Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management for Unified Communications to interoperate with Avaya Aura® Session Manager.

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 for Unified Communications (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 three 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.

2. General Test Approach and Test Results

The general test approach was to use VSM web user interface (dashboard) and historical reporting to display the configurations details of Session Manager. Calls were placed between Avaya SIP endpoints with other endpoints and Virsae dashboard and historical reporting was used to display the 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 capabilities of SFTP, SSH and SNMP as requested by Virsae.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third-party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

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 and Session Managers to simulate system unavailability. Loss of network connectivity to both VSM and Session Managers were also performed during testing.

2.2. Test Results

All test cases passed successfully with the following observation.

- VSM needs to login using the admin account created during installation of Session Manager. This is because any account created after the installation is not part of sudoers 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 G450 Media Gateway. The system has Avaya H323, SIP, Equinox for Windows, digital and analog endpoints 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 2012 R2 with Service Pack 1. 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 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.

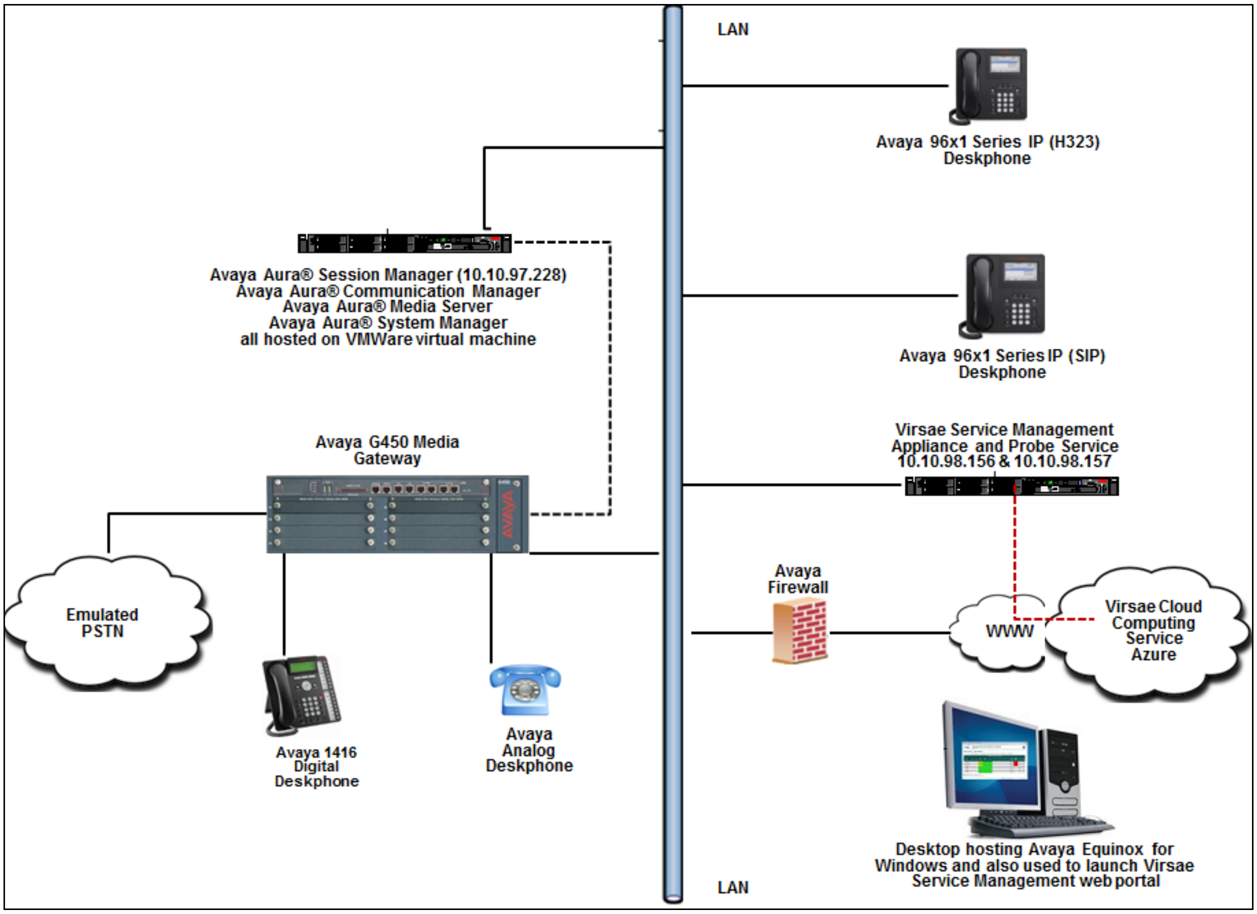

LAN
Avaya 96x1 Series IP (H323) Deskphone
Avaya Aura® Session Manager (10.10.97.228)
Avaya Aura® Communication Manager
Avaya Aura® Media Server
Avaya Aura® System Manager
all hosted on VMWare virtual machine
Avaya 96x1 Series IP (SIP) Deskphone
Avaya G450 Media Gateway
Virsae Service Management Appliance and Probe Service
10.10.98.156 & 10.10.98.157
Avaya Firewall
Emulated PSTN
WWW
Virsae Cloud Computing Service Azure
Avaya 1416 Digital Deskphone
Avaya Analog Deskphone
Desktop hosting Avaya Equinox for Windows and also used to launch Virsae Service Management web portal
LAN

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	7.1.2.0.712004
Avaya Aura® System Manager running on virtual server	7.1.2.0 (Feature Pack 2)
Avaya Aura® Media Server running on virtual server	7.8.0.333
Avaya Aura® Communication Manager running on virtual server	7.1.2.0.0-FP2
Avaya G450 Media Gateway	38.21.0/1
Avaya IP Deskphones - 9641GS (H.323) - 9611G (SIP)	 6.6506 7.1.1.0.9
Avaya Equinox for Windows	3.4.0.152.46-ACW-INTEGRATIONNEXUS1
Avaya 1416 Digital Deskphone	15
Avaya 500 Analog Deskphone	N/A
Virsae Service Management for Unified Communications running on Windows 2012 R2 SP1	R79

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 reporting.

5.1. Configure Login Group

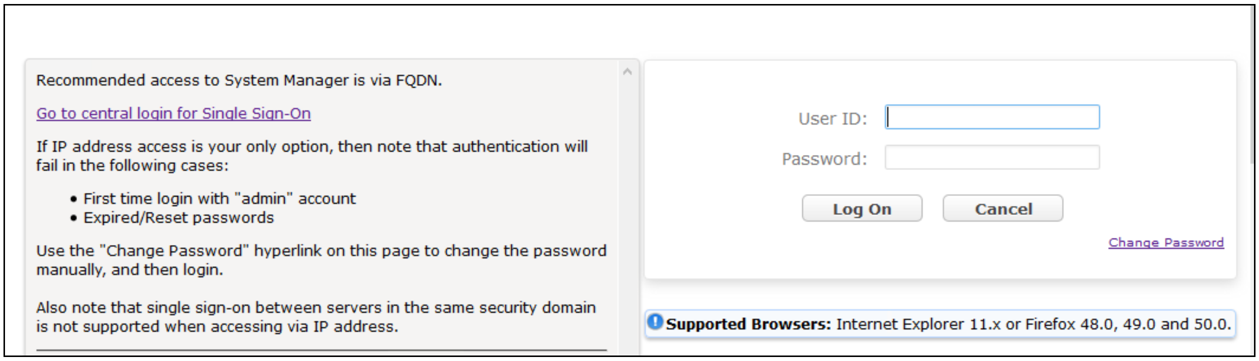
Create an Administrator account on Session Manager since the VSM Probe requires access to Session Manager with Administrative rights. Add an account that when used provides access to the Linux bash prompt.

During compliance testing the "**admin**" 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 sudoers 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.

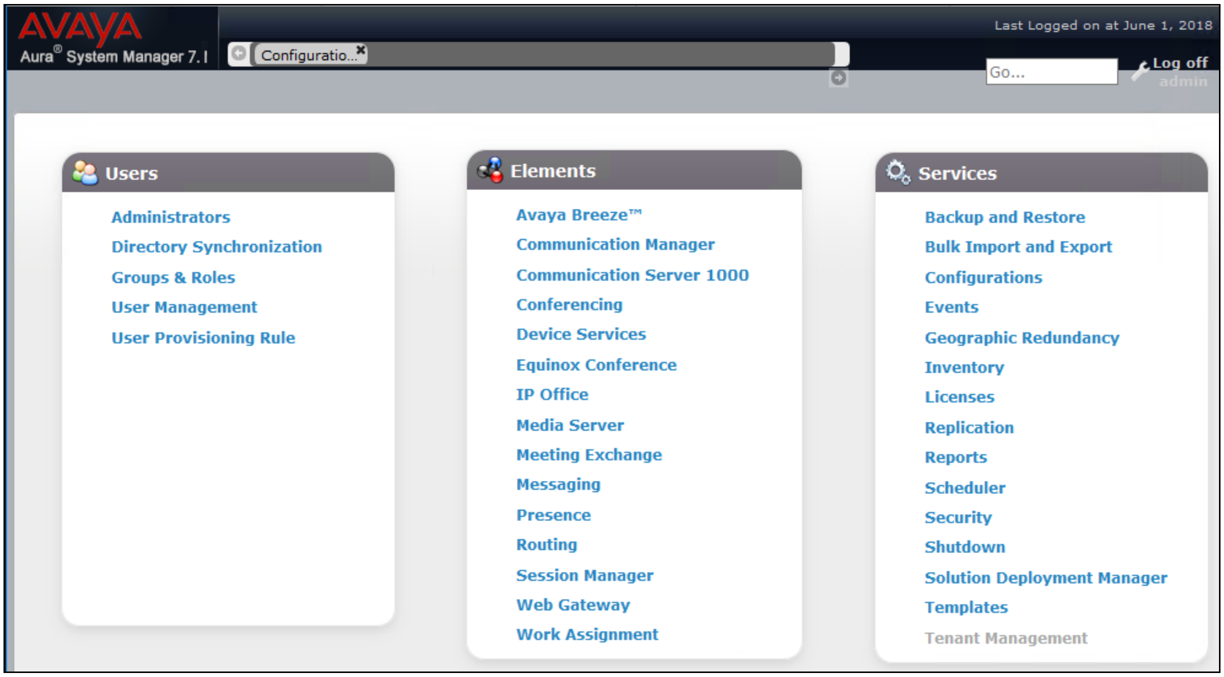
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

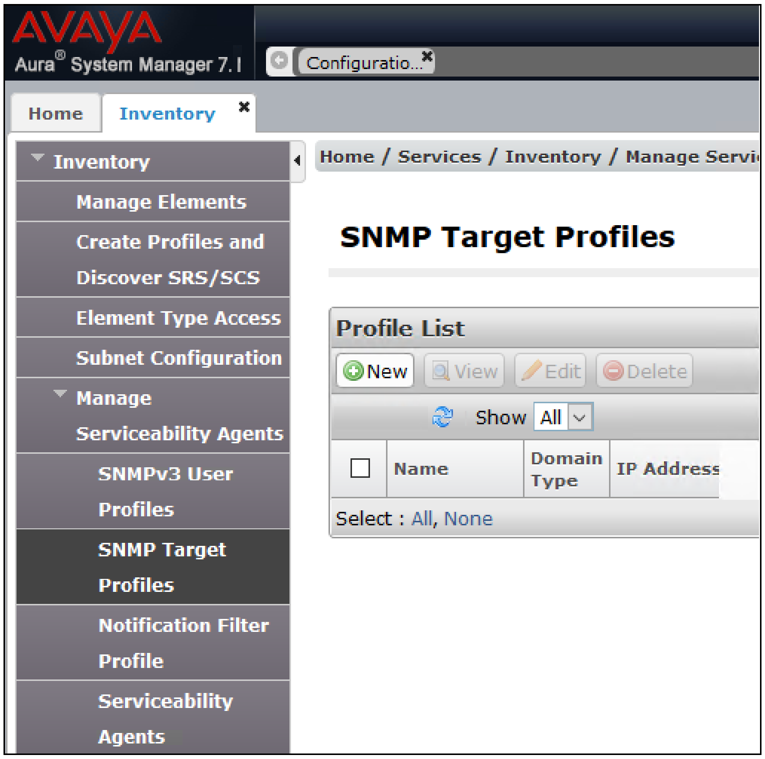
Password:

Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

The main System Manager dashboard page is shown below.



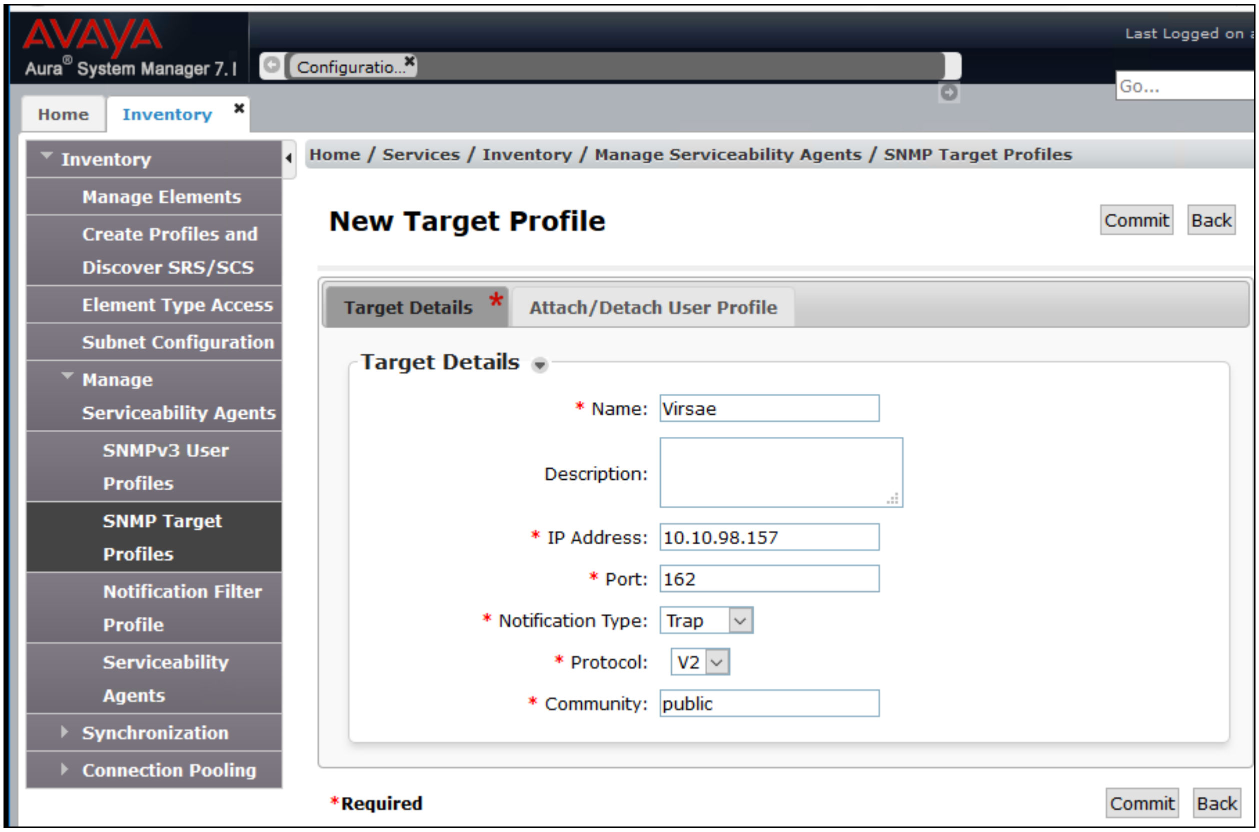
Navigate to **Services → Inventory** from the above shown dashboard. Then navigate to **Manage Servicability Agents → SNMP Target Profiles** as shown in the screen below. Click on **New**.



From the **New Target Profile** window, under the **Target Details** tab, configure the following.

- **Name:** A descriptive name
- **IP Address:** The VSM probe IP address
- **Protocol:** Select **V2** from the drop-down menu

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



Home / Services / Inventory / Manage Serviceability Agents / SNMP Target Profiles

New Target Profile

Target Details

* Name: Virsae

Description:

* IP Address: 10.10.98.157

* Port: 162

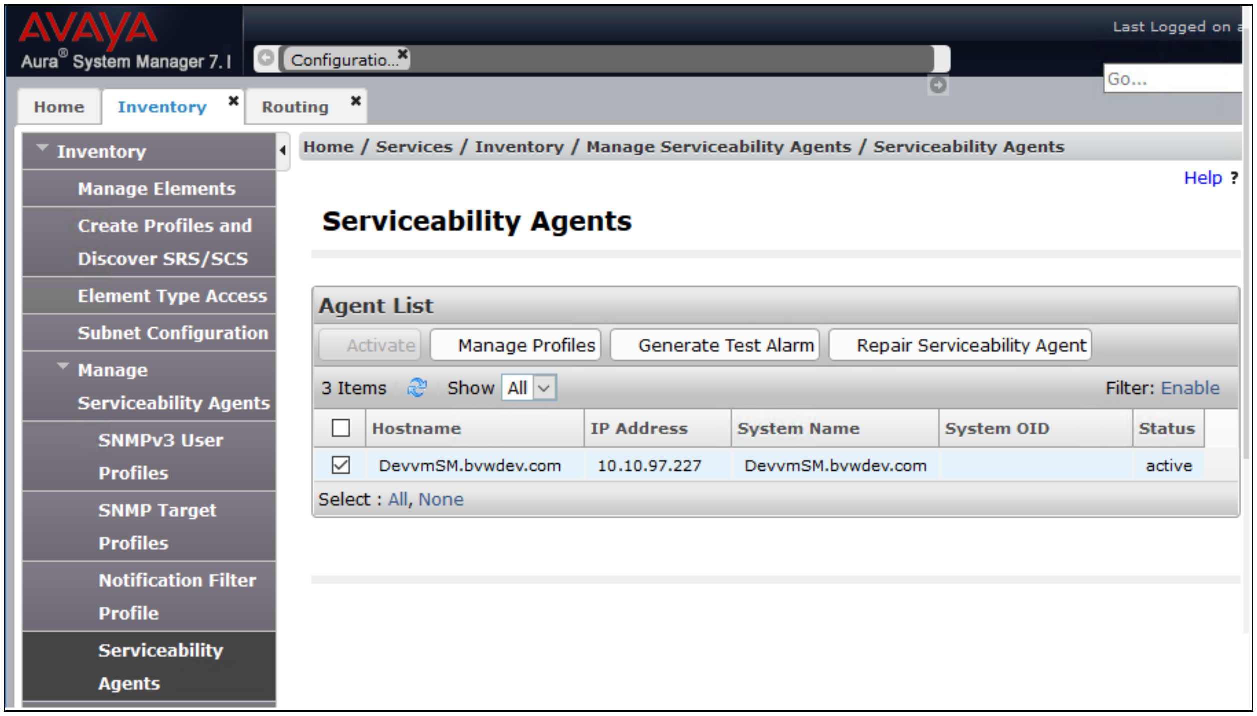
* Notification Type: Trap

* Protocol: V2

* Community: public

*Required

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



Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

Serviceability Agents

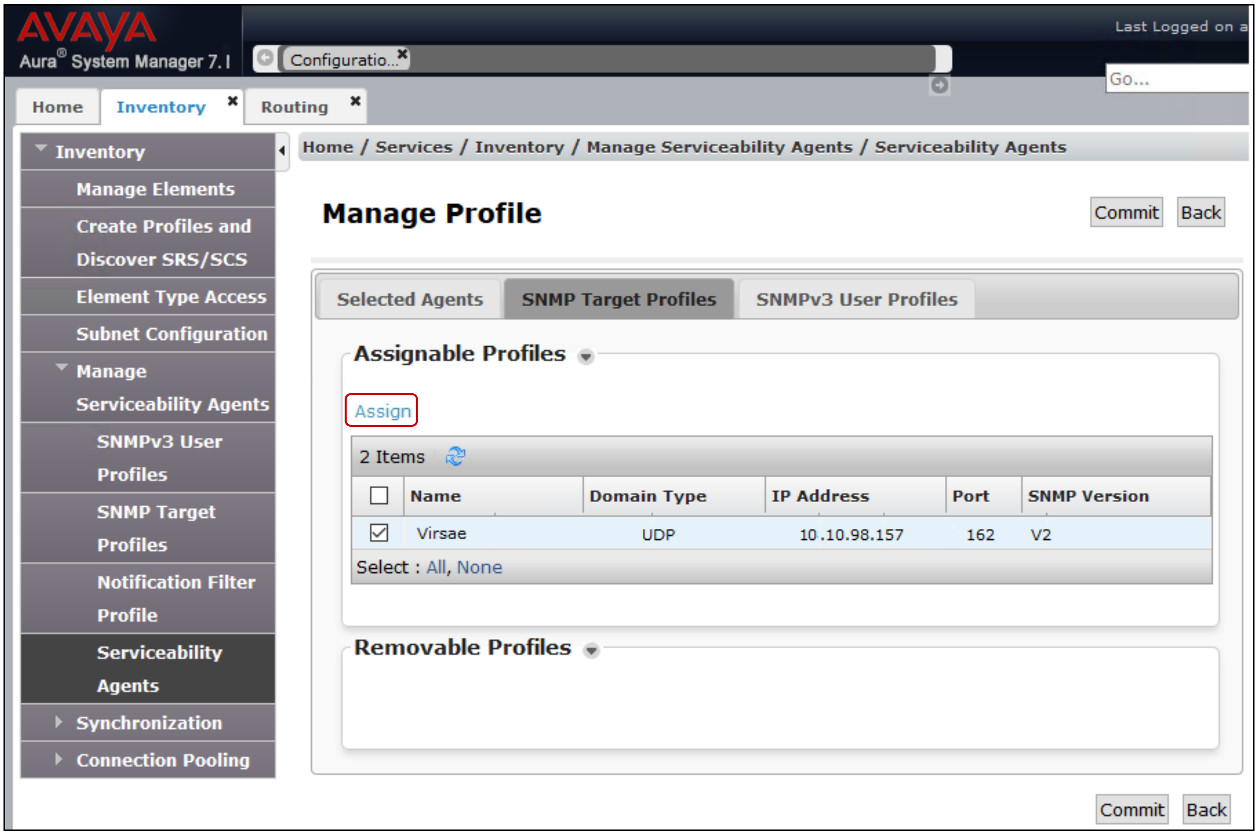
Agent List

3 Items Show All Filter: Enable

□	Hostname	IP Address	System Name	System OID	Status
☑	DevvmSM.bvwdev.com	10.10.97.227	DevvmSM.bvwdev.com		active

Select : All, None

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



Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

Manage Profile

Assignable Profiles

2 Items

□	Name	Domain Type	IP Address	Port	SNMP Version
☑	Virsae	UDP	10.10.98.157	162	V2

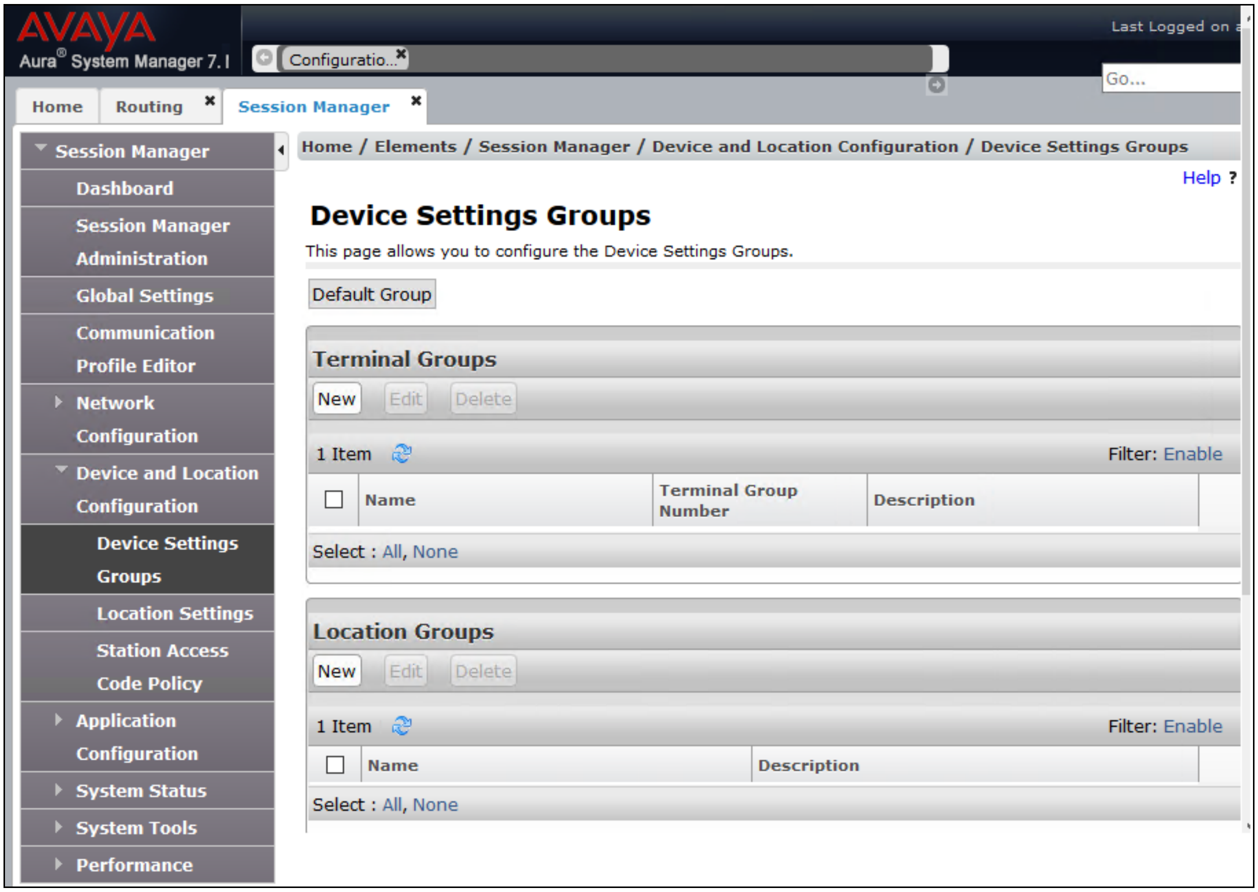
Select : All, None

Removable Profiles

5.3. Configure RTCP Monitoring

To allow VSM to monitor the voice quality of SIP endpoint calls, configure Session Manager to send RTCP reporting to the IP address of the VSM probe.

From the main System Manager dashboard seen in **Section 5.2**, 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.



Home / Elements / Session Manager / Device and Location Configuration / Device Settings Groups

Device Settings Groups

This page allows you to configure the Device Settings Groups.

Default Group

Terminal Groups

New Edit Delete

1 Item Filter: Enable

□	Name	Terminal Group Number	Description

Select : All, None

Location Groups

New Edit Delete

1 Item Filter: Enable

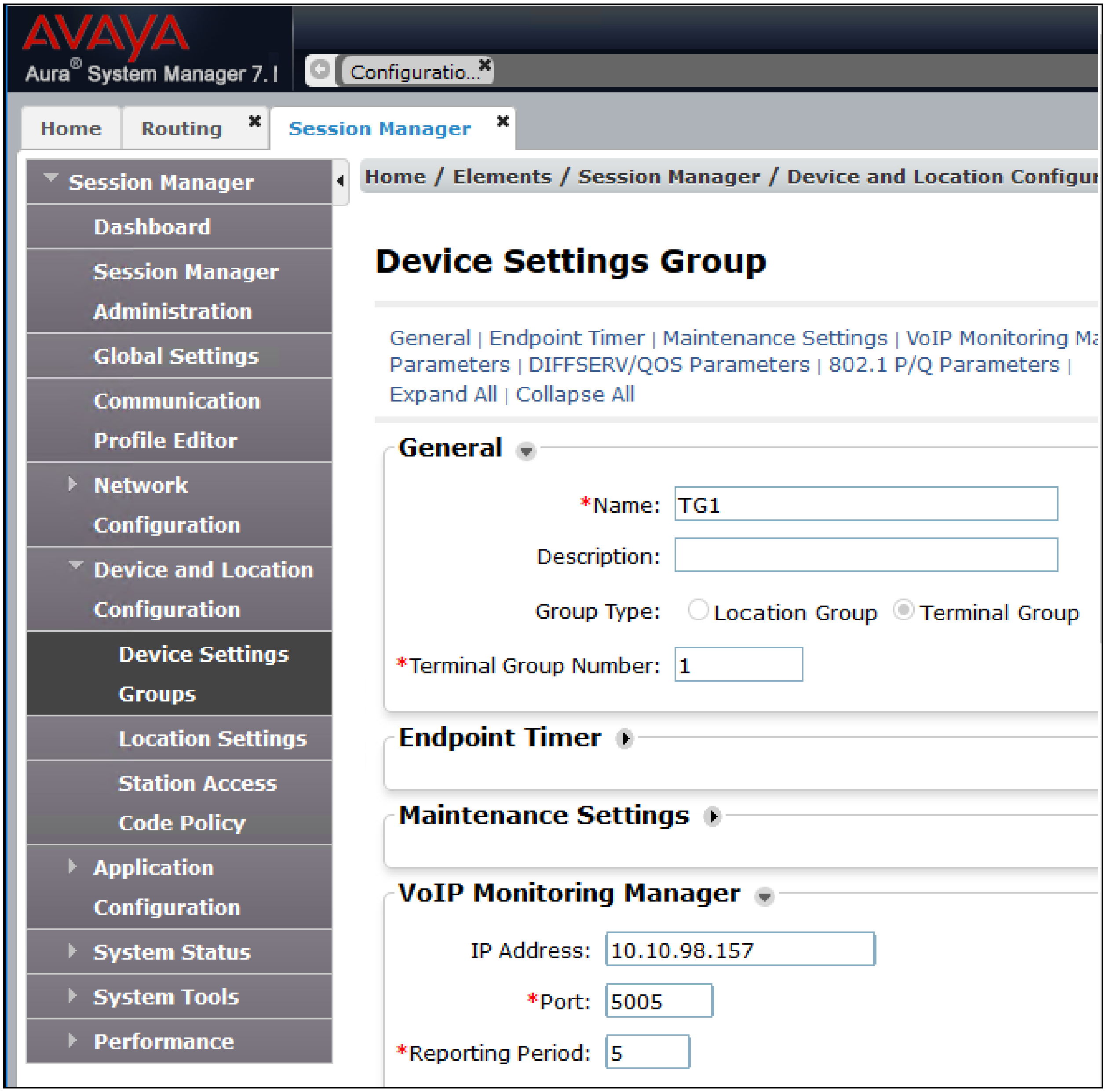
□	Name	Description

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 the VSM probe. Retain default values for all other fields and click on the **Save** (not shown) button.


AVAYA
Aura® System Manager 7.1
Configuratio...
Home
Routing
Session Manager
Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Device Settings Groups
Location Settings
Station Access Code Policy
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Device and Location Configur
General | Endpoint Timer | Maintenance Settings | VoIP Monitoring Ma
Parameters | DIFFSERV/QOS Parameters | 802.1 P/Q Parameters |
Expand All | Collapse All

Device Settings Group

General

*Name: TG1

Description:

Group Type: ○ Location Group ● Terminal Group

*Terminal Group Number: 1

Endpoint Timer

Maintenance Settings

VoIP Monitoring Manager

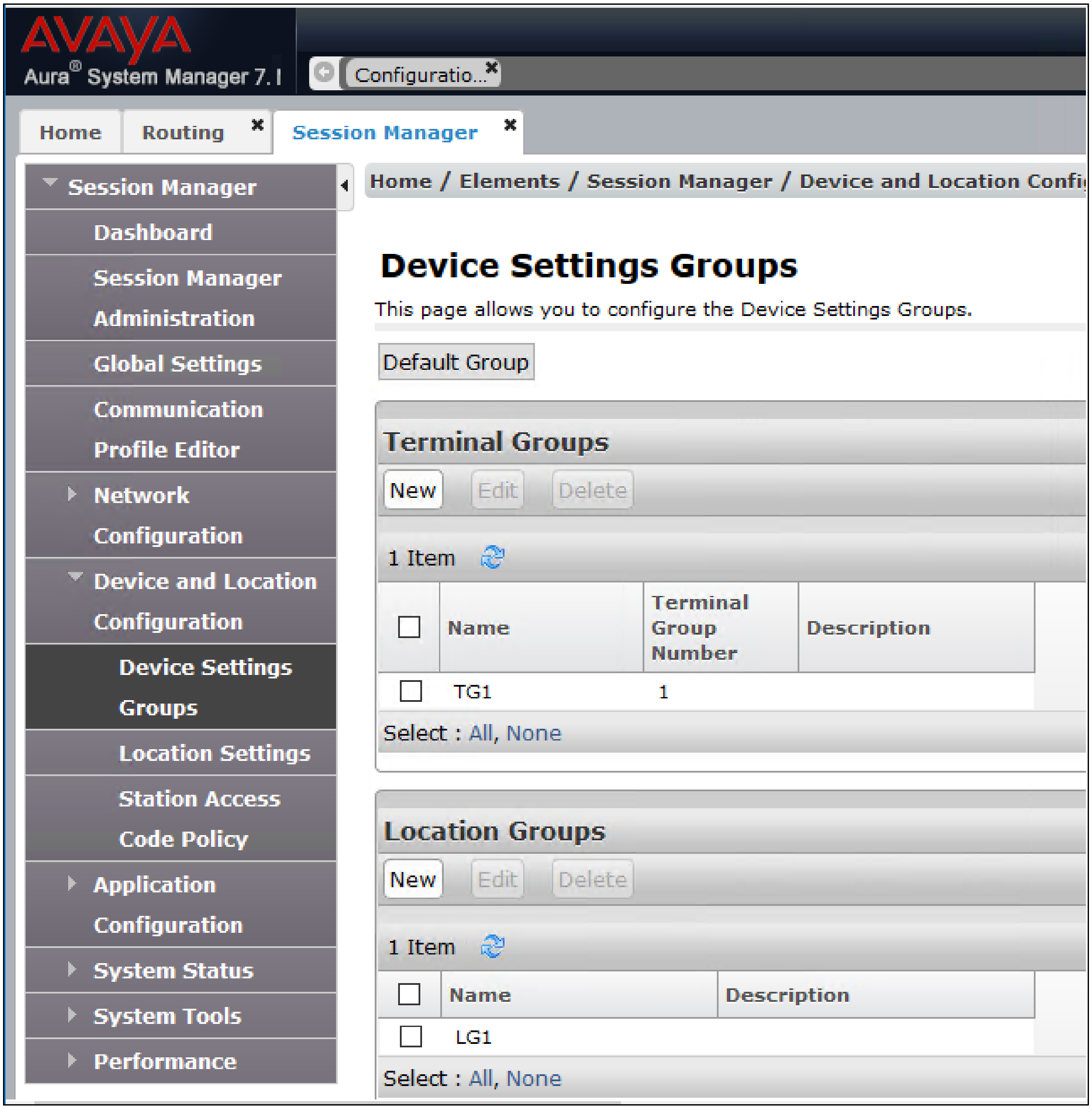
IP Address: 10.10.98.157

*Port: 5005

*Reporting Period: 5

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

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



Device Settings Groups

This page allows you to configure the Device Settings Groups.

Default Group

Terminal Groups

New Edit Delete

1 Item

□	Name	Terminal Group Number	Description
□	TG1	1	

Select : All, None

Location Groups

New Edit Delete

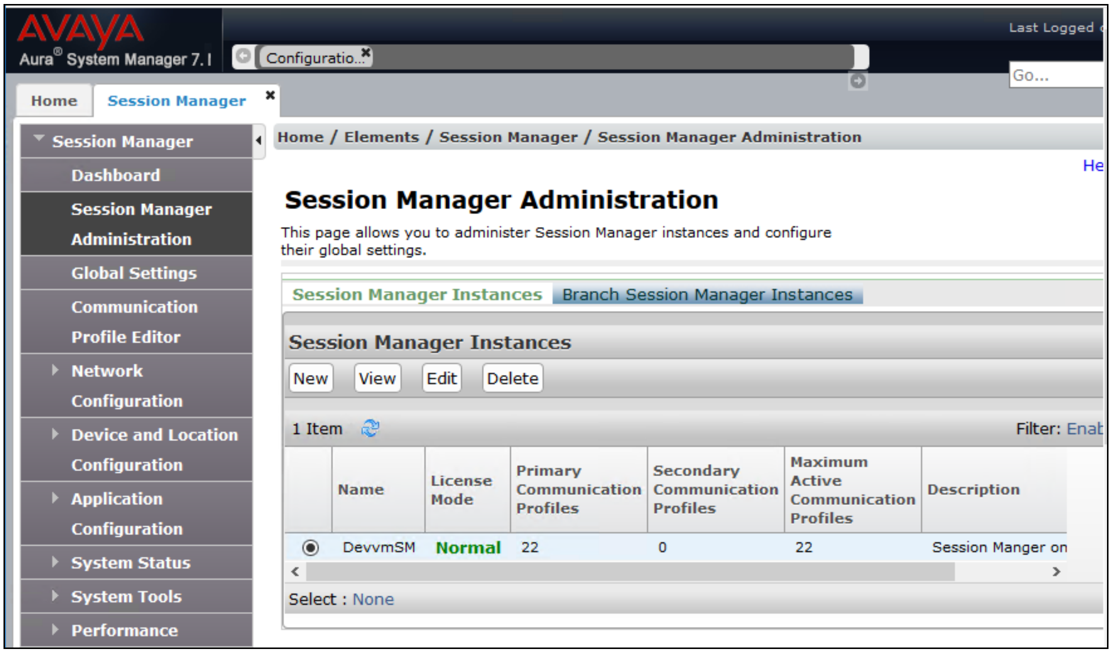
1 Item

□	Name	Description
□	LG1	

Select : All, None

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

From the main System Manager dashboard seen in **Section 5.2**, navigate to **Elements → Session Manager**. Select **Session Manager Administration**. From the **Session Manager Administration** window shown below, select the **Session Manager Instances** tab, select the Session Manager and click on **Edit**.



Home / Elements / Session Manager / Session Manager Administration

Session Manager Administration

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

Session Manager Instances | Branch Session Manager Instances

Session Manager Instances

1 Item

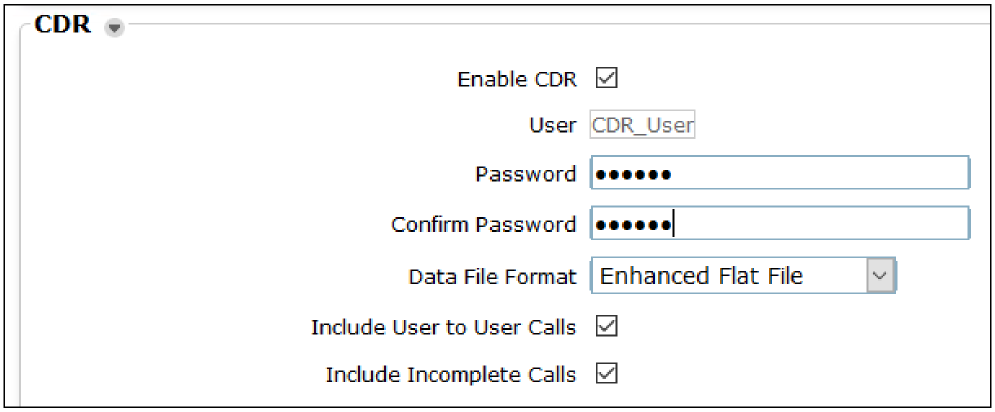
	Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
●	DevvmSM	Normal	22	0	22	Session Manger on

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 **Enhanced Flat File** was selected from the drop-down menu
- Check the boxes for both **Include User to User Calls** and **Include Incomplete Calls**

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



CDR

Enable CDR	☑
User	CDR_User
Password	••••••
Confirm Password	••••••
Data File Format	Enhanced Flat File
Include User to User Calls	☑
Include Incomplete Calls	☑

6. Configure Virsae Service Management

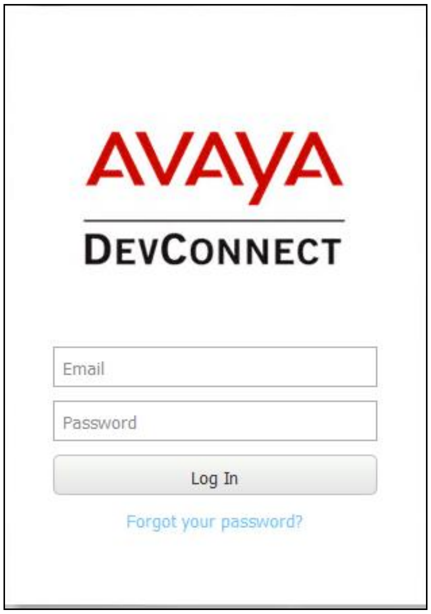
This section describes the configuration of VSM required to interoperate with AES.

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 this Application Notes. The screen shots and partial configuration shown below, supplied by Virsae, 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:

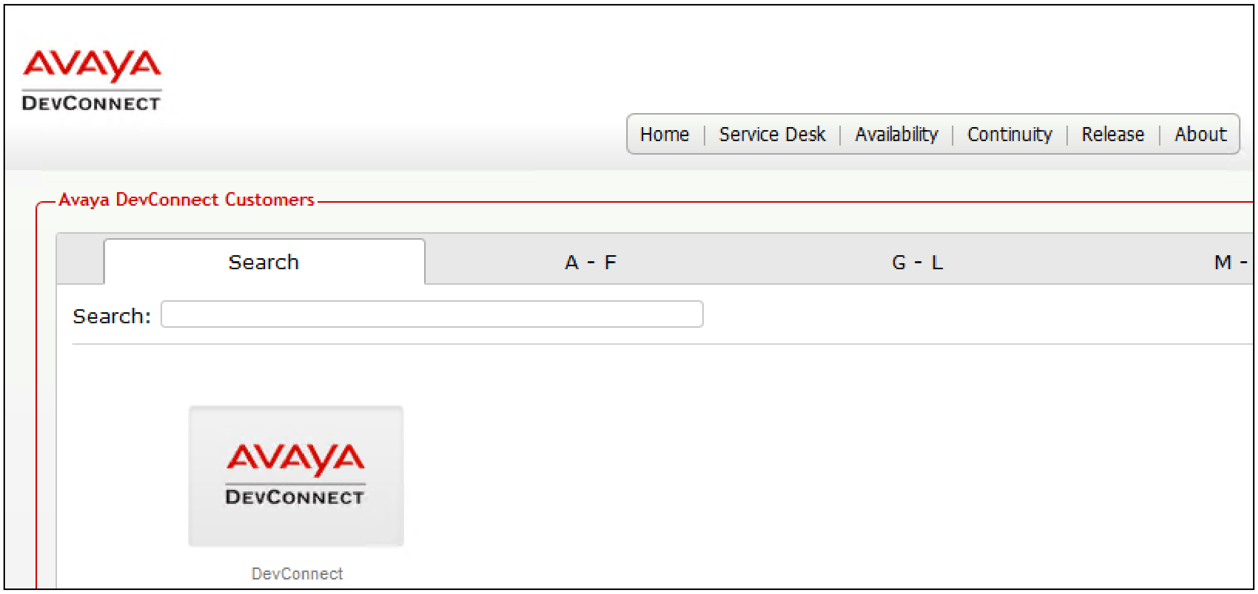
- Login to the Web Portal
- Configuring Avaya Aura® Application Enablement Services
- Configure Dashboard

6.1. Login to the Web Portal

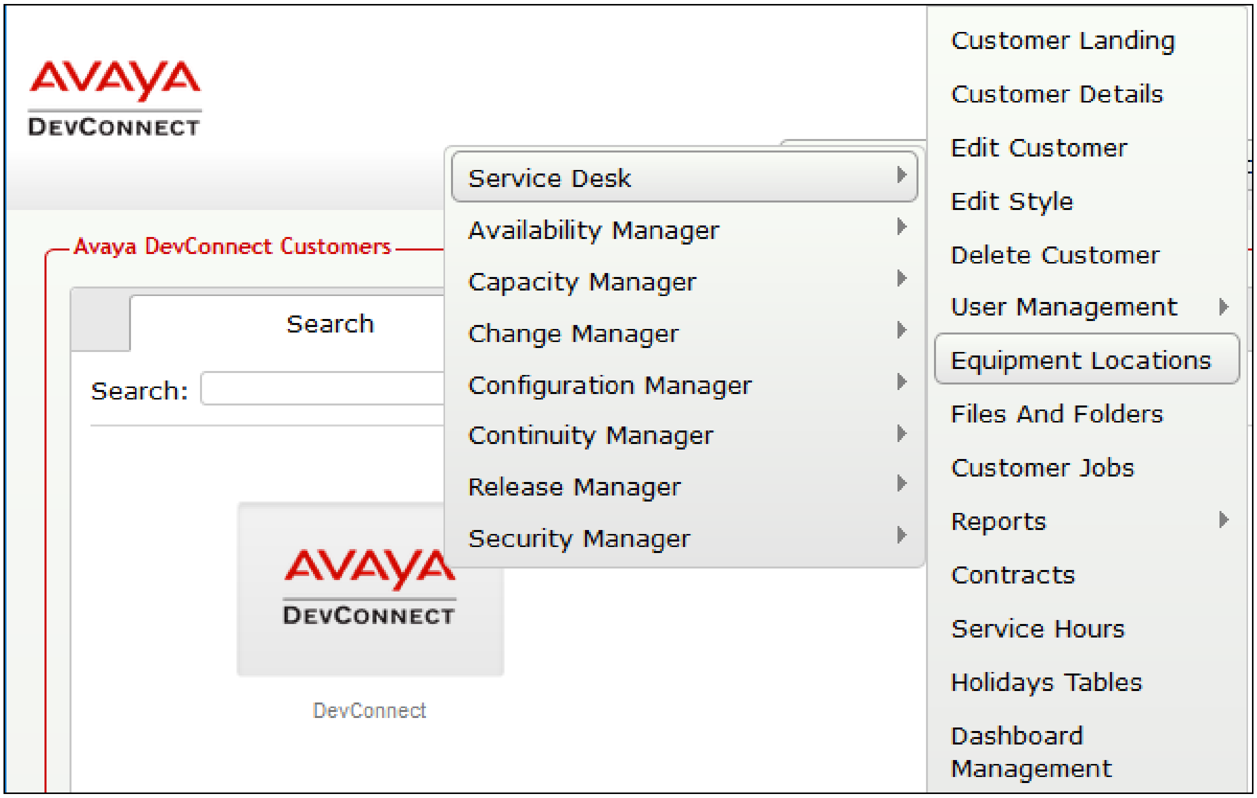
A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL *<business partner name>.virsae.com* in a web browser. During compliance testing the URL used was *devconnect.virsae.com*. The Login screen is shown as below. Enter the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



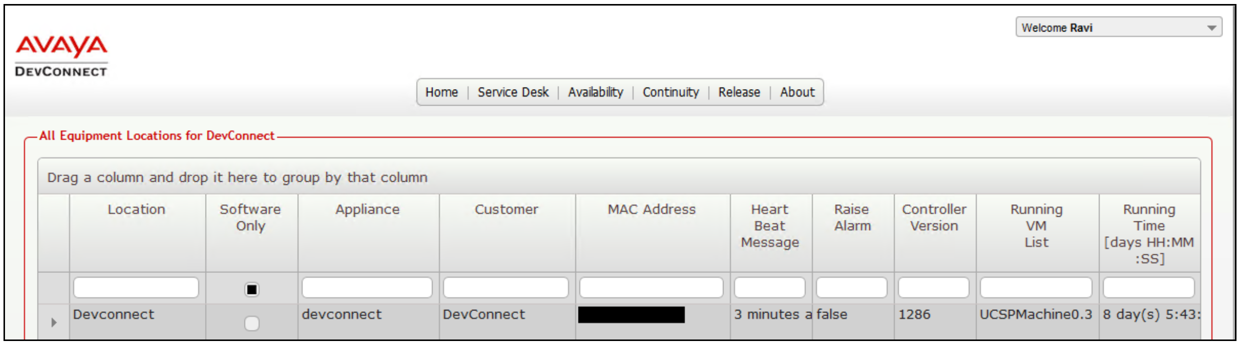
The customers belonging the business partner screen is shown. During compliance testing the customer created by Virsae is **Devconnect**.


AVAYA
DEVCONNECT
Home | Service Desk | Availability | Continuity | Release | About
Avaya DevConnect Customers
Search
A - F
G - L
M -
Search:
AVAYA DEVCONNECT
DevConnect

Click on the customer icon and navigate to **Service Desk → Equipment Locations** as shown below.



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


AVAYA
DEVCONNECT
Welcome Ravi
Home | Service Desk | Availability | Continuity | Release | About

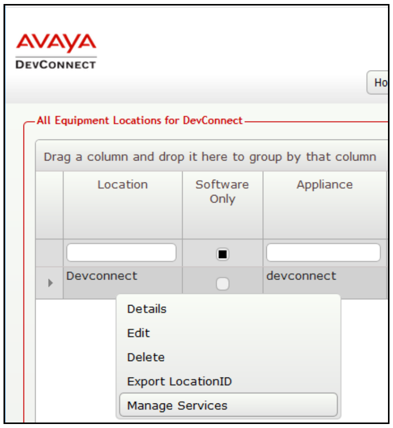
All Equipment Locations for DevConnect

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

Location	Software Only	Appliance	Customer	MAC Address	Heart Beat Message	Raise Alarm	Controller Version	Running VM List	Running Time [days HH:MM :SS]
Devconnect	○	devconnect	DevConnect	[redacted]	3 minutes a	false	1286	UCSPMachine0.3	8 day(s) 5:43:

6.2. Configuring Avaya Aura® Session Manager

To add a Session Manager to the Location created in **Section 6.1**, right click on the location **Devconnect** and select **Manage Services** as shown below.

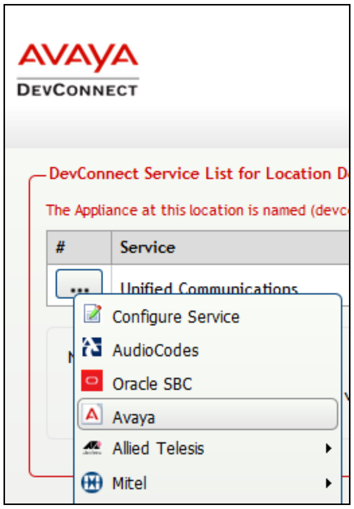


All Equipment Locations for DevConnect

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

Location	Software Only	Appliance
Devconnect	○	devconnect

From the **Unified Communications** Service, select **Avaya**.

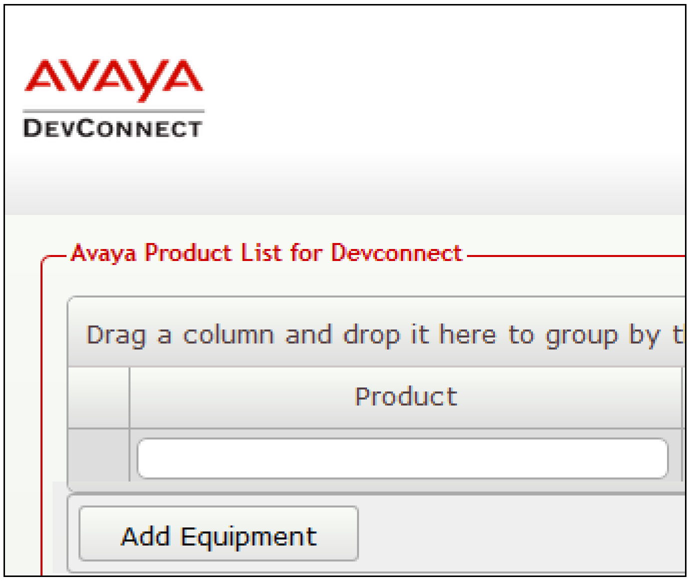


DevConnect Service List for Location D

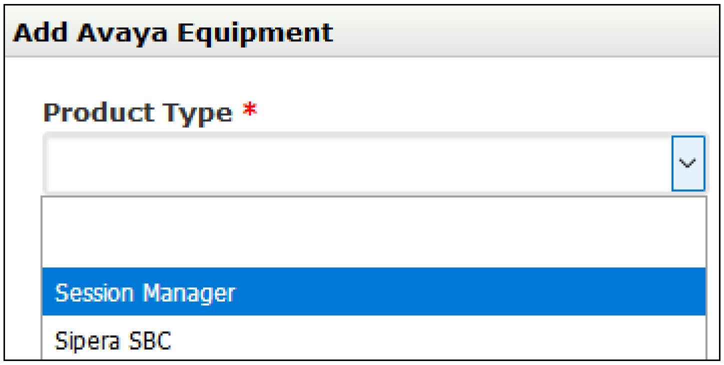
The Appliance at this location is named (devc

#	Service
...	Unified Communications

The product list for the configured location is shown as seen below. Click on the **Add Equipment** button.

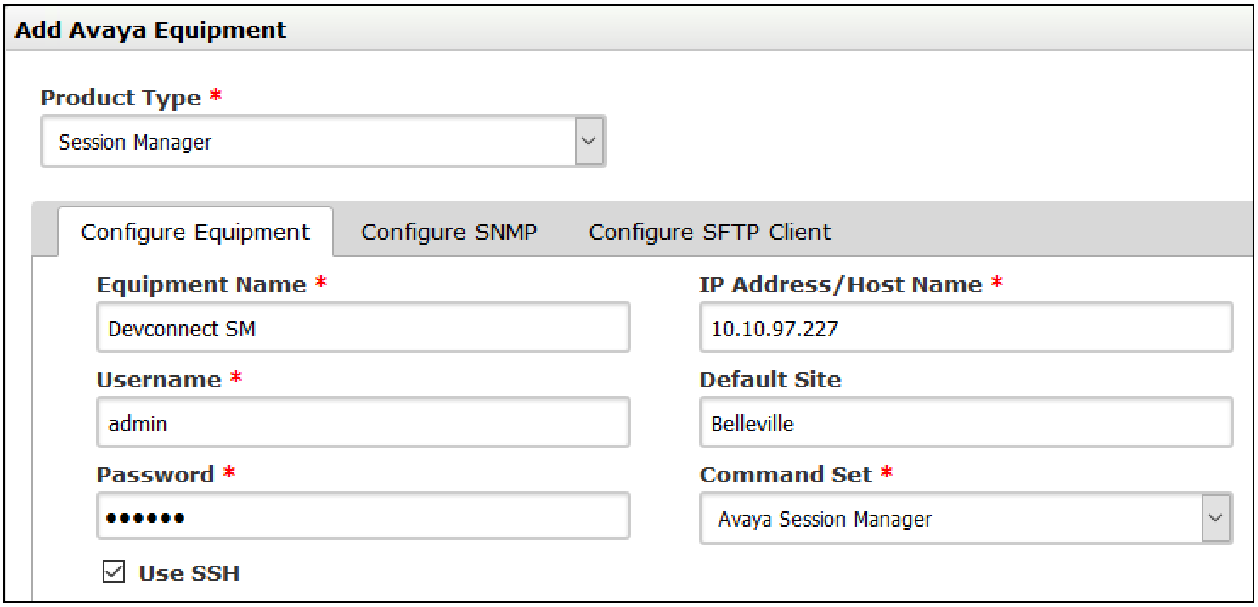

AVAYA
DEVCONNECT
Avaya Product List for Devconnect
Drag a column and drop it here to group by t
Product
Add Equipment

From the **Add Avaya Equipment** window, select **Session Manager** from the **Product Type** drop-down menu.



In the **Configure Equipment** tab, 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
- Check the **Use SSH** box
- **IP Address/Host Name:** Management IP address of Session Manager
- **Default Site:** A descriptive site name
- **Command Set:** Select **Avaya Session Manager** from the drop-down menu



Add Avaya Equipment

Product Type *: Session Manager

Equipment Name *: Devconnect SM

Username *: admin

Password *: ●●●●●●

☑ Use SSH

IP Address/Host Name *: 10.10.97.227

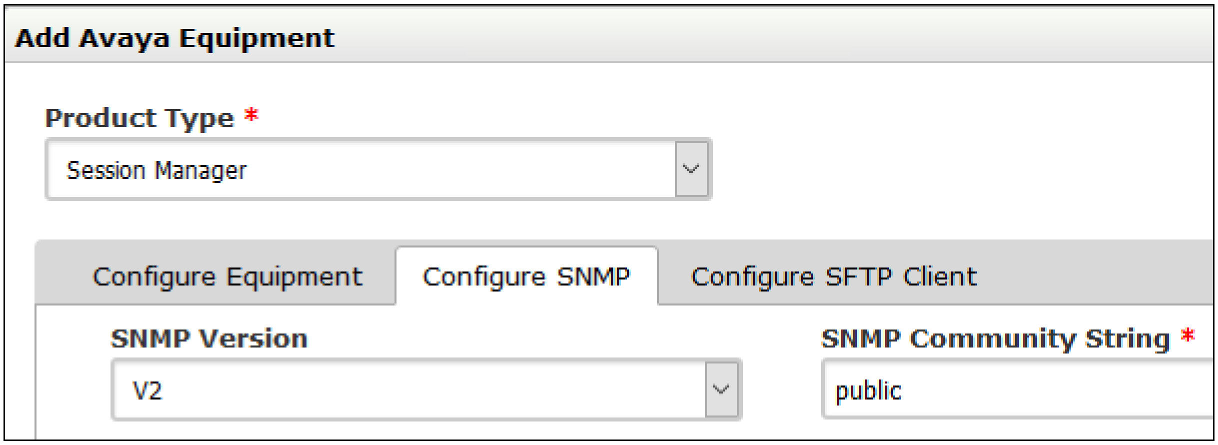
Default Site: Belleville

Command Set *: Avaya Session Manager

In the **Configure SNMP** 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**

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



Add Avaya Equipment

Product Type *
Session Manager

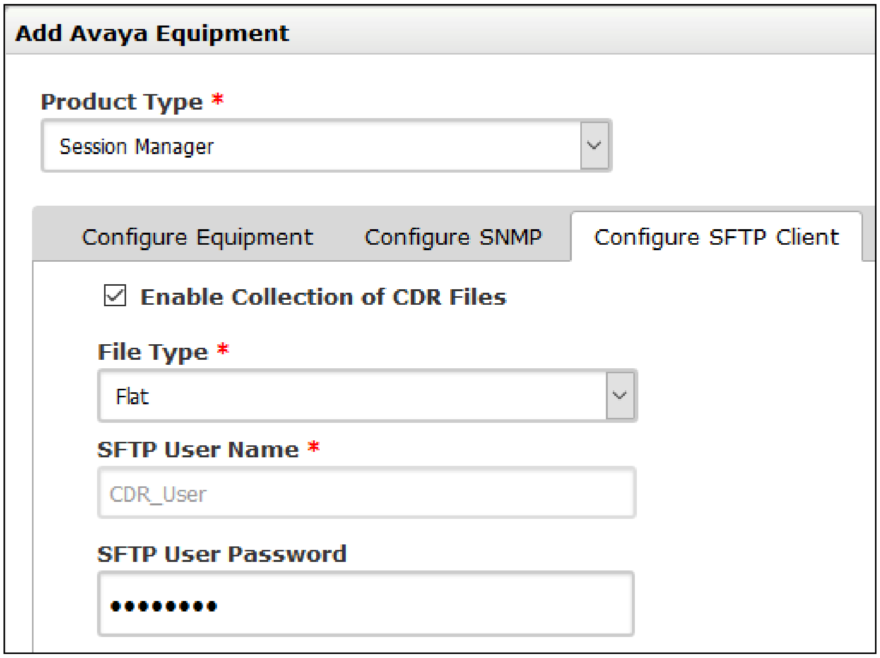
SNMP Version
V2

SNMP Community String *
public

In the **Configure SFTP Client** tab, configure the following values.

- Check the box for **Enable Collection of CDR Files**.
- **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 **Add** (not shown) button to complete the configuration.



Add Avaya Equipment

Product Type *
Session Manager

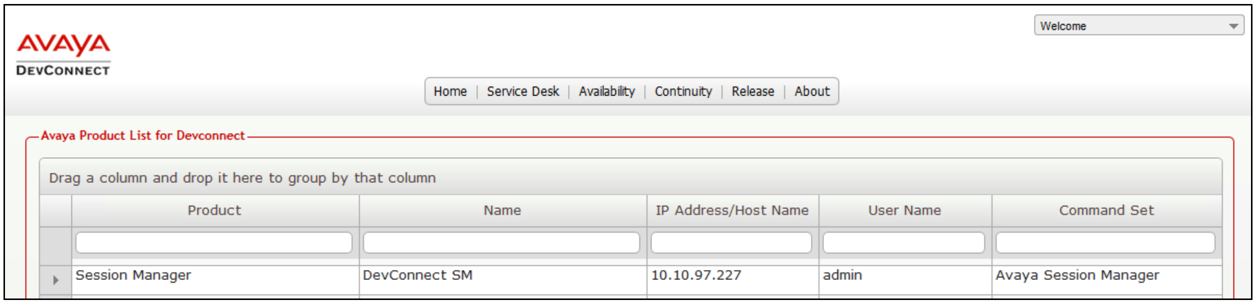
☑ Enable Collection of CDR Files

File Type *
Flat

SFTP User Name *
CDR_User

SFTP User Password
••••••••

The screen below shows the added Session Manager equipment.

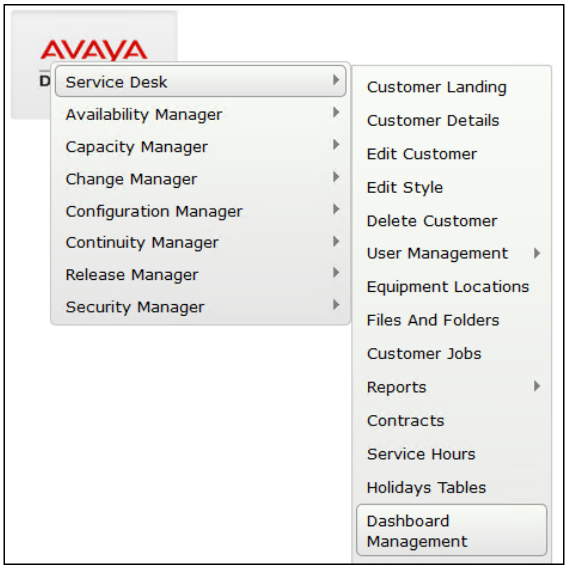

AVAYA
DEVCONNECT
Welcome
Home | Service Desk | Availability | Continuity | Release | About
Avaya Product List for Devconnect
Drag a column and drop it here to group by that column

Product	Name	IP Address/Host Name	User Name	Command Set
Session Manager	DevConnect SM	10.10.97.227	admin	Avaya Session Manager

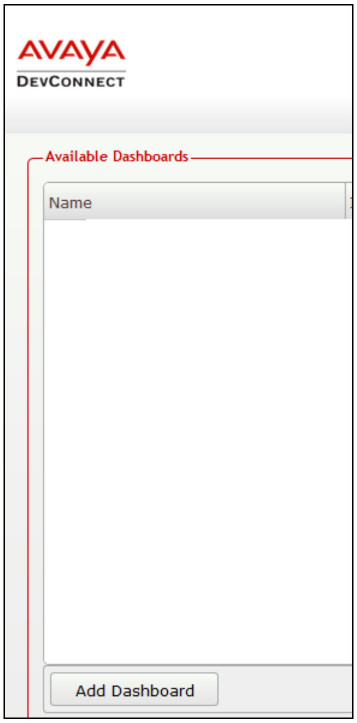
6.3. Configure Dashboard

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

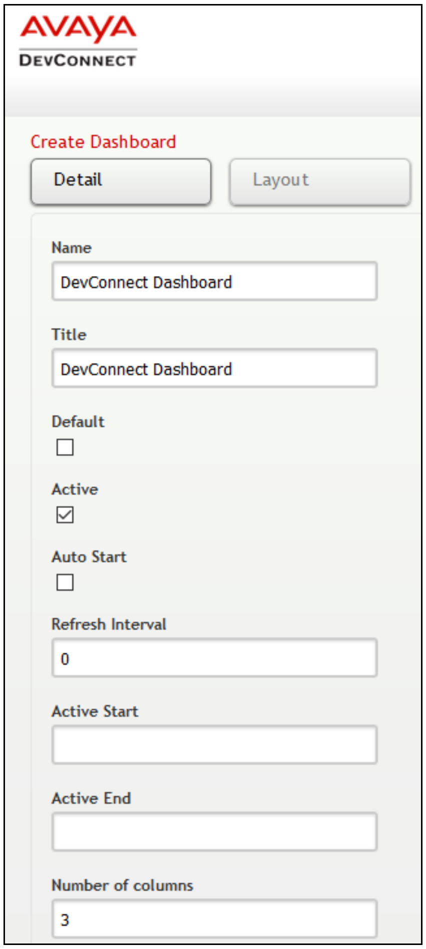
From the customer icon, navigate to **Service Desk → Dashboard Management** as shown below.



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



In the **Create Dashboard** window, type a descriptive name for **Name** and **Title** fields as shown below. Retain default values for all other fields. Click on **Layout** button and then click on **Submit** (not shown) button.



Create Dashboard

Name: DevConnect Dashboard

Title: DevConnect Dashboard

Default: □

Active: ☑

Auto Start: □

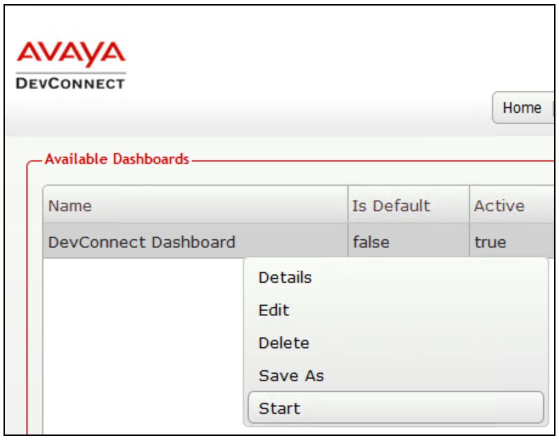
Refresh Interval: 0

Active Start:

Active End:

Number of columns: 3

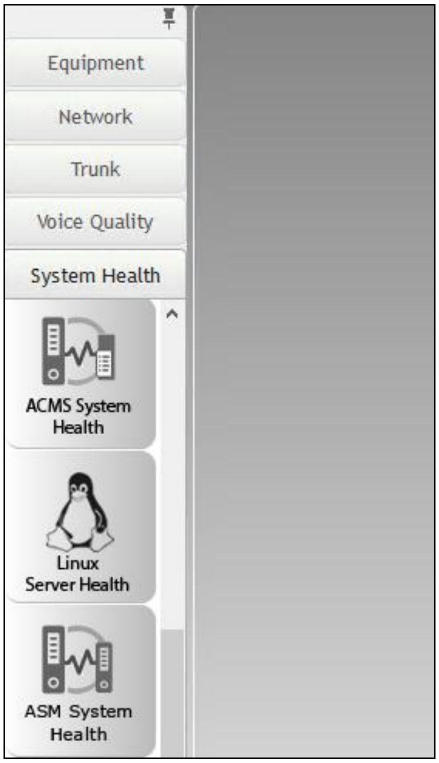
Screen below shows the above created Dashboard. Right click on it and select **Start**.



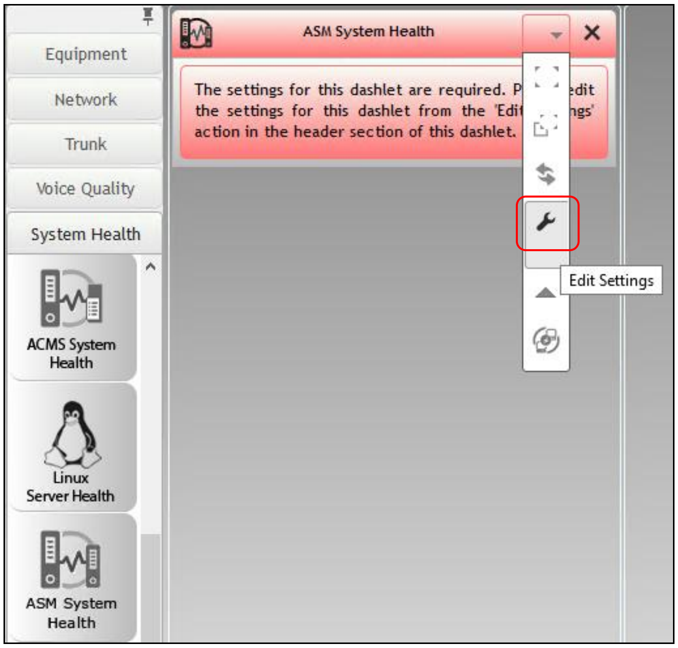
Available Dashboards

Name	Is Default	Active
DevConnect Dashboard	false	true

In the dashboard window shown below, click on **System Health** and drag the **ASM System Health** icon from the left to the right column.



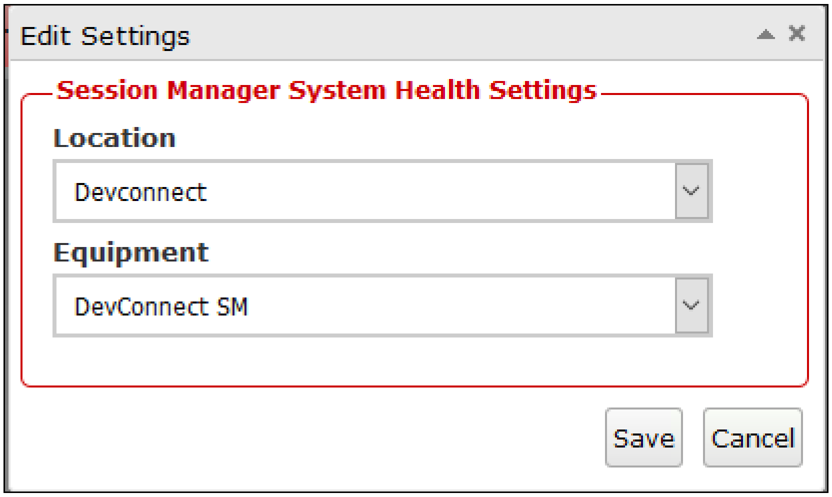
From the drop-down menu for **ASM System Health** window, select the **Edit Settings** button as shown below.



ASM System Health

The settings for this dashlet are required. P edit the settings for this dashlet from the 'Edit ngs' action in the header section of this dashlet.

In the **Edit Settings** window shown below, select the required **Location** and **Equipment** from the drop-down menu and click on the **Save** button.



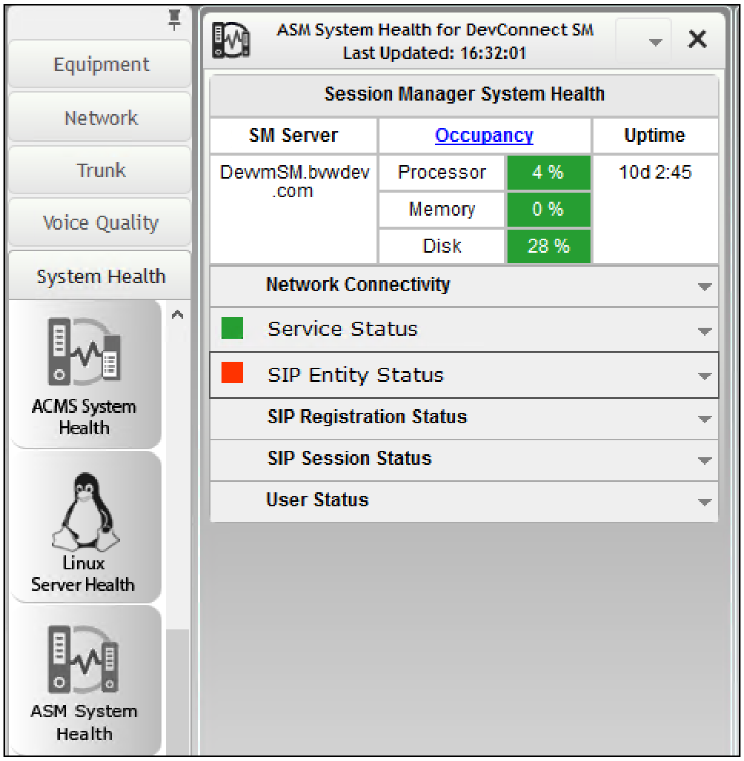
Edit Settings

Session Manager System Health Settings

Location: Devconnect

Equipment: DevConnect SM

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



ASM System Health for DevConnect SM
Last Updated: 16:32:01

Session Manager System Health

SM Server	Occupancy		Uptime
DewmSM.bvwdev .com	Processor	4 %	10d 2:45
	Memory	0 %	
	Disk	28 %	

Network Connectivity

🟩 Service Status

🟥 SIP Entity Status

SIP Registration Status

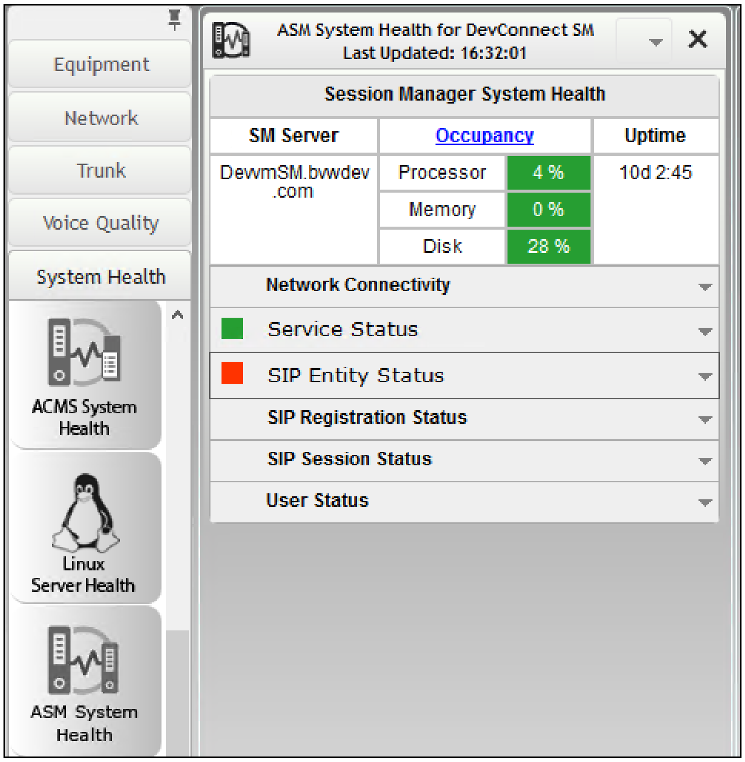
SIP Session Status

User Status

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Session Manager and VSM. The following steps are done by accessing the VSM web portal for the business partner.

After login to the web portal, navigate to **Service Desk → Dashboard Management** (not shown). Start the dashboard and the screens below shows the System Health of the already configured Session Manager for various parameters.



ASM System Health for DevConnect SM
Last Updated: 16:32:01

Session Manager System Health

SM Server	Occupancy		Uptime
DevwmSM.bvwdev.com	Processor	4 %	10d 2:45
	Memory	0 %	
	Disk	28 %	

Network Connectivity

🟩 Service Status

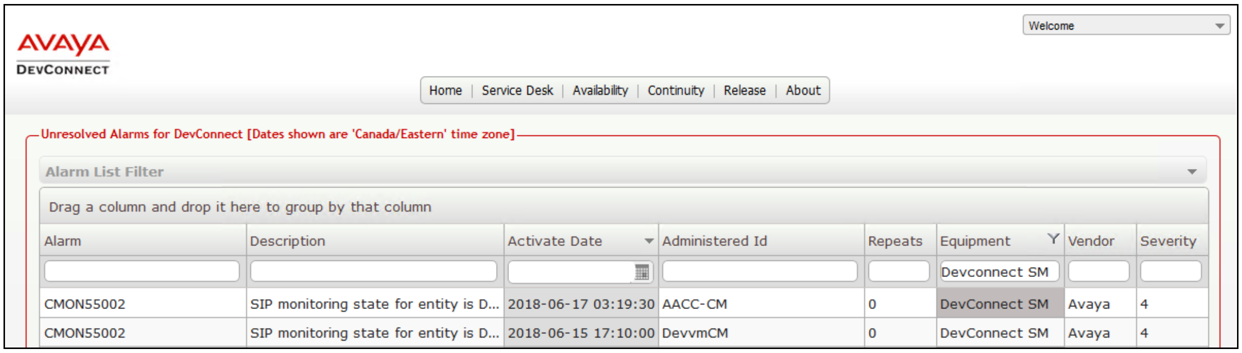
🟥 SIP Entity Status

SIP Registration Status

SIP Session Status

User Status

To view alarms using historical reporting, navigate to **Availability Manager → 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.


AVAYA
DEVCONNECT
Welcome
Home | Service Desk | Availability | Continuity | Release | About

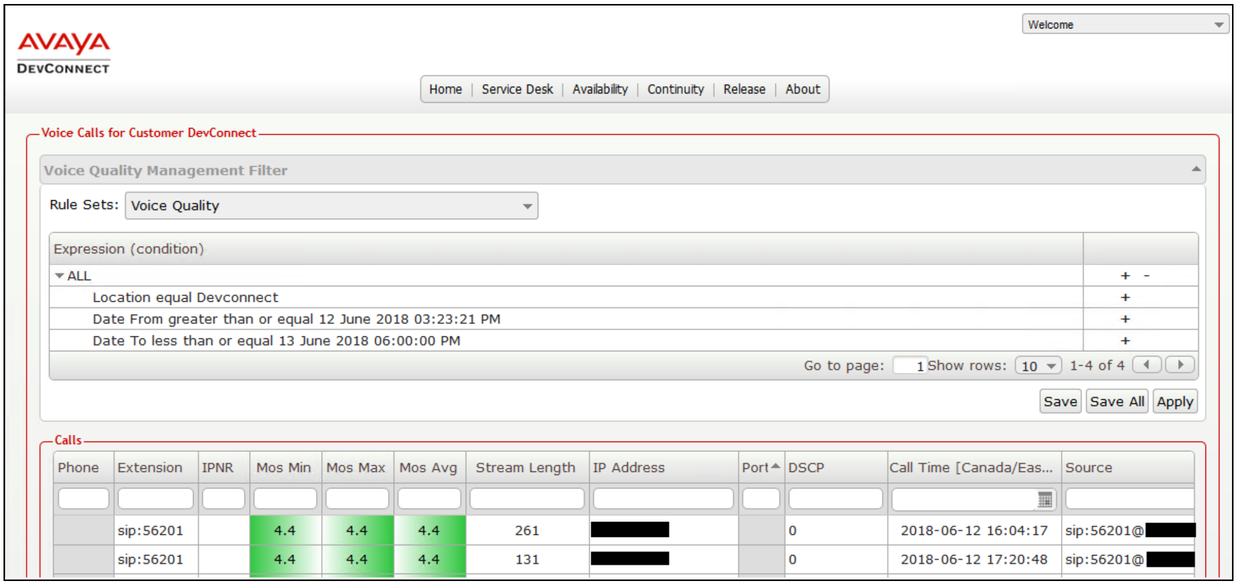
Unresolved Alarms for DevConnect [Dates shown are 'Canada/Eastern' time zone]

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
					Devconnect SM		
CMON55002	SIP monitoring state for entity is D...	2018-06-17 03:19:30	AACC-CM	0	DevConnect SM	Avaya	4
CMON55002	SIP monitoring state for entity is D...	2018-06-15 17:10:00	DevvmCM	0	DevConnect SM	Avaya	4

To view voice quality using historical reporting, navigate to **Availability Manager → 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.


AVAYA
DEVCONNECT
Welcome
Home | Service Desk | Availability | Continuity | Release | About
Save
Save All
Apply

Voice Calls for Customer DevConnect

Voice Quality Management Filter

Rule Sets: Voice Quality

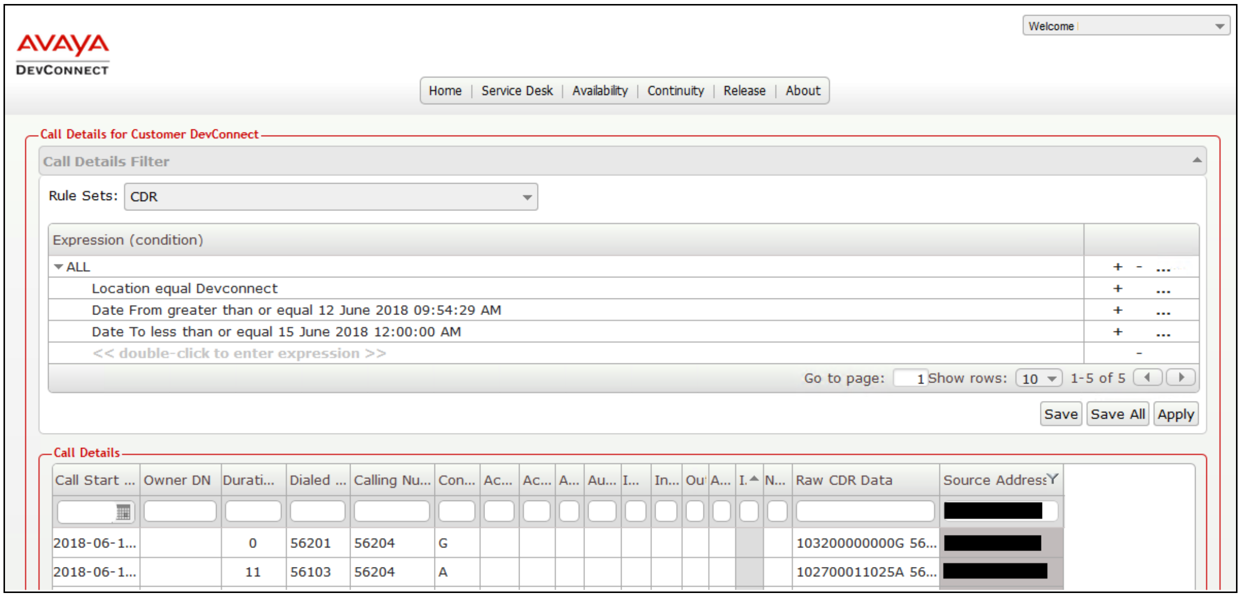
Expression (condition)	
ALL	+ -
Location equal Devconnect	+
Date From greater than or equal 12 June 2018 03:23:21 PM	+
Date To less than or equal 13 June 2018 06:00:00 PM	+

Go to page: 1 Show rows: 10 1-4 of 4

Calls

Phone	Extension	IPNR	Mos Min	Mos Max	Mos Avg	Stream Length	IP Address	Port	DSCP	Call Time [Canada/Eas...	Source
	sip:56201		4.4	4.4	4.4	261	[redacted]		0	2018-06-12 16:04:17	sip:56201@[redacted]
	sip:56201		4.4	4.4	4.4	131	[redacted]		0	2018-06-12 17:20:48	sip:56201@[redacted]

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 Manager by using filters at Source Address.


AVAYA
DEVCONNECT
Welcome
Home | Service Desk | Availability | Continuity | Release | About

Call Details for Customer DevConnect

Call Details Filter

Rule Sets: CDR

Expression (condition)	
ALL	+ - ...
Location equal Devconnect	+ ...
Date From greater than or equal 12 June 2018 09:54:29 AM	+ ...
Date To less than or equal 15 June 2018 12:00:00 AM	+ ...
<< double-click to enter expression >>	-

Go to page: 1 Show rows: 10 1-5 of 5

Call Details

Call Start ...	Owner DN	Durati...	Dialed ...	Calling Nu...	Con...	Ac...	Ac...	A...	Au...	I...	In...	Ou	A...	I.	N...	Raw CDR Data	Source Address
																	[redacted]
2018-06-1...		0	56201	56204	G											103200000000G 56...	[redacted]
2018-06-1...		11	56103	56204	A											102700011025A 56...	[redacted]

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management to interoperate with Avaya Aura® Session Manager. 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*, Release 7.1.2, Issue 4 December 2017
2. *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 March 2018
3. *Deploying Avaya Aura® System Manager*, Release 7.1.2, Issue 6 March 2018
4. *Administering Avaya Aura® System Manager for Release 7.1.2,* Release 7.1.2, Issue 11 March 2018

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

1. *Virsae Service Management - Implementation Guide*
2. *Virsae Service Management – Technical Requirements*

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.