



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Virsae Service Management with Avaya Call Management System - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R135 to interoperate with Avaya Call Management System R19.1.

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 monitored Avaya Call Management System using SNMP and Linux shell access and displayed monitored data on a web-based application. Virsae Service Management can also function as a collector of External Call History data which are SFTP'd from Avaya Call Management System.

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 Call Management System (herein after referred to as CMS). 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.

VSM use Linux shell access connection to monitor CMS statistics such as CPU, Memory and Disk Usage, License information and SNMP to capture alarms, and display monitored data on web-based application. In addition, it can function as a collector of CMS External Call History (ECHI) which are SFTP'd from CMS.

## 2. General Test Approach and Test Results

The general test approach was to verify VSM using SNMP and Linux shell access connections to monitor and display system status from CMS. ECHI was also verified by making inbound ACD calls to Communication Manager and display the call center data from the VSM.

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 capabilities of encrypted SSH and SFTP, and non-encrypted SNMP as requested by Virsae.

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

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

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

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

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager or the Telnet/SSH interface to interact with other Avaya products. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use of these interfaces as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the interfaces in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using these interfaces. Using these interfaces in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real-time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Avaya Product Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at [www.avaya.com/support](http://www.avaya.com/support).

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying proper display of monitored CMS data on VSM.

- Verify that the server statistics information for CMS is populated on VSM dashboard such as CPU, Memory and Disk Usage, licenses and list of Software/Processes.
- Verify alarms are received from SNMP.
- Verify the ECHI call data received from CMS to VSM via SFTP.

The serviceability testing focused on verifying the ability of VSM to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to VSM and rebooting the VSM.

## **2.2. Test Results**

All test cases passed successfully.

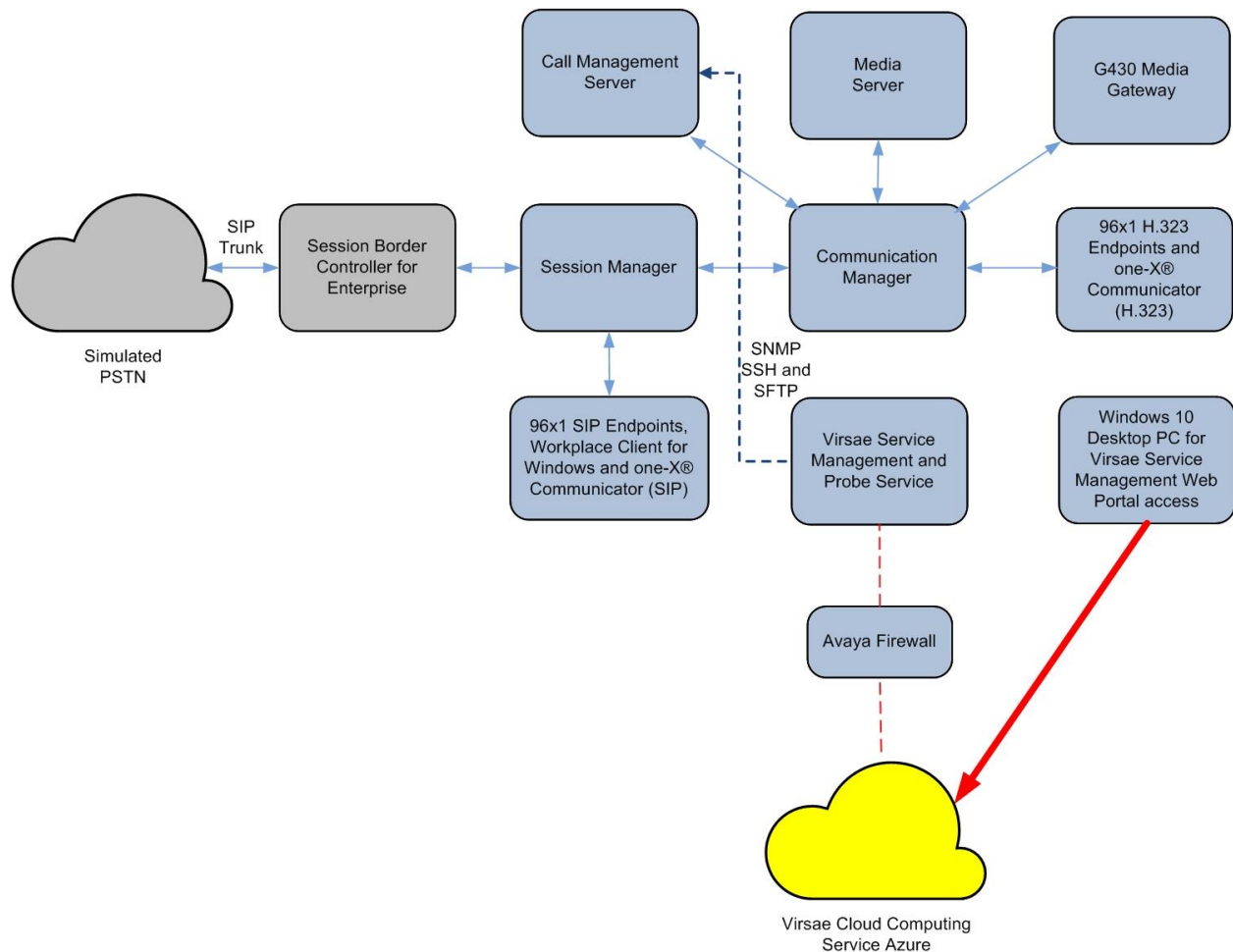
## **2.3. Support**

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 the VSM application with CMS. In the compliance testing, Communication Manager with a G430 Media Gateway connected to CMS using the processor channels. The system has Avaya H323, SIP, Workplace Client for Windows and one-X® Communicator configured for making and receiving calls. Session Manager together with Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution. 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 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:

<b>Equipment/Software</b>	<b>Release/Version</b>
Avaya Call Management System running on virtual server	CMS-R19.1.0.1.fb.i-e78-00-1
Avaya Aura® Communication Manager running on virtual server	8.1.2.0.0-FP2
Avaya G430 Media Gateway	41.16.0
Avaya Aura® Media Server running on virtual server	8.0.2.93
Avaya IP Deskphones - 9641 (H.323) - 9621 (SIP)	6.8304 7.1.10.0
Avaya Workplace Client for Windows	3.9.0.84.8
Avaya one-X® Communicator (SIP and H.323)	6.2.12.04-FP14
Virsa Service Management and Probe Service running on Windows 2016	R135

## 5. Configure Avaya Aura® Communication Manager

The configuration of Communication Manager is assumed to be in place and will not be discussed in this document. For more information of how to configure Communication Manager and CMS, please refer to **Section 10**.

## 6. Configure Avaya Call Management System

The initial administration of CMS and the connection to Communication Manager is assumed to be in place and will not be covered here. This section includes creating a login account for VSM to access the CMS and enabling SNMP. Configuration of the ECHI is installed and supported by Avaya Professional Services. For more information on this package contact your Avaya Sales or Avaya Professional Services contact.

### 6.1. Configure Login Account

Create an Administrator account on CMS since VSM requires access to CMS with Administrative Rights. The new account should be like the default “**cms**” account. Login to CMS console with root 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
```

### 6.2. Configure SNMP

The configuration for the CMS SNMP can be summarized below:

- Creates a SNMP user account
- Setup an alarm destination
- Send a test alarm to destination using the SNMP user account

Log in to CMS with root account and runs the following command.

```
/cms/aol/bin/aom_tool
```

Select the choices from the menu as shown below:

```
(cmsr19)-(xxxx)=# /cms/aom/bin/aom_tool

Welcome to Avaya CMS Alarm Configuration Main Menu.
 1) Set Alarm ID
 2) Set Customer ID
 3) Configure Alarm Destination
 4) Send a Test Alarm
 q) Quit
Enter choice (1-4, q): 3
```

Welcome to the CMS Alarm Origination Manager configuration utility.

You are currently connected to port /dev/pts/6.

Welcome to Avaya CMS Alarm Origination main menu.

- 1) SNMP/SAL
- 2) Socket/SAL
- q) Quit

Enter choice (1-2, q): **1**

Do you want to

- 1) Add an SNMP Connection
- 2) Delete an SNMP Connection
- 3) Modify an SNMP Connection
- 4) Add an SNMP User
- 5) Delete an SNMP User
- 6) Modify an SNMP User
- 7) Clear SNMP Alarms
- q) Quit

Enter choice (1-7, q): **4**

Adding an SNMP user

What is the SNMP user name? VirsaeV3

Select the SNMP version:

- 1) v3

Enter choice (1-1): **1**

Select the access level:

- 1) rouser: Read Only
- 2) rwuser: Read/Write

Enter choice (1-2): **1**

Select the security level:

- 1) noAuthNoPriv: Unauthenticated/Unencrypted (not allowed in FIPS mode)
- 2) authNoPriv: Authenticated/Unencrypted (not allowed in FIPS mode)
- 3) authPriv: Authenticated/Encrypted

Enter choice (1-3): **3**

Select the authentication protocol:

- 1) MD5 (not allowed in FIPS mode)
- 2) SHA

Enter choice (1-2): **1**

Enter authentication password (min 8 chars):

Confirm authentication password (min 8 chars):

Select the encryption protocol:

- 1) AES
- 2) DES

Enter choice (1-2): **2**

Enter encryption password (min 8 chars):

Confirm encryption password (min 8 chars):



The following summary is presented. Press **Enter** to accept.

```
CMS was last rebooted 5 day(s) ago.

You have selected to configure AOM using SNMP.

Add an SNMP User

User Name: VirsaeV3
SNMP version: v3
SNMP Access Level: rouser
SNMP Security Level: authPriv
SNMP authentication protocol: MD5
SNMP authentication password: *****
SNMP encryption protocol: DES
SNMP encryption password: *****

Press [Enter] to continue or [q] to quit
```

The system adds the SNMP user, then displays the following screen when done. Enter the number associated with the **Add an SNMP Connection** option, and press **Enter**.

```
Configuring /cms/aom/data/admin/user.cfg
[started]
done

Do you want to
 1) Add an SNMP Connection
 2) Delete an SNMP Connection
 3) Modify an SNMP Connection
 4) Add an SNMP User
 5) Delete an SNMP User
 6) Modify an SNMP User
 7) Clear SNMP Alarms
 q) Quit
Enter choice (1-7, q): 1

Adding an SNMP connection

Select a destination type:
 1) SAL
 2) NMS
Enter choice (1-2): 2

What is the destination IP address? 10.1.10.124

What is the destination port number? 162

Select a notification type:
 1) trap
Enter choice (1-1): 1

Select an SNMP user:
 1) cmssnmp
 2) VirsaeV3
Enter choice (1-3): 2
```

```
What is the Alarm ID (10 digit alarm ID)? (default:3000004043)
What is the Customer ID (10 digit customer code)? (default:0004558769)
What is the Customer Name? (default:Avaya)

Run a test alarm when done?(y/n):y

CMS was last rebooted 5 day(s) ago.

You have selected to configure AOM using SNMP.

Add an SNMP Connection

Destination Type: NMS
Destination IP: 10.1.10.124
Destination port: 162
Notification Type: trap
User Name: VirsaeV3

Alarm ID: 3000004043

Customer ID: 0004558769

Customer NAME: Avaya

A test alarm will be sent at the end.

Press [Enter] to continue or [q] to quit
```

At the summary screen above, press **Enter** to continue.

```
Configuring /cms/aom/data/admin/dest.cfg
  [started]
reset AOM
  [started]
done
Clearing all current alarms.
  [started]
done
Sending test alarm.
  [started]
done
done

Do you want to
  1) Add an SNMP Connection
  2) Delete an SNMP Connection
  3) Modify an SNMP Connection
  4) Add an SNMP User
  5) Delete an SNMP User
  6) Modify an SNMP User
  7) Clear SNMP Alarms
  q) Quit
Enter choice (1-7, q): (default: 2)
```

Enter **q** to quit, and press **Enter**.

## 7. Configure Virsae Service Management

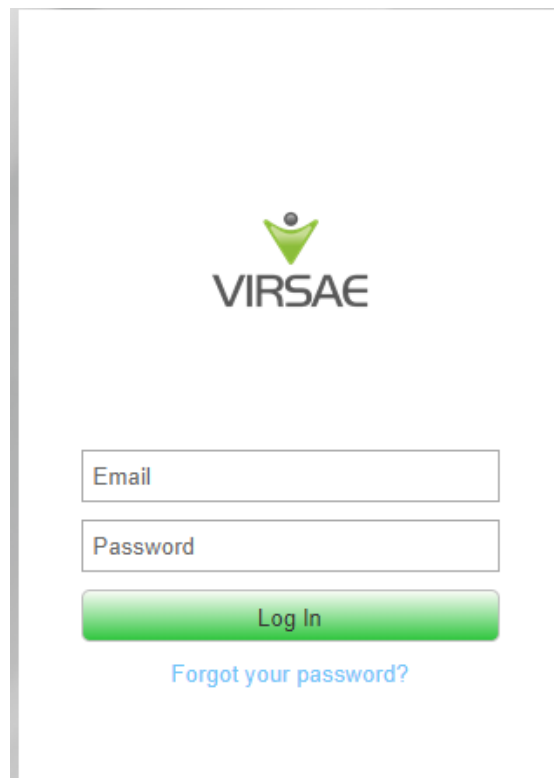
This section describes the configuration of VSM required to interoperate with CMS.

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 these 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® Application Enablement Services
- Configure Dashboard

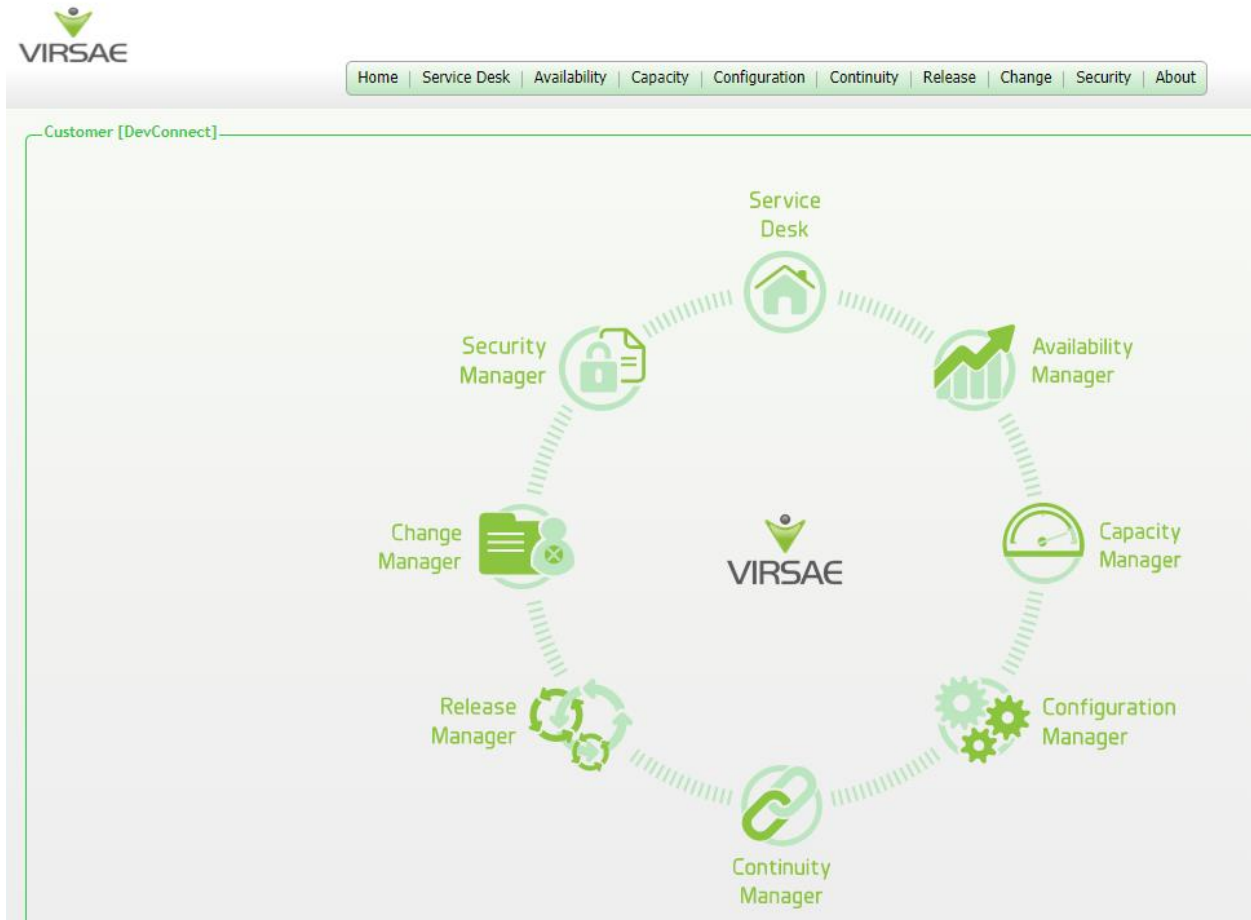
### 7.1. Login to the Web Portal

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



The screenshot shows a login interface for Virsae. At the top center is the Virsae logo, which includes a green stylized figure above the word "VIRSAE". Below the logo are two input fields: "Email" and "Password". Underneath these fields is a green "Log In" button. At the bottom of the form area, there is a blue link that says "Forgot your password?".

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



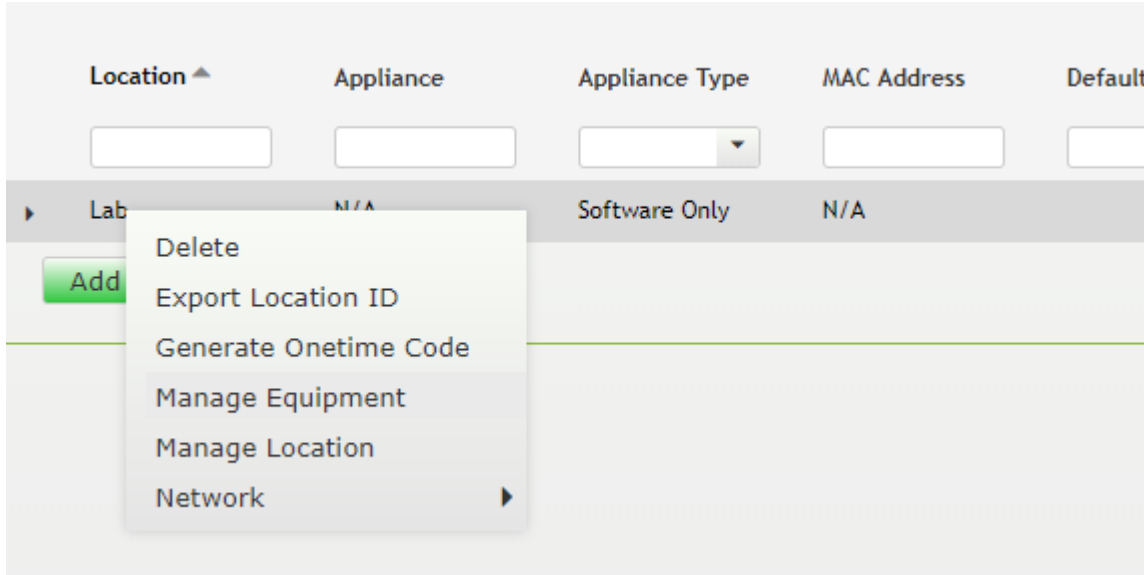
Navigate to **Service Desk** → **Equipment Locations** as shown below.

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

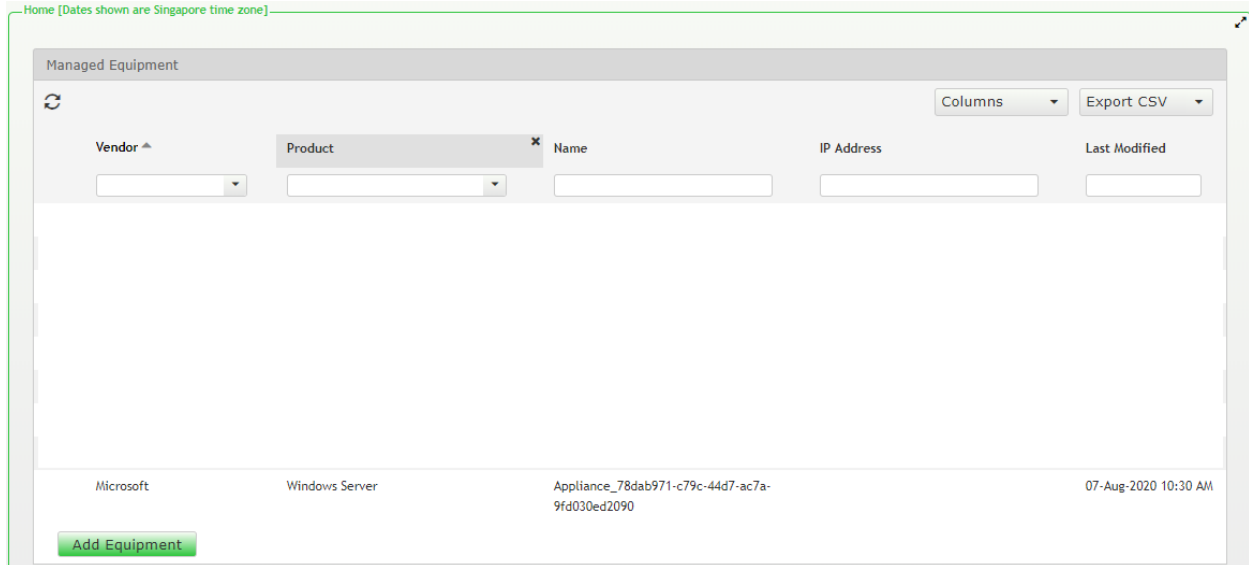
A **Location** called **Lab** is already configured as shown below.

This screenshot is identical to the one above, showing the VIRSAE web interface with the 'Equipment Locations' table. The table contains one entry: 'Lab' with 'N/A' for Appliance, 'Software Only' for Appliance Type, and '0 s' for Running Time. The 'Service Desk' navigation menu is also visible on the right side of the page.

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



Click **Add Equipment** below:



## 7.2. Configuring Avaya Call Management System

From the **Add Equipment** window, add CMS to the Location. Select **Avaya** from the **Vendor** list. Select **Call Management System** from the **Product** list. Configure the following values.

- **Equipment Name:** A descriptive name.
- **Username:** The username configured in **Section 6.1**.
- **Password:** The password configured in **Section 6.1**.
- **IP Address/Host Name:** IP address of CMS.
- **Site:** A descriptive site name.

Below are the configured values of the CMS.

Equipment	SNMP Query	Custom Scripts
Vendor *		Product *
Avaya		Call Management System
Equipment Name *		Username *
Call Management System		virsa
IP Address/Host Name *		Password *
10.1.10.85		.....
Site ⓘ		
Lab		

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

- **SNMP Version:** Select **V3**.
- **Authentication Protocol:** Authentication protocol configured in **Section 6.2**.
- **Authentication Password:** Authentication password configured in **Section 6.2**.
- **Privacy Protocol:** Encryption protocol configured in **Section 6.2**.
- **Privacy Password:** Encryption password configured in **Section 6.2**.

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

Equipment | **SNMP Query** | Custom Scripts

Virsaev Direct can be configured to query this Call Management System 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 Call Management System below.

Version: V3 | Username \*: Virsaev3

Authentication Protocol \*: MD5 | Authentication Password: .....

Privacy Protocol \*: DES | Privacy Password \*: .....

Save | Test Access | Cancel

The screen below shows the added CMS equipment.

Home [Dates shown are Singapore time zone]

New Equipment Detected

Managed Equipment

Columns | Export CSV

Vendor	Product	Name ^	IP Address	Last Modified
Avaya	Call Management System	Call Management System	10.1.10.85	19-Aug-2020 11:34 AM



To create a ECHI SFTP user account in VSM, navigate to **Service Desk → Equipment Locations**. Right click on the “Lab” location and select **Manage Location**. Select **File Transfer** tab and configure the following:

- Tick on **Enable SFTP**.
- Enter **22** for **Port**.

Under **SFTP and FTP user accounts**,

- **User Name:** Obtain user name from Avaya Professional Services.
- **Password:** Obtain SFTP password from Avaya Professional Services.
- **Protocol:** Select **SFTP/SCP**.
- **Upload Type:** Select **Upload Type** as **CMSCallHistory**.
- **Public Key:** Obtain the key from Avaya Professional Service personnel who configured the CMS.

Click the + sign and **Save** (not shown) to complete.

The screenshot shows the 'Edit Location' configuration interface. At the top, there are tabs for 'Details', 'Appliance', 'SNMP Traps', 'File Transfer' (selected), and 'VQM'. Below the tabs, a descriptive text states: '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.'

Under the 'File Transfer' section, there are three checkboxes: 'Enable TFTP', 'Enable FTP', and 'Enable UUCP', all of which are currently unchecked.

The 'SFTP and SCP Configuration' section contains two checkboxes: 'Enable SFTP' (checked) and 'Enable SCP' (unchecked). Below this, there is a 'Port' label and a text input field containing the number '22'.

The 'SFTP and FTP user accounts' section features a table-like structure with the following fields:

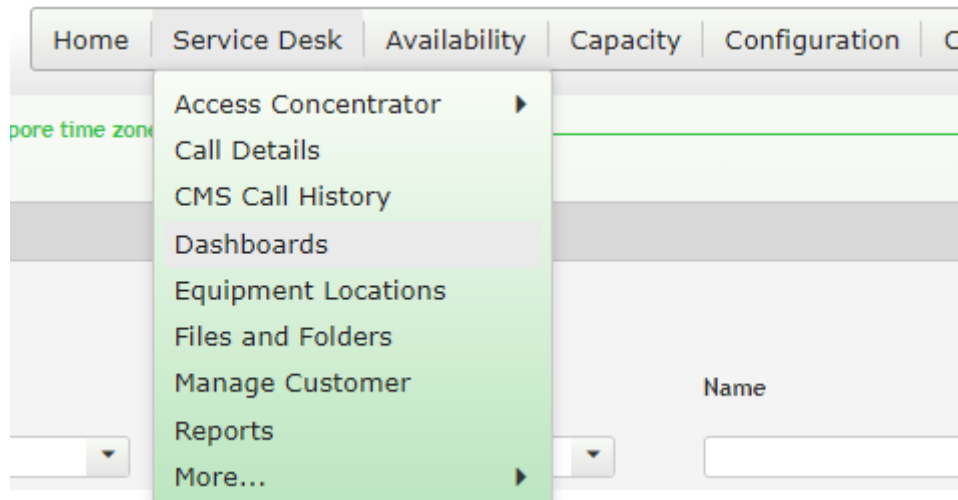
User Name *	Password *	Protocol	Upload Type	Public Key
<input type="text" value="cmechi"/>	<input type="password" value="....."/>	<input type="text" value="SFTP/SCP"/>	<input type="text" value="CMSCallHistc"/>	<input type="text"/>

At the bottom right of this section, there are two buttons: a green '+' button and a circular refresh icon.

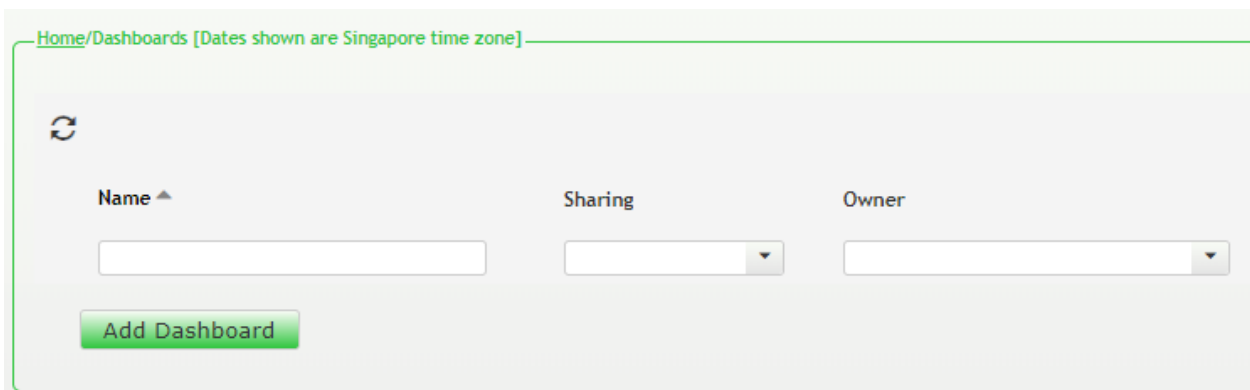
### 7.3. Configure Dashboard

This section shows the steps to configure CMS on the dashboard.

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



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

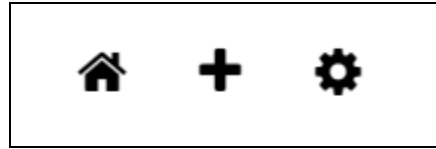


In the **Add Dashboard** window, type a descriptive name for **Name** field as shown below. Retain default values for all other fields. Click on **Start dashboard automatically...** box and then click on **Ok** to submit.

The image shows a dialog box titled "Add Dashboard". It contains the following fields and options:

- Name:** A text input field containing "Devconnect Lab".
- Sharing:** A dropdown menu with "Private" selected.
- Owner:** A text input field containing "Yong Meng Low".
- Description:** An 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 **System Health Summary** from the available dashlet by hovering the “+” image over it and click **Done**.

**Add Dashlet**

system health

System Health Summary

Add new System Health Summary

Avaya Application Enablement Services (AES)

Avaya Call Management System (CMS)

Avaya Communication Manager (ACM)

Avaya Contact Recorder (ACR)

Avaya Experience Portal (AEP)

Avaya Session Border Controller (ASBC)

Avaya Session Manager (SM)

IP Office

Linux Server

Oracle SBC

Windows Server

Trunk

Done

From the **System Health Summary** window, select the **setup wheel** on the top right corner of the box.



Select “Lab” for the **Location** drop-down menu, the appropriate **Equipment** i.e., **Call Management System** 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 Call Management System (CMS)** dashboard and, in addition select the desired **Layout**.



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

Customer  
DevConnect

Location  
Lab

Equipment  
Call Management System

**Layout**

- Show Occupancy Graph
- Show Network Connectivity Graph
- Show Work Force Management Connections

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

System Health Summary  
Lab

Total Servers	1
Total availability last 30 days	100%
Longest outage	< 5 mins
Average Response Time	0 ms

Server	Server Type	Services	CPU <sup>▲</sup>	Memory	Disk	Max Ping <sup>?</sup>	Avg Ping <sup>?</sup>	Availability <sup>?</sup>
	Choose <span style="font-size: 0.8em;">▼</span>	<span style="color: green;">↑</span> <span style="color: red;">↓</span>	<span style="font-size: 0.8em;">0% - 100%</span>	<span style="font-size: 0.8em;">0% - 100%</span>	<span style="font-size: 0.8em;">0% - 100%</span>	<1ms	<1ms	<span style="font-size: 0.8em;">0 - 100</span>
Call Management System	CMS	N/A N/A	0.6%	12.9%	3.1%	<1ms	<1ms	100%

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

Name | Call Management System

Uptime | 5 days

Logged in Users | 8

Processor

0%

Memory

13%

Filesystem	Free	% Used	Mounted on
/dev/sda1	439MB	19%	/boot
/dev/sda2	8GB	18%	/
/dev/dm-2	11GB	9.2%	/opt
/dev/dm-0	9GB	4.2%	/cms
/dev/sda6	84GB	3.1%	/storage

Network Connectivity

Max Ping | 7

< 1 ms

Avg Ping | 3

< 1 ms

Loss | 0

0 %

Backups

Admin  
Unknown

Maintenance  
Unknown

Connections

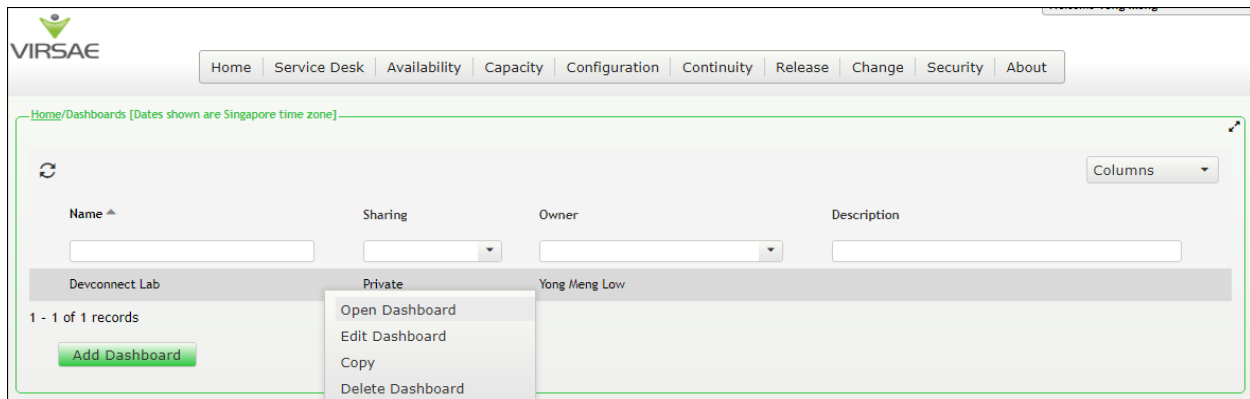
Supervisor Licenses

Total	Windows User	Web User
0	0	0

## 8. Verification Steps

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

After login to the web portal, navigate to **Service Desk → Dashboard** (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 7.3**, once logged in, all the dashboards last configured at the end of **Section 7.3** will be populated in a new tab on the browser.



From the home screen, navigate to **Service Desk** → **Dashboard Management** and select **CMS Call History** (not shown). Create a rule set and apply the rule. Screen below shows a few examples of CMS Call History for an inbound call to the call center agent extracted from the ECHI data.

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 alarm for CMS equipment.

## 9. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R135 to interoperate with Avaya Call Management System R19.1. During compliance testing, all test cases were completed successfully.

## 10. 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. *Avaya Call Management System Call History Interface*, Release 19.1, Issue 1, Feb 2020.
4. *Administering Avaya Call Management System*, Release 19.1, Issue 2, May 2020.

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

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

---

**©2020 Avaya Inc. All Rights Reserved.**

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

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