



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R174 to interoperate with Avaya Aura® Communication 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 integrates directly to Communication Manager using Secure Shell (SSH) and uses Simple Network Management Protocol (SNMP) to query Communication Manager. At the same time, Virsae Service Management processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Communication Manager. Virsae also provides translations backup via SFTP and collects Syslog information for changes in Communication Manager commands and Media Server events.

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® Communication Manager (herein after referred to as Communication 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 VSM product uses the following integration methods to monitor a Communication Manager system.

- System Access Terminal (SAT) - The VSM uses a pool of SSH connections to the SAT using the IP address of Communication Manager. By default, the solution establishes one Linux Shell connection and four concurrent SAT connections to Communication Manager system and uses the connections to execute SAT commands. Communication Manager name and IP address were collected using the Linux shell command.
- Real Time Transport Control Protocol (RTCP) collection - VSM collects RTCP information sent by Avaya resources including IP Media Processor (MEDPRO) boards, Media Gateways, Media Servers and IP Deskphones.
- Call Detail Recording (CDR) collection - VSM collects CDR information sent by Communication Manager.
- Simple Network Management Protocol (SNMP) –VSM uses SNMP to capture the alarms for both Communication Manager and Media Server. SNMP query is used also as part of VSM active monitoring tools for information on the alarms.
- SFTP – VSM uses SFTP to collect the backup files from Communication Manager.
- Syslog collection – VSM collects Syslog information to parse for change commands in Communication Manager and events from Media Server.

The VSM web user interface (dashboard) displays the configurations of Communication Manager and Media Server such as memory and CPU utilizations, disk usage and status from data collected via SSH. For the collection of RTCP, CDR, change command logs and backup files information, historical reporting is used. SNMP is used to receive information of alarms and query of alarm information.

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 of Communication Manager and verify against what is displayed on the SAT interface. The SAT interface is accessed by using Secure Shell (SSH) to Communication Manager. Calls were placed between various Avaya endpoints and VSM

dashboard and historical reporting was used to display the RTCP and CDR information collected. SNMP collection of alarms were also verified. VSM also collects the Syslog and backup files from Communication Manager and uses the Syslog file to parse the change logs.

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 encrypted capabilities of SSH, SFTP and non-encrypted SNMP, RTCP, CDR and Syslog 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 this Application Note, Avaya does not generally recommend use the SAT interface as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the SAT interface in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using this SAT interface. Using the SAT interface 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 this Application Note 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 Communication Manager 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 Communication Manager via collected SAT data such as port networks, cabinets, media gateways, media servers, trunk groups, route patterns, DS1 boards, IP network regions, stations, processor occupancy, alarm and error information. VSM dashboard was also used to view the Communication Manager name and IP address, and configurations of Media Server such as the memory and CPU utilizations, disk usage and status from data collected via SSH.

For the collection of RTCP and CDR information, the endpoints included Avaya H323, SIP, and softphones like Workplace Client for Windows and Avaya Agent for Desktop. The types of calls made included intra-switch calls, inbound/outbound trunk calls using SIP trunks, transfer, and conference calls. A backup schedule was configured for collecting Communication Manager backups and different logging levels were setup to collect Syslog. The change logs were collected by parsing the syslog's collected by VSM.

For serviceability testing, reboots were applied to VSM and removal of ethernet connection to VSM was also implemented.

2.2. Test Results

All test cases passed successfully with the following observations.

- “No processor data received” shown on dashboard beside the name of Media Server. The “sar” command cannot be executed in the Media Server used during this compliance testing since the “Sysstat” directory is not used in this version of Linux platform. By not being able to execute this command, only the CPU occupancy information could not be obtained.

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.

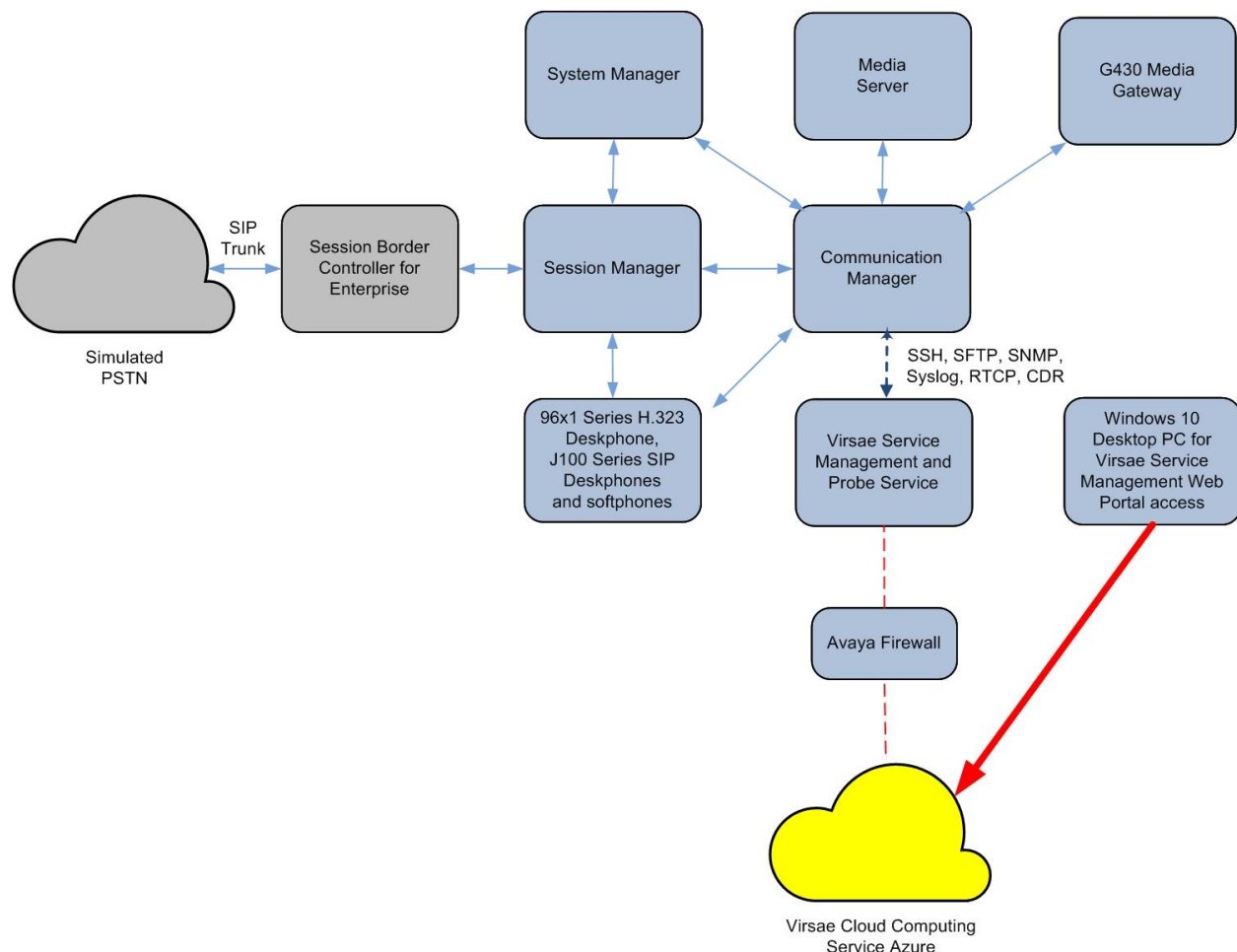


Figure 1: Test Configuration

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 J100 Series (SIP)	4.0.11.0
Avaya 96x1 Series (H.323)	6.8523
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® Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with VSM. This includes creating a login account and a SAT User Profile for VSM to access Communication Manager and enabling SNMP, Syslog, RTCP, SFTP Backup and CDR. In addition, configuration of Media Gateway login and Media Server's login, SNMP, Syslog and RTCP are described.

5.1. Configure Login Group

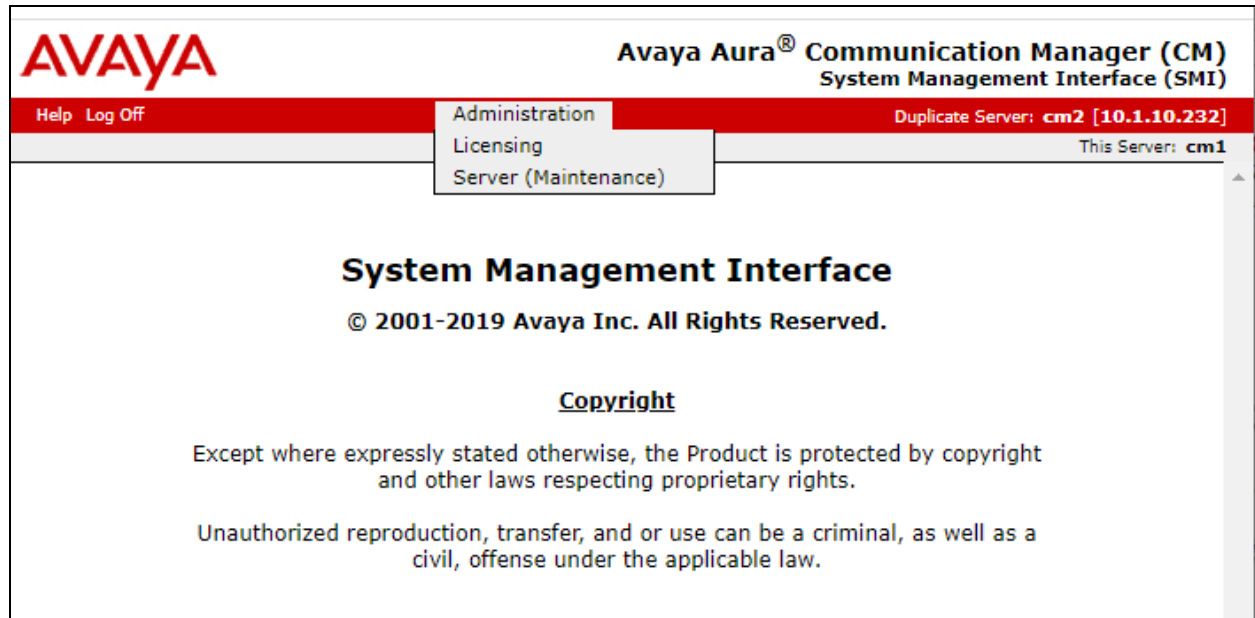
Create a Privileged Administrator account on Communication Manager System Management Interface (SMI) so that VSM can access Communication Manager with Super User rights. This can be achieved by creating a new user within Communication Manager with user profile 18.

Using a web browser, enter ***https://<IP address of Communication Manager>*** to connect to the Communication Manager server being configured and log in using appropriate credentials.



The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) login page. The page has a red header bar with the Avaya logo on the left and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header, there is a red bar with "Help" and "Log Off" links. The main content area is white and contains a login form titled "Logon". The form has a label "Logon ID:" followed by a text input field. Below the input field is a "Logon" button. In the top right corner of the main content area, it says "This Server: cm1".

Click **Administration** → **Server (Maintenance)**. This will open the **Server Administration** (not shown) that will allow the user to complete the configuration process.



Create a login account for VSM to access the Communication Manager SAT. From the navigation panel on the left side, navigate to **Security → Administrator Accounts** (not shown). Select **Add Login** and **Privileged Administrator** to create a new login account with privileged rights. Click **Submit**.

The screenshot displays the Avaya Administration web interface. The top navigation bar includes 'Help' and 'Log Off' on the left, and 'Administration' on the right. Below this, a breadcrumb trail reads 'Administration / Server (Maintenance)'. The left-hand navigation menu is expanded to show the 'Administrator Accounts' page. The main content area is titled 'Administrator Accounts' and contains the text: 'The Administrator Accounts SMI pages allow you to add, delete, or change administrator accounts.' Below this text is a section titled 'Select Action:' with several radio button options: 'Add Login' (selected), 'Privileged Administrator' (selected), 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. There are also three rows of 'Change Login', 'Remove Login', and 'Lock/Unlock Login' options, each with a 'Select Login' dropdown menu. At the bottom of the form are 'Add Group' and 'Remove Group' options, with a 'Select Group' dropdown menu. The 'Submit' and 'Help' buttons are located at the bottom of the page.

For the field **Login name**, enter the login. In this configuration, the login **Virsa** is created along with the password for this user. Retain default values for all other fields. Click **Submit** to continue.

Administration

Administrator Accounts -- Add Login: Privileged Administra

This page allows you to add a login that is a member of the **SUSERS** group. This l
system next to root.

Login name	<input type="text" value="Virsa"/>
Primary group	<input type="text" value="susers"/>
Additional groups (profile)	<input type="text" value="prof18"/>
Linux shell	<input type="text" value="/bin/bash"/>
Home directory	<input type="text" value="/var/home/Virsa"/>
Lock this account	<input type="checkbox"/>
SAT Limit	<input type="text" value="none"/>
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
Enter password	<input type="password" value="....."/>
Re-enter password	<input type="password" value="....."/>
Force password change on next login	<input type="radio"/> Yes <input checked="" type="radio"/> No

5.2. Configure SNMP

SNMP is used to capture alarms raised by Communication Manager. To make changes to SNMP configuration the Master Agent must first be stopped by clicking the ‘Stop Master Agent’ button.

Access the Communication Manager System Management Interface as in **Section 5.1**. Click on **SNMP → Agent Status**. Click **Stop the Master Agent** if the **Master Agent status** is **UP** to allow setup of SNMP Agent.

The screenshot displays the Avaya SMI interface. At the top is the Avaya logo. Below it is a red navigation bar with 'Help' and 'Log Off' on the left, and 'Administration' on the right. Underneath is a grey bar labeled 'Administration / Server (Maintenance)'. A left-hand menu contains several categories: 'Alarms' (with a sub-item 'Current Alarms'), 'SNMP' (with sub-items 'Agent Status', 'Access', 'Incoming Traps', 'FP Traps', 'FP Trap Test', and 'FP Filters'), 'Diagnostics' (with sub-items 'Restarts', 'System Logs', 'Ping', 'Traceroute', and 'Netstat'), and 'Server' (with sub-items 'Status Summary', 'Process Status', and 'Interchange Servers'). The main content area is titled 'Agent Status'. It contains the following text: 'The Agent Status SMI page shows the current state of the Master Agent or Stop the Master Agent.' and 'All of the Sub Agents are connected to the Master Agent.' Below this, the status is listed: 'Master Agent status: UP'. A section titled 'Sub Agent Status' follows, showing: 'FP Agent status: UP', 'CMSubAgent status: UP', and 'Load Agent status: UP'. At the bottom of the main content area are two buttons: 'Stop Master Agent' and 'Help'.

To allow VSM to use SNMP to collect configuration and status information from Communication Manager, navigate to **SNMP → FP Traps** in the left pane. Click **Add/Change** button as shown below.

The screenshot displays the Avaya Administration web interface. The top navigation bar includes 'Help' and 'Log Off' on the left, and 'Administration' in the center. Below this, a breadcrumb trail shows 'Administration / Server (Maintenance)'. The left-hand navigation pane is expanded to show the 'FP Traps' option under the 'SNMP' section. The main content area is titled 'FP Traps' and contains the following information:

- A description: 'The FP Traps page allows specification of the alarms to be sent as traps.'
- A **Note** (indicated by a yellow warning icon): 'The FP Traps SMI page is for the administration of CM Fault Performance Traps. It is configured using the "almenable" and the "almsnmpconf" CLI command. Alarms are sent to SAL IP Addresses.'
- Master Agent status: **UP**
- A link: [View AVAYA-AURA-CM-ALARM-MIB Data](#)
- A section titled **Current Settings** containing a table with the following headers: IP address, Port, Notification, SNMP Version, Community_/_ User Name, V3 Security Model, and Authentication Password.
- At the bottom of the main content area are three buttons: **Add/Change**, **Delete**, and **Help**.

Configure the **SNMP Version 2c** section. Set the **IP address** to the VSM server and **Notification** as **trap** from the drop-down menu. During compliance testing, **Community Name** field was set to **avaya123**. Retain the default **Port** value and click **Submit** button.

FP Traps

The FP Traps page allows specification of the alarms to be sent as traps.

Add Trap Destination

SNMP Version 1

IP address:

Port:

Notification:

Community Name:

SNMP Version 2c

IP address:

Port:

Notification:

Community Name:

SNMP Version 3

IP address:

Port:

Notification:

User Name:

Authentication Protocol:

Authentication Password:

and privacy)

Privacy Protocol:

Privacy Password:

Engine ID:

Minimum 8 character

Minimum 8 character

Submit

Cancel


Help

Lastly, the SNMP agent must be started. Navigate to **SNMP → Agent Status** as shown in the beginning of this section. If the **Master Agent status** is **DOWN**, then click the **Start Master Agent** button (not shown). If the **Master Agent status** is **UP**, then the agent must be stopped and restarted.

After adding the SNMP destination, it should be listed on the **FP Traps** page as below:

FP Traps

The FP Traps page allows specification of the alarms to be sent as traps.



Note:

- The FP Traps SMI page is for the administration of CM Fault Performance Traps only. It is not for configuring using the "almenable" and the "almsnmpconf" CLI command. Additionally, Fault Performance Traps are sent to SAL IP Addresses.

Master Agent status: **UP**

[View AVAYA-AURA-CM-ALARM-MIB Data](#)

Current Settings

IP address	Port	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Authentication Protocol
<input type="checkbox"/> 10.1.10.122	162	trap	2c	avaya123			

Communication Manager also needs to be configured to send INADS alarm information to VSM via SNMP. This is done via the shell command "almsnmpconf". To use this command, log into the Communication Manager server Linux prompt. Execute the command:

```
almsnmpconf [-d IP] [-c community];
```

where IP is the VSM IP and community string used during compliance testing.

Check that the INAD SNMP alarms are enabled by executing the following command:
almenable

If the output is as below:

```
SNMP Alarm Origination:      n
then execute the command almenable -s y to enable it.
```

Note: For customers with duplicated servers, this needs to be done on each server individually.

To complete the SNMP configuration in Communication Manager, the VSM server must be added to the IP Node names table as shown below.

From the SAT prompt, enter the command **change node-names ip** and add an entry for the VSM IP address as shown below.

```
change node-names ip                                     Page 1 of 2
                                     IP NODE NAMES
      Name      IP Address
Virsa      10.1.10.122
( 16 of 35 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

The name created above will be used in the IP Options page as shown below by entering the command **change system-parameters ip-options** and configure the following in **Page 3**.

- **Download Flag:** y; note that when set to yes as shown, then these settings will be downloaded to the phone and will overwrite any 46xxxsettings.txt file settings.
- **Community String:** Community Name for Communication Manager SNMP. Refer to earlier part of this section for the Community Name.
- **SOURCE ADDRESSES:** The node-name IP configured above.

This configuration allows VSM to request information via SNMP for active monitoring.

```
change system-parameters ip-options                     Page 3 of 4
                                     IP-OPTIONS SYSTEM PARAMETERS

SNMP PARAMETERS
  Download Flag? y
  Community String: avaya123

SOURCE ADDRESSES
  1.Virsa      4.
  2.           5.
  3.           6.

SERVICES DIAL PAD PARAMETERS      ALTERNATIVE NETWORK ADDRESS TYPES
  Download Flag? n                  ANAT Enabled? n
  Password: *

MUSIC/ANNOUNCEMENTS IP-CODEC PREFERENCES
  Prefer use of G.711 by Music Sources? n
  Prefer use of G.711 by Announcement Sources? n
  Prefer use of G.711 by IP Endpoints Listening to Music? N
```


The alternative is to make these changes in the 46xxsettings.txt files as follows. In the SNMP section edit and uncomment the following settings. Add text as per below with appropriate values.

```
SET SNMPADD <VSM Probe IP Address>
SET SNMPSTRING <Communication Manager SNMP Community Name>
```

5.3. Configure Syslog

The following changes are required to define VSM as an external destination for Communication Manager Syslog. Access the Communication Manager System Management Interface as in **Section 5.1**. Navigate to **Security → Server Log Files** and configure the following in the **Syslog Servers** section at **Log Server 1** (row 1).

- **Enabled** column, select “Yes”.
- **Protocol** column, select “UDP”.
- **Port** column, enter “514”.
- **Server IP/FQDN** column, enter the VSM IP address.
- Check all the boxes for the type of logs to be sent over.

Retain default values for all other fields. Click on the **Submit** button below (not shown) to complete this configuration.

Server Log Files

This page allows you to select logs to be sent to multiple external syslog servers and to configure log retention times for logs that may have privacy data.

Syslog Servers

This section allows you to select logs to be sent to external syslog servers. The checkboxes in the table below allow you to specify the types of logs to send to the remote servers. Here is a description of the log facilities that are sent for each type:

[Security](#) Security Events - auth.*;authpriv.*
[CM IP](#) CM IP Events - local1.*
[Command](#) Command History of the Shell - local0.*
[Kernel](#) Kernel Events - kern.*
[Messages](#) Everything else

Log Server	Enabled	Protocol	Port	Server IP/FQDN	Security	CM IP	Command	Kernel	Messages
1	Yes ▾	UDP ▾	514	10.1.10.122	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	No ▾	TLS ▾	10514	unset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	No ▾	TLS ▾	10514	unset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	No ▾	TLS ▾	10514	unset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	No ▾	TLS ▾	10514	unset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

At the SAT terminal enter the command **change logging-levels** as shown below. On **Page 1** set the following values.

- **Enable Command Logging:** **y**
- **Log Data Values:** **both**
- Set all actions (with the exception of **display**, **get**, **list**, **monitor** and **status**) to 'y' if it is not set.

```
change logging-levels                                     Page 1 of 2

                                LOGGING LEVELS

Enable Command Logging? y
Log Data Values: both

When enabled, log commands associated with the following actions:

      add? y           export? y           refresh? y
      busyout? y       get? n             release? y
      campon-busyout? y      go? y         remove? y
      cancel? y         import? y          reset? y
      change? y         list? n          save? y
      clear? y          mark? y           set? y
      disable? y        monitor? n       status? n
      display? n       netstat? y         test? y
      duplicate? y       notify? y        traceroute? y
      enable? y          ping? y          upload? y
      erase? y          recycle? y
```

On **Page 2** set the **Log PMS/AD Transactions** field to 'y'.

```
change logging-levels                                     Page 2 of 2

                                LOGGING LEVELS

Log All Submission Failures: y
Log PMS/AD Transactions: y
Log IP Registrations and events: y
Log CTA/PSA/TTI Transactions: y
```

5.4. Configure Off-Site Backups

The following changes are required to define VSM as a destination for Communication Manager Backups. These Backup files will be sent from VSM to the Virsae Cloud Computing Service. Access the Communication Manager System Management Interface as in **Section 5.1**. Navigate to **Data Backup/Restore → Schedule Backup** and configure the following.

- Select the radio button for **Specify Data Sets** and check all the boxes below.
- Select the radio button for **Network Device**.
- **Method:** Select **sftp** from the drop-down menu.
- **User Name and Password:** Configure username and password as in **Section 6.2**.
- **Host Name:** IP Address of VSM.
- **Directory:** Configure a directory path.
- Schedule the **Day of Week** and **Start Time** as desired.

Retain default values for all other fields and click on the **Add New Schedule** button (not shown). Below is the configured schedule.

The screenshot displays the 'Change Current Schedule' configuration page within the Communication Manager System Management Interface. The interface has a red header bar with 'Help' and 'Log Off' links, and a navigation menu on the left. The main content area is titled 'Change Current Schedule' and contains several sections:

- Data Sets:** The 'Specify Data Sets' radio button is selected. Below it, three checkboxes are checked: 'Server and System Files', 'Security File', and 'Avaya Call Processing (ACP) Translations'. Two other options are unselected: 'Save ACP translations prior to backup' and 'Do NOT save ACP translations prior to backup'. A 'Full Backup' radio button is also unselected, with a note stating: 'Note: A CM "save trans" is not executed by the Full Backup procedure.'
- Backup Method:** The 'Network Device' radio button is selected. The 'Method' dropdown menu is set to 'sftp'. The 'User Name' field contains 'Virsae', the 'Password' field is masked with dots, the 'Host Name' field contains '10.1.10.122', and the 'Directory' field contains '/'. There are 'Change Schedule' and 'Help' buttons at the bottom of this section.
- Encryption:** An unchecked checkbox labeled 'Encrypt backup using pass phrase' is present.
- Day of Week:** A list of days from Sunday to Saturday, all of which are checked with blue boxes.
- Start Time:** Two dropdown menus are set to '01' and '10' respectively.

At the bottom of the configuration area, a note states: 'Backups are scheduled once per week on each of the days selected. All backups begin at the same time.'

5.5. Configure CDR Link

The following changes are required to define VSM as a CDR destination.

Use the **change ip-services** command to define the CDR link between Communication Manager and VSM. To define a primary CDR link, provide the following information:

- **Service Type:** **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node:** **procr** [For Communication Manager used during compliance testing, set the Local Node to the node name of the processor board.]
- **Local Port:** **0** [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.]
- **Remote Node:** **Virsa** [The Remote Node is set to the node name previously defined in **Section 5.2.**]
- **Remote Port:** **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in VSM Probe.]

change ip-services							Page 1 of 4
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	TLS Encryption	
CDR1		procr	0	Virsa	9000	n	

On **Page 3** of the ip-services form, set the **Reliable Protocol** field to **n**.

change ip-services							Page 3 of 4
SESSION LAYER TIMERS							
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer		
CDR1	n	30	3	3	60		

Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track, and for the format of the CDR data. The example below shows the settings used during the compliance test. Configure the following information:

- **CDR Date Format:** **month/day**
- **Primary Output Format:** **unformatted**
- **Primary Output Endpoint:** **CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. Refer to the reference in **Section 9** for additional details.

```
change system-parameters cdr                                     Page 1 of 1
                                CDR SYSTEM PARAMETERS
Node Number (Local PBX ID): 1                                CDR Date Format: month/day
Primary Output Format: unformatted    Primary Output Endpoint: CDR1
Secondary Output Format:
CDR Retention (days): 20
Use ISDN Layouts? n                                Enable CDR Storage on Disk? n
Use Enhanced Formats? n                    Condition Code 'T' For Redirected Calls? n
Use Legacy CDR Formats? y                    Remove # From Called Number? n
Modified Circuit ID Display? n                                Intra-switch CDR? y
                                Record Outgoing Calls Only? n                    Outg Trk Call Splitting? y
Suppress CDR for Ineffective Call Attempts? y                    Outg Attd Call Record? y
Disconnect Information in Place of FRL? n                    Interworking Feat-flag? n
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n                    Record Agent ID on Outgoing? n
Inc Trk Call Splitting? y                                Inc Attd Call Record? y
Record Non-Call-Assoc TSC? n                    Call Record Handling Option: warning
Record Call-Assoc TSC? n                    Digits to Record for Outgoing Calls: dialed
Privacy - Digits to Hide: 0                                CDR Account Code Length: 15
Remove '+' from SIP Numbers? y
```

5.6. Configure RTCP Monitoring

To allow VSM to monitor the quality of H.323 IP calls, configure Communication Manager to send RTCP reporting to the IP address of VSM. This is done through the SAT interface. For Avaya SIP endpoints, refer to the reference in **Section 9**.

Enter the **change system-parameters ip-options** command. In the **RTCP MONITOR SERVER** section, set **Server IPV4 Address** to the IP address of VSM. Set **IPV4 Server Port** to **5005** and **RTCP Report Period (secs)** to **5**.

```
change system-parameters ip-options                                     Page 1 of 4
                               IP-OPTIONS SYSTEM PARAMETERS

IP MEDIA PACKET PERFORMANCE THRESHOLDS
  Roundtrip Propagation Delay (ms)      High: 800      Low: 400
      Packet Loss (%)                   High: 40        Low: 15
      Ping Test Interval (sec): 20
  Number of Pings Per Measurement Interval: 10
      Enable Voice/Network Stats? n

RTCP MONITOR SERVER
  Server IPV4 Address: 10.1.10.122      RTCP Report Period(secs): 5
      IPV4 Server Port: 5005
  Server IPV6 Address:
      IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
  Link Failure? y

                               H.323 IP ENDPOINT
H.248 MEDIA GATEWAY
  Link Loss Delay Timer (min): 5          Primary Search Time (sec): 75
  Recover Before LLDT Expiry? y          Periodic Registration Timer (min): 20
      Short/Prefixed Registration Allowed? y
```

Enter the **change ip-network-region *n*** command, where ***n*** is IP network region number to be monitored. On **Page 2**, set **RTCP Reporting to Monitor Server Enabled** to **y** and **Use Default Server Parameters** to **y**.

Note: Only one RTCP MONITOR SERVER can be configured per IP network region. Repeat the above for all IP network regions that are required to be monitored.

```
change ip-network-region 6                                           Page 2 of 20
                               IP NETWORK REGION

RTCP Reporting to Monitor Server Enabled? y

RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? y
```

5.7. Configure Login for G430 Media Gateway

The VSM requires access to the Media Gateways. This can be achieved by creating a new administrator on the Media Gateway. To create a new username with administrator access, login to G430 Media Gateway using administrator access and run the following command.

```
username [choose a username] password [choose a password] accesstype admin
```

The above command will create a username with access type as admin.

5.8. Configure Avaya Aura® Media Server

This section describes the steps needed to configure Media Server to interoperate with VSM. This includes creating a login account and enabling SNMP, Syslog and RTCP.

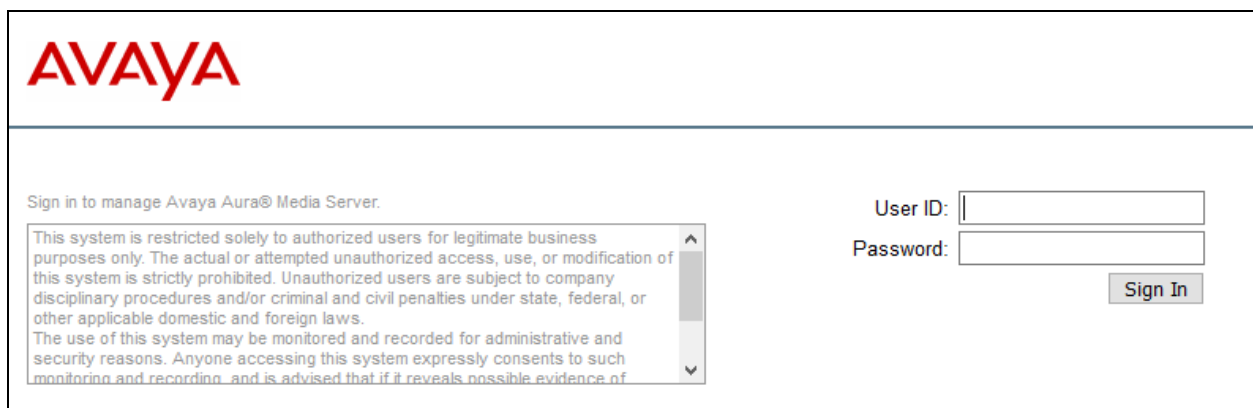
5.8.1. Configure Login

Create an Administrator account on Media Server since VSM requires access to Media Server with Administrative Rights. Log in to Media Server console with administrator access and run the following command.

```
useradd <NAME>          ;Add User
passwd <NAME>           ;Enter password twice
chage -M 99999 <NAME>   ;Lengthen the expiry date of account
```

5.8.2. Configure RTCP

Using a web browser, enter ***https://<IP address of Media Server:8443/emlogin>*** to connect to the media server being configured and log in using appropriate credentials.



AVAYA

Sign in to manage Avaya Aura® Media Server.

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

User ID:

Password:

Sign In

At the home page, navigate to the **System Configuration → Media Processing → General Settings** (not shown).

AVAYA**Avaya Aura® Media Server**[Help](#) | [Sign Out](#) **admin**

Network


- System Status
 - Element Status
 - Cluster Status
 - Alarms
- + Logs
- + Monitoring
- Applications
 - General Settings
 - Operational State
 - Signaling Translations
 - Custom Applications
 - Default Handlers
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Advanced Settings
- System Configuration
 - + Server Profile
 - + Network Settings
 - + Signaling Protocols
 - + Media Processing
 - + Application Interpreters
 - + Monitoring Settings

Managing: aams2.sglab.com, 10.1.10.12
Home

Avaya Aura® Media Server

Welcome to the Element Manager for the following installed software packages:
Avaya Aura® Media Server - v.10.1.0.77

If you are a new user, or need assistance, please click [help](#)


 Select a task from the left pane to get started.


Under **Dual Unicast Monitoring**, configure the following:


- **Dual Unicast Monitoring:** Tick the box.
- **Monitoring Server IP:** Enter the VSM server IP address.
- **Monitoring Server Port:** Enter **5005**.

Managing: aams2.sglab.com, 10.1.10.12


[Home](#) » [System Configuration](#) » [Media Processing](#) » General Settings


Enable Google Cloud Text-To-Speech: ☐ 

Google Cloud Text-To-Speech API Key:  (maximum: 1024 characters)



Google Cloud Referrer Restriction:  (maximum: 1024 characters)



[⌵ IBM Watson Text-To-Speech](#)

Enable IBM Cloud Text-To-Speech: ☐ 



IBM Cloud Text-To-Speech API Key:  (maximum: 1024 characters)



[⌵ Aurix Speech Search Engine](#)



Enable AURIX SSE Real-time Interfaces: ☐  

Enable AURIX SSE Web Service Interfaces: ☐  

[⌵ Dual Unicast Monitoring](#)

Dual Unicast Monitoring: ☒  

Monitoring Server IP:   (1 - 256 characters)

Monitoring Server Port:   (0 - 65535)

LYM; Reviewed:
SPOC 10/6/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

25 of 54
Virsa-CM101

5.8.3. Configure Syslog

From the home page, navigate to the **System Configuration** → **Logging Settings**. Add the VSM Probe server to the **Syslog Destination Server**.

The screenshot shows the 'Avaya Aura® Media Server' interface. At the top, it says 'Managing: aams2.sglab.com, 10.1.10.12' with links for 'Home', 'System Configuration', and 'Logging Settings'. The main heading is 'Logging Settings'. Below it are links for 'Privacy', 'Syslog', 'Session Logging', 'OMs', 'Event Log', and 'Data Collection'. The 'Privacy' section has a 'Mask Sensitive Data' checkbox and options for 'Select all', 'Digit Collection', 'Announcements and Prompts', 'Text-To-Speech', and 'Speech Recognition'. The 'Syslog' section has a 'Syslog Delivery of Logs' checkbox and a 'Syslog Destination Server List' with 'Add' and 'Clear' buttons. Below this is a table with columns 'Server Address' and 'Port (0-65535)'. The first entry shows '10.1.10.122' and '514'.

Server Address	Port (0-65535)
10.1.10.122	514

5.8.4. Configure SNMP

SNMP is used to capture alarms raised by Media Server and to query the Media Server for information. The VSM server must be added as a destination for SNMP traps.

From the home page, navigate to **System Configuration** → **Network Settings** → **SNMP**.

The screenshot shows the 'Avaya Aura® Media Server' interface. At the top, it says 'Managing: aams2.sglab.com, 10.1.10.12' with links for 'Home', 'System Configuration', 'Network Settings', and 'SNMP'. The main heading is 'SNMP'. Below it is a description: 'SNMP consist of tasks that allow administrators to view and modify SNMP settings.' There are three sections: 'Users', 'Agent Settings', and 'Destinations', each with a description of the task. On the left side, there is a navigation menu with 'Network' selected, showing a list of options: System Status, Element Status, Cluster Status, Alarms, Logs, Monitoring, Applications, Cluster Configuration, System Configuration, and Server Profile.

- Users**
This task allows administrators to view and modify the SNMP user profiles.
- Agent Settings**
This task allows administrators to view and modify the SNMP agent settings.
- Destinations**
This task allows administrators to view and modify the SNMP traps configuration.

Click on **SNMP → Users**. Configure the following and click **Save** at the bottom (not shown).

- **Security name:** Desired string.
- **Description:** Descriptive name.
- **Version:** Select version desired. In this compliance test, **v1/v2c** is selected.
- **Access rights:** Select **read-only**.

Below is a screenshot of the configured SNMP User.

The screenshot displays a web interface for managing SNMP users. At the top, a breadcrumb trail shows the navigation path: Home » System Configuration » Network Settings » SNMP » Users » Edit User. The main heading is "Edit SNMP User". Below this, there are four configuration fields: "Security name" with the value "avaya123" and a note "(Allowed characters: a-zA-"; "Description" with the value "virsae"; "Version" with a dropdown menu set to "v1/v2c"; and "Access rights" with a dropdown menu set to "read-only".

Click on **SNMP → Agent Settings**. Configure the following:

- **Agent Enabled:** Tick to enable.
- **Port Number:** 161.
- **System Location, Contact and Name:** Enter descriptive names.
- **Version 1/2c:** Tick to enable and select user security name created above.



Managing: aams2.sglab.com, 10.1.10.12
[Home](#) » [System Configuration](#) » [Network Settings](#) » [SNMP](#) » Agent Settings



Agent Settings



This task allows administrators to view and modify the SNMP agent settings.



[General Settings](#) | [Version 3](#) | [Version 1/2c](#)



General Settings

Agent Enabled: ☒  



Port Number:   (1 - 65535)



System Location:   (maximum: 255 characters)

System Contact:   (maximum: 255 characters)



System Name:   (maximum: 255 characters)



Version 3

Enabled: ☐  

User:  

Version 1/2c

Enabled: ☒  

User:  

Click on **SNMP → Destinations**. Under **General Settings** check the ‘SNMP Alarm Delivery Traps’ box. Add a **Trap Destination** as the VSM server and a **Trap Routes** with the VSM server as the **Destination address**. Note the default **Destination Port** of **162** is used.

Avaya Aura® Media Server

Help | Sign Out admin

Managing: aams2.sglab.com, 10.1.10.12

[Home](#) » [System Configuration](#) » [Network Settings](#) » [SNMP](#) » Destinations

Trap Destinations

This task allows administrators to configure SNMP trap configuration, destinations, and routes.

[General Settings](#) | [Trap Destinations](#) | [Trap Routes](#)

General Settings

SNMP Alarm Delivery Traps ☒

SNMP Event Log Delivery Traps ☐

Trap Destinations

Add... Edit... Delete

<input type="checkbox"/>	Destination Address ▲	Destination Port
<input type="checkbox"/>	10.1.10.122	162
<input type="checkbox"/>		
<input type="checkbox"/>		

Trap Routes

Add... Edit... More Actions ▼

<input type="checkbox"/>	Destination Address ▲	Destination Port	Security Name	Sec
<input type="checkbox"/>	10.1.10.122	162	avaya123	
<input type="checkbox"/>				
<input type="checkbox"/>				

< >

Save Cancel Restore Defaults

6. Configure Virsae Service Management

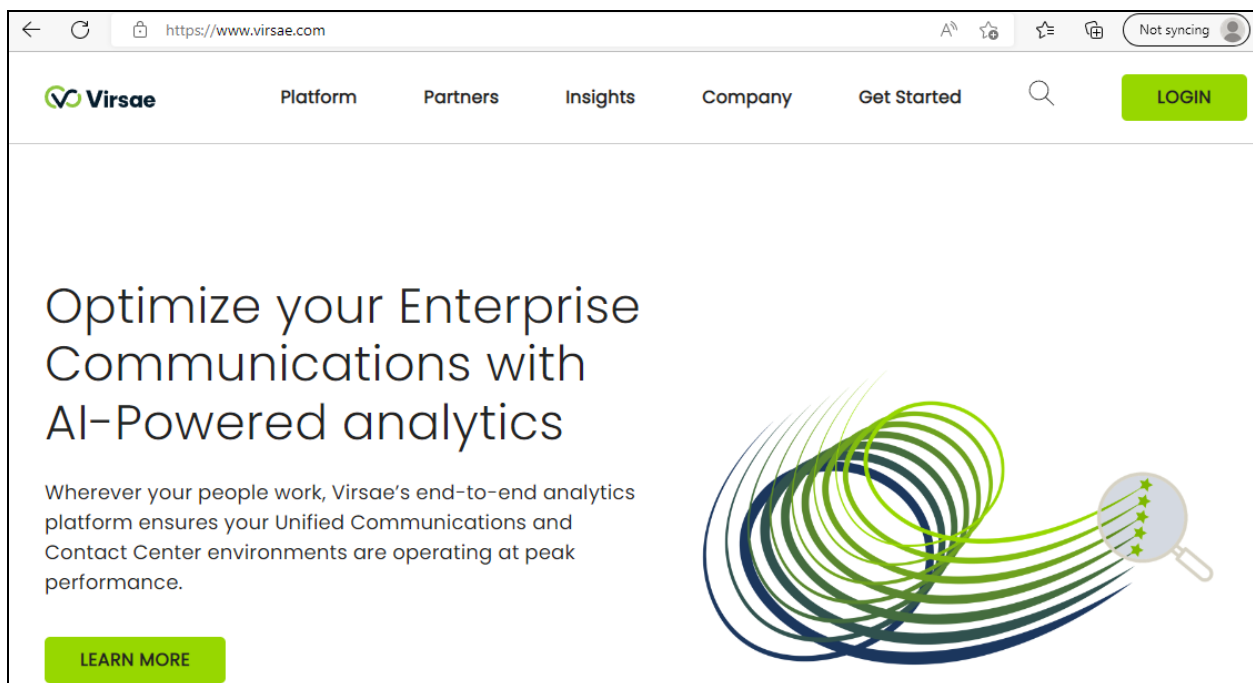
This section describes the configuration of VSM required to interoperate with Communication Manager. Configuration of VSM to interoperate with Session and System Manager can be referred from reference [3] and [4] in **Section 9** and will not be detailed here.

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:

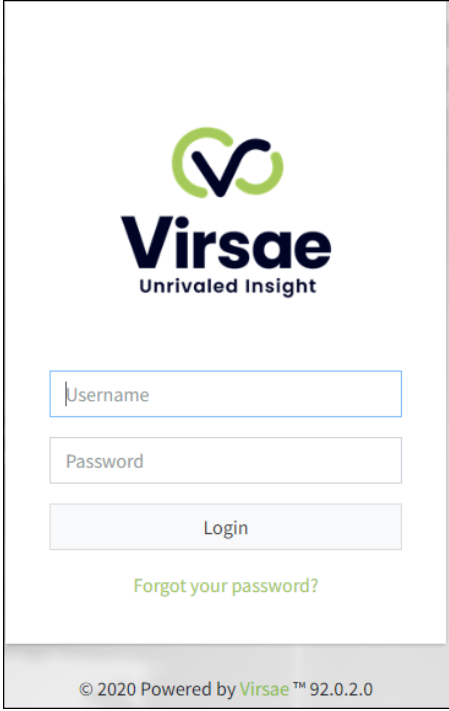
- Login to the Web Portal
- Configuring Avaya Aura® Communication Manager
- Configuring Avaya Aura® Media Server
- Configure Dashboard

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 **Login** button.



The image shows a login form for Virsaе. At the top is the Virsaе logo, which consists of a stylized 'V' made of two interlocking loops, one green and one dark blue, followed by the word 'Virsaе' in a bold, dark blue sans-serif font, and the tagline 'Unrivalled Insight' in a smaller, lighter blue font below it. Below the logo are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Below these fields is a light blue button with the text 'Login'. Below the button is a link that says 'Forgot your password?' in a green font. At the bottom of the form, there is a grey footer bar with the text '© 2020 Powered by Virsaе™ 92.0.2.0'.

Virsaе
Unrivalled Insight

Username

Password

Login

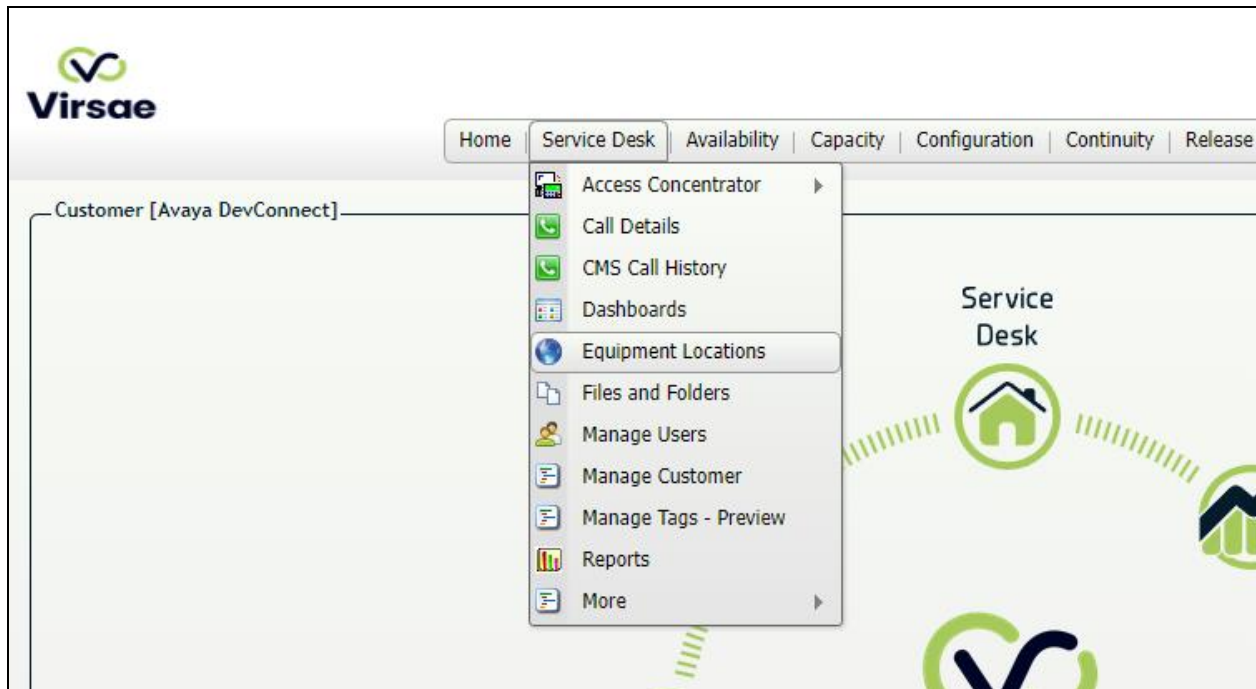
[Forgot your password?](#)

© 2020 Powered by Virsaе™ 92.0.2.0

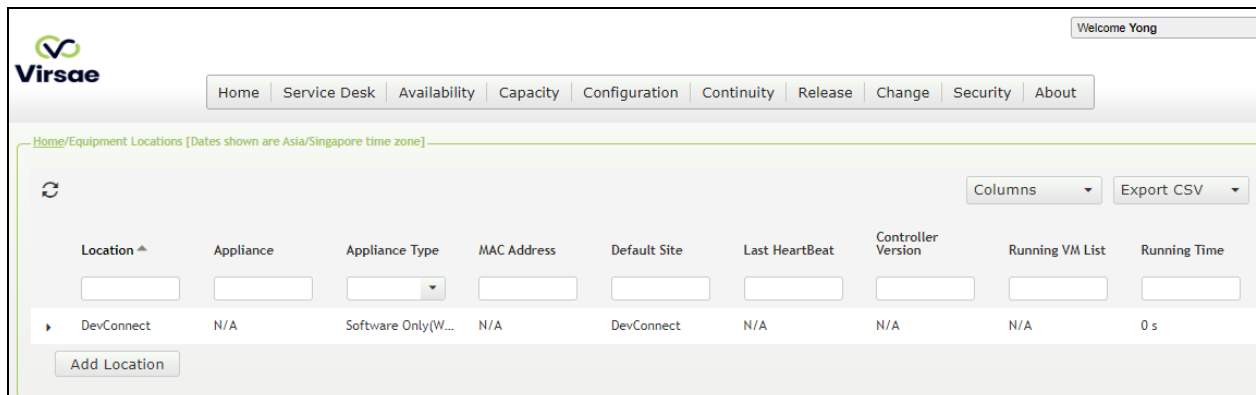
The customers screen is shown. During compliance testing the customer created by Virsae is can be seen near the top right corner. Note the version running is shown at the bottom i.e., **174.1.2.268**.



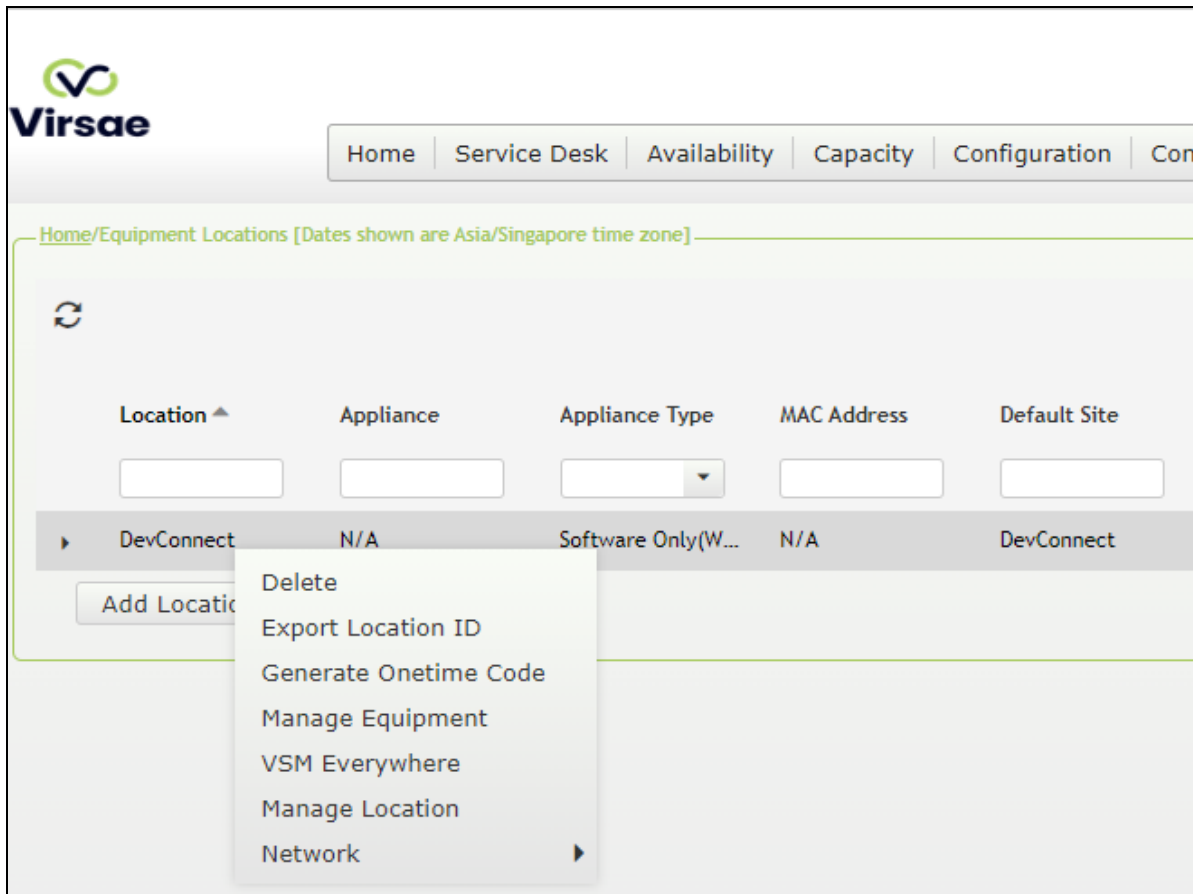
Navigate to **Service Desk → Equipment Locations** as shown below.



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

6.2. Configuring Avaya Aura® Communication Manager

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

- **Equipment Name:** A descriptive name.
- **Username:** The username configured in **Section 5.1**.
- **Password:** The password configured in **Section 5.1**.
- **IP Address/Host Name:** IP address of Communication Manager.
- **Site:** A descriptive site name.
- **Username for Media Gateways:** As configured in **Section 5.7**.
- **Password for Media Gateways:** As configured in **Section 5.7**.
- **Monitored IP Network Regions:** Enter the IP Network Regions to be monitored.
- **Associated RTCP Receiver:** “DevConnect” location is selected in this case.

Equipment	SNMP Query	Network Connectivity	Custom Scripts	Tags	Site Mappings
Vendor * Avaya					
Product * ACM					
Equipment Name * DevConnect ACM 10			Username Virsa		
IP Address/Host Name * 10.1.10.230			Password		
Site ⓘ DevConnect			<input type="checkbox"/> Use Serial Port		
ACM Details					
Username for Media Gateways virsa			Associated RTCP Receiver DevConnect		
Password for Media Gateways			Monitored IP Network Regions 1,2,3,4,5,6,7,8,9,10		
<input type="checkbox"/> Use the above credentials for all Media Gateways ⓘ <input type="checkbox"/> Disable automatic connection to Media Gateways ⓘ					

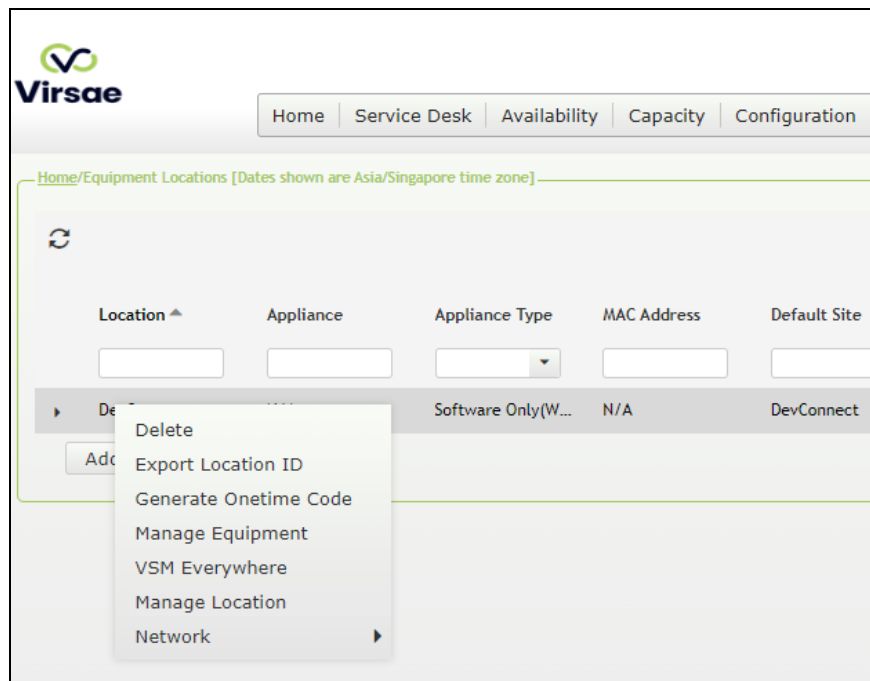
In the **SNMP Query** tab, configure the following values.

- **Version:** Select **V2** from the drop-down menu.
- **SNMP Community String:** Enter the value configured in **Section 5.2**.

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

The screenshot shows the 'SNMP Query' tab in the Virsae interface. At the top, there are tabs for 'Equipment', 'SNMP Query', 'Network Connectivity', 'Custom Scripts', 'Tags', and 'Site Mappings'. The 'SNMP Query' tab is active. Below the tabs, there are two input fields: 'Version' with a dropdown menu set to 'V2', and 'SNMP Community String' with a text input field containing 'avaya123'. Below these fields, there is a section titled 'Avaya Phones' with a sub-section for 'SNMP Community String' containing a text input field with 'avaya123' and a '+', and a list of 'avaya123' with edit and delete icons.

Navigate to **Service Desk → Equipment Locations** (not shown), right click on the **DevConnect** and select **Manage Locations**.



Select the **File Transfer** tab. Check **Enable SFTP** is turn on i.e., tick and configure the SFTP user accounts for Communication Manager backup as below:

- **User Name and Password:** Enter the name and password to be used by Communication Manager in **Section 5.4**.
- **Protocol:** Select **SFTP/SCP**.
- **Upload Type:** Select **Backup**.

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

The screenshot shows the 'File Transfer' configuration page. At the top, there are tabs: 'Details', 'Appliance', 'SNMP Traps', 'File Transfer' (selected), and 'VQM'. Below the tabs, there is an information icon. The main configuration area has four checkboxes: 'Enable TFTP', 'Enable V-Drive', 'Enable FTP', and 'Enable UUCP'. Below these is a section titled 'SFTP and SCP Configuration'. In this section, 'Enable SFTP' is checked and 'Enable SCP' is unchecked. There is a 'Port' field with the value '22'. Below this is another section titled 'SFTP and FTP user accounts'. This section contains a table with the following columns: 'User Name *', 'Password *', 'Protocol', 'Upload Type', and 'Public Key'. There is a '+' button to add a new user and a refresh icon. The table contains one entry: 'Virsaе' for the user name, a masked password '*****' for the password, 'SFTP/SCP' for the protocol, 'Backup' for the upload type, and an empty field for the public key. There are also edit and delete icons for this entry.

User Name *	Password *	Protocol	Upload Type	Public Key
Virsaе	*****	SFTP/SCP	Backup	

6.3. Configuring Avaya Aura® Media Server

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


- **Equipment Name:** A descriptive name.
- **Username:** The username configured in **Section 5.8.1**.
- **Password:** The password configured in **Section 5.8.1**.
- **IP Address/Host Name:** IP address of Media Server.
- **Site:** A descriptive site name.

Equipment	SNMP Query	Network Connectivity	Custom Scripts	Tags
<div><div>Vendor *</div><div>Avaya</div></div> <div><div>Product *</div><div>Media Server</div></div> <div><div>Equipment Name *</div><div>AAMS</div></div> <div><div>Username</div><div>virsa</div></div> <div><div>IP Address/Host Name *</div><div>10.1.10.12</div></div> <div><div>Password</div><div>.....</div></div> <div><div>Site ⓘ</div><div>DevConnect</div></div>				

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

- **Version:** Select **V2** from the drop-down menu.
- **SNMP Community String:** Enter the value configured in **Section 5.8.4**.

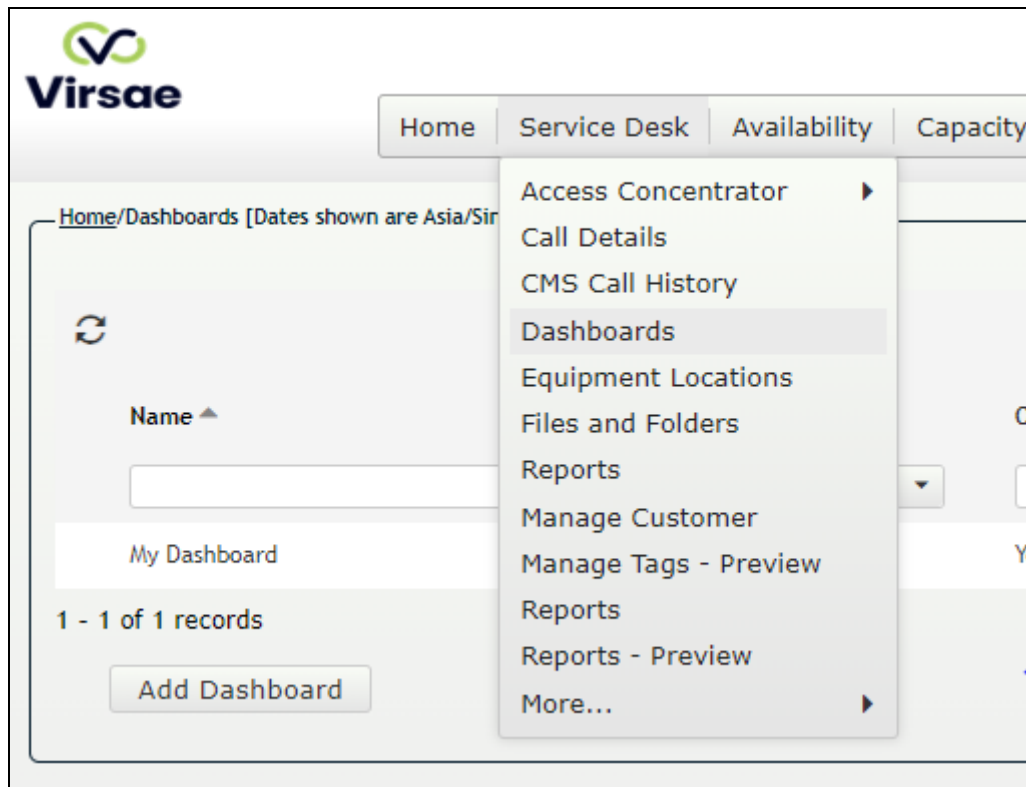
Click on the **Save** button to complete the configuration.

Equipment	SNMP Query	Network Connectivity	Custom Scripts	Tags
Version		SNMP Community String 		
<input type="text" value="V2"/>		<input type="text" value="avaya123"/>		

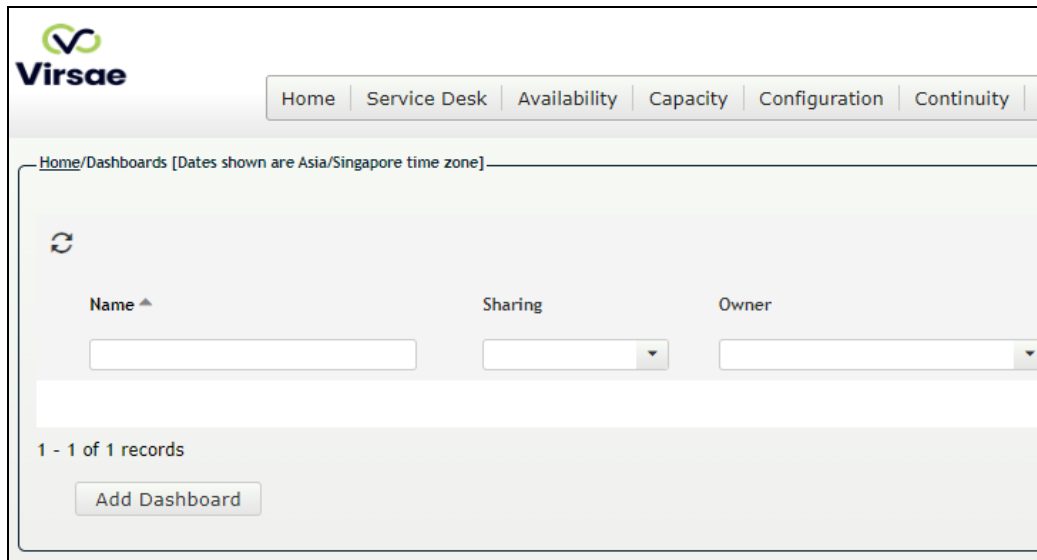
6.4. Configure Dashboard

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

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

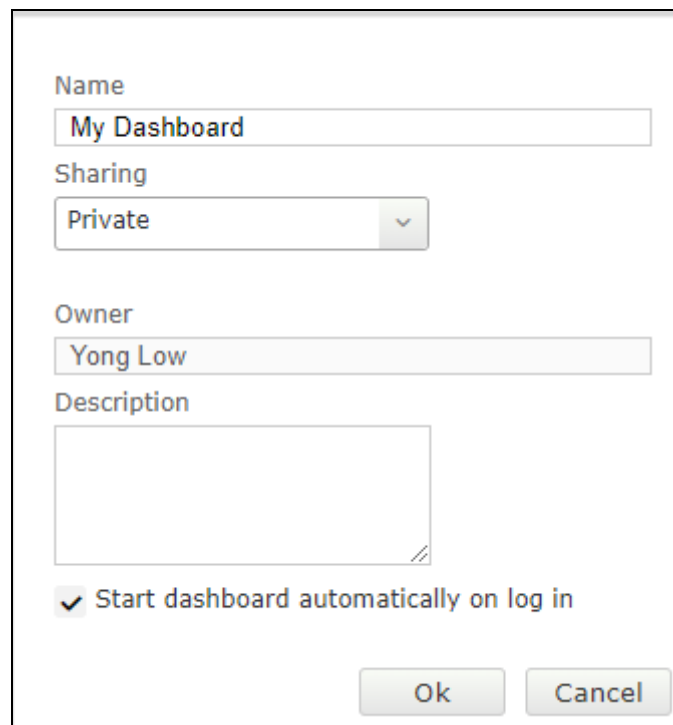


From the **Dashboards** window, click on the **Add Dashboard** button.



The screenshot shows the Virsae application interface. At the top, there is a navigation bar with the Virsae logo and several menu items: Home, Service Desk, Availability, Capacity, Configuration, Continuity, and a partially visible 'P'. Below the navigation bar, the main content area is titled 'Home/Dashboards [Dates shown are Asia/Singapore time zone]'. It features a refresh icon and a table with three columns: Name, Sharing, and Owner. The table contains one record with empty fields. Below the table, it indicates '1 - 1 of 1 records' and includes an 'Add Dashboard' button.

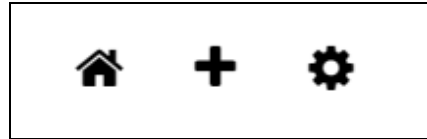
In the **Add Dashboard** window, type a descriptive name for **Name** field as shown below. Retain default values for all other fields. Check on **Start dashboard automatically on log in** box and then click on **Ok** to submit.



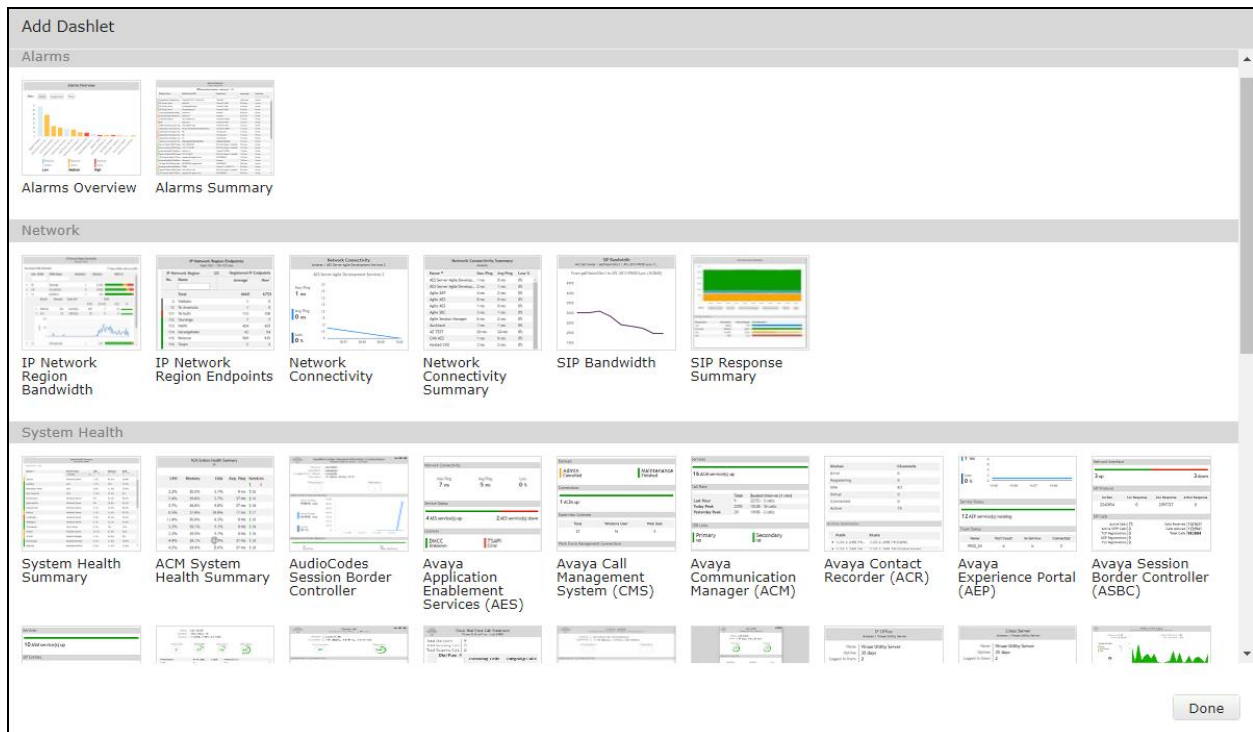
The screenshot shows the 'Add Dashboard' dialog box. It contains the following fields and options:

- Name:** A text field containing 'My Dashboard'.
- Sharing:** A dropdown menu set to 'Private'.
- Owner:** A text field containing 'Yong Low'.
- Description:** A large empty text area.
- Start dashboard automatically on log in:** A checked checkbox.
- Buttons:** 'Ok' and 'Cancel' buttons at the bottom right.

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



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



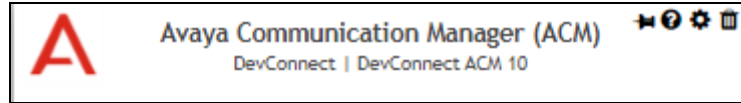
From the **ACM System Health Summary** window created, select the **setup** cog on the top right corner as shown below.



Select “DevConnect” for the **Location** drop-down menu and click **Done** (not shown).

The screenshot displays the 'Settings' window of the Avaya DevConnect application. On the left, a sidebar lists various dashlets under the heading 'All Dashlets'. The dashlets include 'Dashboard', 'ACM System Health Summary DevConnect' (which is currently selected and highlighted), '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', and 'Linux Server DevConnect | SMGR'. On the right side of the window, there are two dropdown menus. The 'Customer' dropdown is set to 'Avaya DevConnect', and the 'Location' dropdown is set to 'DevConnect'.

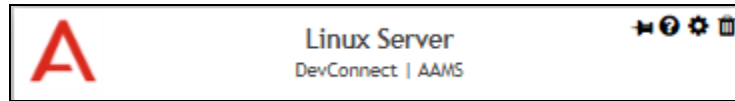
Repeat the same for the **Avaya Communication Manager (ACM)** dashlet below:



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	DevConnect ACM 10
Avaya Session Manager (SM) DevConnect SM1	Layout
Avaya Session Manager (SM) DevConnect SM2	Show Occupancy Graph
Calls In Progress DevConnect DevConnect	Show Network Connectivity Graph
Linux Server DevConnect AAMS	Show Call Rate
Linux Server DevConnect Breeze	Show Services
Linux Server DevConnect SMGR	Show CDR Links
	Show Media Gateways
	Show DS1s
	Show Custom Scripts

As for Media Server, add the **Linux Server** dashlet as below:



Settings

Dashboard

All Dashlets

ACM System Health Summary
DevConnect

Alarms Summary
Avaya DevConnect

Avaya Application Enablement Services (AES)
DevConnect | AES

Avaya Communication Manager (ACM)
DevConnect | DevConnect ACM 10

Avaya Session Manager (SM)
DevConnect | SM1

Avaya Session Manager (SM)
DevConnect | SM2

Calls In Progress
DevConnect | DevConnect

Linux Server
DevConnect | AAMS

Linux Server
DevConnect | Breeze

Linux Server
DevConnect | SMGR

Customer
Avaya DevConnect

Location
DevConnect

Equipment
AAMS

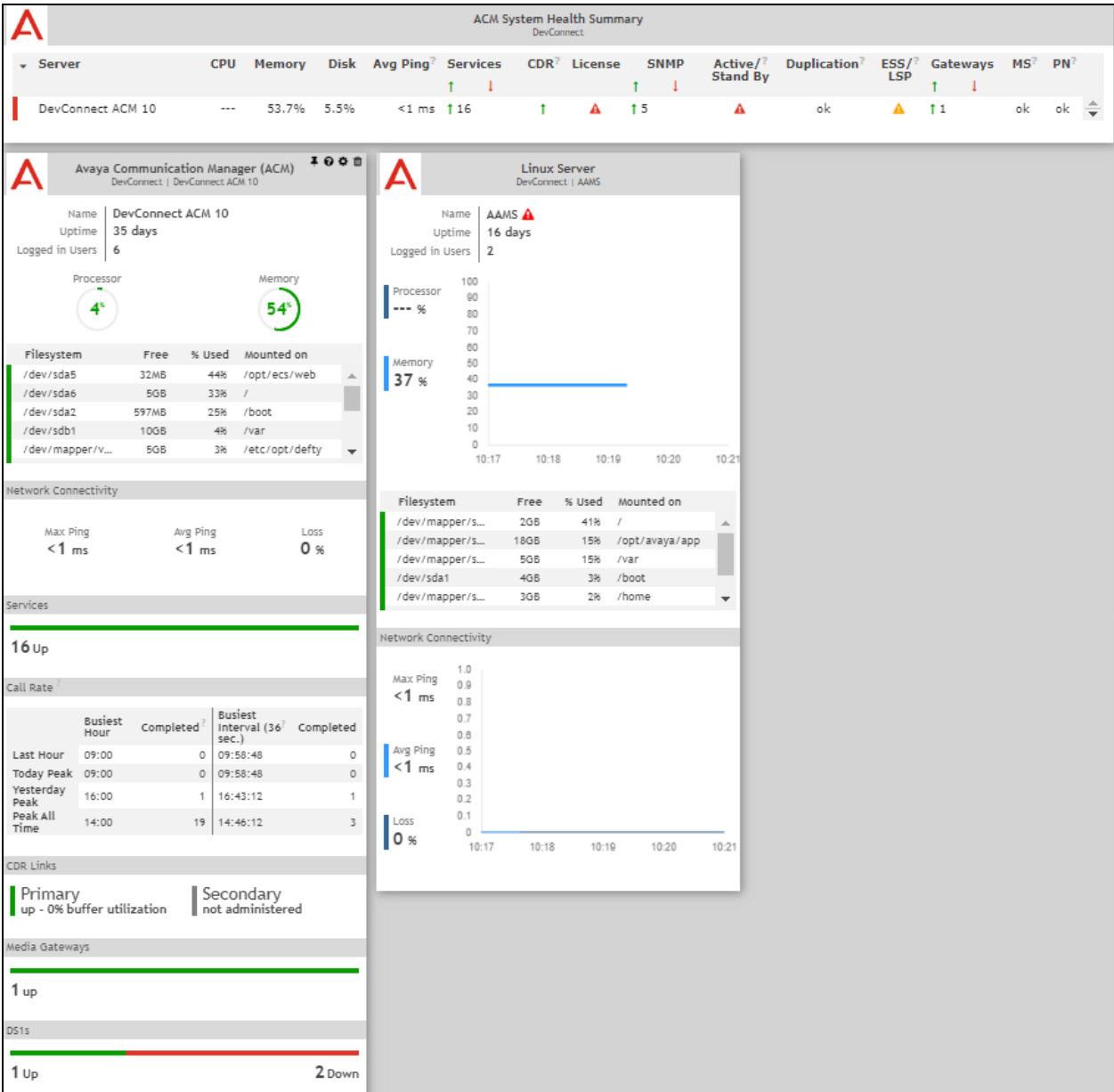
Layout

Show Occupancy Graph ☒

Show Network Connectivity Graph ☒

Show Custom Scripts ☐

The dashboard with the configured equipment is shown below.



7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and VSM.

7.1. Verify Communication Manager

Verify that VSM has established concurrent connections to the Linux shell by using the `who -u` command.

```
dadmin@cm1> who -u
Virsaes pts/0      2022-08-11 19:53 .          53443 (10.1.10.122)
Virsaes pts/1      2022-08-11 19:09 .          45039 (10.1.10.122)
Virsaes pts/2      2022-08-11 19:53 .          53810 (10.1.10.122)
Virsaes pts/3      2022-08-11 19:53 .          53926 (10.1.10.122)
Virsaes pts/4      2022-08-11 19:53 .          53967 (10.1.10.122)
SMGRUser pts/5      2022-08-10 10:21 old        3935538 (10.1.10.46)
dadmin pts/6      2022-08-04 08:33 old        2648425 (10.1.10.99)
dadmin pts/7      2022-08-12 10:13 .          179781 (10.1.10.155)
dadmin@cm1>
```

Verify that VSM has established concurrent connections to the SAT by using the `status logins` command.

```
status logins

COMMUNICATION MANAGER LOGIN INFORMATION

Login      Profile  User's Address      Active Command      Session
-----
Virsaes    18      10.1.10.122         .                    3
Virsaes    18      10.1.10.122         .                    4
Virsaes    18      10.1.10.122         .                    5
Virsaes    18      10.1.10.122         .                    6
SMGRUser   28      10.1.10.46          .                    7
*dadmin    18      10.1.10.155         stat logins         8
```

Using the `status cdr-link` command, verify that the **Link State** of the primary CDR link configured in **Section 5.55.5** shows **up**.

```
status cdr-link

CDR LINK STATUS

Primary      Secondary

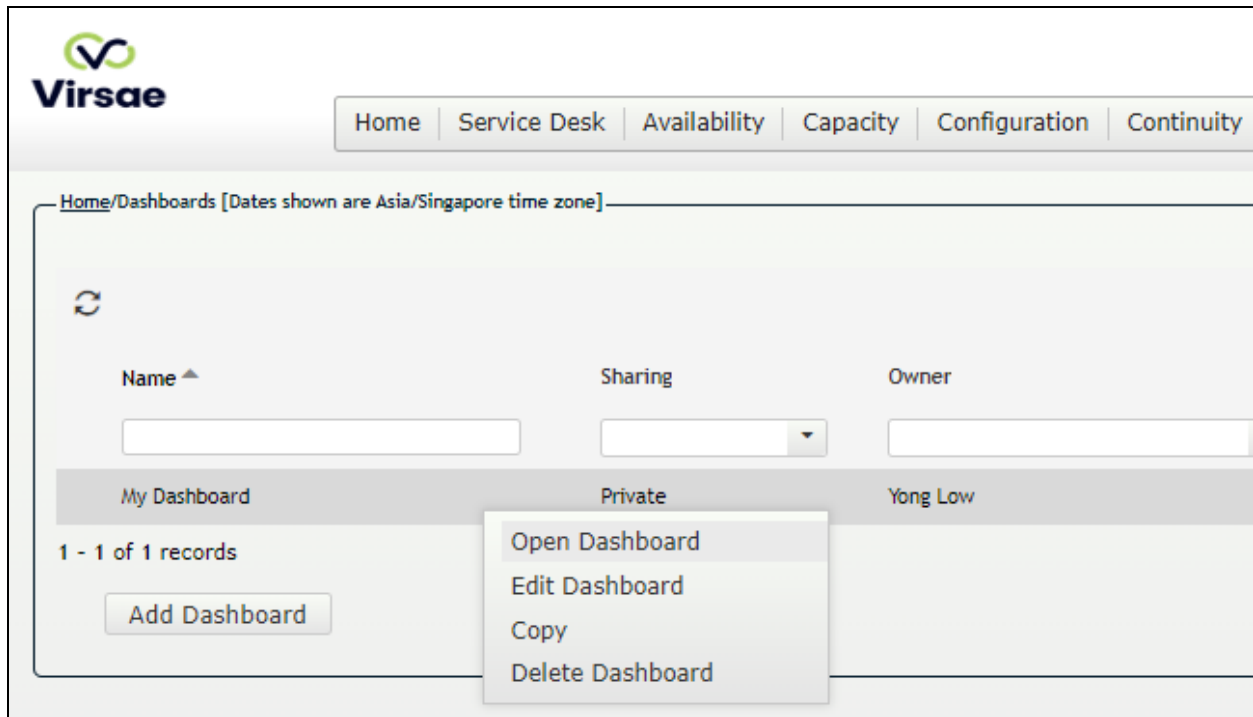
Link State: up      CDR not administered

Date & Time: 2022/08/11 19:09:18      0000/00/00 00:00:00
Forward Seq. No: 0      0
Backward Seq. No: 0      0
CDR Buffer % Full: 0.00      0.00
Reason Code: OK
```

7.2. Verify Virsae Service Management


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 6.4**, once login, all the dashboards last configured at the end of **Section 6.4** 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 Communication Manager equipment. For Media Server, filter accordingly for AAMS.


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
DIG-LINE	Digital Line Port error 1. Error type ...	2022-08-12 11:43:36	400009	0	DevConnect A...	Avaya	6
H323-STN	H323-STN covers implementation o...	2022-08-12 11:41:02	10408	1	DevConnect A...	Avaya	6
H323-STN	H323-STN covers implementation o...	2022-08-12 11:41:02	10409	1	DevConnect A...	Avaya	6
H323-STN	H323-STN covers implementation o...	2022-08-12 11:41:02	10410	1	DevConnect A...	Avaya	6
DIG-IP-S	IP Softphone or 46XX phone error. ...	2022-08-12 11:41:02	19907	1	DevConnect A...	Avaya	6
DIG-IP-S	IP Softphone or 46XX phone error. ...	2022-08-12 11:41:02	19909	1	DevConnect A...	Avaya	6
DIG-IP-S	IP Softphone or 46XX phone error. ...	2022-08-12 11:41:02	19908	1	DevConnect A...	Avaya	6
DIG-IP-S	IP Softphone or 46XX phone error. ...	2022-08-12 11:41:02	10088	1	DevConnect A...	Avaya	6
DIG-IP-S	IP Softphone or 46XX phone error. ...	2022-08-12 11:41:02	10087	1	DevConnect A...	Avaya	6
DIG-IP-S	IP Softphone or 46XX phone error. ...	2022-08-12 11:41:02	10013	1	DevConnect A...	Avaya	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 Communication Manager extensions. Real time voice quality can also be viewed in the dashboard.

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
	10009	N/A	4.41	4.41	4.41	0	10.1.10.166	3292	
	10001	N/A	4.41	4.41	4.41	0	10.1.10.172	2466	
9611G H.323	10001	1	4.41	4.41	4.41	20	10.1.10.154		
9611G H.323	10001	1	4.41	4.41	4.41	20	10.1.10.154		
1616 H.323	10002	1	4.41	4.41	4.41	331	10.1.10.198	2876	
9608 H.323	10003	1	4.4	4.41	4.41	331	10.1.10.174	3300	
XFire2a09	gwp	1	4.41	4.41	4.41	331	10.1.50.25		
XFire2a09	gwp	1	4.41	4.41	4.41	321	10.1.50.25		

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 for Communication Manager extensions.

Filters: CDR1

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

Details

Location = DevConnect
Equipment = DevConnect ACM 10, 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	Acc
2022-08-02 14:27:00	0 - 5	0 - 5	0 - 5		426	10001	10048	A		
2022-08-02 15:03:00					552	10048	10004	9		
2022-08-02 15:25:00					54	10001	10048	A		
2022-08-03 01:08:00					35994	10004	10048	4		
2022-08-03 10:58:00					35364	10004	10048	A		

To view off-site backups, navigate to **Continuity** → **Browse Backups** (not shown). Screen below shows an example of backups for Communication Manager.

Home Service Desk Availability Capacity Configuration Continuity Release Change Security About

Home/Files and Folders [Dates shown are Asia/Singapore time zone]

Root
As Built Schematics
Back Up
DevConnect ACM 10
System Log

Search Files and Folders

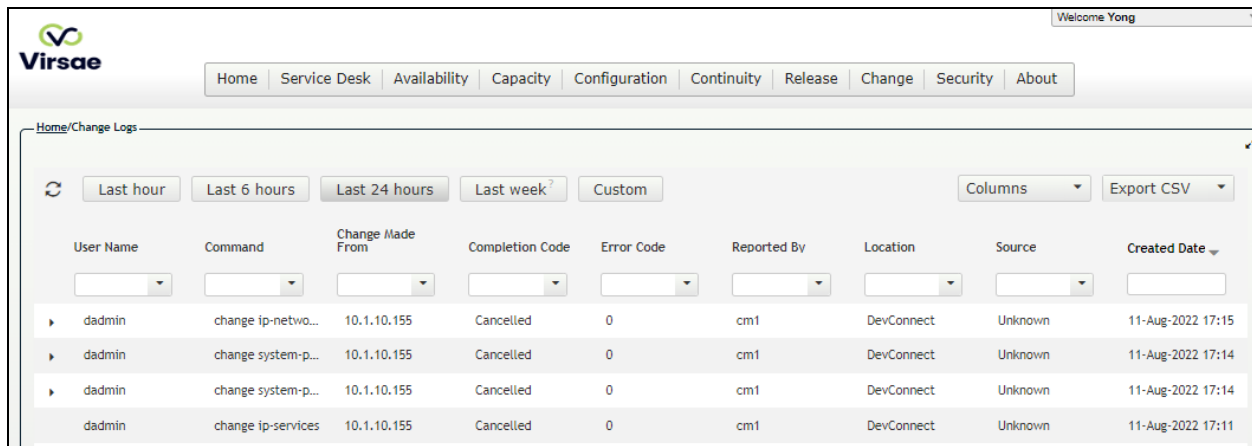
Name	Last modified	File size	Owner
xln_cm1_011128_20220812.tar.gz.zip	12-Aug-2022 1:13 AM	1.08 MB	
security_cm1_011020_20220812.tar.gz.zip	12-Aug-2022 1:13 AM	1.37 MB	
os_cm1_011001_20220812.tar.gz.zip	12-Aug-2022 1:12 AM	11.00 KB	

LYM; Reviewed:
SPOC 10/6/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

51 of 54
Virsa-CM101

To view change history of Communication Manager, navigate to **Change → View Change Logs**. Screen below shows a few examples of changes made by selecting the **Last 24 hours** tab.



User Name	Command	Change Made From	Completion Code	Error Code	Reported By	Location	Source	Created Date
dadmin	change ip-netwo...	10.1.10.155	Cancelled	0	cm1	DevConnect	Unknown	11-Aug-2022 17:15
dadmin	change system-p...	10.1.10.155	Cancelled	0	cm1	DevConnect	Unknown	11-Aug-2022 17:14
dadmin	change system-p...	10.1.10.155	Cancelled	0	cm1	DevConnect	Unknown	11-Aug-2022 17:14
dadmin	change ip-services	10.1.10.155	Cancelled	0	cm1	DevConnect	Unknown	11-Aug-2022 17:11

To view Syslog files, navigate to **Availability → SysLog → Browse Syslog Files**. Screen below shows a few examples of syslog for Communication Manager.



The top screenshot shows the Virsae interface with the 'Availability' menu open. The 'Syslog' option is selected, and the 'Browse Syslog Files' sub-menu item is highlighted.

The bottom screenshot shows the 'Browse Syslog Files' page. The left sidebar shows a tree view with 'Root', 'As Built Schematics', 'Back Up', 'DevConnect ACM 10', and 'System Log'. The 'System Log' folder is selected, and the main area displays a table of files.

Name	Last modified	File size
20220809021802149.txt.zip	11-Aug-2022 3:58 AM	1.91 MB
20220805013412443.txt.zip	07-Aug-2022 10:22 AM	1.91 MB
20220803024640984.txt.zip	05-Aug-2022 9:34 AM	1.91 MB

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R174 to interoperate with Avaya Aura® Communication 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® Communication Manager in Virtualized Environment*, Release 10.1, Issue 1, Feb 2022.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1, Issue 1, Feb 2022.
3. *Application Notes for Virsae Service Management R174 with Avaya Aura® Session Manager R10.1*.
4. *Application Notes for Virsae Service Management R174 with Avaya Aura® System Manager R10.1*.

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.