



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Virsae Service Management with Avaya Aura® Communication Manager - Issue 1.1**

### **Abstract**

These Application Notes describe the procedures for configuring Virsae Service Management R135 to interoperate with Avaya Aura® Communication Manager R8.1.2.

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

Virsae Service Management integrates directly to Communication Manager using Secure Shell (SSH) or Telnet 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 Telnet/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 is 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 also used 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) display 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](http://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, Workplace client for Windows, digital and analog endpoints. 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.

- A total of only five sessions with same credentials can be established with Communication Manager.
- Media Server RTCP information does not provide call path information. Avaya are investigating this issue.

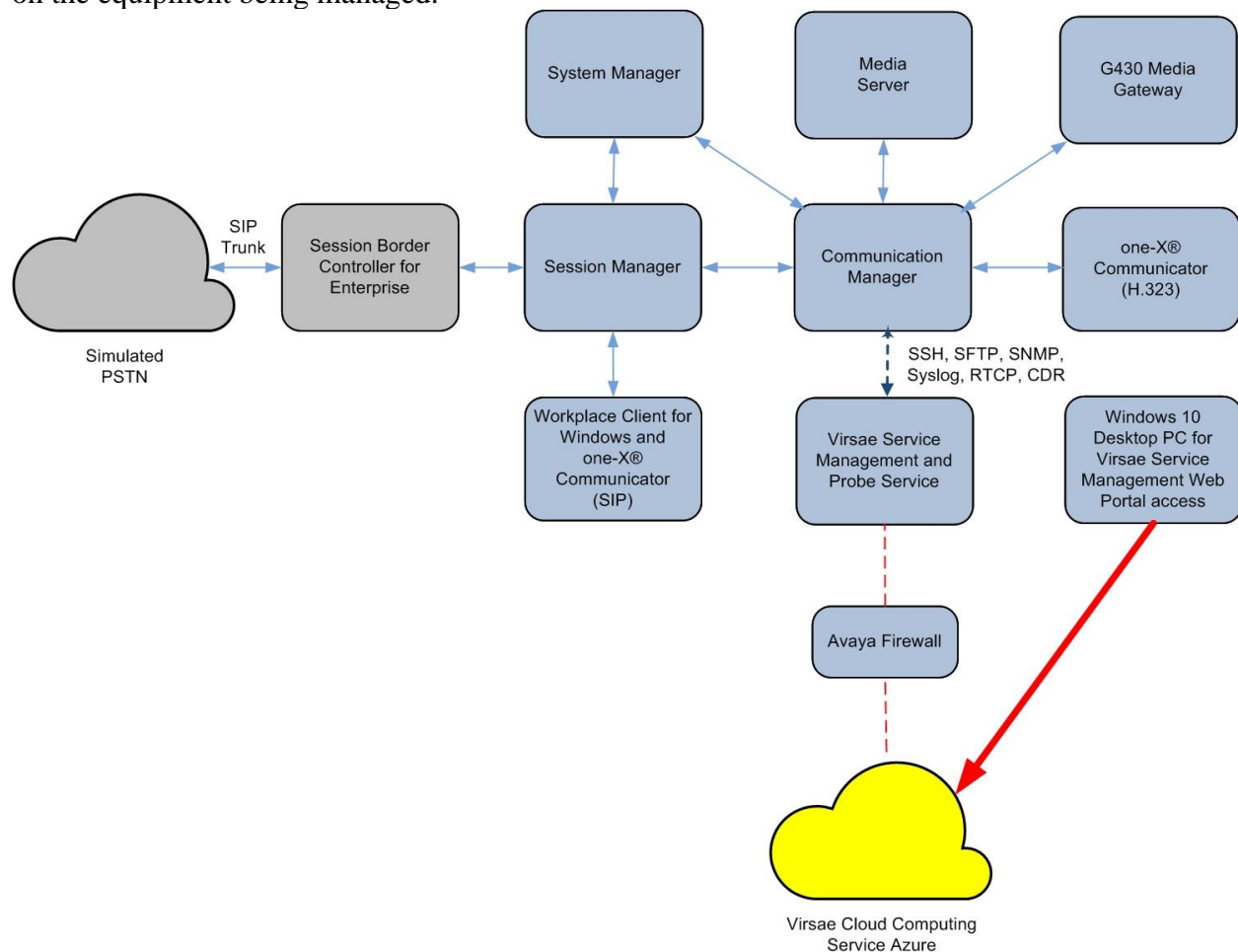
## 2.3. Support

For technical support on Virsae Service Management, contact the Virsae Support Team at:

- Tel: +1 800 248 7080 (Americas)  
+44 0808 234 2729 (UK and Europe)  
+64 9 477 0696 (Asia Pacific)
- Email: [support@virsae.com](mailto:support@virsae.com)

### 3. Reference Configuration

**Figure 1** illustrates the test configuration used to verify VSM interoperability with Communication Manager. The configuration consists of a Communication Manager system with an Avaya G430 Media Gateway. The system has Workplace Client for Windows and one-X® Communicator (SIP and H.323) softphones configured for making and receiving calls. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. VSM was installed on a server running Microsoft Windows Server 2016. Architecturally the VSM Service relies on an appliance being placed on a corporate LAN and being configured to connect to a Unified Communication platform as well as the Microsoft Azure cloud via the internet. The VSM appliance contains Probe Service use to collect service management data. The VSM appliance acts as a collector and compresses, encrypts then forwards data from all sources to the Virsae cloud computing service. A PC/Laptop is used to access the Virsae portal to manage VSM services, add additional users and view reporting data on the equipment being managed.



**Figure 1: Test Configuration**

## 4. Equipment and Software Validated

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

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

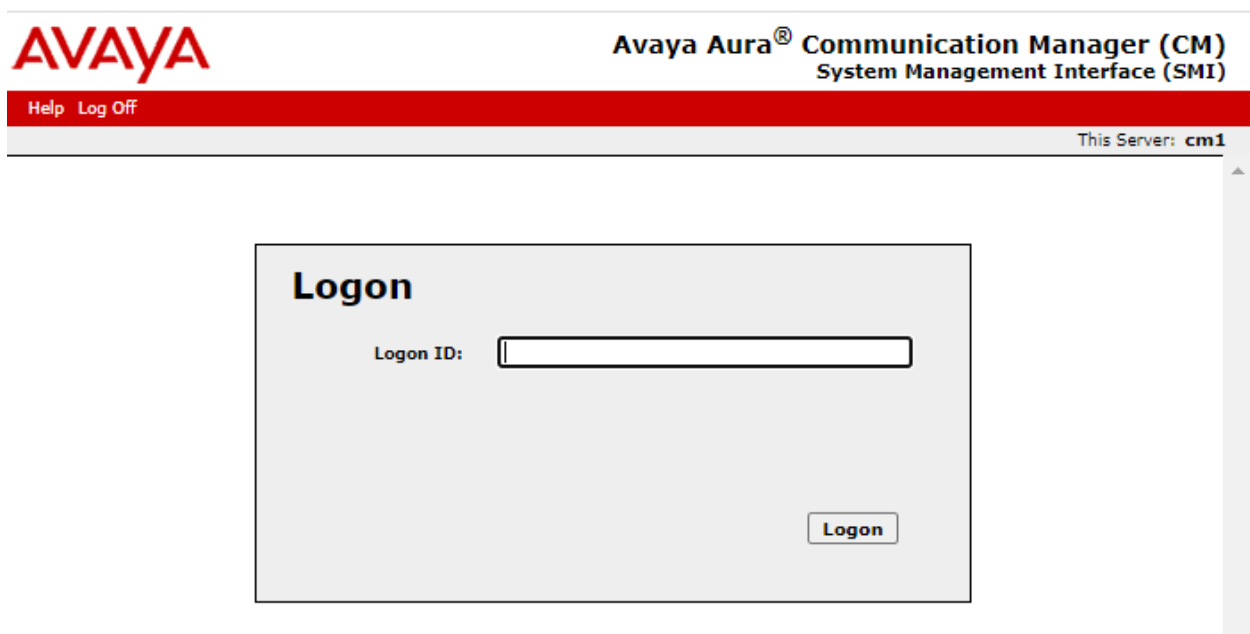
## 5. Configure Avaya Aura® Communication Manager

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.

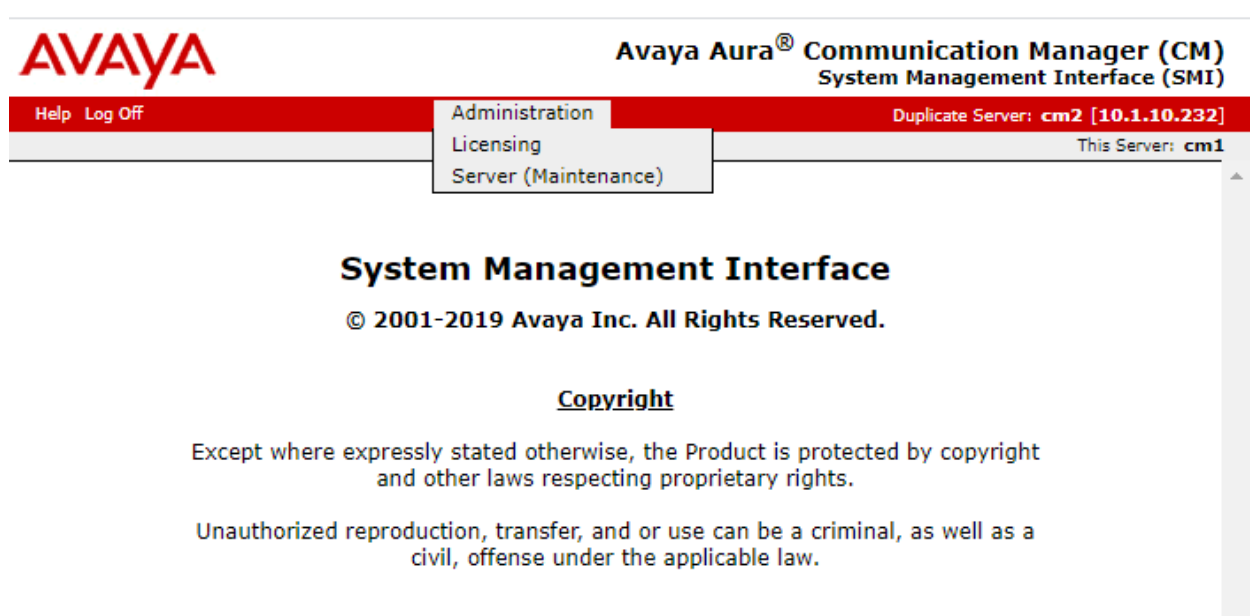
Using a web browser, enter ***https://<IP address of Communication Manager>*** to connect to the Communication Manager server being configured and log in using appropriate credentials.



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. On the right side of the page, it says "This Server: cm1". The main content area is a light gray box with the title "Logon". Inside this box, there is a label "Logon ID:" followed by a text input field. At the bottom right of the box is a "Logon" button.



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**. Select **Add Login** and **Privileged Administrator** to create a new login account with privileged rights. Click **Submit**.

The screenshot shows the Avaya Aura Communication System Management interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® Communication System Management", and links for "Help", "Log Off", "Administration", and "Duplicate Server". Below this is a breadcrumb trail: "Administration / Server (Maintenance)".

The left sidebar contains a navigation menu with the following categories and items:

- FP trap test
- FP Filters
- Diagnostics**
  - Restarts
  - System Logs
  - Ping
  - Traceroute
  - Netstat
- Server**
  - Status Summary
  - Process Status
  - Interchange Servers
  - Busy-Out/Release Server
  - Shutdown Server
  - Server Date/Time
  - Software Version
- Server Configuration**
  - Server Role
  - Network Configuration
  - Duplication Parameters
  - Static Routes
  - Display Configuration
  - Time Zone Configuration
  - NTP Configuration
- Server Upgrades**
  - Pre Update/Upgrade Step
  - Manage Updates
- IPSI Firmware Upgrades**
  - IPSI Version
  - Download IPSI Firmware
  - Download Status
  - Activate IPSI Upgrade
  - Activation Status
- Data Backup/Restore**
  - Backup Now
  - Backup History
  - Schedule Backup
  - Backup Logs
  - View/Restore Data
  - Restore History
- Security**
  - Administrator Accounts**

The main content area is titled "Administrator Accounts". It includes a description: "The Administrator Accounts SMI pages allow you to add, delete, or change Linux groups." Below this is a "Select Action:" section with the following options:

- ☒ Add Login
  - ☐ Privileged Administrator
  - ☐ Unprivileged Administrator
  - ☐ SAT Access Only
  - ☐ Web Access Only
  - ☐ CDR Access Only
  - ☐ Business Partner Login (dadmin)
  - ☐ Business Partner Craft Login
  - ☐ Custom Login
- ☐ Change Login
- ☐ Remove Login
- ☐ Lock/Unlock Login
- ☐ Add Group
- ☐ Remove Group

At the bottom of the form are two buttons: "Submit" and "Help".

For the field **Login name**, enter the login. In this configuration, the login **Virsa**e 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 Administrator**

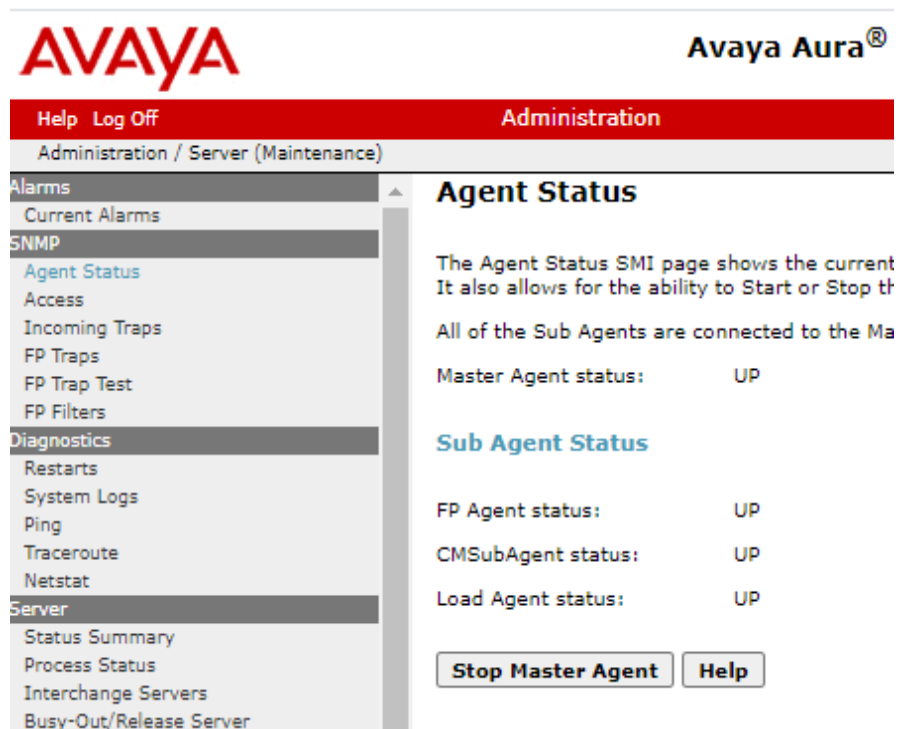
This page allows you to add a login that is a member of the **SUSERS** group. This login has system next to root.

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 checked="" type="radio"/> No <input type="radio"/> Yes

## 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.



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 shows the Avaya Aura® Communication Manager Administration interface. The left navigation pane is expanded to show the 'FP Traps' option under the 'SNMP' category. The main content area displays the 'FP Traps' configuration page. At the top, there is a red header bar with 'AVAYA' on the left and 'Avaya Aura® Commu System' on the right. Below this is a red bar with 'Help Log Off' on the left, 'Administration' in the center, and a 'D' icon on the right. The navigation pane on the left lists various categories: Alarms, SNMP, Diagnostics, and Server. The 'FP Traps' page content includes a note about the SMI page, a master agent status of 'UP', a link to view MIB data, and a table for current settings with columns for IP address, Port, Notification, SNMP Version, and Community / User Name. At the bottom, there are three buttons: 'Add/Change', 'Delete', and 'Help'.

**AVAYA** Avaya Aura® Commu System

Help Log Off Administration D

Administration / Server (Maintenance)

**FP Traps**

The FP Traps page allows specification of the alarms to be

**Note:**

- The FP Traps SMI page is for the administration of CM is not for INADS. INADS traps are configured using the "almsnmpconf" CLI command. Additionally, Fault Perfo 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

**Add/Change** **Delete** **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:	<input type="text"/>	Port:	<input type="text" value="162"/>
Notification:	<input type="text" value="trap"/>		
Community Name:	<input type="text"/>		

#### SNMP Version 2c

IP address:	<input type="text" value="10.1.10.124"/>	Port:	<input type="text" value="162"/>
Notification:	<input type="text" value="trap"/>		
Community Name:	<input type="text" value="avaya123"/>		

#### SNMP Version 3

IP address:	<input type="text"/>	Port:	<input type="text" value="162"/>
Notification:	<input type="text"/>		
User Name:	<input type="text"/>		
Authentication Protocol:	<input type="text"/>		
Authentication Password:	<input type="text"/>		Minimum 8 characters. (for
privacy)			
Privacy Protocol:	<input type="text"/>		
Privacy Password:	<input type="text"/>		Minimum 8 characters. (for
Engine ID:	<input type="text"/>		

**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.

- **Success: Requested FP trap destination successfully added.**
- **Administration successfully changed.**



**Note:**

- The FP Traps SMI page is for the administration of CM Fault Performance Traps only. It is not for INADS. INADS traps are configured using the "almenable" and the "almsnmpconf" CLI command. Additionally, Fault Performance Traps should not be 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	Privacy Password	Privacy Protocol	Engine ID
<input type="checkbox"/>	10.1.10.124	162	trap	2c	avaya123						
<div><div>Add/Change</div><div>Delete</div><div>Help</div></div>											

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
Virsaes                           10.1.10.124
( 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.Virsaes                                              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.

Syslog Server Result

- The logging configurations have been changed

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 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	10.1.10.124	<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**'.

```
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.
- **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.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help', 'Log Off', 'Administration', and 'Duplicate Server: cm2 [10.1.10.232]'. The left sidebar shows a tree view with categories like 'Diagnostics', 'Server', 'Server Configuration', 'Server Upgrades', 'IPSI Firmware Upgrades', 'Data Backup/Restore', and 'Security'. The 'Data Backup/Restore' category is expanded, showing 'Backup Now', 'Backup History', 'Schedule Backup', 'Backup Logs', 'View/Restore Data', and 'Restore History'. The main content area is titled 'Add New Schedule' and contains the following sections:

- Data Sets:** Includes radio buttons for 'Specify Data Sets' (selected) and 'Full Backup'. Under 'Specify Data Sets', there are checkboxes for 'Server and System Files', 'Security File', and 'Avaya Call Processing (ACP) Translations'. The 'Do NOT save ACP translations prior to backup' option is selected.
- Backup Method:** Includes a radio button for 'Network Device' (selected). Below it, there are fields for 'Method' (set to 'sftp'), 'User Name' (set to 'virsaae'), 'Password' (masked with dots), 'Host Name' (set to '10.1.10.124'), and 'Directory' (set to '/').
- Encryption:** Includes a checkbox for 'Encrypt backup using pass phrase'.
- Day of Week:** Includes checkboxes for 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday', all of which are checked.
- Start Time:** Includes a time selection field set to '01:10'.

At the bottom of the form, there is a note: 'Backups are scheduled once per week on each of the days selected. All backups begin at the same time.' Below this note are two buttons: 'Add New Schedule' and 'Help'.

## 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 [2] 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? y
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 [3] 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: 10.1.10.124      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. Administrative Rights Login

VSM requires access to the Avaya Media Server using a login that has Administrative Rights. This login/password needs to be provided by the customer since the Avaya Media Server does not support the creation of custom logins.

### 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.



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:

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

The screenshot shows the Avaya Aura® Media Server Element Manager web interface. At the top left is the Avaya logo. To its right is the title "Avaya Aura® Media Server" and a navigation bar with "Help | Sign Out admin". Below the title bar, a grey header indicates "Managing: aams1.sglab.com, 10.1.10.13" with a "Home" link and a status icon. A left-hand navigation pane is visible, containing a tree structure with categories like "System Status", "Applications", "Cluster Configuration", and "System Configuration". The main content area displays the "Avaya Aura® Media Server" title, a welcome message for the Element Manager, the installed software package "Avaya Aura® Media Server - v.8.0.2.93", a link to "help", and a red arrow icon pointing left with the text "Please 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**.

## Avaya Aura® Media Server

Managing: aams1.sglab.com, 10.1.10.13

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

### General Settings

This task allows administrators to view and modify media general settings.

[QOS Monitoring](#) | [QOS Streaming](#) | [Media Audits](#) | [Network Address Translation](#) | [Google Speech Recognition](#) | [Cloud Text Speech](#) | [IBM Watson Text-To-Speech](#) | [Aurix Speech Search Engine](#) | [Dual Unicast Monitoring](#) | [Compositor Resource](#)

#### Google Text-To-Speech

Enable Google Cloud Text-To-Speech: ☐ 

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



Google Cloud Referer 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)

### 5.8.3. Configure Syslog

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

**Avaya Aura® Media Server**Help | Sign

Managing: aams1.sglab.com, 10.1.10.13  
[Home](#) » [System Configuration](#) » [Logging Settings](#)

## Logging Settings

[Privacy](#) | [SysLog](#) | [Session Logging](#) | [OMs](#) | [Event Log](#) | [Data Collection](#)

**Privacy**

Mask Sensitive Data: ☐ Select all

☐ Digit Collection☐ Announcements and Prompts☐ Text-To-Speech☐ Speech Recognition

**SysLog**

SYSLOG Delivery of Logs: ☒


SYSLOG Destination Server List:

<input checked="" type="checkbox"/>	<a href="#">Server Address</a> ▲	Port (0 - 65535)
<input checked="" type="checkbox"/>	10.1.10.124	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**.



Avaya Aura® Media Server

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

Managing: aams1.sglab.com, 10.1.10.13

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

## SNMP

SNMP consist of tasks that allow administrators to view and modify SNMP settings.

[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**.

## Avaya Aura® Media Server

Managing: aams1.sglab.com, 10.1.10.13

[Home](#) » [System Configuration](#) » [Network Settings](#) » [SNMP](#) » [Users](#) » Add User

### Add User

Security name:   
(Allowed characters: a-zA-Z0-9\_-)

Description:

Version:

Access rights:

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: aams1.sglab.com, 10.1.10.13



[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


Managing: aams1.sglab.com, 10.1.10.13


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

## Traps Destinations

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

### General Settings

SNMP Alarm Delivery Traps: ☒ 

SNMP Event Log Delivery Traps: ☐ 

### Traps Destinations

Add... Edit... Delete

<input type="checkbox"/>	<a href="#">Destination address</a> ▲	<a href="#">Destination port</a>
1 <input type="checkbox"/>	<a href="#">10.1.10.124</a>	162

### Traps Routes

Add... Edit... More Actions ▼

<input type="checkbox"/>	<a href="#">Destination address</a> ▲	<a href="#">Destination port</a>	<a href="#">Security name</a>	<a href="#">Security model</a>
1 <input type="checkbox"/>	<a href="#">10.1.10.124</a>	162	avaya123	v1v2c

## 6. Configure Virsae Service Management

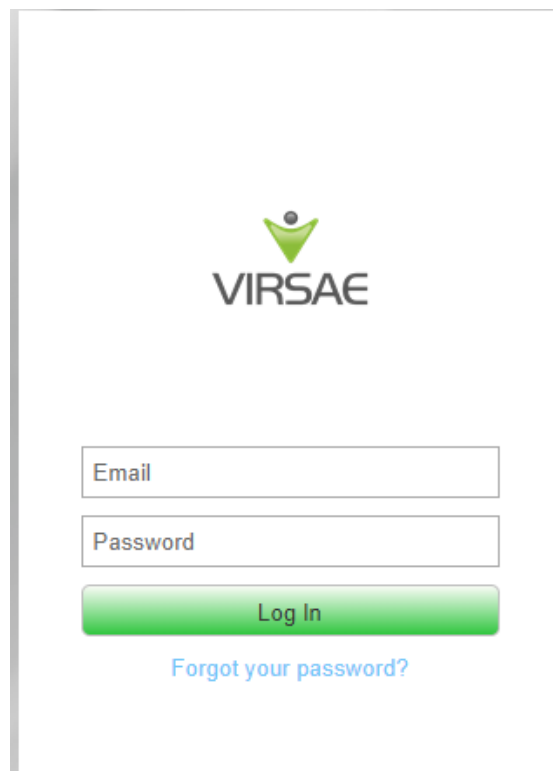
This section describes the configuration of VSM required to interoperate with Communication Manager. Configuration of VSM to interoperate with Session and System Manager can be referred from reference [3] and [4] in **Section 9** and will not be detailed here.

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 *<business partner name>.virsae.com* in a web browser. During compliance testing the URL used was “*preview.virsae.com*”. The Login screen is shown as below. Enter the **Email** and **Password** and click on the **Log In** button.

The image shows a login screen for the Virsae web portal. At the top center is the Virsae logo, which consists of a green stylized figure with arms raised above the word "VIRSAE" in a bold, sans-serif font. Below the logo are two input fields: the first is labeled "Email" and the second is labeled "Password". Both labels are in a small, grey font and are positioned to the left of their respective input boxes. Below these fields is a green button with the text "Log In" in white. At the bottom of the login area is a blue hyperlink that says "Forgot your password?". The entire login form is enclosed in a thin grey border.

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





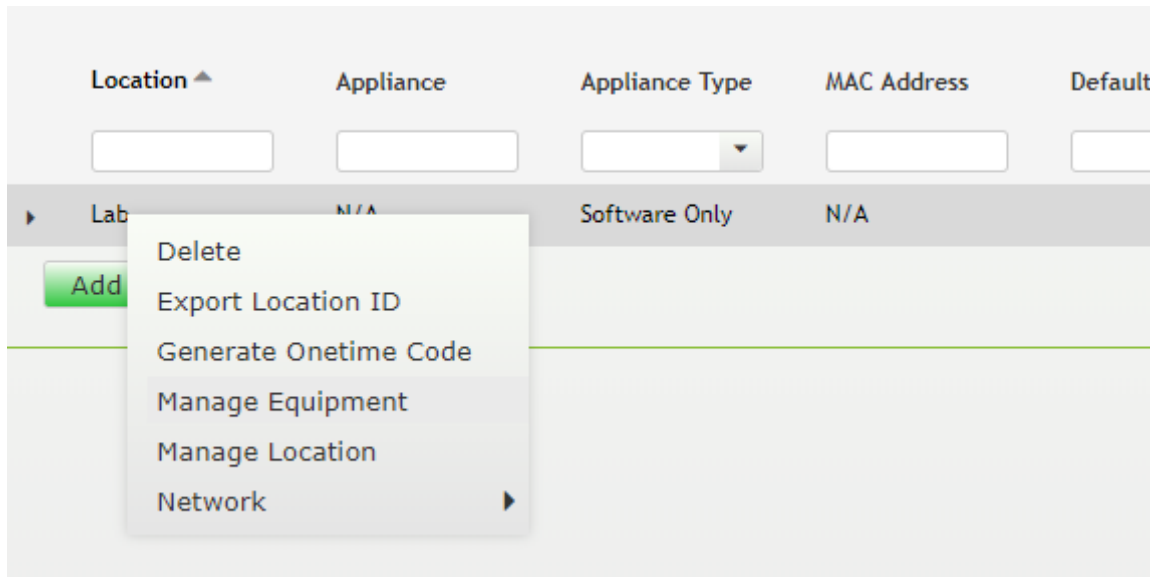
Navigate to **Service Desk** → **Equipment Locations** as shown below.

The screenshot displays the VIRSAE Service Desk interface. The top navigation bar includes links for Home, Service Desk, Availability, Capacity, Configuration, Continuity, Release, Change, Security, and About. The main content area is titled 'Home/Equipment Locations [Dates shown are Singapore time zone]'. It features a table with the following columns: Location, Appliance, Appliance Type, MAC Address, Default Site, Last HeartBeat, Controller Version, Running VM List, and Running Time. The table contains one entry: 'Lab' with 'N/A' for Appliance, 'Software Only' for Appliance Type, 'N/A' for MAC Address, and '0 s' for Running Time. An 'Add Location' button is located below the table. A dropdown menu is open from the 'Service Desk' tab, showing options: Access Concentrator, Call Details, CMS Call History, Dashboards, Equipment Locations (highlighted), Files and Folders, Manage Customer, Reports, and More. The background features a diagram with 'Service Desk' and 'Availability Manager' icons.

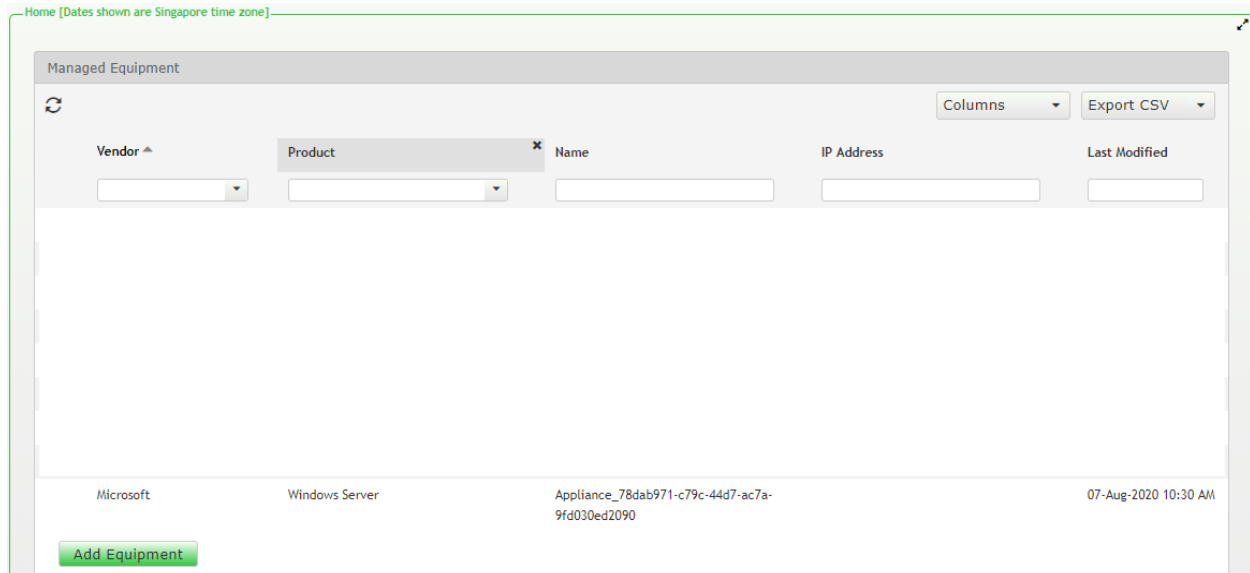
A **Location** called **Lab** is already configured as shown below.

This screenshot shows the same VIRSAE Service Desk interface as the previous one, but with the 'Equipment Locations' dropdown menu closed. The table still shows the 'Lab' location with 'N/A' for Appliance, 'Software Only' for Appliance Type, 'N/A' for MAC Address, and '0 s' for Running Time. The 'Add Location' button is still present below the table.

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



Click **Add Equipment** below:



## 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 **Communication Manager** 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:** “Lab” location is selected in this case.

The screenshot shows the 'Add Equipment' configuration window for Avaya Aura Communication Manager. The 'Equipment' tab is selected. The configuration fields are as follows:

Field	Value
Vendor *	Avaya
Product *	Communication Manager
Equipment Name *	Communication Manager
Username *	Virsae
IP Address/Host Name *	10.1.10.230
Password *	.....
Site ⓘ	DevConnect
ACM Details	
Username for Media Gateways	virsae
Associated RTCP Receiver	Lab
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 ⓘ

At the bottom of the window are three buttons: **Save**, **Test Access**, and **Cancel**.

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 to complete the configuration.

Equipment

SNMP Query

Custom Scripts

Site Mappings

Virsa Direct can be configured to query this Communication Manager for configuration and system health metrics, which are used in the dashboards, and historic reports.

To enable this, please enter the SNMP configuration details for this Communication Manager below.

Version

SNMP Community String \*

V2

avaya123

Avaya Phones

When configuring an ACM or IP Office, Virsa Direct can also query the Avaya phones associated with the ACM. The configuration data obtained is used to populate historic station data reports, end point summaries, and voice quality associated with Avaya handsets.

To enable this, please enter the SNMP community string for the Avaya phones below. Please note that the list below is used to configure all ACMs in this location, not just this piece of equipment.

SNMP Community String\*

+

avaya123

Save

Test Access

Cancel

Navigate to **Service Desk → Equipment Locations** (not shown), right click on the **Lab** and select **Manage Locations** (not shown). Select the **File Transfer** tab. Check **Enable SFTP** is turn on i.e., tick and configure the SFTP user accounts for Communication Manager backup.

- **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**.

Details	Appliance	SNMP Traps	File Transfer	VQM
---------	-----------	------------	---------------	-----

VSM provides various methods for uploading data, which can be configured below. Data uploads can be used as an offsite back-up, and for collecting voice quality information, syslog and other data from unified communication servers and adjuncts.

☐ Enable TFTP

☐ Enable FTP

☐ Enable UUCP

#### SFTP and SCP Configuration



☒ Enable SFTP

☐ Enable SCP

Port

22

#### SFTP and FTP user accounts

User Name *	Password *	Protocol	Upload Type	Public Key	
devconnect	.....	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 described in **Section 5.8**.
- **Password:** The password described in **Section 5.8**.
- **IP Address/Host Name:** IP address of Media Server.
- **Site:** A descriptive site name.

Edit Equipment

Equipment

SNMP Query

Vendor \*

Avaya

Product \*

Media Server

Equipment Name \*

Media Server

Username \*

virsa

IP Address/Host Name \*

10.1.10.13

Password \*

.....

Site ⓘ

Lab

Save

Test Access

Cancel

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.

Edit Equipment

Equipment

SNMP Query

Virsa Direct can be configured to query this Media Server for configuration and system health metrics, which are used in the dashboards, and historic reports.

To enable this, please enter the SNMP configuration details for this Media Server below.

Version

SNMP Community String \*

V2

avaya123

Save

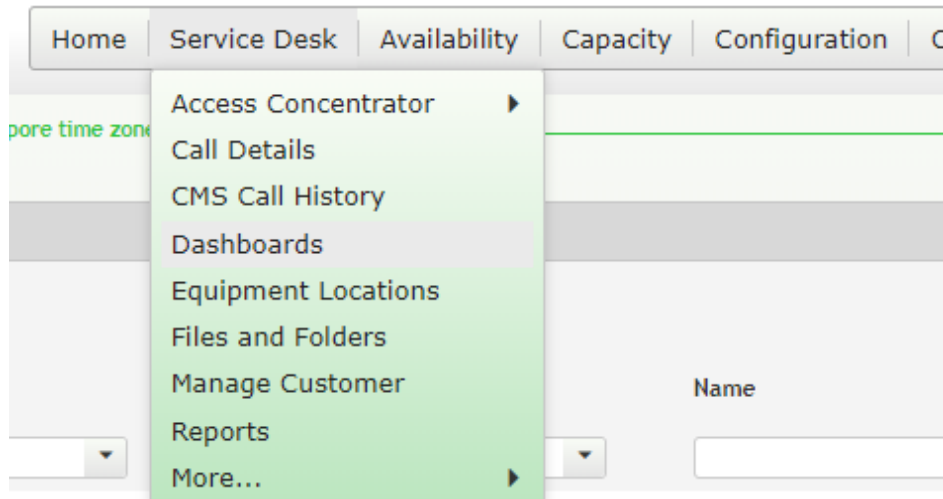
Test Access

Cancel

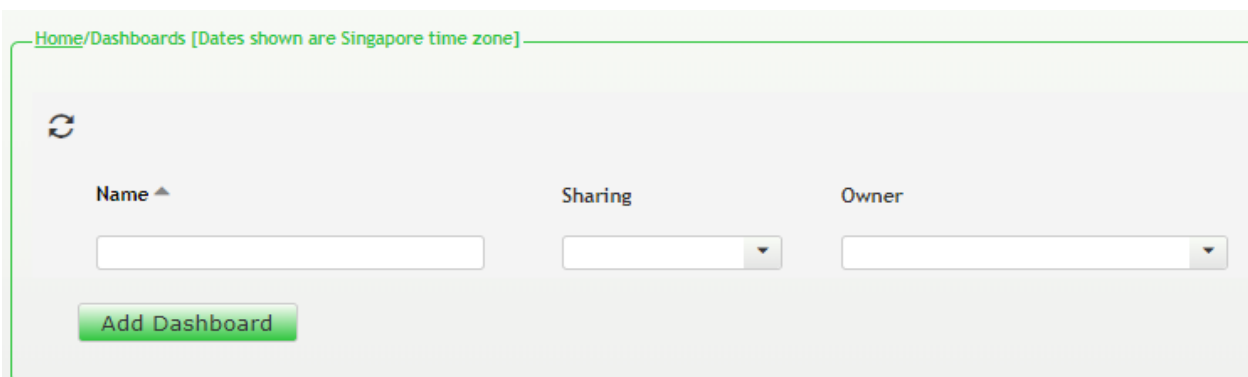
## 6.4. Configure Dashboard

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

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



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





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

The screenshot shows a window titled "Add Dashboard". It contains the following fields and controls:

- Name:** A text input field containing "Devconnect Lab".
- Sharing:** A dropdown menu showing "Private".
- Owner:** A text input field containing "Yong Meng Low".
- Description:** A large, empty text area.
- Start dashboard automatically on log in:** A checkbox that is checked.
- Buttons:** "Ok" and "Cancel" buttons at the bottom right.

---

Add Dashlet

system health

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

ACM System Health Summary

Lab

Select “Lab” for the **Location** drop-down menu, the appropriate **Equipment** i.e., **Communication Manager** and click **Done** (not shown).

Settings

Dashboard

All Dashlets

ACM System Health Summary  
Lab

Active Streams  
Lab | Lab

Alarms Summary  
DevConnect

Avaya Application Enablement Services (AES)  
Lab | AES

Avaya Call Management System (CMS)  
Lab | Call Management System

Avaya Communication Manager (ACM)  
Lab | Communication Manager

Avaya Experience Portal (AEP)  
DevConnect, Lab | AAEP EPM

Avaya Experience Portal (AEP)  
DevConnect, Lab | AAEP MPP

Avaya Session Border Controller (ASBC)  
Lab | SBCE

Avaya Session Manager (SM)  
Lab | Session Manager1

Avaya Session Manager (SM)

Customer  
DevConnect

Location  
Lab

Equipment  

Communication Manager

AES

Call Management System

AAEP EPM

AAEP MPP

Media Server

SBCE

Session Manager1




Session Manager2

System Manager

Appliance\_78dab971-c79c-44d7-ac7a-9fd030ed2090

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

Avaya Communication Manager (ACM)  
Lab | Communication Manager



Settings

Dashboard

All Dashlets

Active Streams  
Lab | Lab

Alarms Summary  
DevConnect

Avaya Application Enablement Services (AES)  
Lab | AES

Avaya Communication Manager (ACM)  
Lab | Communication Manager

Avaya Experience Portal (AEP)  
DevConnect, Lab | AAEP EPM

Avaya Experience Portal (AEP)  
DevConnect, Lab | AAEP MPP

Avaya Session Manager (SM)  
Lab | Session Manager1

Avaya Session Manager (SM)  
Lab | Session Manager2

Calls In Progress  
Lab | Lab

Linux Server  
Lab | Media Server

Linux Server  
Lab | System Manager

Multiple Trunk Groups Traffic  
Lab | Communication Manager

System Health Summary  
Lab

Customer  
DevConnect

Location  
Lab

Equipment

☒ Communication Manager

☐ AES

☐ AAEP EPM

☐ AAEP MPP

☐ Media Server

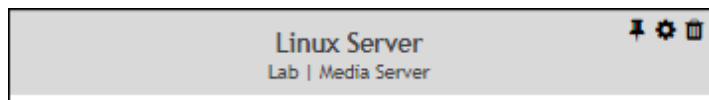
☐ Session Manager1

☐ Session Manager2

☐ System Manager

☐ Appliance\_78dab971-c79c-44d7-ac7a-9fd030ed2090

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



Settings

Dashboard

All Dashlets

Active Streams  
Lab | Lab

Alarms Summary  
DevConnect

Avaya Application Enablement Services (AES)  
Lab | AES

Avaya Call Management System (CMS)  
Lab | Call Management System

Avaya Communication Manager (ACM)  
Lab | Communication Manager

Avaya Experience Portal (AEP)  
DevConnect, Lab | AAEP MPP

Avaya Experience Portal (AEP)  
DevConnect, Lab | AAEP MPP

Avaya Session Border Controller (ASBC)  
Lab | SBCE

Avaya Session Manager (SM)  
Lab | Session Manager1

Avaya Session Manager (SM)  
Lab | Session Manager2

Calls In Progress  
Lab | Lab

Linux Server  
Lab | Media Server

Linux Server  
Lab | System Manager

Customer  
DevConnect

Location  
Lab

Equipment  
Media Server

ACM

Communication Manager

AES

AES

CMS

Call Management System

Experience Portal

AAEP EPM

AAEP MPP

Media Server

Media Server

SBC

SBCE

Session Manager

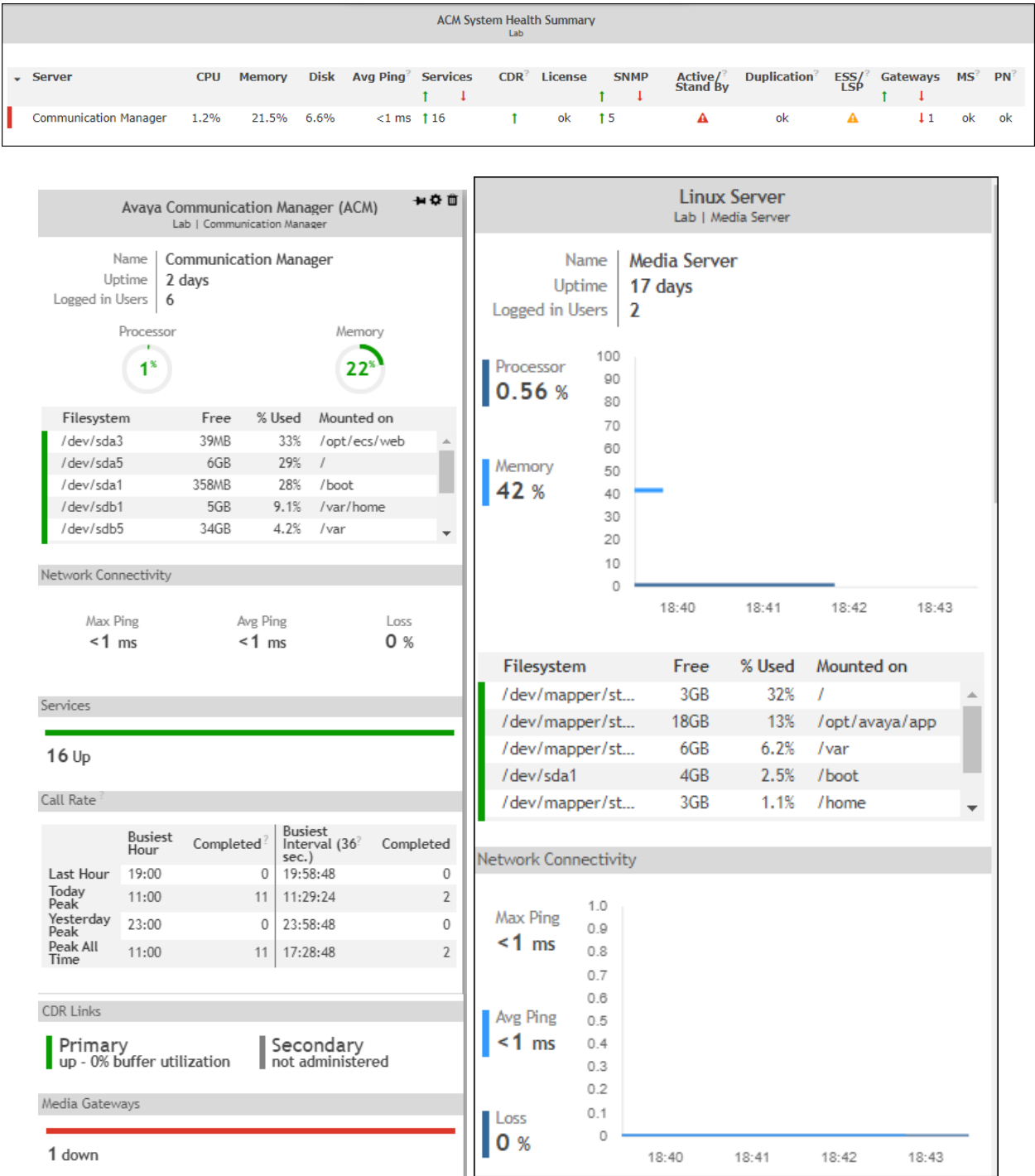
Session Manager1

Session Manager2

System Manager

System Manager

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@cml> who -u
Virsaes pts/0      2020-08-31 11:32 .          21599 (10.1.10.124)
Virsaes pts/1      2020-08-31 11:32 .          21537 (10.1.10.124)
Virsaes pts/2      2020-08-31 11:32 .          21574 (10.1.10.124)
Virsaes pts/3      2020-08-31 11:32 .          21639 (10.1.10.124)
dadmin  pts/4      2020-08-31 10:30 .          11810 (10.1.10.155)
Virsaes pts/5      2020-08-27 12:55 .          10243 (10.1.10.124)
dadmin@cml>
```

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      10.1.10.124         stat logins         3
Virsaes    18      10.1.10.124         stat logins         4
Virsaes    18      10.1.10.124         stat logins         5
Virsaes    18      10.1.10.124         stat logins         6
*dadmin    18      10.1.10.155         stat logins         7
```

Using the `status cdr-link` command, verify that the **Link State** of the primary CDR link configured in **Section 5.5** shows **up**.

```
status cdr-link

CDR LINK STATUS

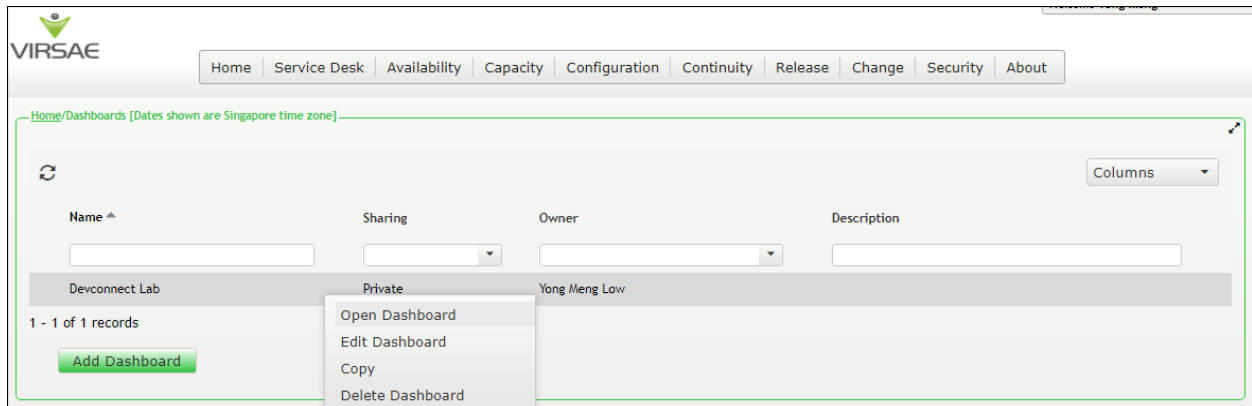
Primary      Secondary
-----
Link State: up      CDR not administered

Date & Time: 2020/08/27 12:20:05      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 → Dashboard** (not shown) and the screen is shown as below. Right click “Devconnect lab” and select “Open Dashboard”.



Whatever is configured during setup will be shown here. However, if the dashboard is configured to open automatically on startup in **Section 6.4**, 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 and Media Server equipment.

Welcome Yong Meng

[Home](#) | [Service Desk](#) | [Availability](#) | [Capacity](#) | [Configuration](#) | [Continuity](#) | [Release](#) | [Change](#) | [Security](#) | [About](#)

Unresolved Alarms for DevConnect [Dates shown are 'Singapore' time zone]

Alarm List Filter - CM

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

Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Vendor	Severity
SIP-SGRP	A SIP Signaling Group is down. A S...	2020-08-17 19:47:03	8	1	Communicati...	Avaya	2
SIP-SGRP	A SIP Signaling Group is down. A S...	2020-08-17 19:47:03	7	1	Communicati...	Avaya	2
GAM	The Global Alarm Manager determi...	2020-08-17 18:06:10	Unknown	0	Communicati...	Avaya	4
Media Server Out Of Service	The list media server command on ...	2020-08-17 17:54:47	2	55	Communicati...	Avaya	4
FSY	The File Synchronization (FSY) pro...	2020-08-17 17:24:44	A	5	Communicati...	Avaya	2
IPMEDPRO	IP Media Processor Alarm Check Cir...	2020-08-17 17:03:42	01A14	62	Communicati...	Avaya	2
IPMEDPRO	IP Media Processor Alarm Check Cir...	2020-08-17 17:03:33	02A08	14	Communicati...	Avaya	2
IPMEDPRO	IP Media Processor Alarm Check Cir...	2020-08-17 17:03:33	02A07	14	Communicati...	Avaya	2
MED-GTWY	The MED-GTWY alarm indicates a p...	2020-08-17 17:02:45	003	15	Communicati...	Avaya	2

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

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

Manage Filters

Filters: VQM\_24\_HOUR\_SUMMARY\_Lab

Expression (condition)

Details

- Location = Lab
- Date From >= 13 August 2020 01:00:00 AM
- Date To <= 14 August 2020 01:00:00 AM
- RTCP Receiver Name = Lab

Save Save All Apply

VQM - Streams

Columns Export CSV

Name	Endpoint	IPNR	Mos Min	Mos Max	Mos Avg	Stream Length	IP Address	Port	DSCP	Call
	10001	0	4.41	4.41	4.41	30	10.1.10.155		-1	
	gwp	0	4.41	4.41	4.41	30	10.1.10.32		46	
	gwp	0	4.41	4.41	4.41	20	10.1.10.32		46	
	10001	0	4.41	4.41	4.41	0	10.1.10.155		-1	
	gwp	0	4.41	4.41	4.41	0	10.1.10.32		46	
	10001	0	4.41	4.41	4.41	0	10.1.10.155		-1	
	10001	0	4.41	4.41	4.41	0	10.1.10.155		-1	
	gwp	0	4.41	4.41	4.41	0	10.1.10.32		46	
	10001	0	4.41	4.41	4.41	0	10.1.10.155		-1	

1 - 12 of 12 records

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.

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

Call Details Filters

Filters: CDR

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

Details

- Location = Lab
- Equipment = Communication Manager
- Date Time Range: Last 24 hours

Save Save All Apply

Call Details

Columns Export CSV

Call Start Date-Time	Mos Min	Mos Max	Mos Avg	Owner DN	Duration Seconds	Dialed Number	Calling Number	Condition	Access Code Dialed	Ac
2020-08-26 09:45:56	0 - 5	0 - 5	0 - 5	10049	12	10000	10049	7	8	
2020-08-26 09:46:02	4.41	4.41	4.41	10001	6	33411311	10001	7	8	
2020-08-26 09:58:31	4.41	4.41	4.41	10004	18	10004	33411311	9		
2020-08-26 09:58:37	4.41	4.41	4.41	10004	12	10004	33411311	9		
2020-08-26 10:00:14	4.41	4.41	4.41	10004	54	10004	33411311	9		

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

VIRSAE

Home Service Desk Availability Capacity Configuration Continuity Release Change Security About

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

Search Files and Folders

Back Up

Name	Last modified	File size	Owner
full_cm1_095556_20200813.tar.gz.zip	13-Aug-2020 9:57 AM	3.25 MB	Virsa (auto - generated)

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.

Home/Change Logs

Home Service Desk Availability Capacity Configuration Continuity Release **Change** Security About

View Change Logs  
Change Calendar

Columns Export CSV

User Name	Command	Change Made From	Completion Code	Error Code	Reported By	Location	Source	Created Date
dadmin	change vector 1 ...	10.1.10.155	Success	0	cm1	Lab	Unknown	17-Aug-2020 19:52
dadmin	add announcem...	10.1.10.155	Success	0	cm1	Lab	Unknown	17-Aug-2020 19:52
dadmin	add announcem...	10.1.10.155	Success	0	cm1	Lab	Unknown	17-Aug-2020 19:52
dadmin	add announcem...	10.1.10.155	Success	0	cm1	Lab	Unknown	17-Aug-2020 19:52
dadmin	change mst defa...	10.1.10.155	Cancelled	0	cm1	Lab	Unknown	17-Aug-2020 19:43
dadmin	change signaling...	10.1.10.155	Cancelled	0	cm1	Lab	Unknown	17-Aug-2020 19:43

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

Welcome Yong Meng

Home Service Desk **Availability** Capacity Configuration Continuity Release Change Security About

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

Manage Alarms  
Resolve All Alarms  
Network Connectivity Logs  
Call Out Lists  
Options  
Reports  
Management  
Syslog  
Voice Quality Management  
Events  
SIP Session Trace

System Log

Search

Name	Last modified	File size	Owner
Browse Syslog Files	PM	1.91 MB	Virsa (auto - generated)
	17-Aug-2020 7:55 PM	1.91 MB	Virsa (auto - generated)
20200817113049603.txt.zip	17-Aug-2020 7:41 PM	1.91 MB	Virsa (auto - generated)
20200817112014426.txt.zip	17-Aug-2020 7:31 PM	1.93 MB	Virsa (auto - generated)

## 8. Conclusion

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

## 9. Additional References

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

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

1. *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 5, Jun 2020.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1.x, Issue 8, May 2020.
3. *Application Notes for Virsae Service Management R135 with Avaya Aura® Session Manager R8.1.2*.
4. *Application Notes for Virsae Service Management R135 with Avaya Aura® System Manager R8.1.2*.

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

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

---

**©2021 Avaya Inc. All Rights Reserved.**

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

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