



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R174 to interoperate with Avaya Aura® Session 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 uses Simple Network Management Protocol (SNMP) and Secure shell (SSH) to query Session Manager for information and status. At the same time, Virsae Service Management processes Real-time Transport Control Protocol (RTCP) from Avaya SIP endpoints and collects Call Detail Recording (CDR) information from each Session 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® Session Manager (herein after referred to as Session 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 four integration methods to monitor Session Manager.

- Linux shell (SSH) - Virsae uses SSH to collect configuration and status information from Session Manager.
- Real Time Transport Control Protocol (RTCP) collection - Virsae collects RTCP information sent by Avaya SIP Deskphones.
- Call Detail Recording (CDR) collection - Virsae collects CDR information via SFTP connection to Session Manager.
- SNMP collection – VSM uses SNMP to capture the alarms.

VSM web user interface (dashboard) displays the configurations of Session Manager such as the memory and CPU utilizations, disk usage and status from data collected via SSH. For the collection of RTCP and CDR information, historical reporting is used. SNMP is used to receive information of alarms.

2. General Test Approach and Test Results

The general test approach was to place calls between Avaya SIP endpoints with other endpoints including internal extensions and PSTN. VSM dashboard and historical reporting was used to display the configuration, alarms, RTCP and CDR information collected.

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 encrypted capabilities of SFTP, 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

For feature testing, VSM dashboard was used to view the configurations of Session Manager such as the memory and CPU utilizations, disk usage and status from data collected via SSH. For the collection of RTCP and CDR information, only SIP endpoints are included. The types of calls made included intra-switch calls, inbound and outbound trunk calls. Information on alarms were collected using SNMP.

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.

- SIP Tracer Syslog was not sent by Session Manager. This is fixed on Session Manager 10.1.0.2.

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 Communication 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.

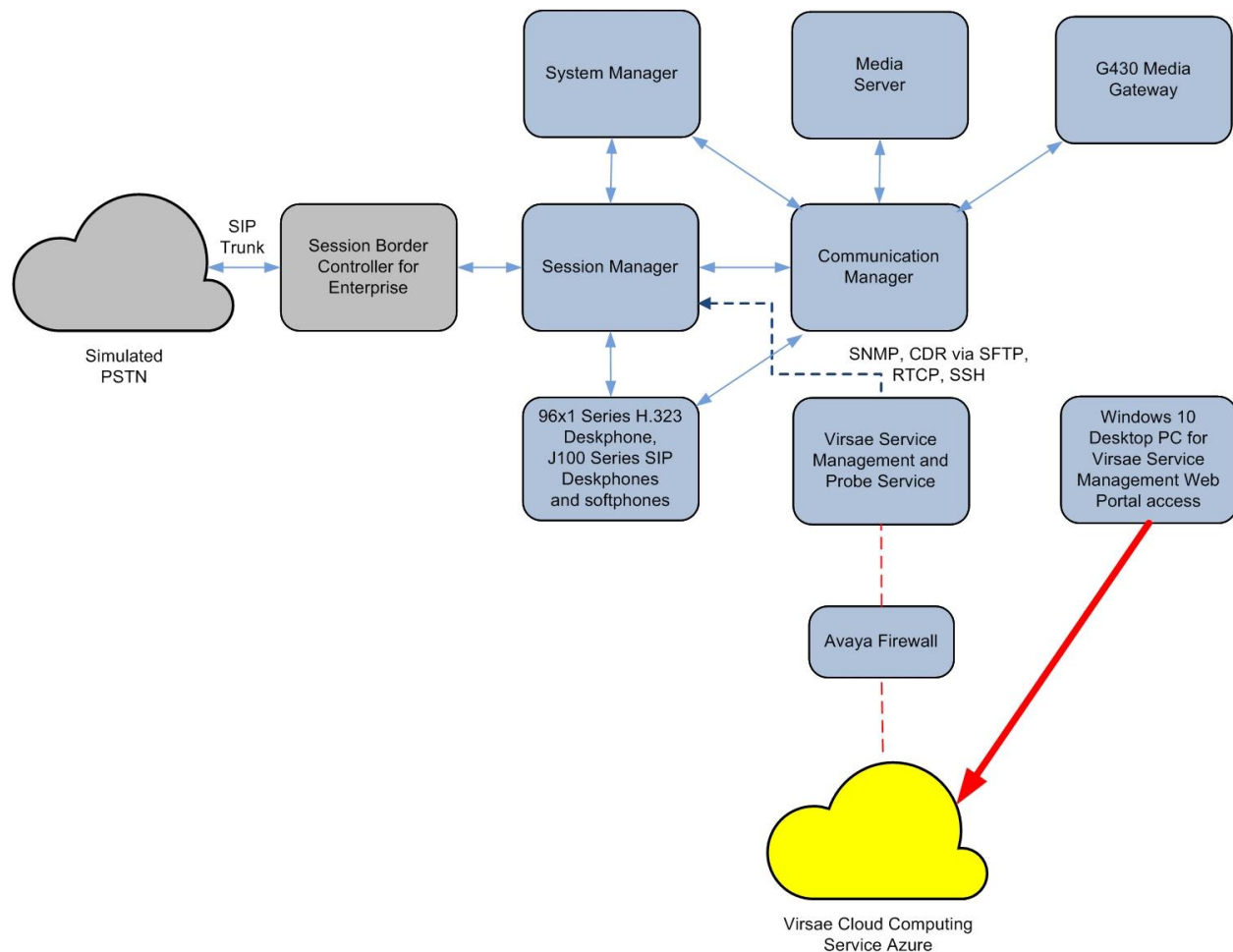


Figure 1: Test Configuration

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® Session Manager

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

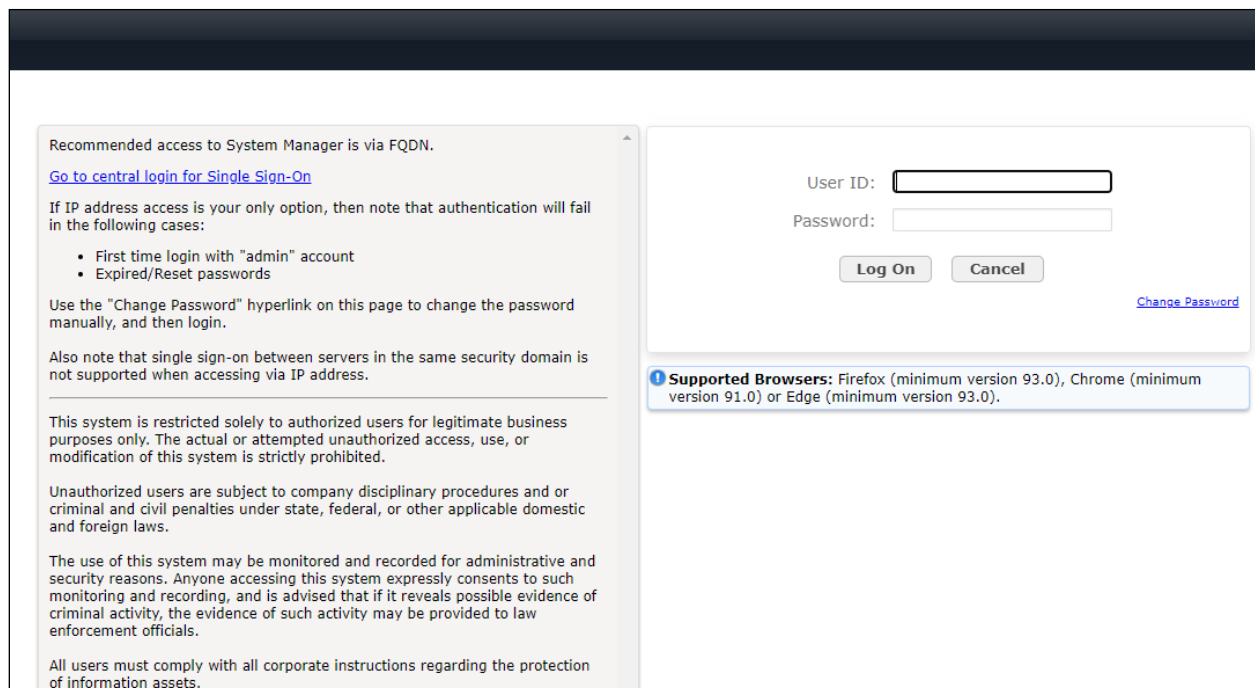
5.1. Configure Login Group

During compliance testing the default administrator account created during installation of Session Manager was used. This is because any account created after installation of Session Manager is not updated in the sudo users file system and therefore will not have administrative rights.

5.2. Configure SNMP

SNMP is used to capture alarms raised by Session Manager. All configurations to Session Manager 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.

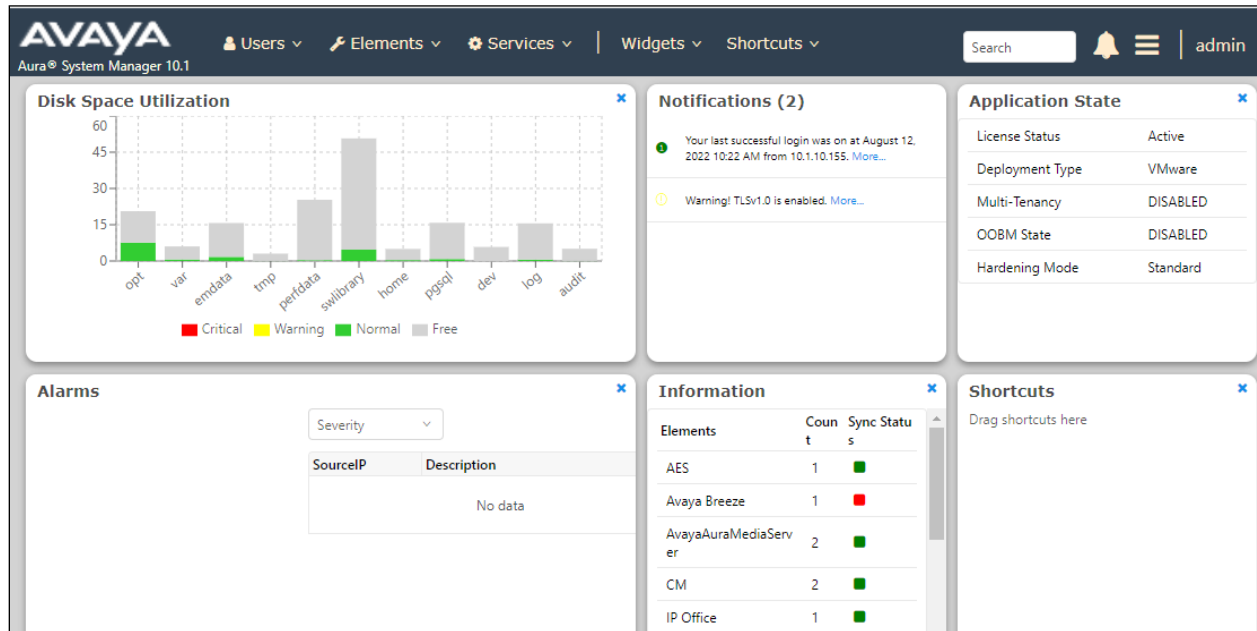
User ID:

Password:

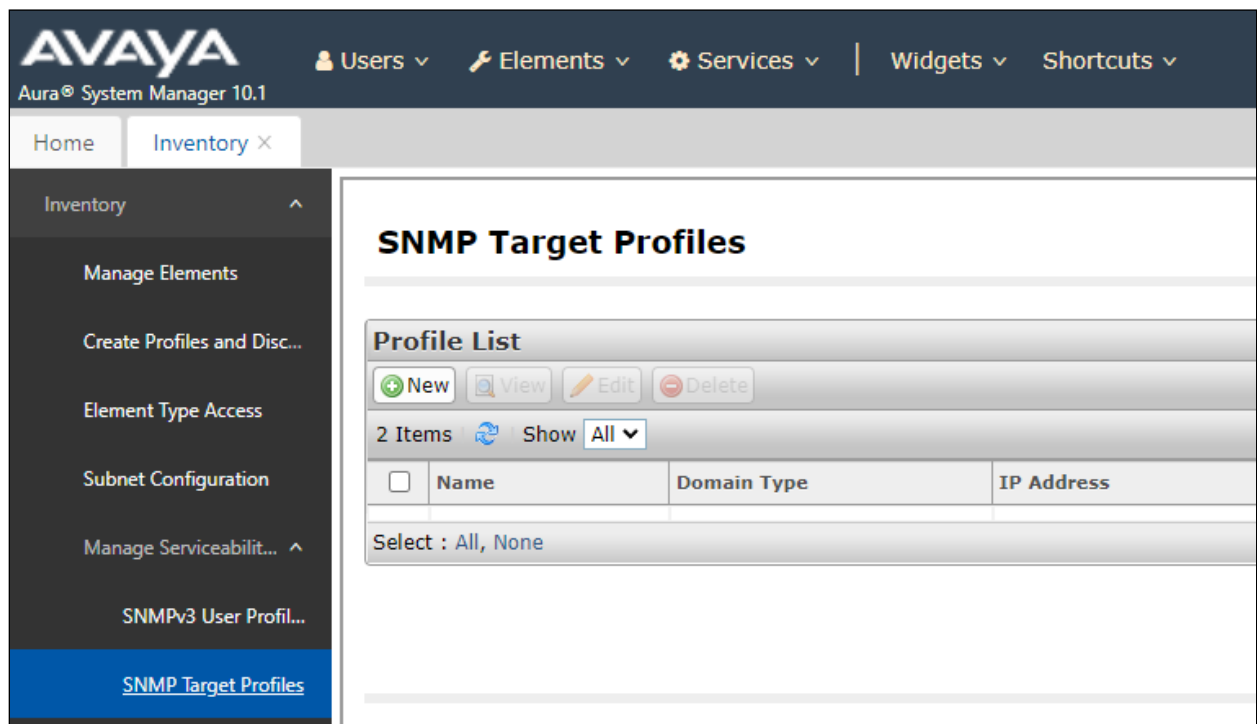
[Change Password](#)

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.



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 **V2** from the drop-down menu.

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

New Target Profile Commit Back

Target Details Attach/Detach User Profile

Target Details

* Name:

Description:

* IP Address:

* Port:

* Notification Type:

* Protocol:

* Community:

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

AVAYA Users Elements Services Widgets Shortcuts Search Notification

Aura® System Manager 10.1

Home Session Manager Avaya Breeze® Inventory

Serviceability Agents

Agent List

Activate Manage Profiles Generate Test Alarm Repair Serviceability Agent Manage Profile Job Status

8 Items Show All

	Hostname	IP Address	System Name	System OID
<input type="checkbox"/>	g450-US	127.0.0.1	g450-US	
<input type="checkbox"/>	Utility-Services	10.1.40.14	Utility-Services	
<input type="checkbox"/>	sm1.sglab.com	10.1.10.60	sm1.sglab.com	
<input type="checkbox"/>	sm1.sglab.com	10.1.10.59	Session Manager	.1.3.6.1.4.1.6889.1.36
<input type="checkbox"/>	sm3.sglab.com	10.1.10.47	sm3.sglab.com	
<input type="checkbox"/>	smgr.sglab.com	10.1.10.46	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35
<input type="checkbox"/>	sm2.sglab.com	10.1.10.41	Session Manager	.1.3.6.1.4.1.6889.1.36
<input type="checkbox"/>	avaya-ce-sm100	10.1.10.19	avaya-ce-sm100	

From the **Manage Profile** window, under the **SNMP Target Profiles** tab, select the **Virsaev2** profile, click on **Assign** and the profile is moved to the **Removable Profiles** as shown in the following screenshot. Click the **Commit** button to save it.

Manage Profile

Commit Back

Selected Agents

SNMP Target Profiles

SNMPv3 User Profiles

Assignable Profiles

Assign

0 Items

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

Removable Profiles

Remove

Assign/Remove

Filter Profiles

2 Items

	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
<input type="checkbox"/>	Virsaev2	UDP	10.1.10.122	162	V2	

Select : All, None

5.3. Configure RTCP Monitoring

To allow VSM to monitor the voice quality of SIP endpoint calls, configure Session Manager to send RTCP data to VSM.

From the System Manager homepage, navigate to **Elements** → **Session Manager**. Navigate to **Device and Location Configuration** → **Device Settings Groups** as shown in the screen below. Click on **New** to add a Terminal Group and a Location Group.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar is located on the right. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Ad..., Global Settings, Communication Profile..., Network Configuration, Device and Location..., Device Settings Gr..., Location Settings, Station Access Cod..., Application Configur..., and System Status. The 'Device Settings Gr...' option is currently selected and highlighted in blue.

The main content area is titled 'Device Settings Groups' and includes a subtitle: 'This page allows you to configure the Device Settings Groups.' Below this, there is a 'Default Group' dropdown menu. The interface is divided into two sections: 'Terminal Groups' and 'Location Groups'.

Terminal Groups

Buttons: New, Edit, Delete

1 Item

<input type="checkbox"/>	Name	Terminal Group Number	Description
Select : All, None			

Location Groups

Buttons: New, Edit, Delete

1 Item

<input type="checkbox"/>	Name	Description
Select : All, None		

In the **Device Settings Group** window, under **General** configure the following.

- **Name:** A descriptive name.
- **Terminal Group Number:** Any valid number.

Under the **VoIP Monitoring Manager**, configure the **IP Address** of VSM. Retain default values for all other fields and click on the **Save** button.

The screenshot shows the 'Device Settings Group' configuration window. At the top, there is a navigation bar with links: 'General', 'Endpoint Timer', 'Maintenance Settings', 'VoIP Monitoring Manager', 'Volume Settings', 'Parameters', '802.1 P/Q Parameters', 'Expand All', and 'Collapse All'. The 'General' tab is selected and expanded, showing fields for 'Name' (set to 'TG1'), 'Description' (empty), 'Group Type' (radio buttons for 'Location Group' and 'Terminal Group', with 'Terminal Group' selected), and '*Terminal Group Number' (set to '1'). Below the 'General' tab are other tabs: 'Endpoint Timer', 'Maintenance Settings', 'VoIP Monitoring Manager', 'Volume Settings', and 'VLAN Parameters'. The 'VoIP Monitoring Manager' tab is expanded, showing fields for 'IP Address' (set to '10.1.10.122'), '*Port' (set to '5005'), and '*Reporting Period' (set to '5').

The example above is for Terminal group and the same process is repeated for the **Location Groups**.

The **Device Settings Group** window shown below once the above-mentioned Terminal and Location groups configuration is completed.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, version information, and tabs for Users, Elements, Services, Widgets, and Shortcuts. Below this is a secondary navigation bar with links to Home, Session Manager, Avaya Breeze, and Backup and Restore. A left-hand sidebar contains a list of configuration categories, with 'Device Settings Groups' highlighted in blue. The main content area is titled 'Device Settings Groups' and includes a description: 'This page allows you to configure the Device Settings Groups.' Below the title is a 'Default Group' dropdown menu. The interface is divided into two sections: 'Terminal Groups' and 'Location Groups'. Each section has 'New', 'Edit', and 'Delete' buttons. The 'Terminal Groups' section shows one item, 'TG1', with a checkbox and a 'Terminal Group Number' of 1. The 'Location Groups' section shows one item, 'SIP Endpoint', with a checkbox and a 'Description' field. Both sections include a 'Select : All, None' dropdown menu.

Device Settings Groups

This page allows you to configure the Device Settings Groups.

Default Group

Terminal Groups

New Edit Delete

1 Item

<input type="checkbox"/>	Name	Terminal Group Number
<input type="checkbox"/>	TG1	1

Select : All, None

Location Groups

New Edit Delete

1 Item

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	SIP Endpoint	

Select : All, None

5.4. Configure CDR User Account for Avaya Aura® Session Manager

From the System Manager home page, navigate to **Elements** → **Session Manager** (not shown). Select **Session Manager Administration** (not shown). From the **Session Manager Administration** window shown below, select the **Session Manager Instances** tab, select the pertinent appropriate Session Manager and click on **Edit**.

The screenshot shows the 'Session Manager Administration' window. At the top, it says 'This page allows you to administer Session Manager instances and view assigned SM Communication Profile counts'. Below this are three tabs: 'Session Manager' (selected), 'Branch Session Manager', and 'SM Communication Profile Counts'. Under the 'Session Manager' tab, there is a section titled 'Session Manager Instances' with buttons for 'New', 'View', 'Edit', and 'Delete'. Below these buttons, it says '2 Items' with a refresh icon. A table follows with columns: 'Name', 'License Mode', and 'Data Center'. The table has two rows: 'sm1' with 'Normal' license mode and '---' data center, and 'sm2' with 'Normal' license mode and '---' data center. Below the table, it says 'Select : None'.

	Name	License Mode	Data Center
<input checked="" type="radio"/>	sm1	Normal	---
<input type="radio"/>	sm2	Normal	---

Select : None

Scroll down to the **CDR** section and configure the following.

- Check the **Enable CDR** box.
- Configure a valid **Password** and confirm the same.
- **Data file Format:** During compliance testing **Standard Flat File** was selected from the drop-down menu.

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

The screenshot shows the 'CDR' configuration section. It has a title 'CDR' with a dropdown arrow. Below the title, there are several fields and checkboxes. 'Enable CDR' is checked with a blue checkbox. 'User' is set to 'CDR_User'. 'Password' and 'Confirm Password' are empty text boxes. 'Data File Format' is a dropdown menu set to 'Standard Flat File'. At the bottom, there are two checkboxes: 'Include User to User Calls' and 'Include Incomplete Calls', both of which are unchecked.

CDR ▾

Enable CDR ☒

User

Password

Confirm Password

Data File Format

Include User to User Calls ☐

Include Incomplete Calls ☐

6. Configure Virsae Service Management

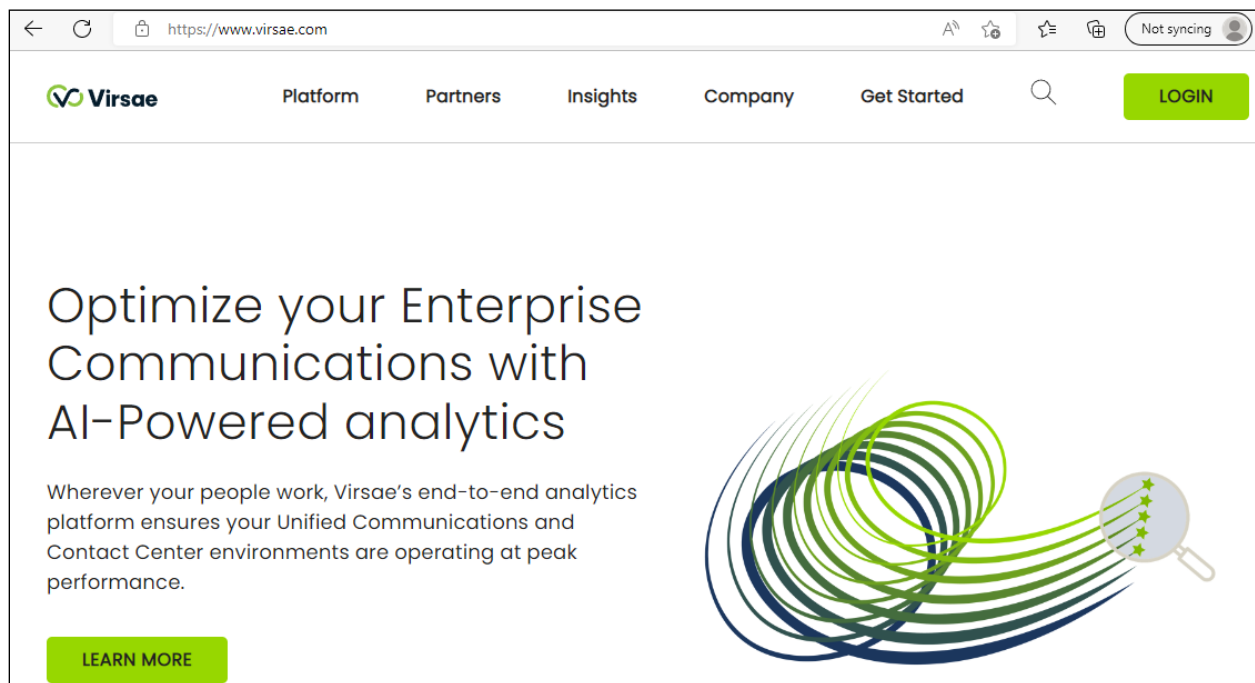
This section describes the configuration of VSM required to interoperate with Session Manager.

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® Session 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 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 for VIRSAE, featuring a green stylized figure with arms raised above the word "VIRSAE" in a grey, sans-serif font.

Email

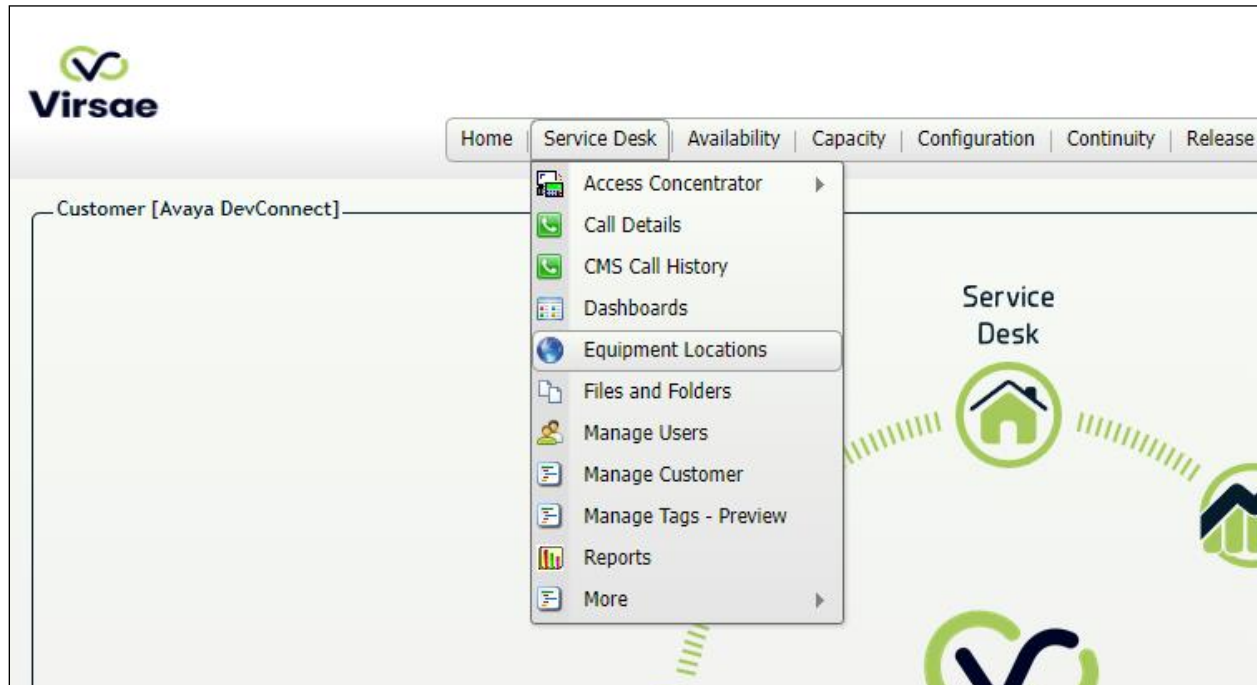
Password

[Forgot your password?](#)

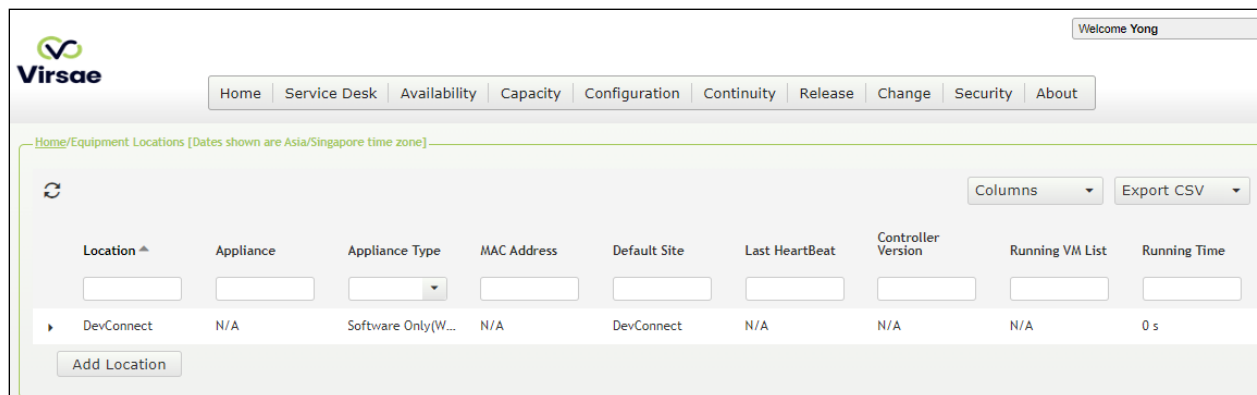
The customer screen is shown. During compliance testing the customer created by Virsae can be seen near the top right corner. Note the version running is shown at the bottom i.e., **174.1.2.268**.



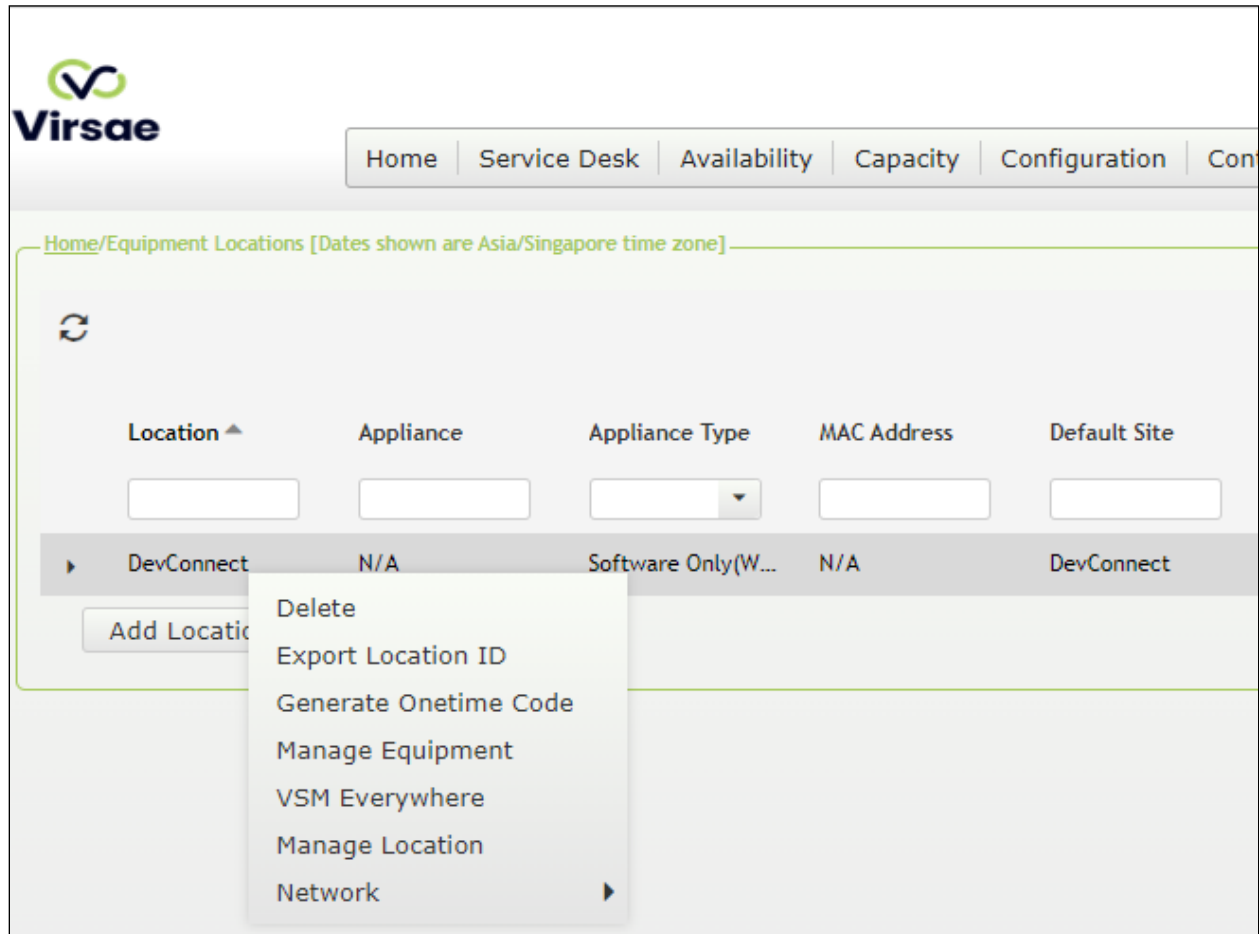
Navigate to **Service Desk → Equipment Locations** as shown below.



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



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



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

The screenshot shows the 'Add Equipment' dialog box. It has a title bar 'Add Equipment' and four tabs: 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.

6.2. Configuring Avaya Aura® Session Manager

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

- **Equipment Name:** A descriptive name.
- **Username:** The username mentioned in **Section 5.1**.
- **Password:** The password for the above-mentioned user.
- **IP Address/Host Name:** Management IP address of Session Manager.
- **Site:** A descriptive site name.

Below are the configured values of a Session Manager.

Equipment	SNMP Query	Network Connectivity	Custom Scripts	Tags	CDR
Vendor * <input type="text" value="Avaya"/>		Product * <input type="text" value="Session Manager"/>			
Equipment Name * <input type="text" value="SM2"/>		Username <input type="text" value="cust"/>			
IP Address/Host Name * <input type="text" value="10.1.10.41"/>		Password <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 5.2**.

Equipment	SNMP Query	Network Connectivity	Custom Scripts	Tags	CDR
<div>Version</div> <div>V2</div>					
<div>SNMP Community String *</div> <div>public</div>					

In the **CDR** tab, configure the following values.

- Check the box for **Enable Collection of CDR Files**.
- Check the box for **Delete CDR Files After Download**.
- **File Type:** Select **Flat** from the drop-down menu.
- **SFTP User Name:** **CDR_User** is populated by default which is the default user in Session Manager as seen in **Section 5.4**.
- **SFTP Password:** Enter the password configured in **Section 5.4**.

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

Equipment	SNMP Query	Network Connectivity	Custom Scripts	Tags	CDR
<div><input checked="" type="checkbox"/> Enable Collection of CDR Files</div> <div><input checked="" type="checkbox"/> Delete CDR Files After Download ⓘ</div> <div>File Type *</div> <div>Flat</div> <div>SFTP User Name *</div> <div>CDR_User</div> <div>SFTP User Password</div> <div>.....</div>					

The screen below shows the added Session Manager equipment.

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

New Equipment Detected

Managed Equipment

Columns Export CSV

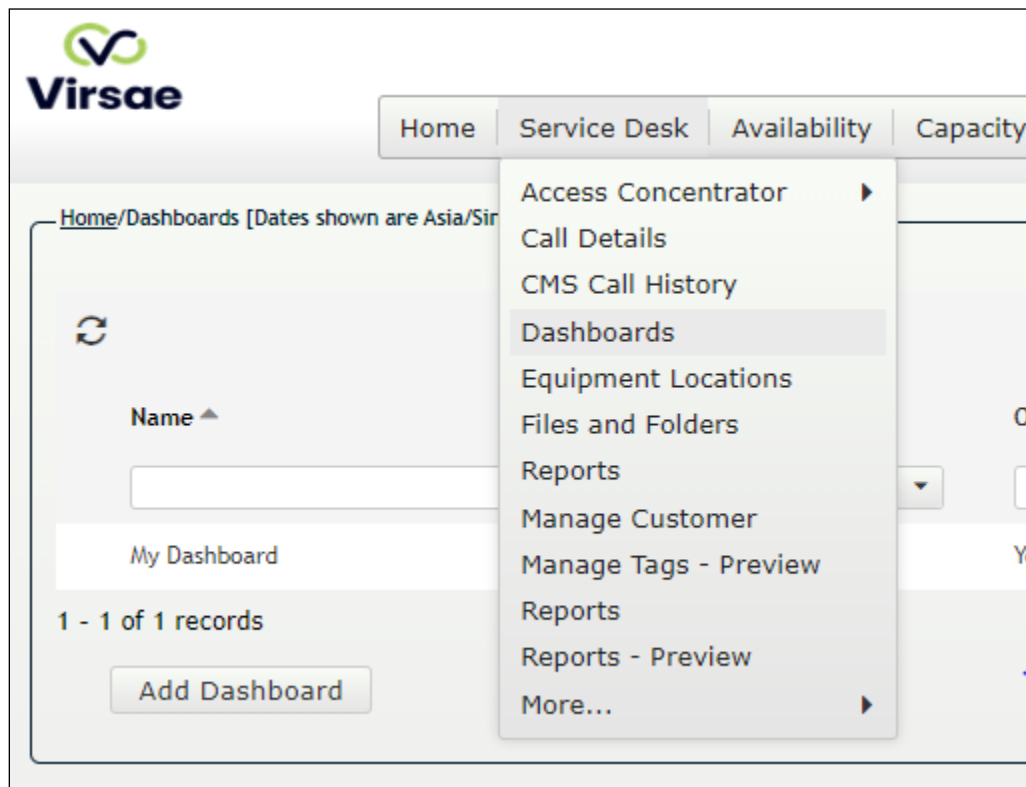
Vendor	Product	Name	IP Address	Tag Key	Last Modified
Avaya	Application Enablement Server	AES	10.1.10.70		02-Aug-2022 10:28 AM
Avaya	Breeze	Breeze	10.1.10.19		02-Aug-2022 10:29 AM
Avaya	Communication Manager	DevConnect ACM 10	10.1.10.230		02-Aug-2022 10:09 AM
Avaya	Media Server	AAMS	10.1.10.12		02-Aug-2022 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		15-Aug-2022 3:47 PM

Add Equipment

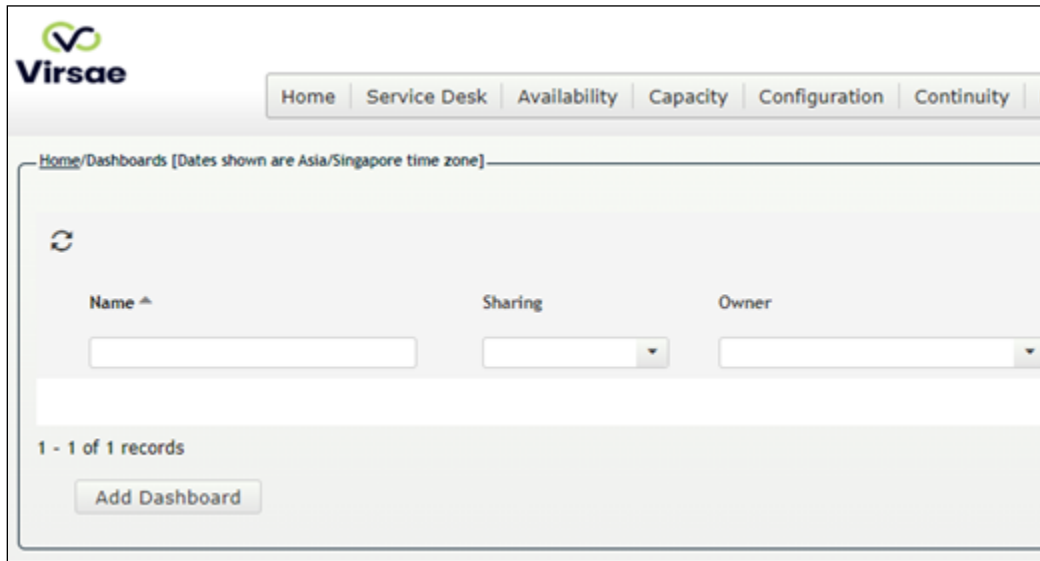
6.3. Configure Dashboard

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

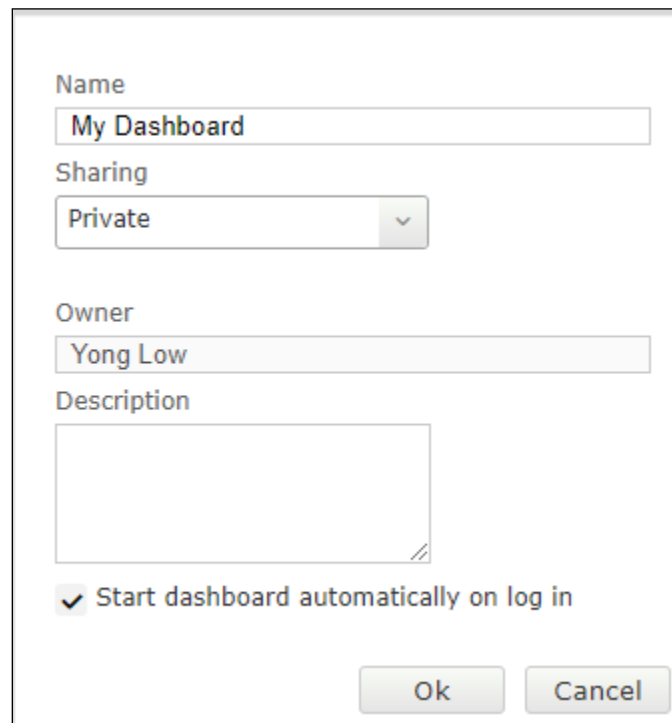
From the home screen, navigate to **Service Desk** → **Dashboards** as shown below.



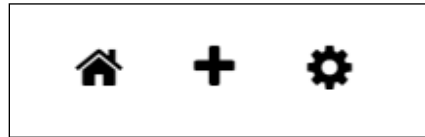
From the **Available Dashboards** window, click on the **Add Dashboard** button.



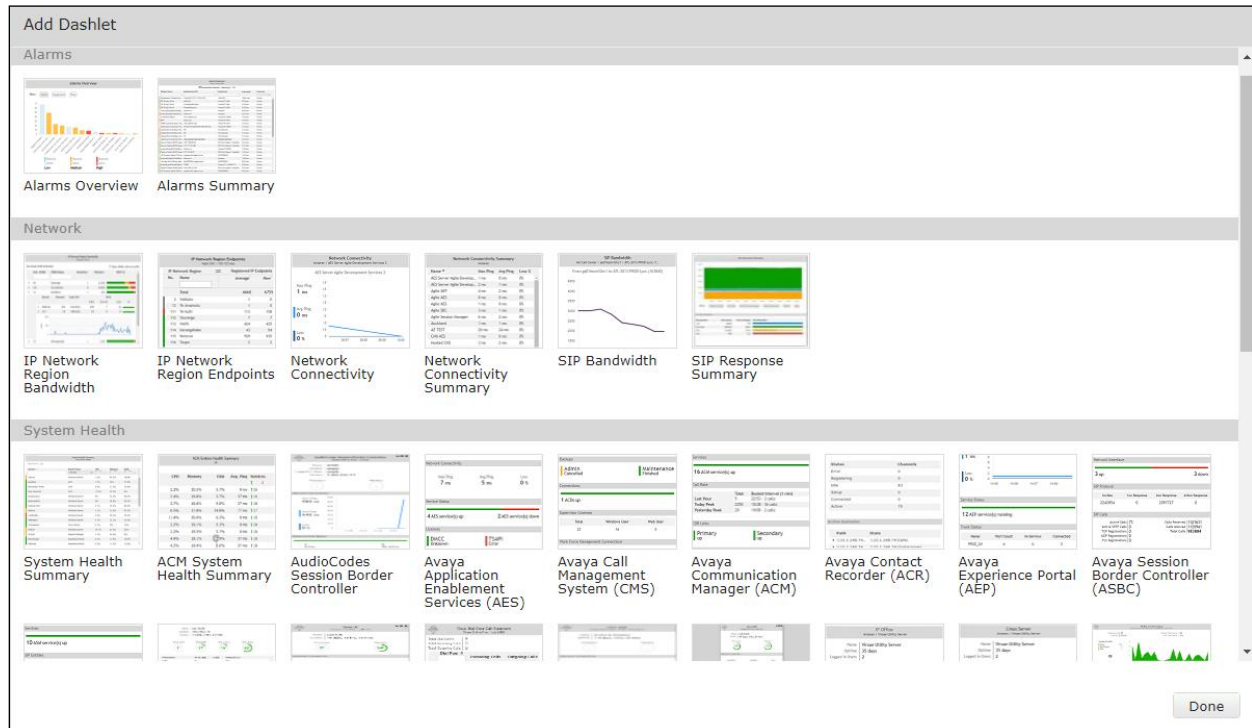
In the **Add Dashboard** window, type a descriptive name for **Name** field as shown below. Retain default values for all other fields. Check on **Start dashboard automatically on log in** box and then click on **Ok** to submit.



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



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



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



Select the appropriate **Equipment** e.g., **SM1** for Session 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

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

System Health Summary
DevConnect

Equipment

☐ Backup Receiver

☐ Backup Receiver

☐ Backup Receiver

☐ 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

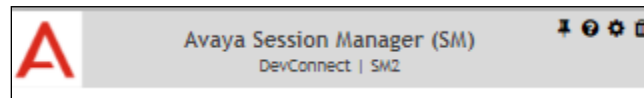
☐ 6 - Low

☐ 7 - Low

☐ 8 - Low

☐ 9 - Low

Repeat the same for the **Avaya Session Manager (SM)** dashlet for say **SM1** and in addition select the desired **Layout**.

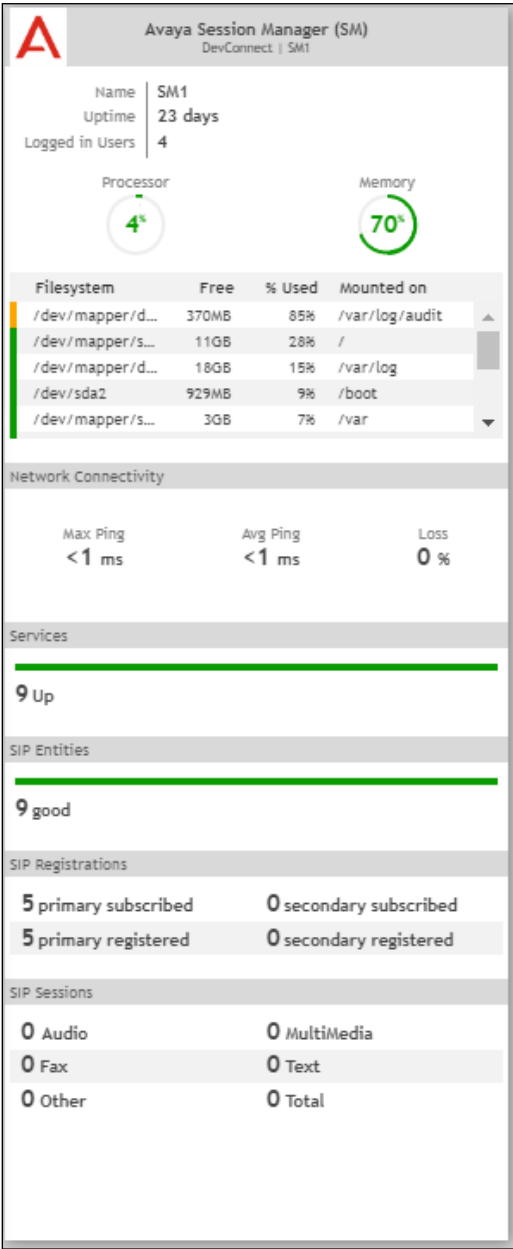


Settings

Dashboard	Customer
All Dashlets	Avaya DevConnect
ACM System Health Summary DevConnect	Location
Alarms Summary Avaya DevConnect	DevConnect
Avaya Application Enablement Services (AES) DevConnect AES	Equipment
Avaya Communication Manager (ACM) DevConnect DevConnect ACM 10	SM1
Avaya Session Manager (SM) DevConnect SM1	Layout
Avaya Session Manager (SM) DevConnect SM1	Show Occupancy Graph
Calls In Progress DevConnect DevConnect	Show Network Connectivity Graph
Linux Server DevConnect AAMS	Show Services
Linux Server DevConnect Breeze	Show SIP Entities
Linux Server DevConnect SMGR	Show SIP Registrations
	Show SIP Sessions
	Show Custom Scripts

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

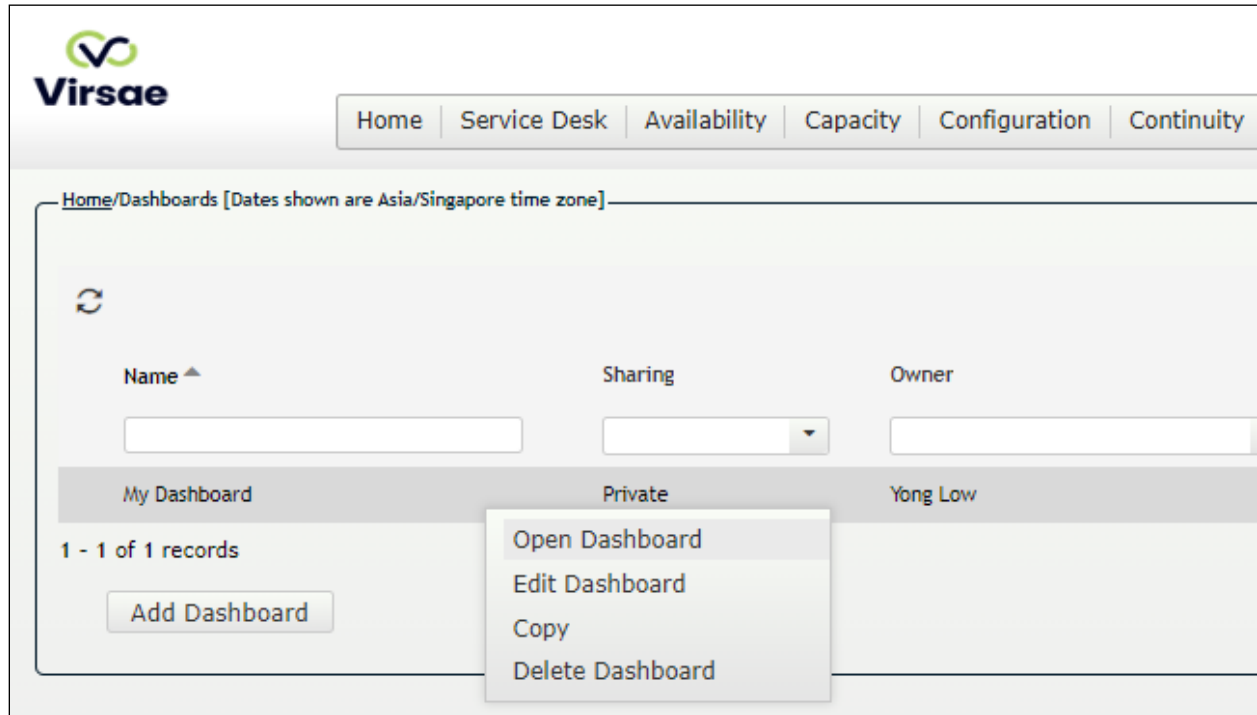
Alarms Summary		
Avaya DevConnect		
2 unresolved alarms?		
Display Name	Admin ID	Equipment
<input type="text"/>	<input type="text"/>	<input type="text"/>
TALM00100	Unknown	SM1
TALM00100	Unknown	SM2



7. Verification Steps

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



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.

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 alarms by filtering for Session Manager 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
TALM00100	Test alarm, no recovery action nec...	2022-08-17 11:30:36	Unknown	0	SM1	Avaya	6
TALM00100	Test alarm, no recovery action nec...	2022-08-17 11:30:08	Unknown	0	SM2	Avaya	6
_WD	The Watchdog is a server process t...	2022-08-17 11:01:52	Unknown	0	DevConnect A...	Avaya	2
_WD	The Watchdog is a server process t...	2022-08-17 11:01:52 A		3	DevConnect A...	Avaya	2

To view voice quality using historical reporting, navigate to **Availability → Voice Quality Management** (not shown). Create a rule set and apply the rule. Screen below shows a few examples of voice quality for SIP extensions registered to Session Manager. Real time voice quality can also be viewed in the dashboard.

Filters: VQM1

Expression (condition)

Details

Location = DevConnect

Date Time Range: 01-Aug-2022 12:00 AM-03-Aug-2022 12:00 AM

Save Save All Apply

VQM - Streams

Columns Export CSV

Name	Endpoint	IPNR	Mos Min	Mos Max	Mos Avg	Stream Length	IP Address	Port	D
9608 H.323	10003	1	4.41	4.41	4.41	3593	10.1.10.174	3300	
XFire2a09	gwp	1	4.21	4.41	4.41	3593	10.1.50.25		
AVAYA, SIP10048	10048	N/A	4.41	4.41	4.41	3593	10.1.10.158		
1616 H.323	10002	1	4.41	4.41	4.41	3593	10.1.10.198	2876	
9608 H.323	10003	1	4.4	4.41	4.41	3593	10.1.10.174	3300	
XFire2a09	gwp	1	4.21	4.41	4.41	3593	10.1.50.25		
AVAYA, SIP10048	10048	N/A	4.41	4.41	4.41	3593	10.1.10.158		
1616 H.323	10002	1	4.41	4.41	4.41	3593	10.1.10.198	2876	

To view CDR using historical reporting, navigate to **Service Desk → Call Details** (not shown). Create a rule set and apply the rule. Screen below shows a few examples of CDR collected from Session Managers.

Filters: CDR1

Expression (condition) [Dates shown are Asia/Singapore time zone]

Details

Location = DevConnect
+

Equipment = SM2, SM1
+

Date Time Range: 01-Aug-2022 12:00 AM-04-Aug-2022 12:00 AM
+

Save Save All Apply

Call Details

Columns Export CSV

Call Start Date-Time	Mos Min	Mos Max	Mos Avg	Owner DN	Duration Seconds	Dialed Number	Calling Number	Condition	Access Code Dialed	Ac
<input type="text"/>	<input type="text"/> 0 - 5	<input type="text"/> 0 - 5	<input type="text"/> 0 - 5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2022-08-03 14:33:00					0	60000	60049	A		
2022-08-02 13:56:00					6	10001	10048	A		
2022-08-02 13:57:00					6	10001	10048	A		
2022-08-02 13:57:00					0	10048	11001	9		
2022-08-02 13:57:00					6	10048	11001	9		
2022-08-02 14:27:00					426	10001	10048	A		
2022-08-02 15:03:00					552	10048	10004	9		
2022-08-02 15:25:00					54	10001	10048	A		

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R174 to interoperate with Avaya Aura® Session 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® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*, Release 10.1., Issue 2, Mar 2022.
2. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, Apr 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.