



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 R135 to interoperate with Avaya Aura® Session Manager R8.1.2.

Virsae Service Management provides real-time monitoring and management solutions for IP telephony networks. Virsae Service Management provides visibility of Avaya and other vendor's IP Telephony solutions from a single console and enables a reduction in complexity when managing complex IP telephony environments.

Virsae Service Management 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) display 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.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager or the Telnet/SSH interface to interact with other Avaya products. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use of these interfaces as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the interfaces in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using these interfaces. Using these interfaces in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real-time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Avaya

Product Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

For feature testing, VSM dashboard was used to view the configurations of 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.

- VSM needs to login using the administrative account created during installation of Session Manager. This is because any account created after the installation is not part of sudo users file as per current design of Session Manager.

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 Workplace Client for Windows and one-X® Communicator (SIP and H.323) softphones configured for making and receiving calls. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. VSM was installed on a server running Microsoft Windows Server 2016. Architecturally the VSM Service relies on an appliance being placed on a corporate LAN and being configured to connect to a Unified Communication platform as well as the Microsoft Azure cloud via the internet. The VSM appliance contains Probe Service use to collect service management data. The VSM appliance acts as a collector and compresses, encrypts then forwards data from all sources to the Virsae cloud computing service. A PC/Laptop is used to access the Virsae portal to manage VSM services, add additional users and view reporting data on the equipment being managed.

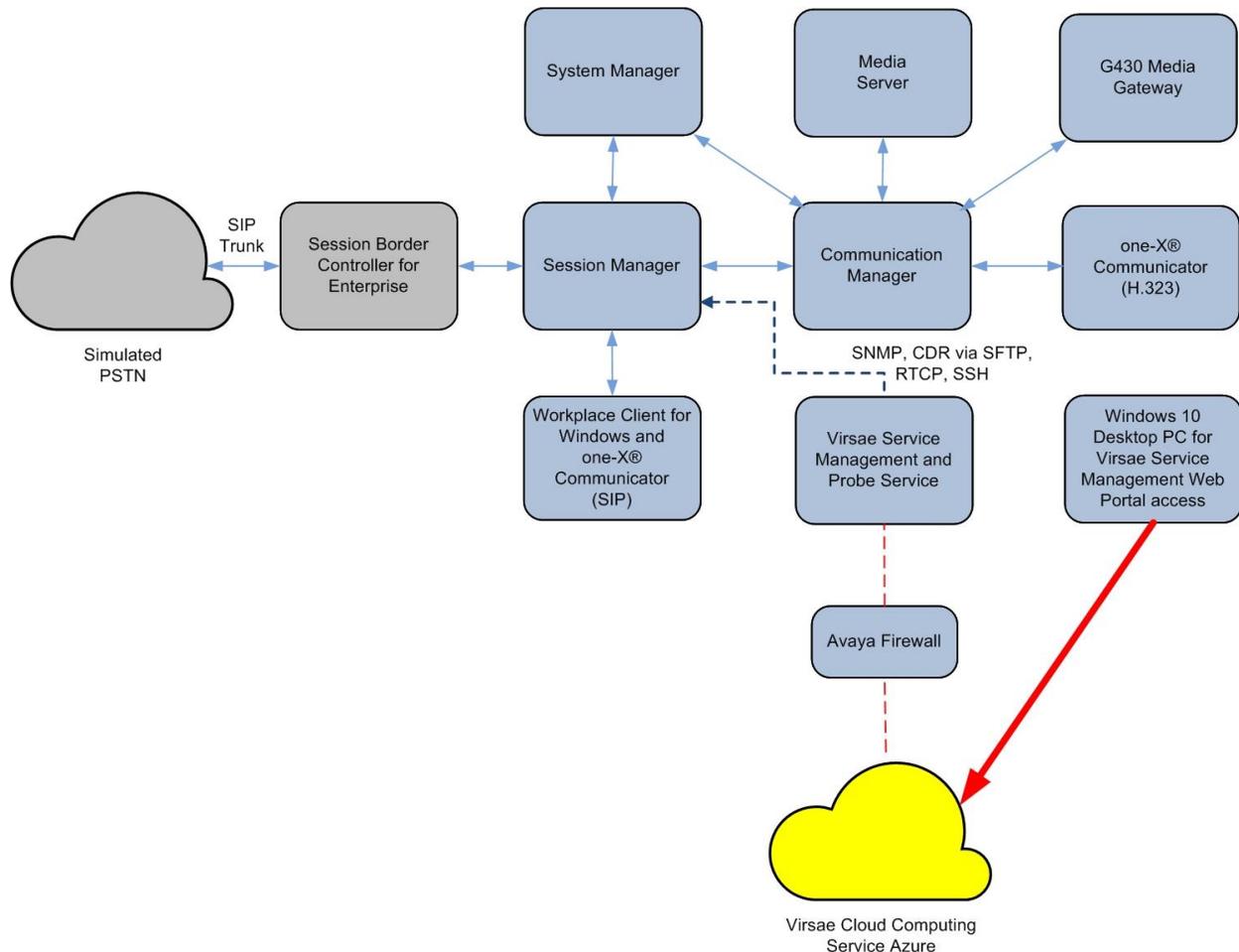


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Session Manager running on virtual server	8.1.2.1.812101
Avaya Aura® System Manager running on virtual server	8.1.2.0.0611588
Avaya Aura® Communication Manager running on virtual server	8.1.2.0.0-FP2
Avaya G430 Media Gateway	41.16.0
Avaya Aura® Media Server running on virtual server	8.0.2.93
Avaya Workplace Client for Windows	3.9.0.84.8
Avaya one-X® Communicator (SIP and H.323)	6.2.12.04-FP14
Virsa Service Management and Probe Service running on Windows 2016	R135

5. Configure Avaya Aura® 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.

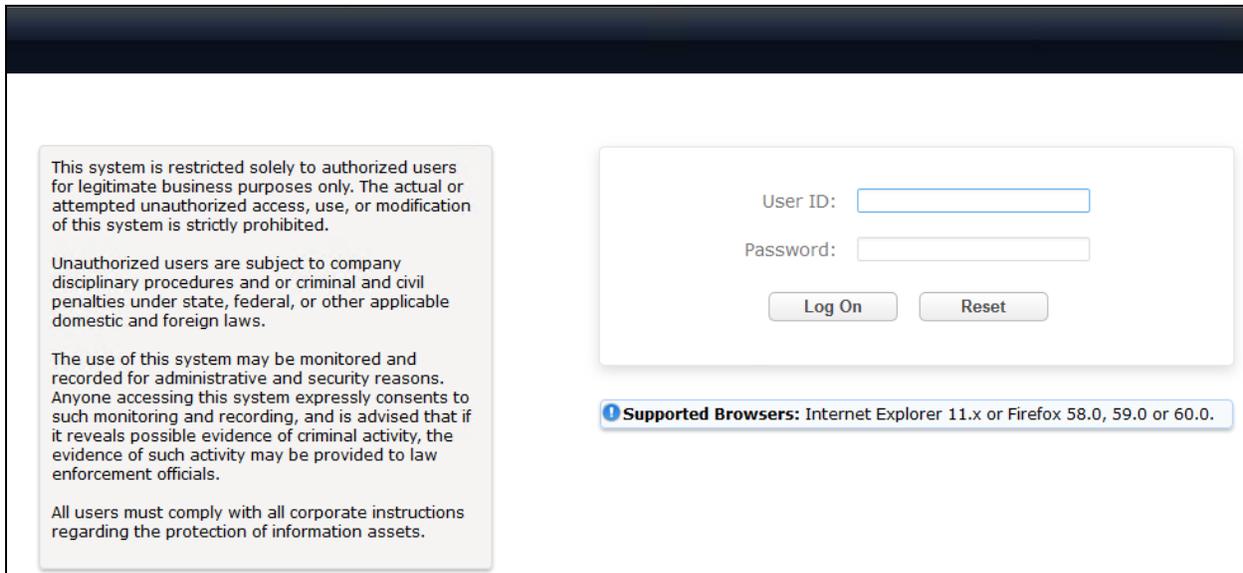
5.1. Configure Login Group

During compliance testing the default administrator account created during installation of Session Manager was used. This is because as mentioned in **Section 2.2**, 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.



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.

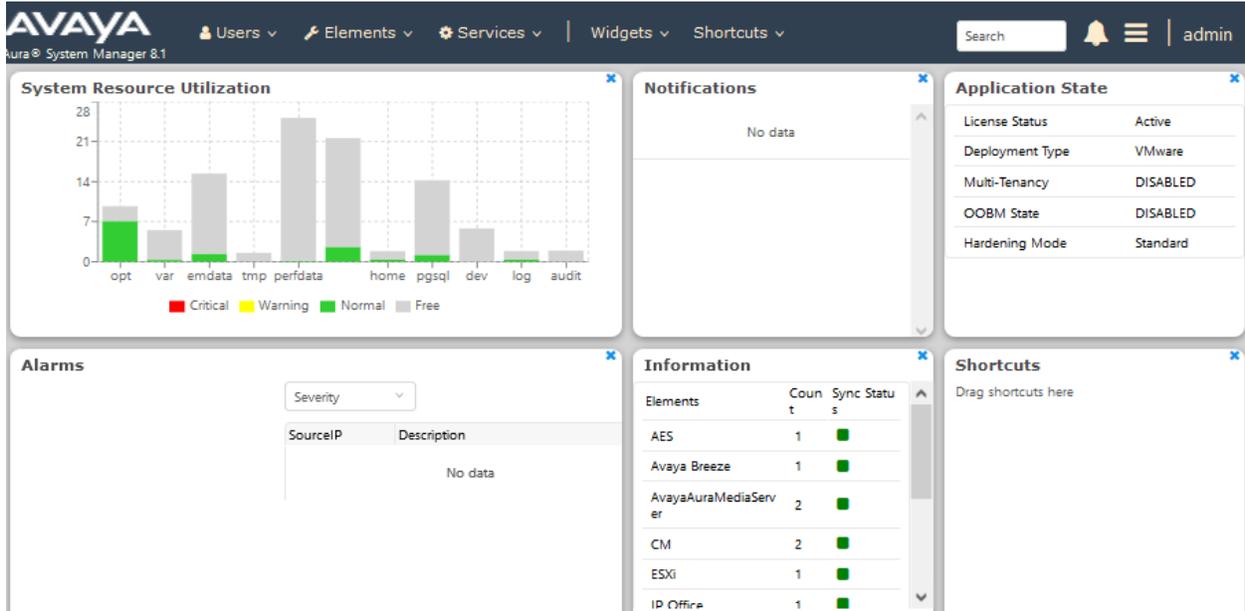
User ID:

Password:

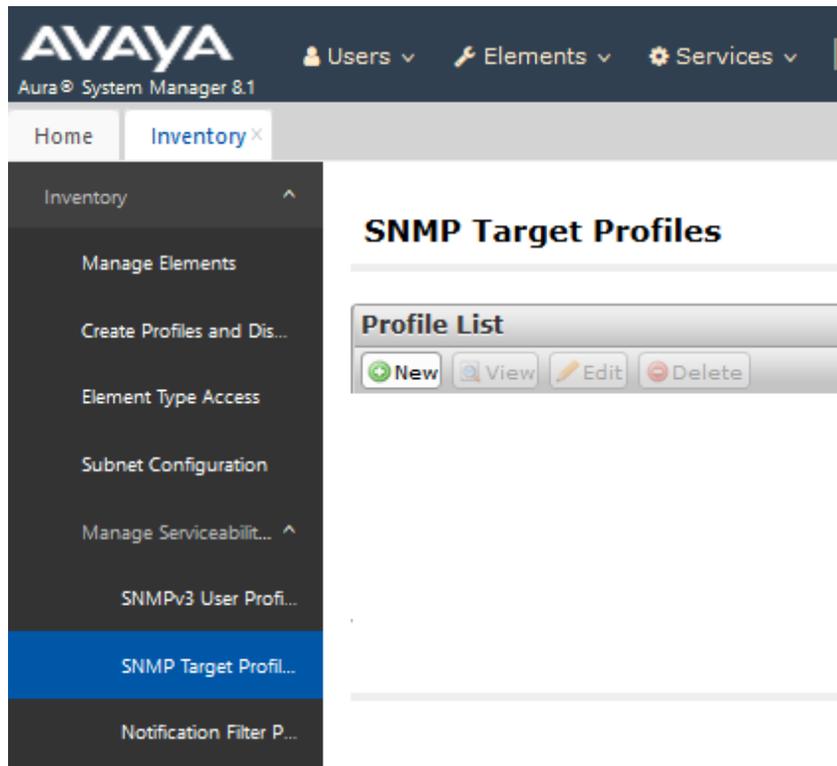
Log On Reset

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

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 Aura System Manager 8.1

Users Elements Services Widgets Shortcuts Search

Home Inventory

Serviceability Agents

Agent List

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

8 Items Show All

<input type="checkbox"/>	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 checked="" 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

From the **Manage Profile** window, under the **SNMP Target Profiles** tab, select the **Virsaev2** profile, click on **Assign** and then the **Commit** button.

Manage Profile

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

Selected Agents **SNMP Target Profiles** SNMPv3 User Profiles

Assignable Profiles ▾

[Assign](#)

2 Items

<input type="checkbox"/>	Name	Domain Type	IP Address	Port	SNMP Version
<input type="checkbox"/>	Virsaev2	UDP	10.1.10.124	162	V2

Select : All, None

Removable Profiles ▾

Remove [Assign/Remove](#)
[Filter Profiles](#)

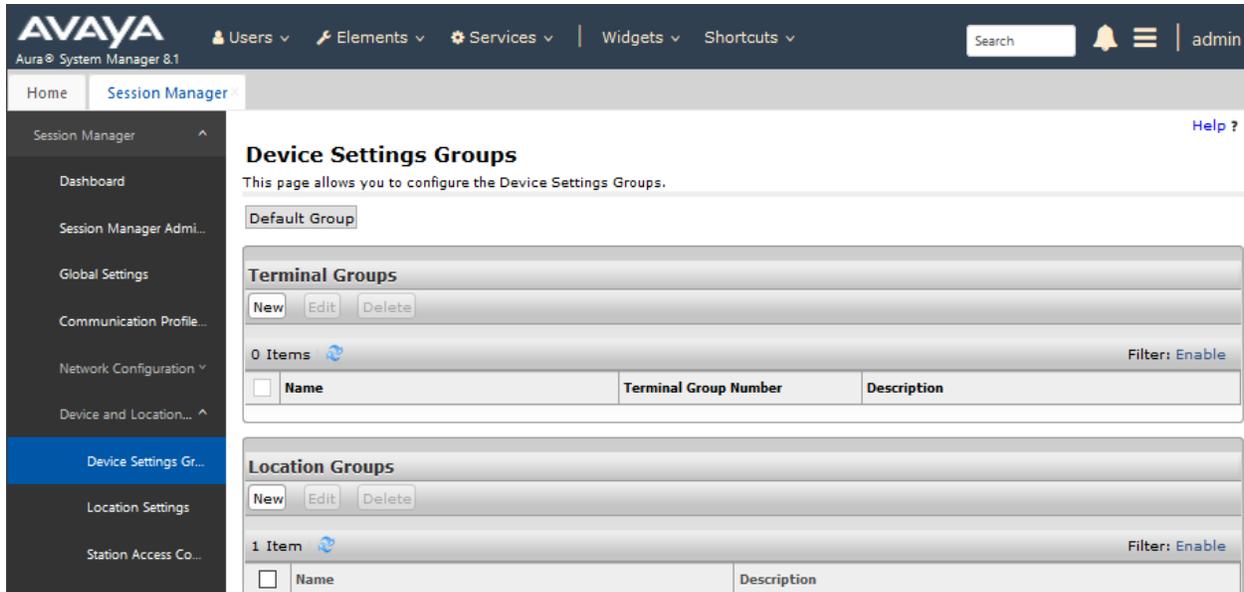
0 Items

<input type="checkbox"/>	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
No records to display						

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.



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.

Device Settings Group Restore Cancel Save

General | Endpoint Timer | Maintenance Settings | VoIP Monitoring Manager | Volume Settings | VLAN Parameters | 802.1 P/Q Parameters |
Expand All | Collapse All

General ▾

*Name:

Description:

Group Type: Location Group Terminal Group

*Terminal Group Number:

Endpoint Timer ▶

Maintenance Settings ▶

VoIP Monitoring Manager ▾

IP Address:

*Port:

*Reporting Period:

Volume Settings ▶

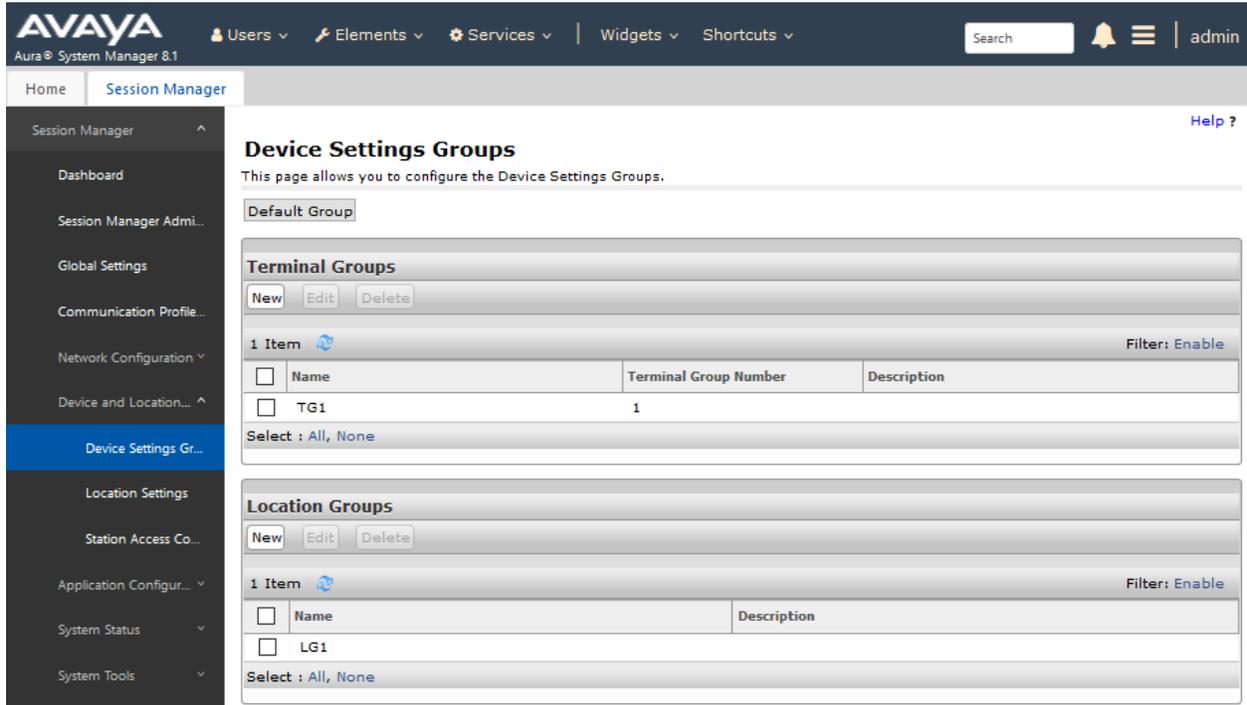
VLAN Parameters ▶

DIFFSERV/QOS Parameters ▶

802.1 P/Q Parameters ▶

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

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



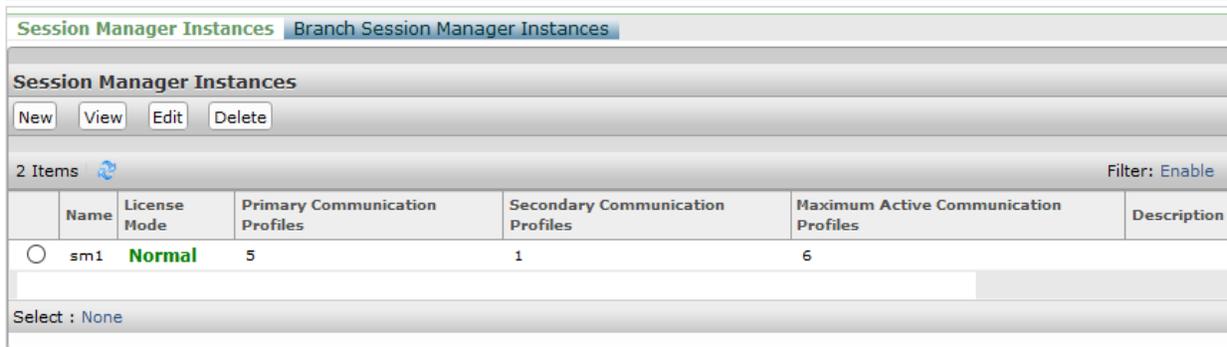
The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). A search bar and a user profile (admin) are also visible. The left sidebar contains a navigation menu with options like Home, Session Manager, Dashboard, Session Manager Admin..., Global Settings, Communication Profile..., Network: Configuration, Device and Location..., Device Settings Groups (highlighted), Location Settings, Station Access Co..., Application Configur..., System Status, and System Tools. The main content area is titled 'Device Settings Groups' and includes a sub-header 'This page allows you to configure the Device Settings Groups.' Below this, there are two sections: 'Terminal Groups' and 'Location Groups'. Each section has a 'Default Group' label, a 'New', 'Edit', and 'Delete' button, and a table with one item. The 'Terminal Groups' table has columns for Name, Terminal Group Number, and Description, with one row for 'TG1' with Terminal Group Number '1'. The 'Location Groups' table has columns for Name and Description, with one row for 'LG1'. Both sections also have a 'Filter: Enable' link and a 'Select: All, None' link.

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 Session Manager and click on **Edit**.

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.



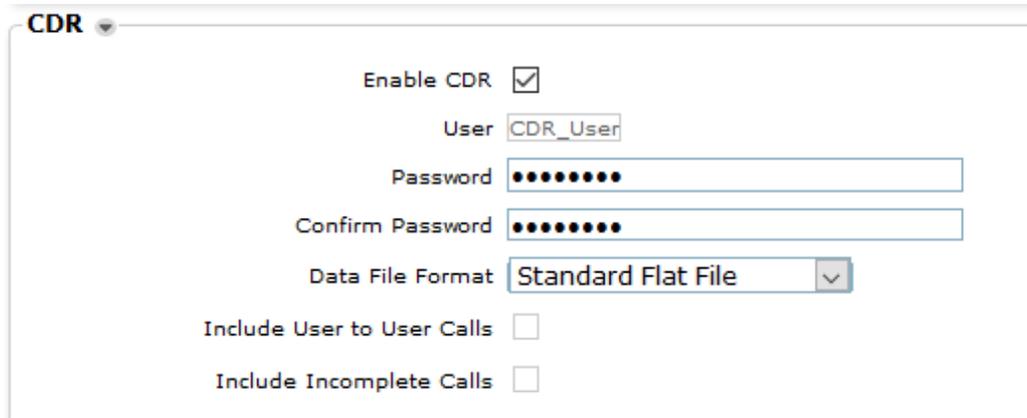
The screenshot shows the 'Session Manager Administration' window. At the top, there are tabs for 'Session Manager Instances' and 'Branch Session Manager Instances'. Below the tabs, there is a header 'Session Manager Instances' and a row of buttons: 'New', 'View', 'Edit', and 'Delete'. Below the buttons, it says '2 Items' and 'Filter: Enable'. The main part of the screenshot is a table with the following columns: 'Name', 'License Mode', 'Primary Communication Profiles', 'Secondary Communication Profiles', 'Maximum Active Communication Profiles', and 'Description'. There is one row of data with the following values: 'sm1', 'Normal', '5', '1', '6', and an empty description. Below the table, it says 'Select : None'.

Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
sm1	Normal	5	1	6	

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 configuration options: 'Enable CDR' with a checked checkbox, 'User' with a text input field containing 'CDR_User', 'Password' with a password input field, 'Confirm Password' with a password input field, 'Data File Format' with a dropdown menu showing 'Standard Flat File', 'Include User to User Calls' with an unchecked checkbox, and 'Include Incomplete Calls' with an unchecked checkbox.

6. Configure Virsae Service Management

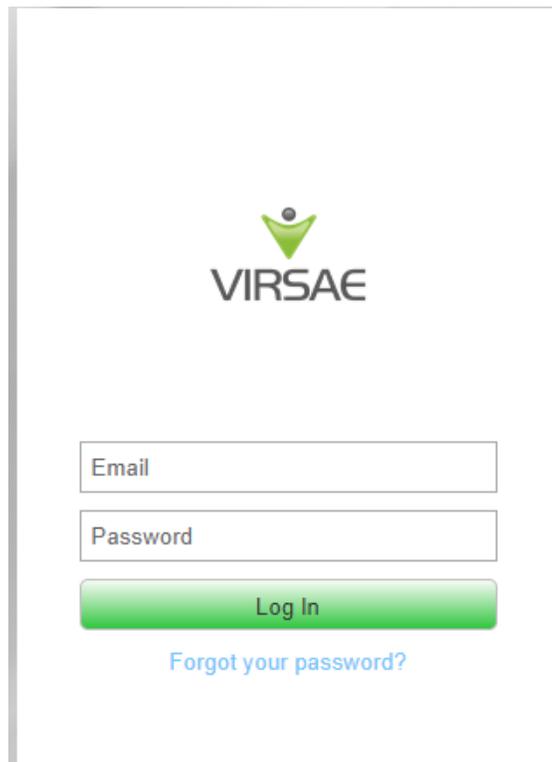
This section describes the configuration of VSM required to interoperate with Session Manager.

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 *<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 screenshot shows a login interface for the Virsae web portal. At the top center is the Virsae logo, which includes a green stylized figure above the word "VIRSAE". Below the logo are two input fields: "Email" and "Password". A green "Log In" button is positioned below the password field, and a blue link "Forgot your password?" is located below the button.

The customers screen is shown. During compliance testing the customer created by Virsae is **Devconnect** as can be seen near the top left corner.



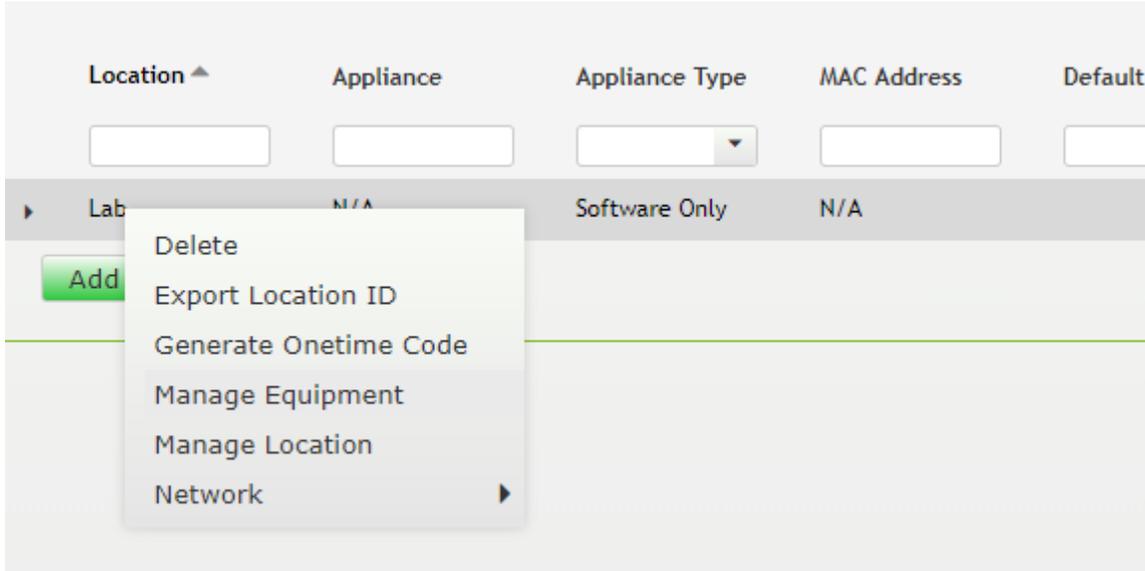
Navigate to **Service Desk** → **Equipment Locations** as shown below.

The screenshot shows the VIRSAE web interface. At the top, there is a navigation bar with the following items: Home, Service Desk, Availability, Capacity, Configuration, Continuity, Release, Change, Security, and About. Below this, the breadcrumb path is 'Home/Equipment Locations [Dates shown are Singapore time zone]'. The main content area features a table with the following columns: Location, Appliance, Appliance Type, MAC Address, Default Site, Last HeartBeat, Controller Version, Running VM List, and Running Time. A single row is visible with the following values: Lab, N/A, Software Only, N/A, N/A, N/A, N/A, N/A, and 0 s. Below the table is an 'Add Location' button. On the left, a dropdown menu is open under 'Service Desk', listing: Access Concentrator, Call Details, CMS Call History, Dashboards, Equipment Locations (highlighted), Files and Folders, Manage Customer, Reports, and More. In the background, there are icons for 'Service Desk' (a house) and 'Availability Manager' (a bar chart with an upward arrow).

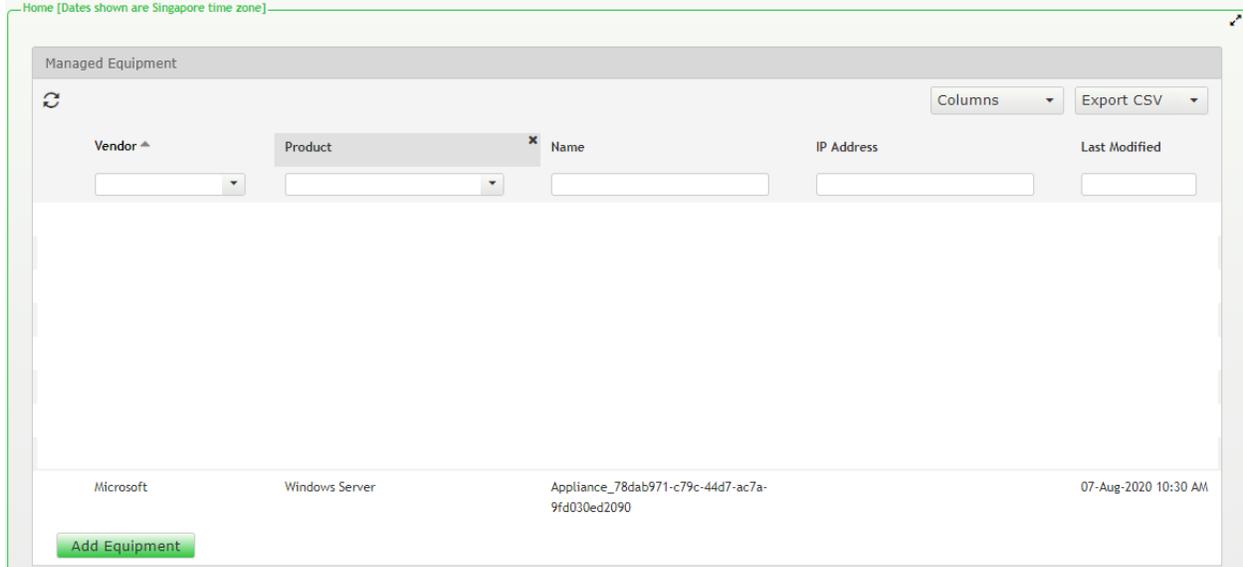
A **Location** called **Lab** is already configured as shown below.

This screenshot is identical to the one above, showing the VIRSAE interface with the 'Equipment Locations' table. The table contains one entry for 'Lab' with the following details: Appliance: N/A, Appliance Type: Software Only, MAC Address: N/A, Default Site: N/A, Last HeartBeat: N/A, Controller Version: N/A, Running VM List: N/A, and Running Time: 0 s. The 'Add Location' button is visible below the table.

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



Click **Add Equipment** below:



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	Custom Scripts	CDR
Vendor *		Product *	
Avaya		Session Manager	
Equipment Name *		Username *	
Session Manager1		cust	
IP Address/Host Name *		Password *	
10.1.10.59		
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 5.2**.

The screenshot shows the 'SNMP Query' tab selected. The page contains the following text: 'Virsa Direct can be configured to query this Session Manager for configuration and system health metrics, which are used in the dashboards, and historic reports. To enable this, please enter the SNMP configuration details for this Session Manager below.' Below this text are two input fields: 'Version' with a dropdown menu showing 'V2', and 'SNMP Community String *' with a text input field containing 'public'.

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

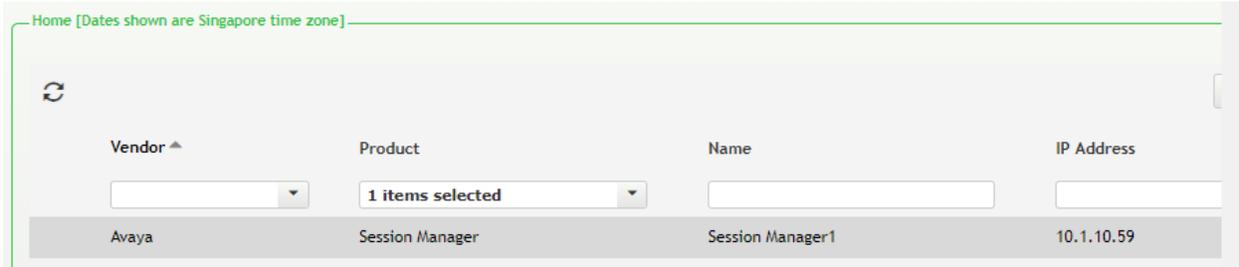
- Check the box for **Enable Collection of CDR Files**.
- Check the box for **Delete CDR Files After Download**.
- **File Type:** Select **Flat** from the drop-down menu.
- **SFTP User Name:** **CDR_User** is populated by default which is the default user in Session Manager as seen in **Section 5.4**.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

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

The screenshot shows the 'CDR' tab selected. The page contains the following text: 'Virsa Direct can be configured to collect CDR data. To do this, enable below, and configure accordingly.' Below this text are four configuration items: 1) 'Enable Collection of CDR Files' with a checked checkbox. 2) 'Delete CDR Files After Download' with a checked checkbox and an information icon. 3) 'File Type *' with a dropdown menu showing 'Flat'. 4) 'SFTP User Name *' with a text input field containing 'CDR_User'. Below these is 'SFTP User Password' with a password input field containing seven dots.

Save **Test Access** **Cancel**

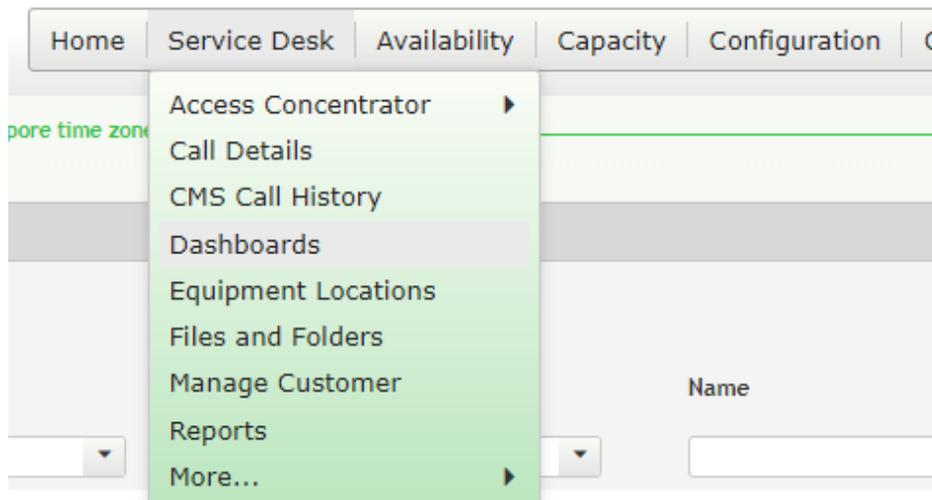
The screen below shows the added Session Manager equipment.



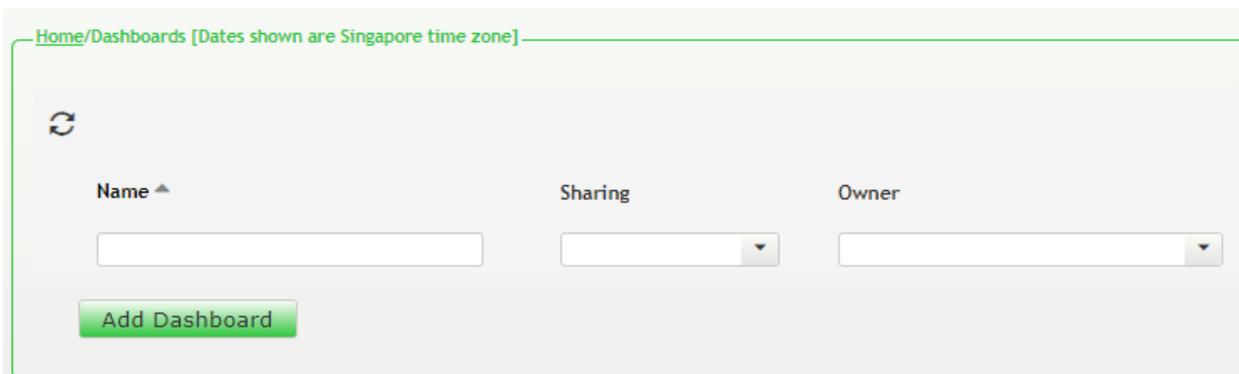
6.3. Configure Dashboard

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

Add Dashboard

Name
Devconnect Lab

Sharing
Private

Owner
Yong Meng Low

Description

Start dashboard automatically on log in

Ok Cancel

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



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

Add Dashlet

system health

System Health Summary

Add new System Health Summary

Avaya Application Enablement Services (AES)

Avaya Call Management System (CMS)

Avaya Communication Manager (ACM)

Avaya Contact Recorder (ACR)

Avaya Experience Portal (AEP)

Avaya Session Border Controller (ASBC)

Avaya Session Manager (SM)

IP Office

Linux Server

Oracle SBC

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., **Session Manager 1** 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 **Avaya Session Manager (SM)** dashboard and in addition select the desired **Layout**.



Settings

<p>Dashboard</p> <p>All Dashlets</p> <p>ACM System Health Summary Lab</p> <p>Active Streams Lab Lab</p> <p>Alarms Summary DevConnect</p> <p>Avaya Application Enablement Services (AES) Lab AES</p> <p>Avaya Call Management System (CMS) Lab Call Management System</p> <p>Avaya Communication Manager (ACM) Lab Communication Manager</p> <p>Avaya Experience Portal (AEP) DevConnect, Lab AAEP EPM</p> <p>Avaya Experience Portal (AEP) DevConnect, Lab AAEP MPP</p> <p>Avaya Session Border Controller (ASBC) Lab SBCE</p> <p>Avaya Session Manager (SM) Lab Session Manager1</p> <p>Avaya Session Manager (SM) Lab Session Manager2</p>	<p>Customer</p> <p>DevConnect</p> <p>Location</p> <p>Lab</p> <p>Equipment</p> <p>Session Manager1</p> <p>Layout</p> <p>Show Occupancy Graph <input type="checkbox"/></p> <p>Show Network Connectivity Graph <input type="checkbox"/></p> <p>Show Services <input type="checkbox"/></p> <p>Show SIP Entities <input checked="" type="checkbox"/></p> <p>Show SIP Registrations <input checked="" type="checkbox"/></p> <p>Show SIP Sessions <input checked="" type="checkbox"/></p>
--	---

The two dashboards with the configured equipment are 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	Memory	Disk	Max Ping ?	Avg Ping ?	Availability?
Session Manager1	Session Manager	↑ 9 ---	41%	74.9%	9%	<1ms	<1ms	100%

Avaya Session Manager (SM)
Lab | Session Manager1

Name	Session Manager1
Uptime	14 days
Logged in Users	4

Processor


3%

Memory


75%

Filesystem	Free	% Used	Mounted on
/dev/mapper/lo...	1GB	66%	/var/log/audit
/dev/sda1	257MB	49%	/boot
/dev/mapper/sy...	8GB	32%	/
/dev/mapper/lo...	26GB	4.9%	/var/log
/dev/mapper/sy...	12GB	2.6%	/var

Network Connectivity

Max Ping	Avg Ping	Loss
<1 ms	<1 ms	0 %

SIP Entities

10 good

SIP Registrations

4 primary subscribed	0 secondary subscribed
4 primary registered	0 secondary registered

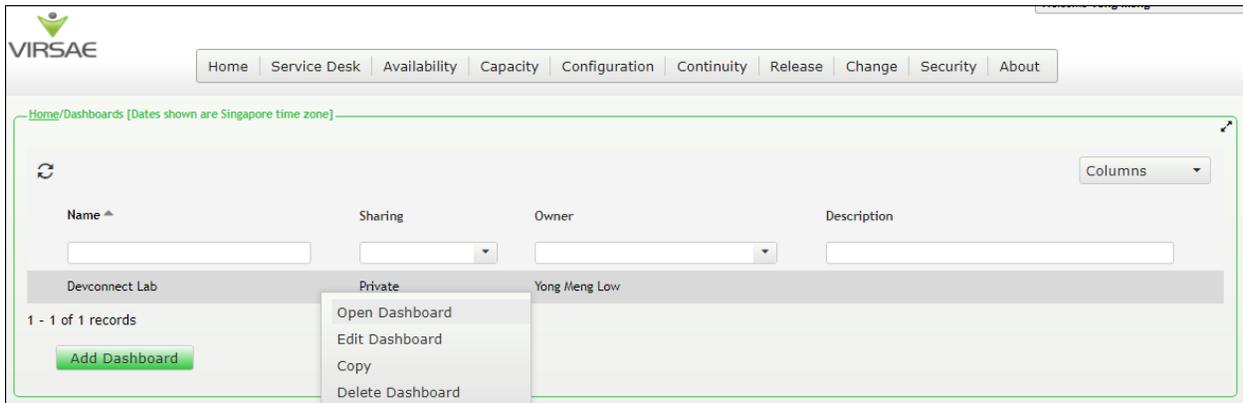
SIP Sessions

0 Audio	0 MultiMedia
0 Fax	0 Text
0 Other	0 Total

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** → **Dashboard** (not shown) and the screen is shown as below. Right click “Devconnect lab” and select “Open Dashboard”.



Whatever is configured during setup will be shown here. However, if the dashboard is configured to open automatically on startup in **Section 6.3**, once login, all the dashboards last configured at the end of **Section 6.3** will be populated in a new tab on the browser.

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.

The screenshot shows the VIRSAE web portal's "Unresolved Alarms for DevConnect" page. The page title is "Unresolved Alarms for DevConnect [Dates shown are 'Singapore' time zone]". Below the title is an "Alarm List Filter" section with a dropdown menu and a text prompt: "Drag a column and drop it here to group by that column". The main content is a table with the following columns: Alarm, Description, Activate Date, Administered Id, Repeats, Equipment, Vendor, and Severity. The table contains two rows of data:

Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Vendor	Severity
SNMP Cold Start	An SNMP Cold Start trap has been ...	2020-08-31 22:02:41	10.1.10.59	0	Session Manager1	Internet...	2
nsNotifyShutdown	An indication that the agent is in th...	2020-08-31 22:02:40	10.1.10.59	0	Session Manager1	Net SN...	6

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.

Home/Voice Quality Management [Dates shown are Singapore time zone]

Manage Filters

Filters: VQM Dates for filter are based on user's local time settings

Expression (condition)

Details

Location = Lab

Date Time Range: 17-Aug-2020 09:25 AM-31-Aug-2020 09:25 AM

VQM - Streams

Name	Endpoint	IPNR	Mos Min	Mos Max	Mos Avg	Stream Length	IP Address	Port	DSCP	Call Time	Source
AWAYA, SIP10048	sip:10048	1	4.41	4.41	4.41	90	10.1.10.155		-1	2020-08-18 14:58:07	2 items selected sip:10048@10.1.10.155
AWAYA, SIP10048	sip:10048	1	4.41	4.41	4.41	10	10.1.10.155		-1	2020-08-18 14:59:47	sip:10048@10.1.10.155
AWAYA, SIP10048	sip:10048	1	4.41	4.41	4.41	0	10.1.10.155		-1	2020-08-18 15:00:07	sip:10048@10.1.10.155
AWAYA, SIP10048	sip:10048	1	4.41	4.41	4.41	20	10.1.10.155		-1	2020-08-18 15:01:27	sip:10048@10.1.10.155
AWAYA, SIP10049	sips:10049	0	4.41	4.41	4.41	130	10.1.10.154		-1	2020-08-18 18:17:25	sips:10049@10.1.10.154
AWAYA, SIP10049	sips:10049	0	4.41	4.41	4.41	40	10.1.10.154		-1	2020-08-18 18:19:45	sips:10049@10.1.10.154
AWAYA, SIP10049	sips:10049	0	4.41	4.41	4.41	310	10.1.10.154		-1	2020-08-19 09:12:45	sips:10049@10.1.10.154
AWAYA, SIP10049	sips:10049	0	4.41	4.41	4.41	170	10.1.10.154		-1	2020-08-19 09:19:45	sips:10049@10.1.10.154
AWAYA, SIP10048	sip:10048	1	4.41	4.41	4.41	50	10.1.10.155		-1	2020-08-19 11:09:55	sip:10048@10.1.10.155

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.

Home/Call Details [Dates shown are Singapore time zone]

Call Details Filters

Filters: CDR

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

Details

- Location = Lab
- Equipment = Session Manager1, Session Manager2
- Date Time Range: Last 24 hours

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
	0 - 5	0 - 5	0 - 5							
2020-08-26 19:43:00					12	10000	10049	A		
2020-08-26 19:43:00					6	833411311	10049	A		
2020-08-26 19:44:00					6	14001	33411311	9		
2020-08-26 19:44:00					6	14001	33411311	9		
2020-08-26 19:45:00					6	14001	33411311	9		
2020-08-26 19:50:00					0	14001	33411311	9		
2020-08-26 19:52:00					6	14001	33411311	9		
2020-08-26 19:52:00					6	14001	33411311	9		

8. Conclusion

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

9. Additional References

This section references the product documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

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

Product documentation for Virsae products can be obtained directly from Virsae.

1. *Virsae Service Management - Adding Avaya Aura Applications and Servers*.
2. *Virsae Service Management – Service Definition, May 2020*.

©2020 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.