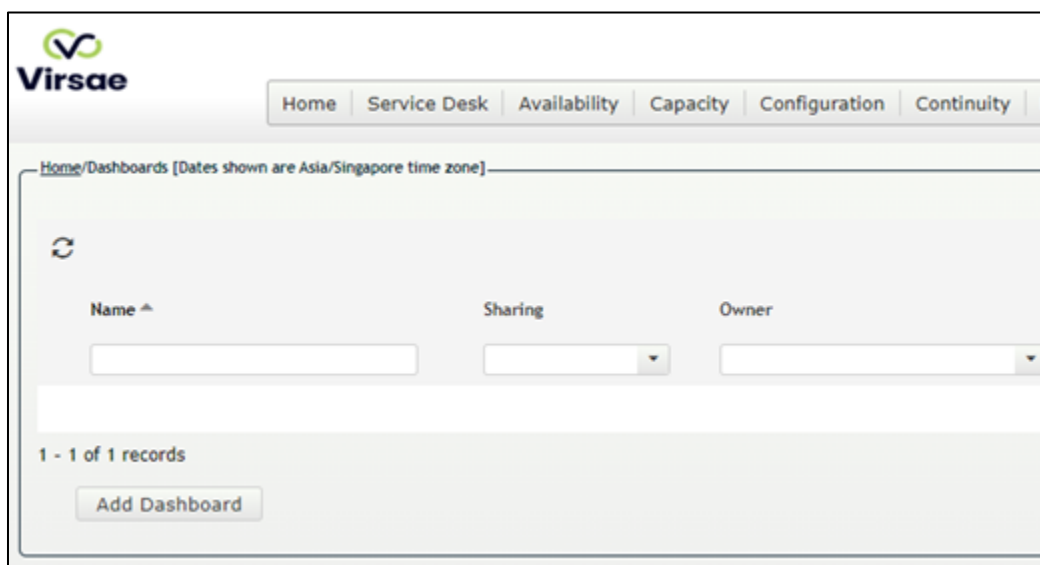
### 7.3. Configure Dashboard

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

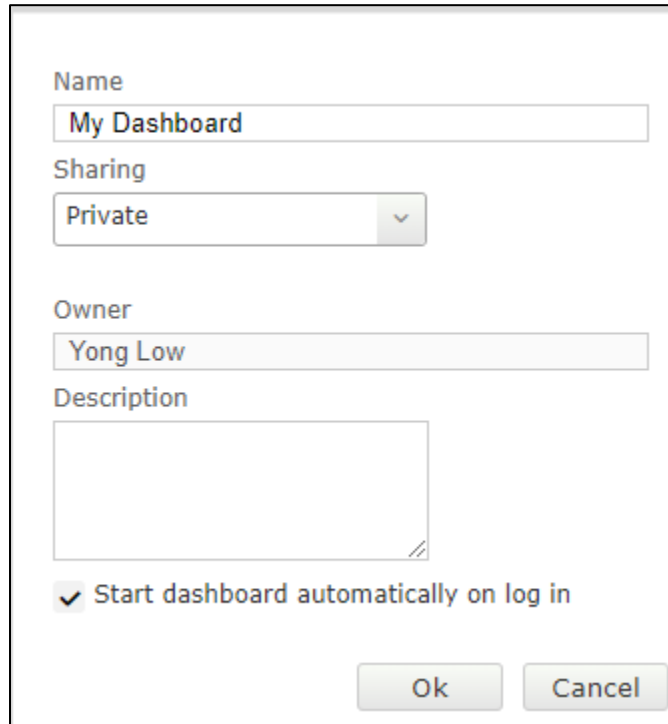
From the home screen, navigate to **Service Desk** → **Dashboards** as shown below.



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 on log in** box and then click on **Ok** to submit.



Name  
My Dashboard

Sharing  
Private

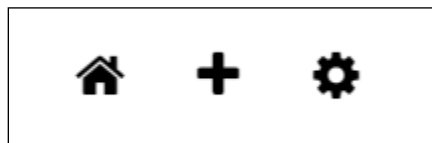
Owner  
Yong Low

Description

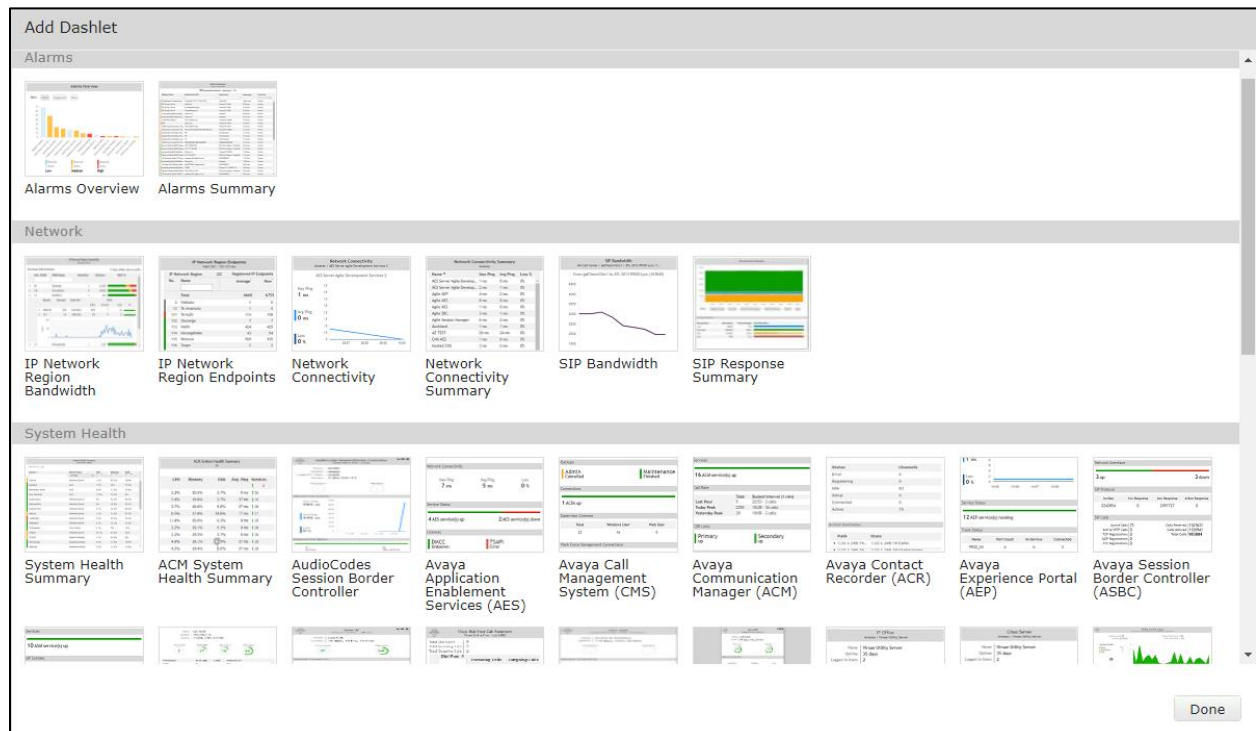
☒ Start dashboard automatically on log in

Ok Cancel

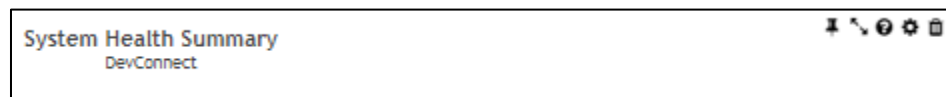
In the dashboard window bottom shown below, click on “+” sign at the bottom.



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**.



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



Select the correct **Location** i.e., **DevConnect** and the appropriate **Equipment** i.e., **AES** for Application Enablement Services. 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 | SM1

Calls In Progress  
DevConnect | DevConnect

Linux Server  
DevConnect | AAMS

Linux Server  
DevConnect | Breeze

Linux Server  
DevConnect | SMGR

System Health Summary  
DevConnect

Customer

Avaya DevConnect

Location

DevConnect

Equipment

☐

☐ DevConnect ACM 10

☒ AES

☐ Breeze

☐ AAMS

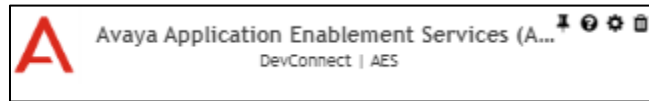
☐ SM1

☐ SM2

☐ SMGR

☐ Appliance\_372ec645-97f9-49b9-aa5f-9c67988a2596

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



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 | SM1

Calls In Progress  
DevConnect | DevConnect

Linux Server  
DevConnect | AAMS

Linux Server  
DevConnect | Breeze

Linux Server  
DevConnect | SMGR

Customer  
Avaya DevConnect

Location  
DevConnect

Equipment  
AES

Layout

Show Occupancy Graph ☐

Show Network Connectivity Graph ☐

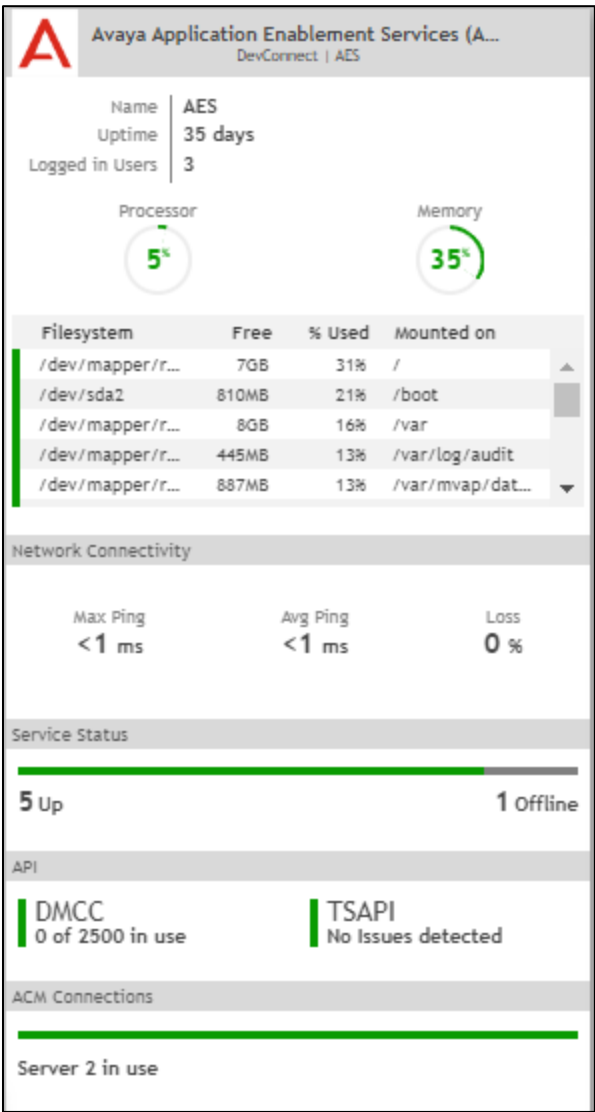
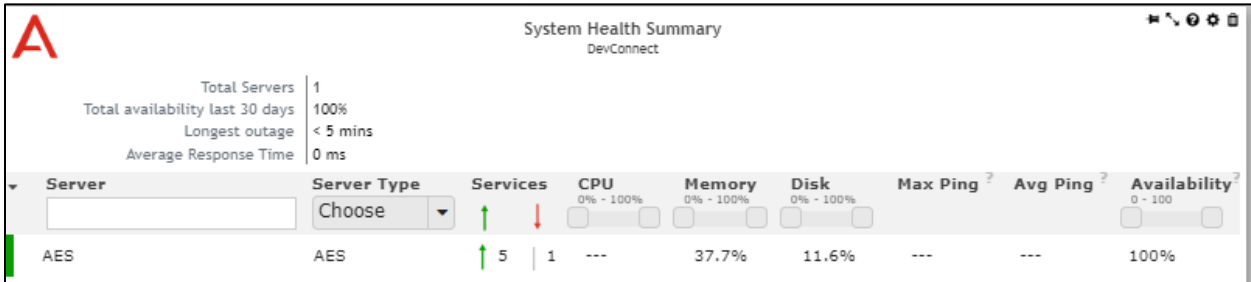
Show Service Status ☒

Show Licences ☒

Show ACM Connections ☒

Show Custom Scripts ☐

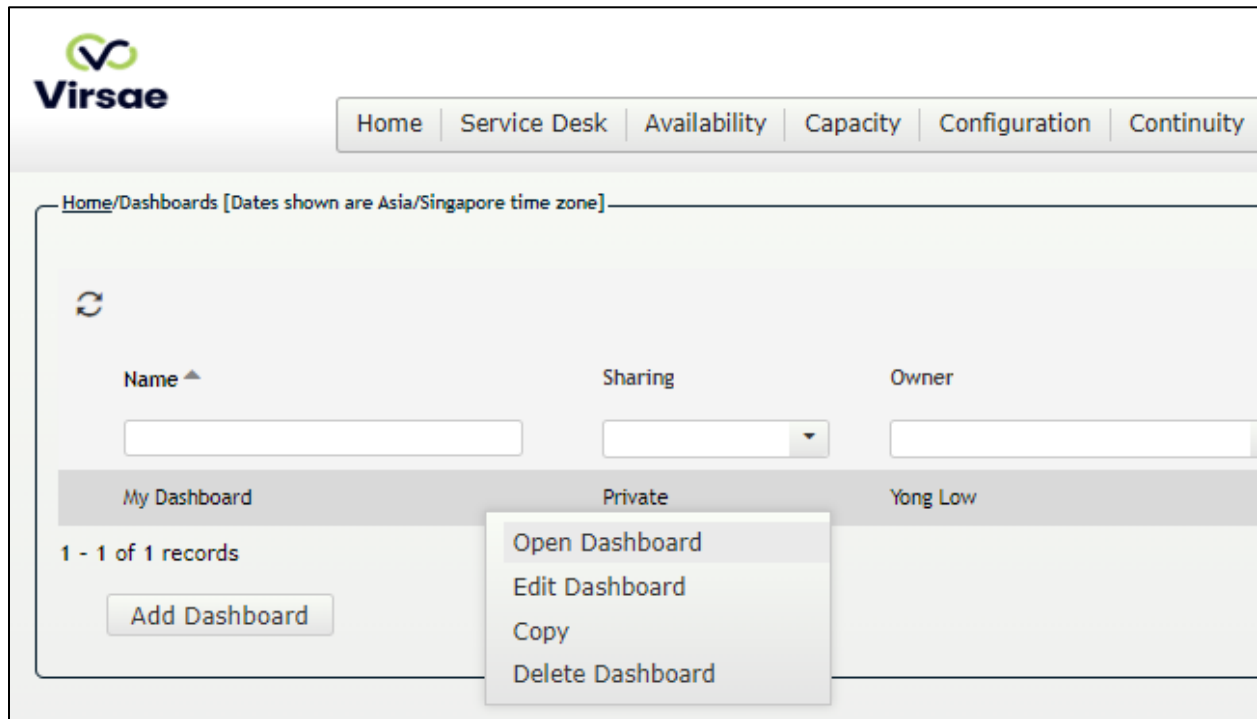
The dashboard with the configured equipment is shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.



## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of 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 “My Dashboard” and select “Open Dashboard”.



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

The screens below show the System Health of a configured AES for various parameters by drilling down from the ACM Connections, Service and API status (not shown).

AES - DevConnect / ACM Connection Status

Lab | AES

Server 2

Link	Tx <sup>2</sup>	Rx <sup>2</sup>
01	0.35	0.34
Total	0.35	0.34

Link	Status
Link 3	Established
Link 4	Established

CTI<sup>2</sup>

AES - Avaya DevConnect / AES Service Status - up

DevConnect | AES

5 of 6 Service(s) up

ASAI ONLINE	DMCC ONLINE
CVLAN ONLINE	TSAPI ONLINE
TRANSPORT ONLINE	

AES - Avaya DevConnect / TSAPI

DevConnect | AES

Switch Links

Link	Status	Uptime
G450	Talking	Wed Aug 17 15:56:25...
Duplex	Talking	Wed Aug 17 15:56:25...

TSDI Buffers

Buffer	Allocated	%	Size
AVAYA#G450#CSTA[-S]#...	0 b	0%	5 Mb
NA=	-1 b	100%	-1 b

Licenses

Name	Acquired	%	Total
VALUE_AES_TSAPI_USE...	0	0%	2500
VALUE_AES_AEC_SMAL...	0	0%	16
VALUE_AES_AEC_MEDI...	0	0%	16
VALUE_AES_AEC_LARG...	0	0%	16
VALUE_AES_AEC_UNIFI...	0	0%	2500

AES - Avaya DevConnect / DMCC API

DevConnect | AES

Equipment

Used Monitors	Active Devices	Active Sessions
0 of 80000	0	0

Licenses

Name	Acquired	%	Total
DmccLic	0	0%	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 Yong

Home
Service Desk
Availability
Capacity
Configuration
Continuity
Release
Change
Security
About

Unresolved Alarms for Avaya DevConnect [Dates shown are 'Asia/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
avAesGracePeriodFailure	License Grace Period Active. Proba...	2022-08-17 15:56:22	DMCC	1	AES	Avaya	2
avAesServiceColdStart	AES Service start request received.	2022-08-17 15:56:12	LCM	1	AES	Avaya	2
avAesServiceColdStart	AES Service start request received.	2022-08-17 15:56:11	CVLAN	1	AES	Avaya	2
avAesServiceColdStart	AES Service start request received.	2022-08-17 15:55:38	TSAPI	1	AES	Avaya	2
avAesServiceColdStart	AES Service start request received.	2022-08-17 15:55:34	TRANSPORT	1	AES	Avaya	2
avAesServiceColdStart	AES Service start request received.	2022-08-17 15:55:34	ASAI	1	AES	Avaya	2

## 9. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R174 to interoperate with Avaya Aura® Application Enablement Services 10.1. 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 10.1, Issue 1, Feb 2022.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1, Issue 1, Feb 2022.
3. *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*, Release 10.1, Issue 1, Dec 2021.
4. *Administering Avaya Aura® Application Enablement Services*, Release 10.1, Issue 2, Jan 2022.

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

---

**©2022 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](mailto:devconnect@avaya.com).