



Avaya Solution & Interoperability Test Lab

Application Notes for Virsae Service Management with Avaya Session Border Controller for Enterprise - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management R135 to interoperate with Avaya Session Border Controller for Enterprise R8.1.0.

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 Avaya Session Border Controller for Enterprise using Secure Shell (SSH) and uses Simple Network Management Protocol (SNMP) to query Avaya Session Border Controller for Enterprise. At the same time, Virsae Service Management processes Real-time Transport Control Protocol (RTCP) from Avaya Session Border Controller for Enterprise using its RTCP monitoring feature. Syslog is also used to collect trace sent from Avaya SBCE for troubleshooting purpose.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Virsae Service Management for Unified Communications (herein after referred to as VSM) with Avaya Session Border Controller for Enterprise (herein after referred to as Avaya SBCE). VSM is a cloud-based service management platform that brings visibility, service transparency and cost savings to Unified Communications environments over the short, medium and long term.

The Virsae product uses SNMP, Syslog, RTCP and Linux shell access integration methods to monitor Avaya SBCE.

- SNMP collection –Virsae uses SNMP to collect alarm and connectivity, service and application status information from Avaya SBCE.
- SSH – Virsae establishes a Linux Shell connection to run the “sar” command and obtain system information. This command typically collects, reports and saves CPU, Memory, I/O usage in the Linux operating system.
- Real Time Transport Control Protocol (RTCP) collection - Virsae collects RTCP information sent by Avaya SBCE through its RTCP monitoring feature.
- Syslog is also used to collect trace sent from Avaya SBCE for troubleshooting purpose.

2. General Test Approach and Test Results

The general test approach was to verify VSM using SNMP, SSH connection to monitor and display system status of Avaya SBCE and VSM dashboard to display RTCP information collected through its monitoring feature.

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 and non-encrypted SNMP, Syslog and RTCP as requested by Virsae.

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

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

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

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

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

2.1. Interoperability Compliance Testing

For feature testing, VSM dashboard was used to view the configurations of Avaya SBCE such as the memory and CPU utilizations, disk usage and status from data collected via SSH and alarms via SNMP. For collection of RTCP information, calls will be made included intra-switch calls, inbound and outbound trunk calls.

For serviceability testing, reboots were applied to the VSM to simulate system unavailability. Loss of network connectivity to VSM was also performed during testing.

2.2. Test Results

All test cases passed successfully with the following observations.

- Syslog trace on SBCE could not be activated for this load. Avaya is investigating this issue.
- Some SNMP Traps not decoded properly by VSM and therefore some alarms are not shown. Virsae is investigating the 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

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify VSM interoperability with Avaya SBCE. The configuration consists of an Avaya SBCE along with Communication Manager system with an Avaya G430 Media Gateway. The system has Workplace Client for Windows and one-X® Communicator (SIP and H.323) 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.

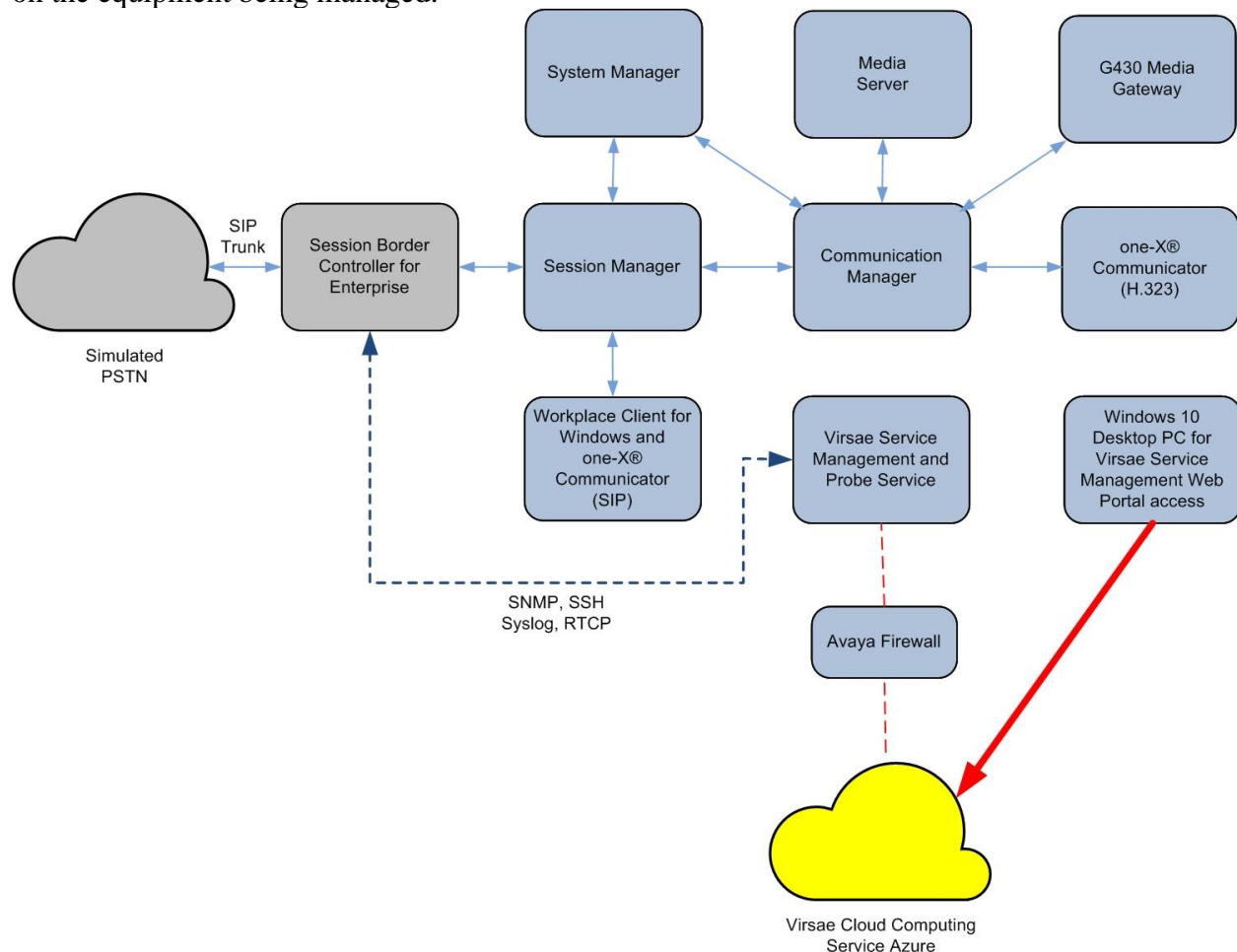


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Session Border Controller for Enterprise running on virtual server	8.1.0.0-14-18490
Avaya Aura® Session Manager running on virtual server	8.1.2.1.812101
Avaya Aura® System Manager running on virtual server	8.1.2.0.0611588
Avaya Aura® Communication Manager running on virtual server	8.1.2.0.0-FP2
Avaya G430 Media Gateway	41.16.0
Avaya Aura® Media Server running on virtual server	8.0.2.93
Avaya Workplace Client for Windows	3.9.0.84.8
Avaya one-X® Communicator (SIP and H.323)	6.2.12.04-FP14
Virsa Service Management and Probe Service on Windows 2016	R135

5. Configure Avaya Session Border Controller for Enterprise

This section describes the steps needed to configure Avaya SBCE to interoperate with VSM. This includes creating a login account for VSM to access Avaya SBCE, enabling SNMP, enabling Syslog for trace and events as well as RTCP monitoring.

5.1. Configure Login Group

Create an Administrator account on Avaya SBCE since VSM requires access to Avaya SBCE with Administrative Rights. Add an account that when used provides access to the Linux bash prompt.

The new account should be like the default administrator account. Login to Avaya SBCE console with root access and run the following command.

During compliance testing the “**ipcs**” account created during installation of Avaya SBCE was used. This is because “**ipcs**” account has access to the SBCE console other than the root account.

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

If administrator does not have the required privileges to create a new account, then the “**ipcs**” account will also work. In this compliance testing, **ipcs** login is used.

5.2. Configure SNMP

SNMP is used to capture alarms raised by Avaya SBCE. All configurations are done via Avaya SBCE web interface.

Using a web browser, enter <https://<IP address of Avaya SBCE>> to connect to the Avaya SBCE server and log in using appropriate credentials as shown below.



Log In

Username:

Continue

Session Border Controller for Enterprise

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

Once logged in, a dashboard is presented with a menu on the left-hand side for EMS (not shown). Select “SBCE” under **Device** from the left top drop-down options for SBCE configuration as shown below:

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

SNMP

Syslog Management

Debugging

Trace

Log Collection

DoS Learning

CDR Adjunct

Dashboard

Information	
System Time	04:13:52 PM SGT Refresh
Version	8.1.0.0-14-18490
GUI Version	8.1.0.0-18490
Build Date	Mon Feb 03 17:23:09 UTC 2020
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	09/02/2020 15:24:38 SGT
Failed Login Attempts	0

Installed Devices

EMS

SBCE

Navigate to **Backup/Restore** → **Monitoring & Logging** → **SNMP** from the dashboard. The **SNMP** page is seen as shown below. Select **SNMP v3** tab. Click on the **Add** button.

Session Border Controller for Enterprise

AVAYA

- EMS Dashboard
- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging
 - SNMP**

SNMP: SBCE

SNMP v3	Management Servers	Trap Severity Settings			
<input type="button" value="Add"/>					
User Name	Auth Schema	Auth Protocol	Priv Protocol	Privilege	Traps

In the **Add User** window shown below, configure the following.

- **User Name:** A descriptive name.
- **Authentication Scheme:** Select the radio button for **authPriv**.
- Enter a password for **AuthPassPhrase** and confirm the same in **Confirm AuthPassPhrase**.
- **Authentication Protocol:** Select the radio button for **SHA**.
- Enter a password for **PrivPassPhrase** and confirm the same in **Confirm PrivPassPhrase**.
- **Privacy Protocol:** Select **DES** radio button.
- **Privilege:** Select **Read** radio button.
- **Trap IP Address:** Enter the IP Address of the VSM.
- **Port:** Enter **162**.

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

User Name:

Authentication Scheme: ☐ noAuthNoPriv ☐ authNoPriv ☒ authPriv

AuthPassPhrase:
Leave blank to keep existing passphrase

Confirm AuthPassPhrase:

Authentication Protocol: ☒ SHA

PrivPassPhrase:
Leave blank to keep existing passphrase

Confirm PrivPassPhrase:

Privacy Protocol: ☐ AES ☒ DES

Privilege: ☒ Read ☐ Read/Write

Trap IP Address	Port	Trap Profile
<input type="text" value="10.1.10.124"/>	<input type="text" value="162"/>	<input type="text" value="default"/> <input type="button" value="Delete"/>

Screen below shows the SNMP v3 configured for SBCE device. Now select the **Management Servers** tab and click on the **Add** button.

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
‣ System Parameters
‣ Configuration Profiles
‣ Services
‣ Domain Policies
‣ TLS Management
‣ Network & Flows
‣ DMZ Services
‣ Monitoring & Logging
SNMP

SNMP: SBCE

SNMP v3

Management Servers

Trap Severity Settings

Add

User Name	Auth Schema	Auth Protocol	Priv Protocol	Privilege	Traps	
virsa	authPriv	SHA	DES	READ	10.1.10.124:162 [default]	Clone Edit Delete

In the **Add IP Address** window shown below, configure the VSM IP Address and click the **Finish** button.

Incidents Status Logs Diagnostics Users

Add IP Address X

IP Address(es)
Separate entries with commas

10.1.10.124

Finish

Screen below shows the Management Servers configured for **SBCE** device.

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
‣ System Parameters
‣ Configuration Profiles
‣ Services
‣ Domain Policies
‣ TLS Management
‣ Network & Flows

SNMP: SBCE

SNMP v3 Management Servers Trap Severity Settings

Add

IP Address
10.1.10.124

Clone Edit Delete

5.3. Configure Syslog Management

To setup syslog output from Avaya SBCE to VSM, under **Device: SBCE**, navigate to **Backup/Restore → Monitoring & Logging → Syslog Management** from the dashboard shown below. Select the **Collectors** tab. Click on **Edit** on any of the LOG_LOCALx entry except 5 and 6. In this compliance testing, **LOG_LOCAL0** was picked.

Device: SBCE Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
‣ System Parameters
‣ Configuration Profiles
‣ Services
‣ Domain Policies
‣ TLS Management
‣ Network & Flows
‣ DMZ Services
‣ Monitoring & Logging
 SNMP
 Syslog Management
 Debugging
 Trace
 Log Collection
 DoS Learning

Syslog Management: SBCE

Log Level Collectors

Add

Facility	Destination Location	
LOG_LOCAL5	/archive/syslog/ipcs/slic.log	Edit
LOG_LOCAL6	/archive/syslog/ipcs/audit.log	Edit
LOG_LOCAL0	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_DAEMON	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL1	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL3	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL2	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL4	/archive/syslog/ipcs/ipcs.log	Edit Delete

In the **Edit Collector** window shown below, configure the following.

- **Collector Type:** Select the **Remote Syslog** radio button.
- **Protocol:** Select **UDP**.
- **Address:** Select the **(ip:port)** radio button and enter the IP Address of VSM and the port as **514**.

Click on the **Finish** button.

The screenshot shows the 'Edit Collector' window with the following settings:

- Facility:** LOG_LOCAL0 (selected from a dropdown menu)
- Collector Type:** Remote Syslog (selected with a radio button)
- Remote Syslog Settings:**
 - Protocol:** UDP (selected with a radio button)
 - TLS Profile:** None (selected from a dropdown menu)
 - Address:** (ip:port) (selected with a radio button), 10.1.10.124:514 (entered in the text field)

A 'Finish' button is located at the bottom of the window.

Screen below shows the Collectors configured for SBCE device. Now select the **Log Level** tab.

Syslog Management: SBCE

Log Level

Collectors

Add

Facility	Destination Location	
LOG_LOCAL5	/archive/syslog/ipcs/slic.log	Edit
LOG_LOCAL6	/archive/syslog/ipcs/audit.log	Edit
LOG_LOCAL0	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_DAEMON	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL1	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL3	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL2	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL4	/archive/syslog/ipcs/ipcs.log	Edit Delete
LOG_LOCAL0	UDP:10.1.10.124:514	Edit Delete

In the **Log Level** tab screen shown below, select the **Facility** configured above for the **Platform**, **Trace**, **Security**, **Protocol**, **Registrations** and **Audit** under **Class**. During compliance testing **All** levels of logs were selected. Click on the **Save** button. Note that the **Trace** is grey out as mentioned in the observations in **Section 2.2**.

Session Border Controller for Enterprise

AVAYA

- EMS Dashboard
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging
 - SNMP
 - Syslog Management**
 - Debugging
 - Trace
 - Log Collection
 - DoS Learning

Syslog Management: SBCE

Log Level

Collectors

Class	Facility	All	Info	Notice	Warning	Error	Critical	Alert	Emergency
Platform	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Trace	LOG_LOCAL0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Protocol	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Registrations	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Audit	LOG_LOCAL6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save

5.4. Configure RTCP Monitoring feature

To setup RTCP Monitoring, under **Device: SBCE** navigate to **Backup/Restore → Network & Flows → Advance Options**. Select the **RTCP Monitoring** tab and configure the following:

- Tick **Enabled** the **RTCP Monitoring Relay**.
- **Node Type:** **Core** since only one SBCE is setup.
- **Relay IP:** Select the internal interface as relay IP.
- **Port:** Enter **5005**.
- Tick **Enabled** the **RTCP Monitoring Report Generation**.
- **SBCE Interface IP:** Select the external interface as IP for public trunk. This feature is only for public SIP trunk with Avaya SBCE receiving RTCP streams without having specific control. Avaya SBCE converts the RTCP streams into Avaya specific format before sending it to the monitoring server.
- **SBCE Interface Port:** Enter **5005**.
- **Monitoring server IP/FQDN and Port:** Enter VSM Probe IP address and port **5005**.

Device: SBCE ▼ Alarms Incidents Status ▼ Logs ▼ Diagnostics Users Settings ▼ Help ▼ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
 > System Parameters
 > Configuration Profiles
 > Services
 > Domain Policies
 > TLS Management
 ▾ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
 > DMZ Services
 > Monitoring & Logging

Advanced Options

Periodic Statistics	Feature Control	SIP Options	Network Options	Port Ranges	RTCP Monitoring	Load
Monitoring						
Changes to the settings below take effect immediately and will impact sessions that are using them. It is recommended to change these values only during a maintenance window.						
RTCP Monitoring Configuration						
RTCP Monitoring Relay		<input checked="" type="checkbox"/> Enabled				
Node Type		Core ▼				
Relay IP		Internal A1 (A1, VLAN 0) ▼ 10.1.10.65 ▼				
Port		5005				
RTCP Monitoring Report Generation		<input checked="" type="checkbox"/> Enabled				
SBCE Interface IP		External B1 (B1, VLAN 0) ▼ 10.1.60.65 ▼				
SBCE Interface Port		5005				
Monitoring server IP/FQDN and Port IP:Port		10.1.10.124 : 5005				
Monitoring Frequency based on RTCP Report		2 ▼				
Monitoring interval in absence of RTCP Report		10 seconds				
Save						

In a back-to-back Avaya SBCE deployment, two relay services need to be configured to send RTCP monitoring traffic to VSM on each SBCE. This is needed for Core Avaya SBCE, DMZ Avaya SBCE and remote Avaya SBCE. In this compliance testing, only Core Avaya SBCE is setup. Refer to **Section 9** reference [3] for overview and further explanation.

To configure application relay services to send the RTCP monitoring traffic to VSM, under **Device: SBCE**, navigate to **Backup/Restore → DMZ Services → Relay**. Click **Add**.

Configure the following. A screen shot is shown on the next page.

- **Name:** Enter descriptive name.
- **Service Type:** **RTCP**.
- **Remote IP/FQDN:** VSM IP address.
- **Remote Port:** Enter **5005**.
- **Remote Transport:** Select **UDP**.
- **Listen IP:** Select internal private interface.
- **Listen Port:** Enter **5005**.
- **Connect IP:** Select another internal private interface to relay which is routable to VSM.
- **Listen Transport:** Select **UDP**.
- Tick **Use Relay Actors** and select **Options** as **Hop-By-Hop Traceroute**.

Repeat the same for Relay 2 with the **Listen IP** using the external public interface.

The RTCP monitoring server i.e., the Listen IP where RTCP traffic will be received, needs to be configured on phone groups via System Manager for SIP endpoints in Session Manager, Media Server and Communication Manager. Refer to the reference [5] and [4] in **Section 9**.

General Configuration	
Name	Relay 2
Service Type	RTCP ▾

Remote Configuration	
Remote IP/FQDN	10.1.10.124
Remote Port	5005
Remote Transport	UDP ▾

Device Configuration	
Listen IP	Internal A1 (A1, VLAN 0) ▾
	10.1.10.65 ▾
Listen Port	5005
Connect IP	Internal B2 (B2, VLAN 0) ▾
	10.1.60.65 ▾
Listen Transport	UDP ▾

Additional Configuration	
Whitelist Flows	<input type="checkbox"/>
Use Relay Actors	<input checked="" type="checkbox"/>
Options <small>Use Ctrl+Click to select or deselect multiple items.</small>	<div> RTCP Monitoring End-to-End Rewrite Hop-by-Hop Traceroute Bridging </div>
<div>Finish</div>	

6. Configure Virsae Service Management

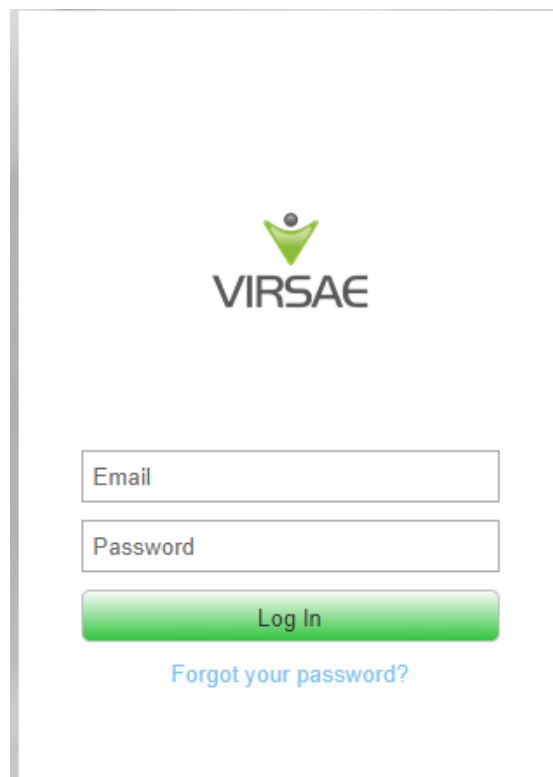
This section describes the configuration of VSM required to interoperate with Avaya SBCE.

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 Session Border Controller for Enterprise
- Configure Dashboard

6.1. Login to the Web Portal

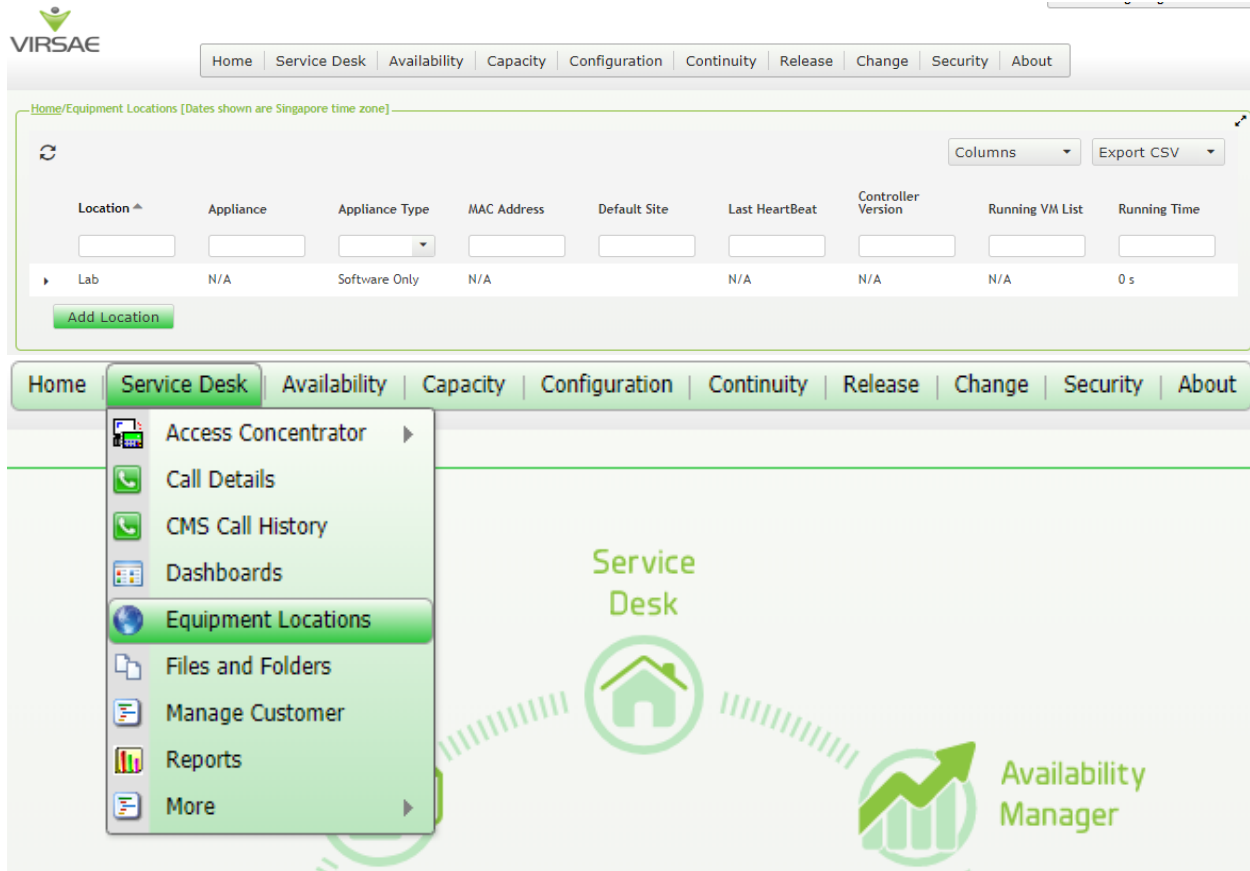
A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL *<business partner name>.virsae.com* in a web browser. During compliance testing the URL used was “*preview.virsae.com*”. The Login screen is shown as below. Enter the **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, light blue font. Below the password field is a green button with the text "Log In" in white. At the bottom of the form is a blue hyperlink that says "Forgot your password?". The entire login form is enclosed in a thin grey border.

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

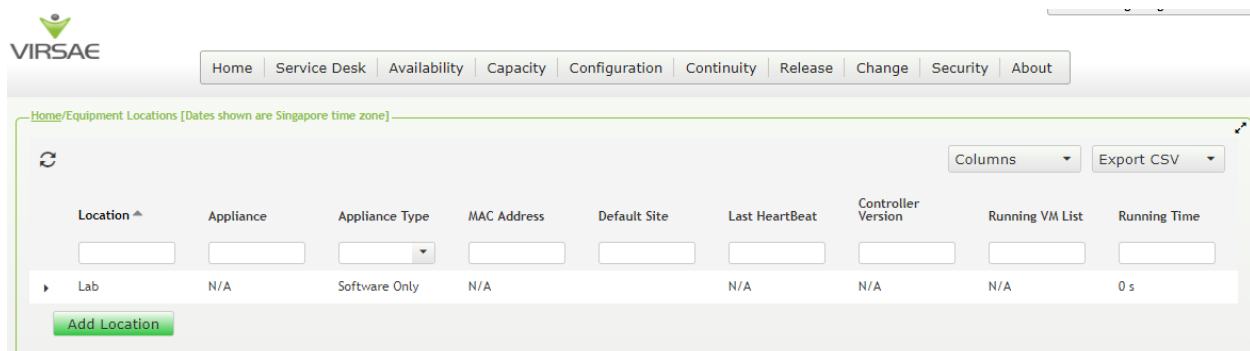


Navigate to **Service Desk** → **Equipment Locations** as shown below.



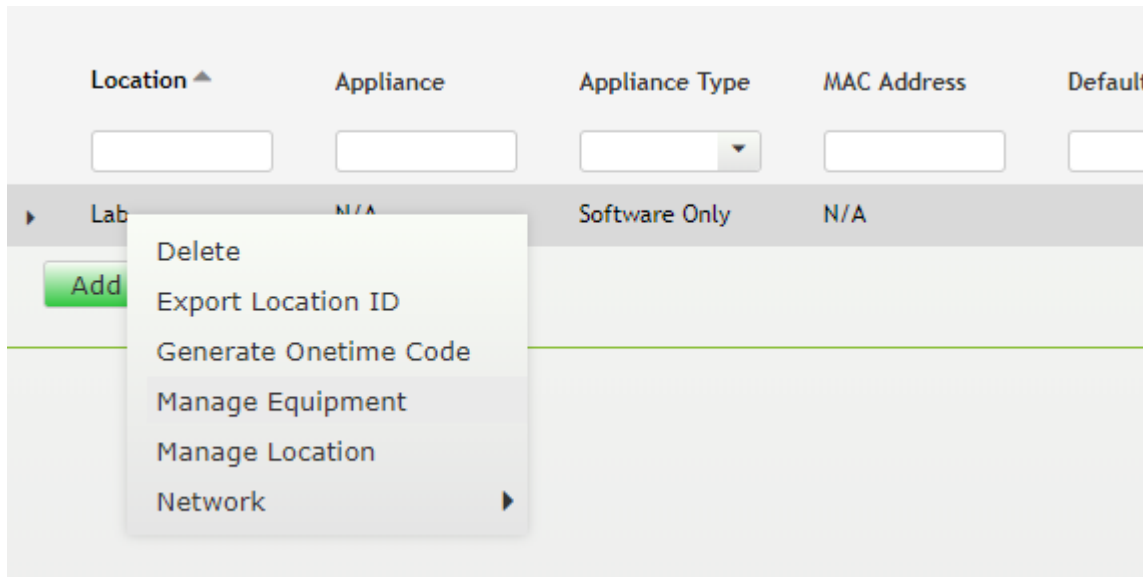
The screenshot shows the VIRSAE web application interface. At the top, there is a navigation bar with the VIRSAE logo and a menu with the following items: Home, Service Desk, Availability, Capacity, Configuration, Continuity, Release, Change, Security, and About. Below this, a breadcrumb trail reads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

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

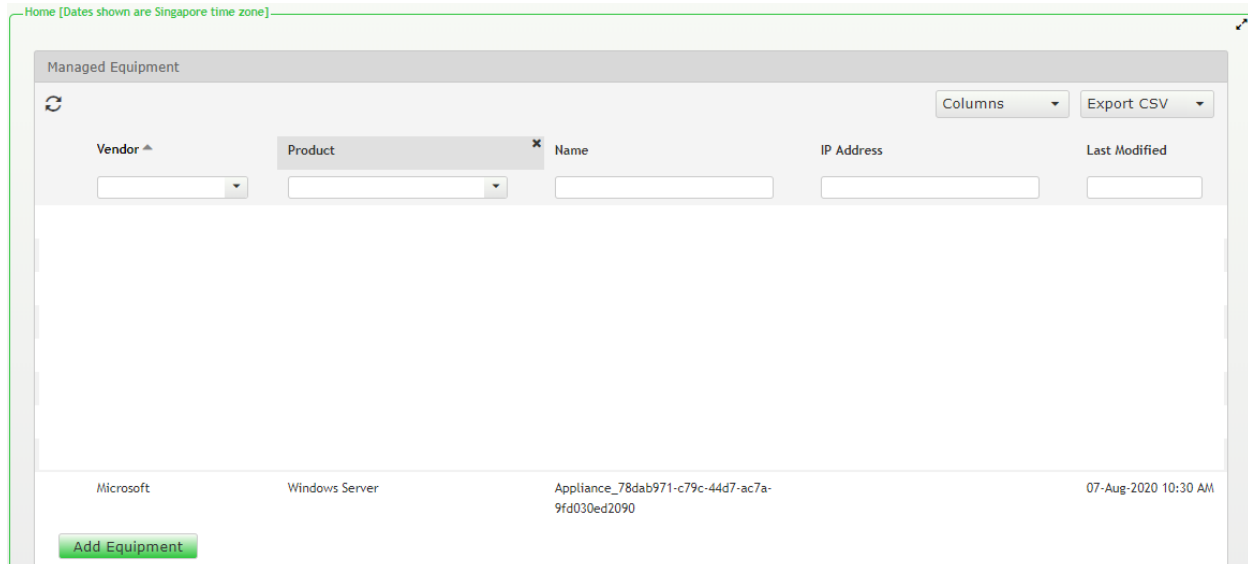


This screenshot is identical to the one above, showing the VIRSAE web application interface. The navigation bar and breadcrumb trail are the same. The table in the main content area shows the same data: Location: Lab, Appliance: N/A, Appliance Type: Software Only, MAC Address: N/A, Default Site: N/A, Last HeartBeat: N/A, Controller Version: N/A, Running VM List: N/A, and Running Time: 0 s. The "Add Location" button is also present. The dropdown menu is not open in this screenshot.

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



Click **Add Equipment** below:



6.2. Configuring Avaya Session Border Controller for Enterprise

From the **Add Equipment** window, add Avaya SBCE to the Location. Select **Avaya** from the **Vendor** list. Select **Session Border Controller** from the **Product** list. Configure the following values.

- **Equipment Name:** A descriptive name.
- **Username:** The account name mentioned in **Section 5.1**.
- **Password:** The password for the above account user.
- **IP Address/Host Name:** IP address of Avaya SBCE.
- **Site:** A descriptive site name.

Equipment	SNMP Query	Custom Scripts
<div><div>Vendor *</div><div>Avaya ▼</div></div> <div><div>Product *</div><div>Session Border Controller ▼</div></div> <div><div>Equipment Name *</div><div>SBCE</div></div> <div><div>Username *</div><div>ipcs</div></div> <div><div>IP Address/Host Name *</div><div>10.1.10.66</div></div> <div><div>Password *</div><div>.....</div></div> <div><div>Site ⓘ</div><div>Lab</div></div>		

In the **SNMP Query** tab, select **Version** as **V3** from the drop-down menu and populate all other fields based on the configuration described in **Section 5.2**.

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

Equipment

SNMP Query

Custom Scripts

VirsaE Direct can be configured to query this Session Border Controller for configuration and system health metrics, which are used in the dashboards, and historic reports.

To enable this, please enter the SNMP configuration details for this Session Border Controller below.

Version

Username *

V3

virsae

Authentication Protocol *

Authentication Password

SHA

.....

Privacy Protocol *

Privacy Password *

DES


.....

Save

Test Access

Cancel

The screen below shows the added Avaya SBCE equipment.



Home | Service Desk | Availability | Capacity | Configuration | Continuity | Release | Change | Security | Abo

Home [Dates shown are Singapore time zone]

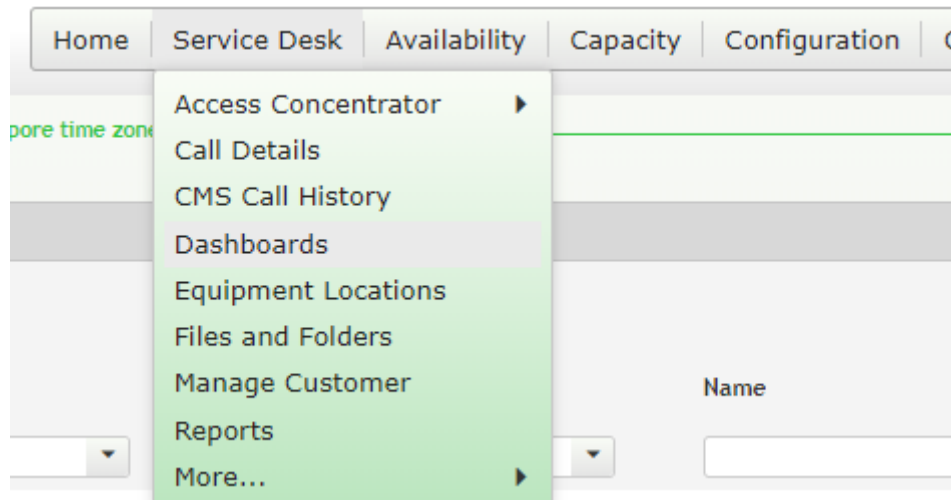
Columns

Vendor ^	Product	Name	IP Address
	1 items selected		
Avaya	Session Border Controller	SBCE	10.1.10.66

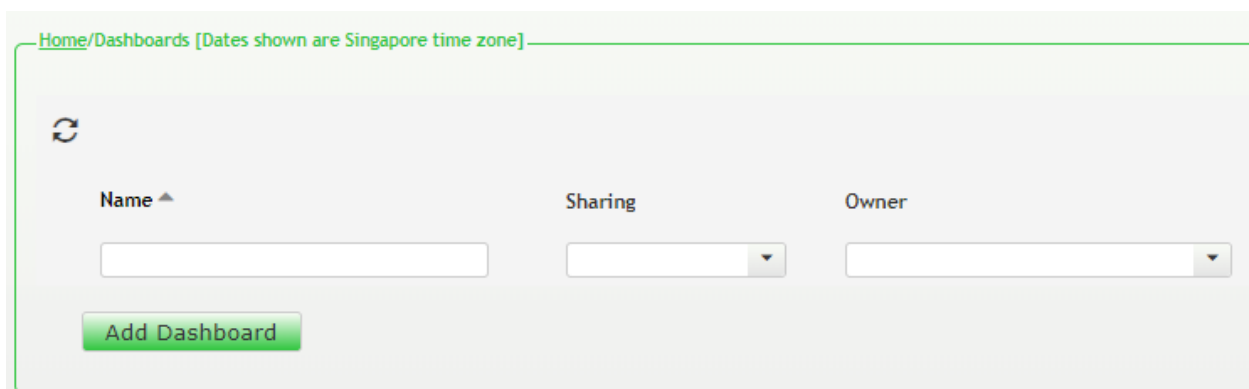
6.3. Configure Dashboard

This section shows the steps to configure Avaya SBCE on the dashboard.

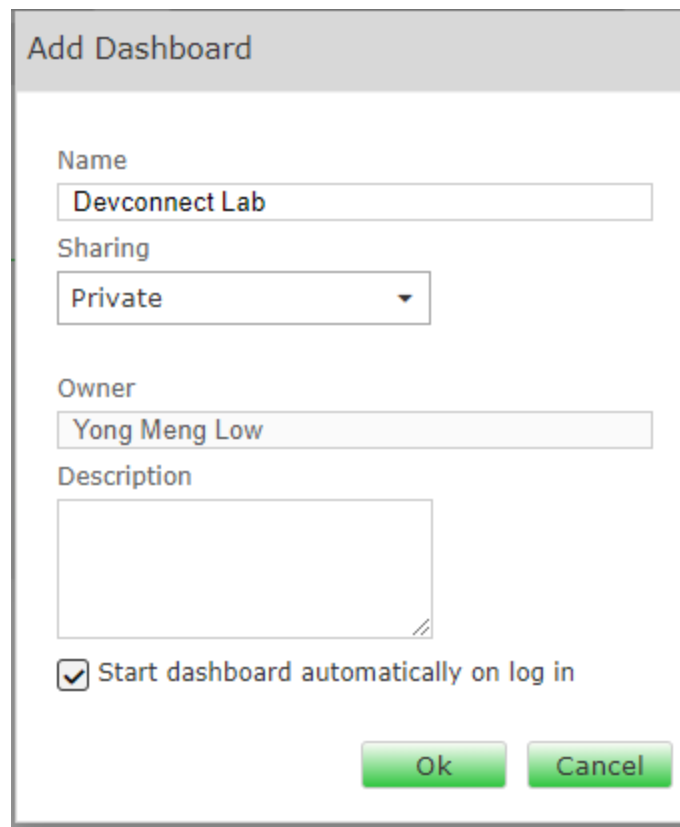
From the home screen, navigate to **Service Desk** → **Dashboards** as shown below.



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



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



Add Dashboard

Name
Devconnect Lab

Sharing
Private

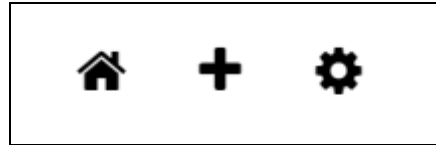
Owner
Yong Meng Low

Description

☒ Start dashboard automatically on log in

Ok Cancel

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



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

Add Dashlet

system health

System Health Summary

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

Multiple Trunk Groups

Trunk Group Traffic

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., **SBCE** 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 SBC Server Health dashlet** and in addition select the desired **Layout**.

Avaya Session Border Controller (ASBC)
Lab | SBCE

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

Customer

DevConnect

Location

Lab

Equipment

SBCE

Layout

Show Occupancy Graph

Show Network Connectivity Graph

Show Network Interface

Show Services

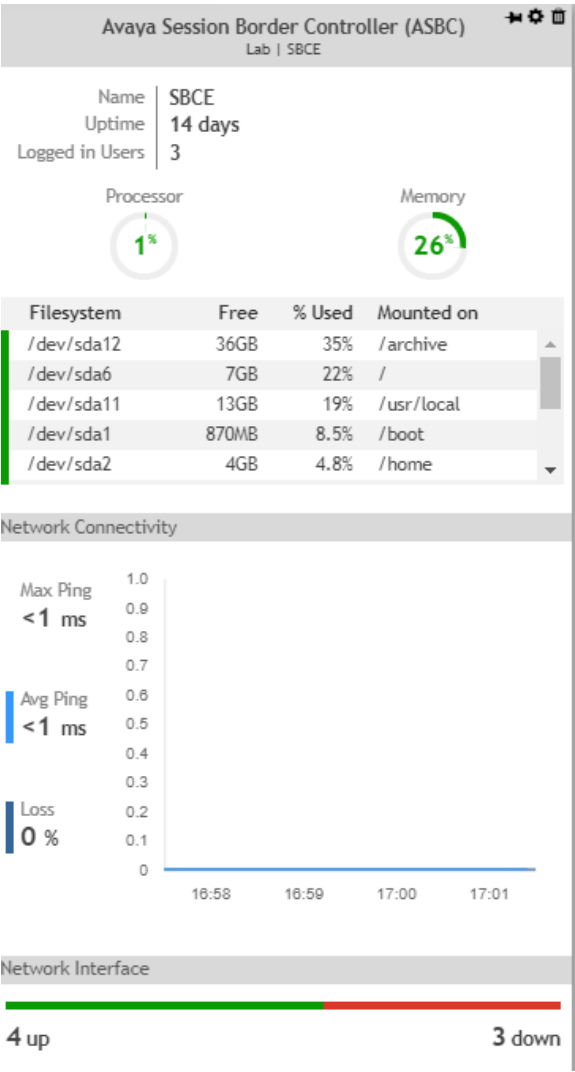
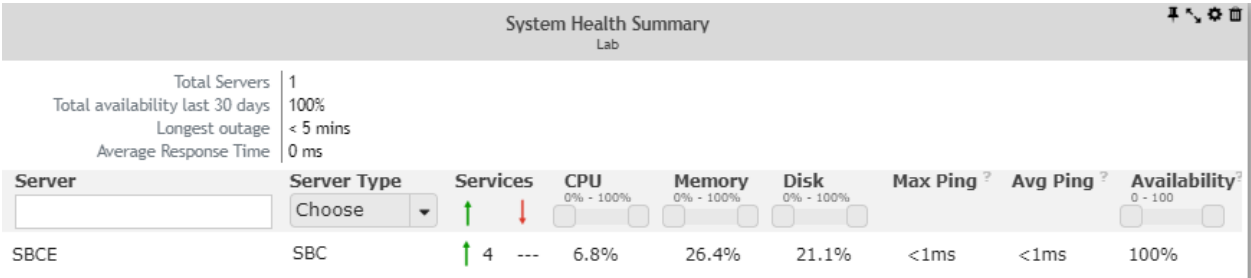
Show Application Status

Show SIP Protocol

Show SIP Calls

Show Security Violations

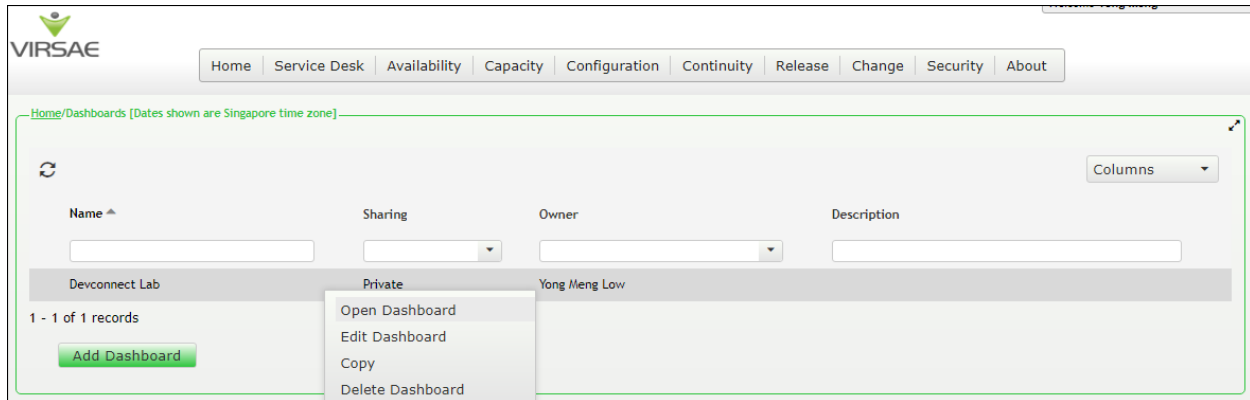
The dashboard with the configured equipment is shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.



7. Verification Steps

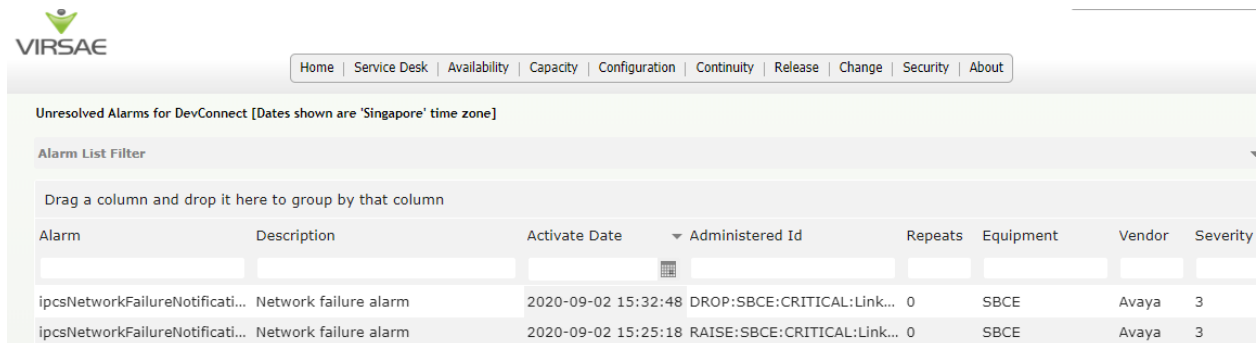
This section provides the tests that can be performed to verify proper configuration of Avaya SBCE and VSM. The following steps are done by accessing the VSM web portal for the business partner.

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 6.3**, once logged in, all the dashboards last configured at the end of **Section 6.3** will be populated in a new tab on the browser.

To view alarms via reporting, navigate to **Availability → Manage Alarms** (not shown). A list of all unresolved alarms for equipment's are shown. Screen below shows an alarm for Avaya SBCE equipment.



Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Vendor	Severity
ipcsNetworkFailureNotificati...	Network failure alarm	2020-09-02 15:32:48	DROP:SBCE:CRITICAL:Link...	0	SBCE	Avaya	3
ipcsNetworkFailureNotificati...	Network failure alarm	2020-09-02 15:25:18	RAISE:SBCE:CRITICAL:Link...	0	SBCE	Avaya	3

To view Syslogs via historical reporting, navigate to **Availability → Syslog → Browse Syslog Files** (not shown). A list of all files for all equipment are shown. Screen below shows a snapshot.

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

WELCOME **rong meng**

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

System Log

Name	Last modified	File size	Owner
20200902054645334.txt.zip	02-Sep-2020 5:11 PM	1.91 MB	Virsa (auto - generated)
20200902022150625.txt.zip	02-Sep-2020 1:47 PM	1.91 MB	Virsa (auto - generated)
20200901230009164.txt.zip	02-Sep-2020 10:22 AM	1.91 MB	Virsa (auto - generated)

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. 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

Expression (condition)

Details

Location = Lab

Date Time Range: 25-Aug-2020 06:00 PM-26-Aug-2020 01:00 PM

VQM - Streams

Name	Endpoint	IPNR	Mos Min	Mos Max	Mos Avg	Stream Length	IP Address	Port	DSCP	Call Time	Source
AVAYA, SIP10049	slps:10049	0	4.41	4.41	4.41	20	10.1.10.154		-1	2020-08-25 18:58:12	slps:10049@10.1.10.154
	slp:medsvr	0	4.41	4.41	4.41	10	10.1.10.13		0	2020-08-25 18:58:22	slp:medsvr@10.1.10.13;d320e747-a...
	slp:medsvr	0	4.41	4.41	4.41	10	10.1.10.13		0	2020-08-25 18:58:22	slp:medsvr@10.1.10.13;d320e747-a...

8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management R135 to interoperate with Avaya Session Border Controller for Enterprise R8.1.0. 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 Session Border Controller for Enterprise on a Virtualized Environment Platform*, Release 8.1.x. Issue 3. Aug 2020.
2. *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x. Issue 3, Aug 2020.
3. *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 8.0.x, Issue 3, May 2020.
4. *Application Notes for Virsae Service Management R135 with Avaya Aura® Communication Manager R8.1.2*.
5. *Application Notes for Virsae Service Management R135 with Avaya Aura® Session 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.

©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.