Avaya Solution & Interoperability Test Lab

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

## Abstract

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

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) to query Avaya Session Border Controller for Enterprise and receives Simple Network Management Protocol (SNMP) traps from Avaya Session Border Controller for Enterprise.

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.

VSM uses SNMP and Linux shell access integration method to monitor Avaya SBCE.

- SNMP collection –Virsae uses SNMP traps to collect alarm and 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.

# 2. General Test Approach and Test Results

The general test approach was to verify VSM using SNMP and SSH connection to monitor and display system status from Avaya SBCE.

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 SSH and SNMPv3 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 SNMPv3.

For serviceability testing, reboots were applied to the VSM and Avaya SBCEs to simulate system unavailability. Loss of network connectivity to both VSM and Avaya SBCE were also performed during testing.

## 2.2. Test Results

All test cases passed.

## 2.3. Support

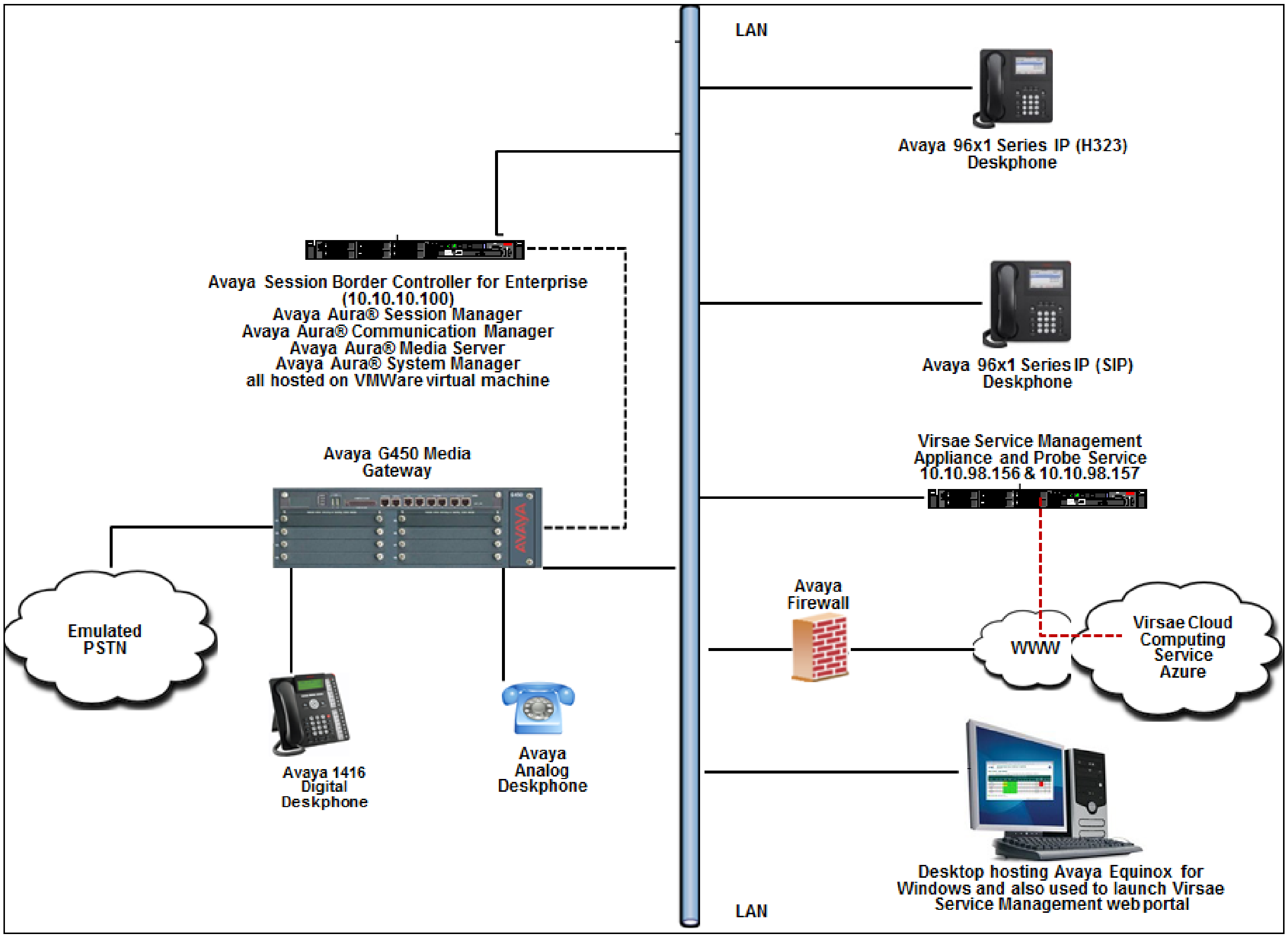
For technical support on Virsae Service Management, contact the Virsae Support Team at:

- 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 G450 Media Gateway. The system has Avaya H323, SIP, Equinox for Windows, digital and analog endpoints configured for making and receiving calls. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. VSM was installed on a server running Microsoft Windows Server 2012 R2 with Service Pack 1. Architecturally the VSM Service relies on an appliance being placed on a corporate LAN and being configured to connect to a Unified Communication platform as well as the Microsoft Azure cloud via the internet. The VSM appliance acts as a collector and compresses, encrypts then forwards data from all sources to the Virsae cloud computing service. A PC/Laptop is used to access the Virsae portal to manage VSM services, add additional users and view reporting data on the equipment being managed.

Also note that for security purposes, any public IP addresses used during the compliance test have been masked or altered in this document.



LAN
Avaya 96x1 Series IP (H323) Deskphone
Avaya Session Border Controller for Enterprise (10.10.10.100)
Avaya Aura® Session Manager
Avaya Aura® Communication Manager
Avaya Aura® Media Server
Avaya Aura® System Manager
all hosted on VMWare virtual machine
Avaya 96x1 Series IP (SIP) Deskphone
Virsae Service Management Appliance and Probe Service 10.10.98.156 & 10.10.98.157
Avaya G450 Media Gateway
Avaya Firewall
Emulated PSTN
WWW
Virsae Cloud Computing Service Azure
Avaya 1416 Digital Deskphone
Avaya Analog Deskphone
Desktop hosting Avaya Equinox for Windows and also used to launch Virsae Service Management web portal
LAN

**Figure 1: Test Configuration**

# 4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| Avaya Session Border Controller for Enterprise running on virtual server | 7.2.2.0-11-15522 |
| Avaya Aura® System Manager running on virtual server | 7.1.3.0 |
| Avaya Aura® Session Manager running on virtual server | 7.1.3.0.713014 |
| Avaya Aura® Media Server running on virtual server | 7.8.0.384 |
| Avaya Aura® Communication Manager running on virtual server | 7.1.3.0.0-FP3 |
| Avaya G450 Media Gateway | 39 .12 .0 /1 |
| Avaya 96x1 Series IP Deskphones:<br>- 9611G (H.323)<br>- 9641GS (SIP) | <br>6.6401<br>7.0.1.2.9 |
| Avaya Equinox for Windows | 3.3.2.20 |
| Avaya 9404 Digital Deskphone | 18.0 |
| Avaya 500 Analog Deskphone | N/A |
| Virsae Service Management for Unified Communications running on Windows 2012 R2 SP1 | 88.2.2.182 |

# 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 and enabling SNMP.

## 5.1. Configure Login Group

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

At the command prompt, type `su root`. When prompted, enter the '**root**' user password.

Use the command `useradd NAME`; where `NAME` is the account name to create and hit enter.

Use the command `passwd NAME`; where `NAME` is the account name created above and hit enter. Enter the password then hit enter (need to do this twice).

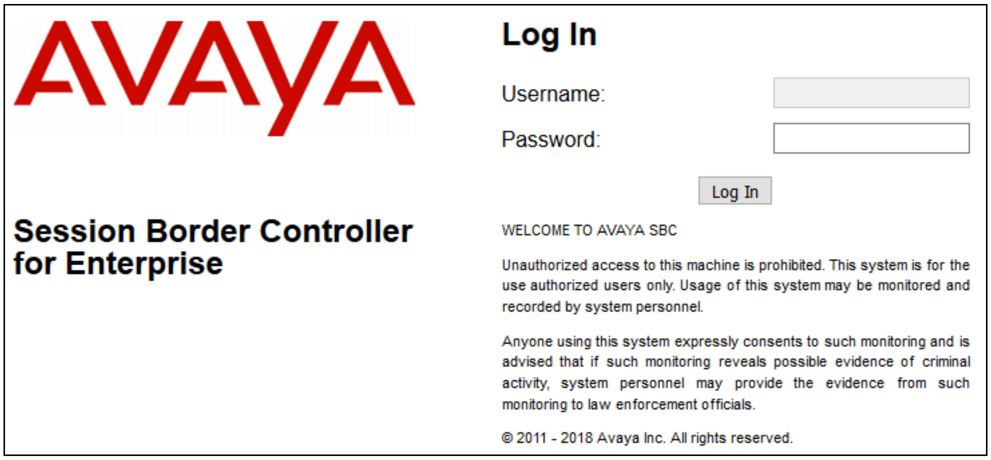
Enter the command `change –M 99999 NAME`; where `NAME` is the account created above and hit enter to set the Avaya SBCE account password to not expire.

If administrator does not have the required privileges to create a new account, then the "ipcs" account will also work. During compliance testing, "ipcs" account was used.

## 5.2. Configure SNMP

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

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.



Session Border Controller for Enterprise

Log In

Username:

Password:

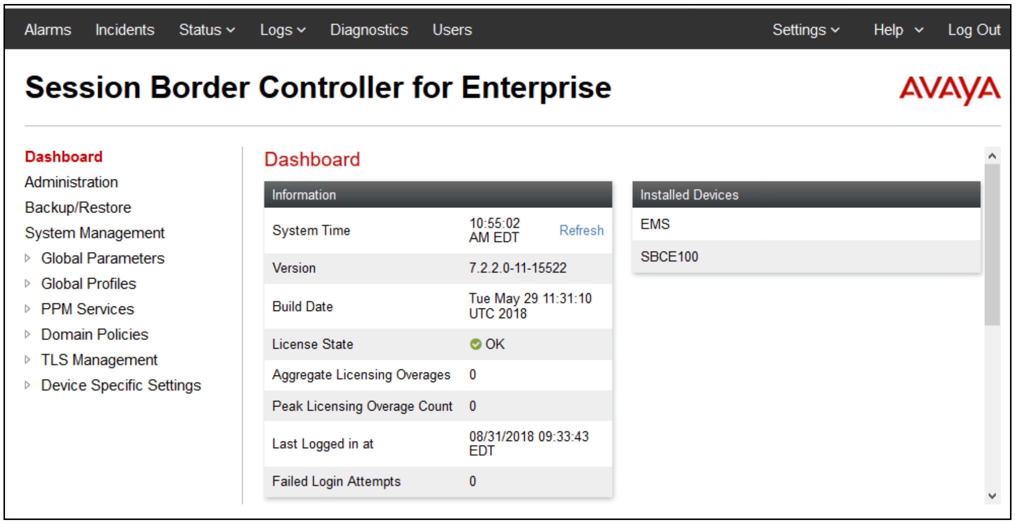
WELCOME TO AVAYA SBC

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.

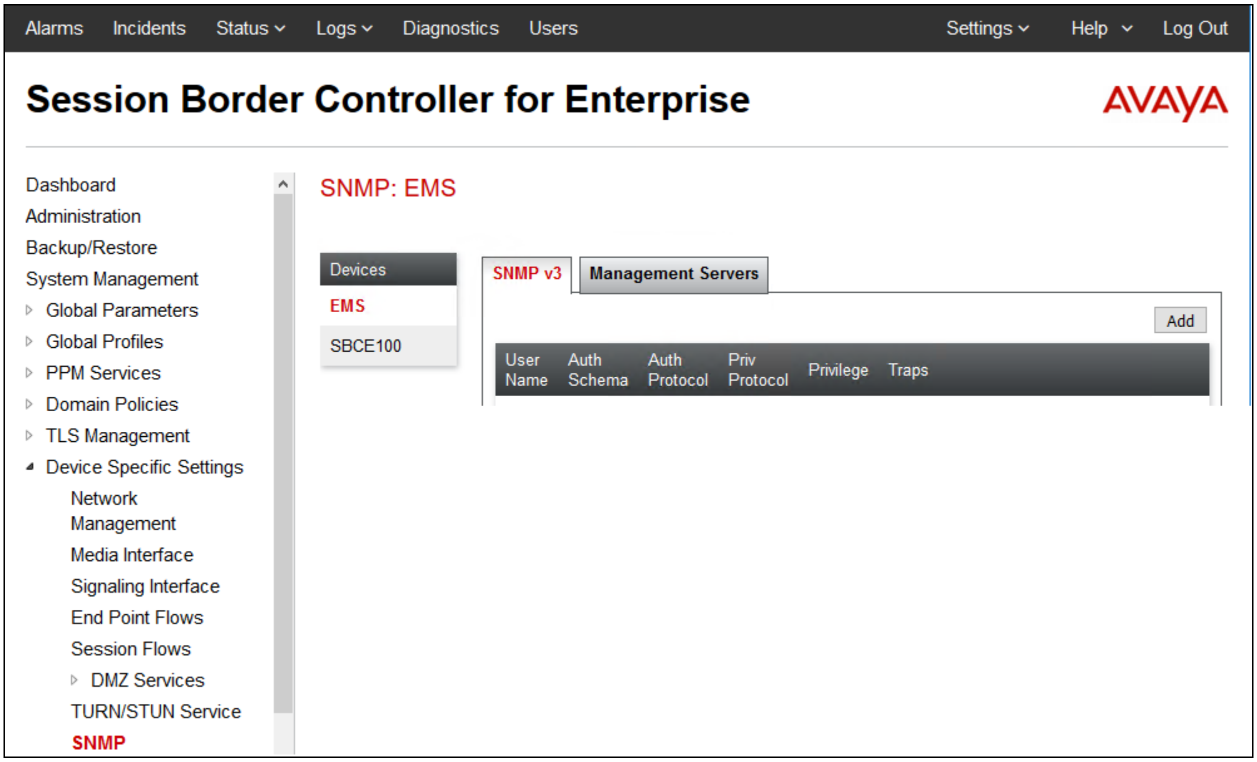
© 2011 - 2018 Avaya Inc. All rights reserved.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



| Information | |
|---|---|
| System Time | 10:55:02 AM EDT |
| Version | 7.2.2.0-11-15522 |
| Build Date | Tue May 29 11:31:10 UTC 2018 |
| License State | ✓ OK |
| Aggregate Licensing Overages | 0 |
| Peak Licensing Overage Count | 0 |
| Last Logged in at | 08/31/2018 09:33:43 EDT |
| Failed Login Attempts | 0 |

Navigate to **Device Specific Settings → SNMP** from the above shown dashboard. The **SNMP:EMS** page is seen as shown below. Under **Devices**, **EMS** and **SBCE100** are seen. Select **EMS** and then select **SNMP v3** tab. Click on the **Add** button.

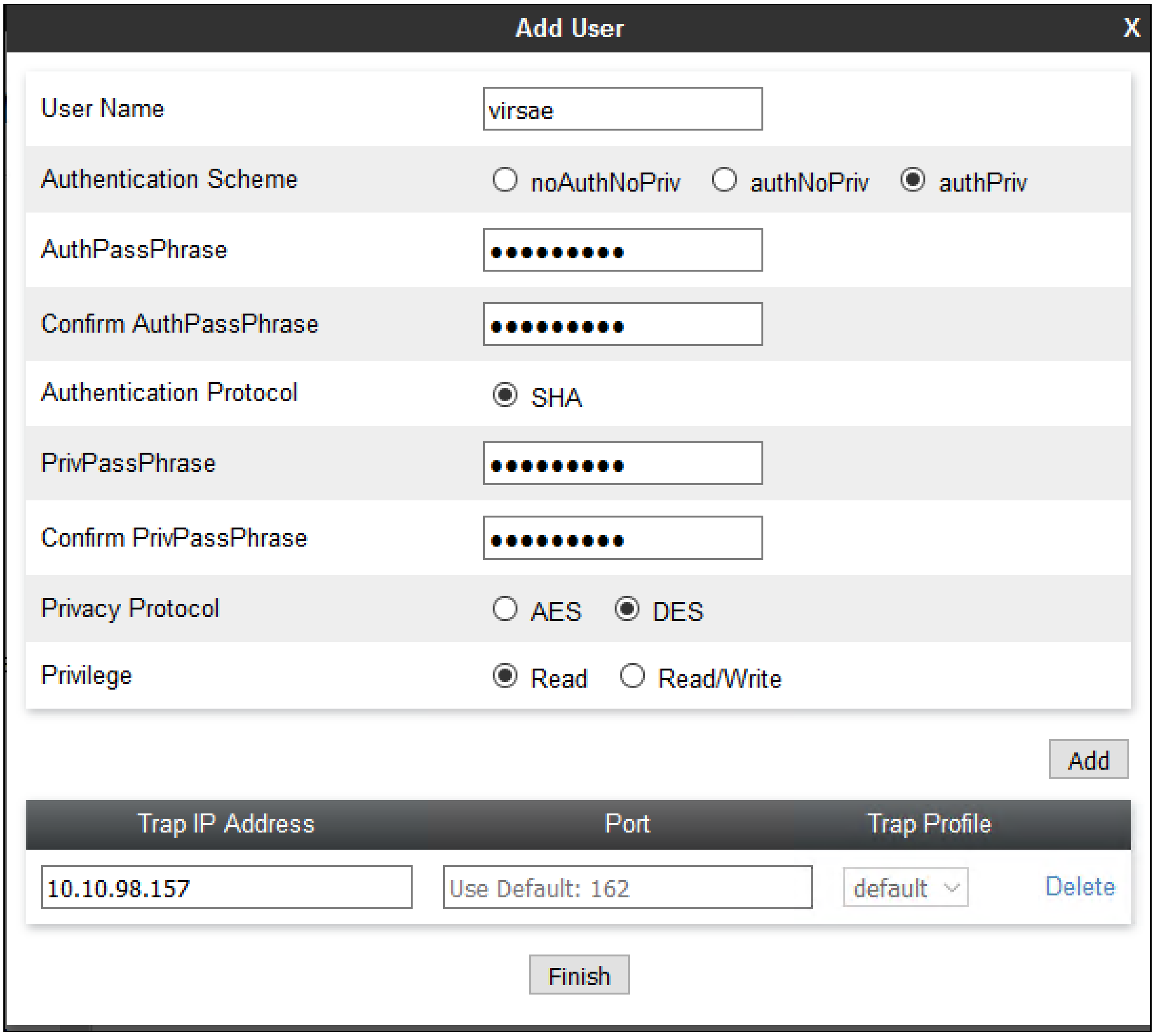


| User Name | Auth Schema | Auth Protocol | Priv Protocol | Privilege | Traps |
|---|---|---|---|---|---|

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 probe.

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

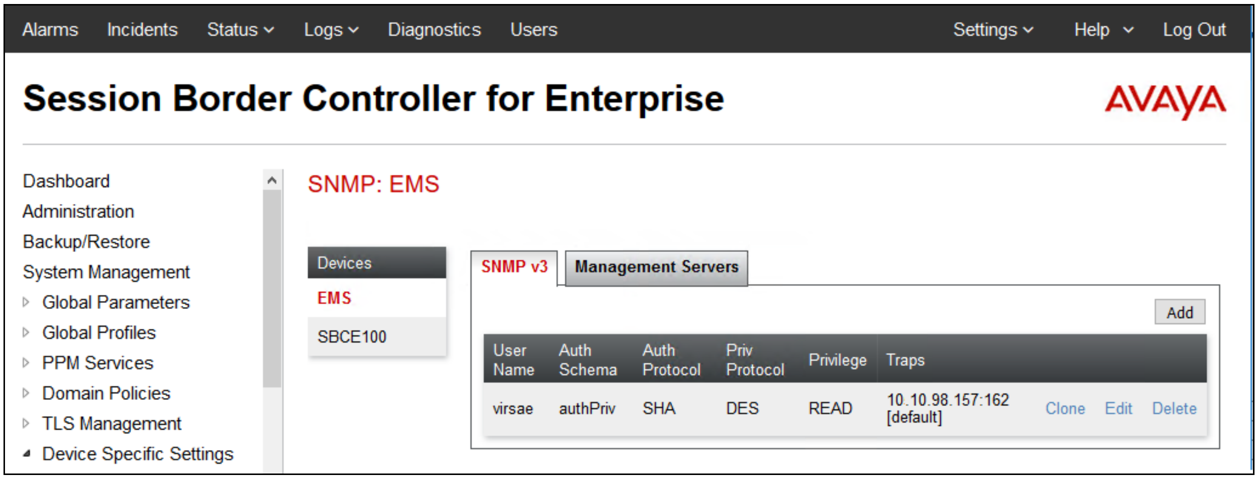


Add User

| | |
|---|---|
| User Name | virsae |
| Authentication Scheme | ○ noAuthNoPriv ○ authNoPriv ● authPriv |
| AuthPassPhrase | ••••••••• |
| Confirm AuthPassPhrase | ••••••••• |
| Authentication Protocol | ● SHA |
| PrivPassPhrase | ••••••••• |
| Confirm PrivPassPhrase | ••••••••• |
| Privacy Protocol | ○ AES ● DES |
| Privilege | ● Read ○ Read/Write |

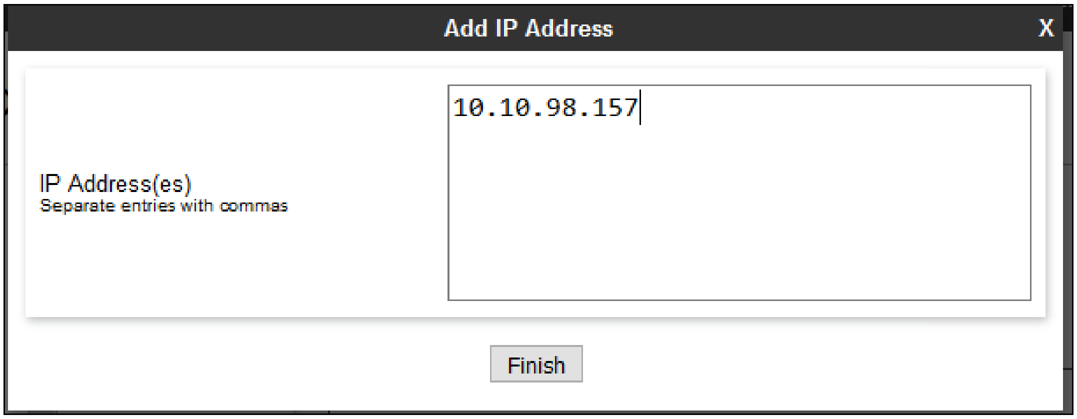
| Trap IP Address | Port | Trap Profile | |
|---|---|---|---|
| 10.10.98.157 | Use Default: 162 | default | Delete |

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



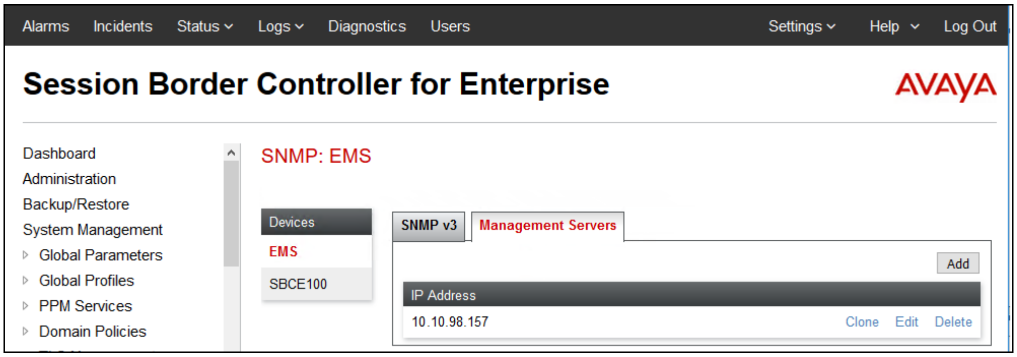
| User Name | Auth Schema | Auth Protocol | Priv Protocol | Privilege | Traps | | | |
|---|---|---|---|---|---|---|---|---|
| virsae | authPriv | SHA | DES | READ | 10.10.98.157:162<br>[default] | Clone | Edit | Delete |

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



IP Address(es)
Separate entries with commas
10.10.98.157

Screen below shows the Management Servers configured for EMS device.

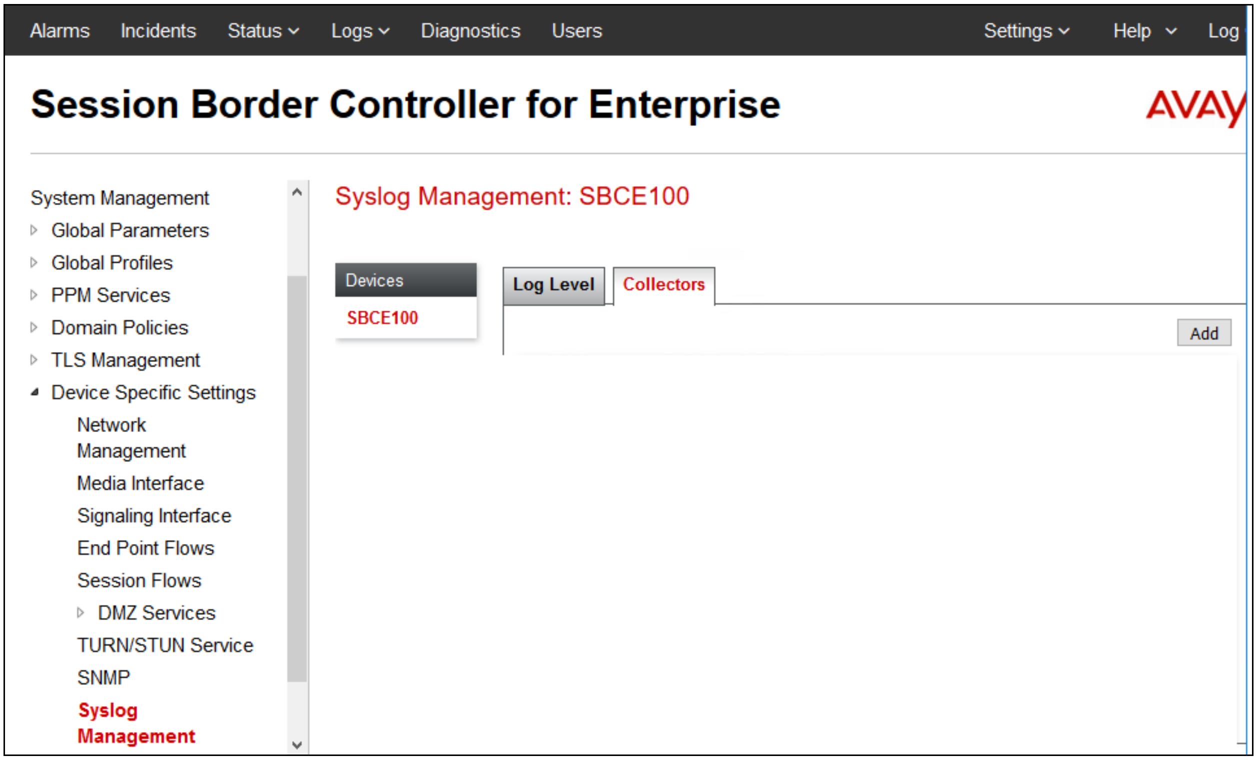


| IP Address | | | |
|---|---|---|---|
| 10.10.98.157 | Clone | Edit | Delete |

Repeat all the above steps for **SBCE100** under **Devices** too.

## 5.3. Configure Syslog Management

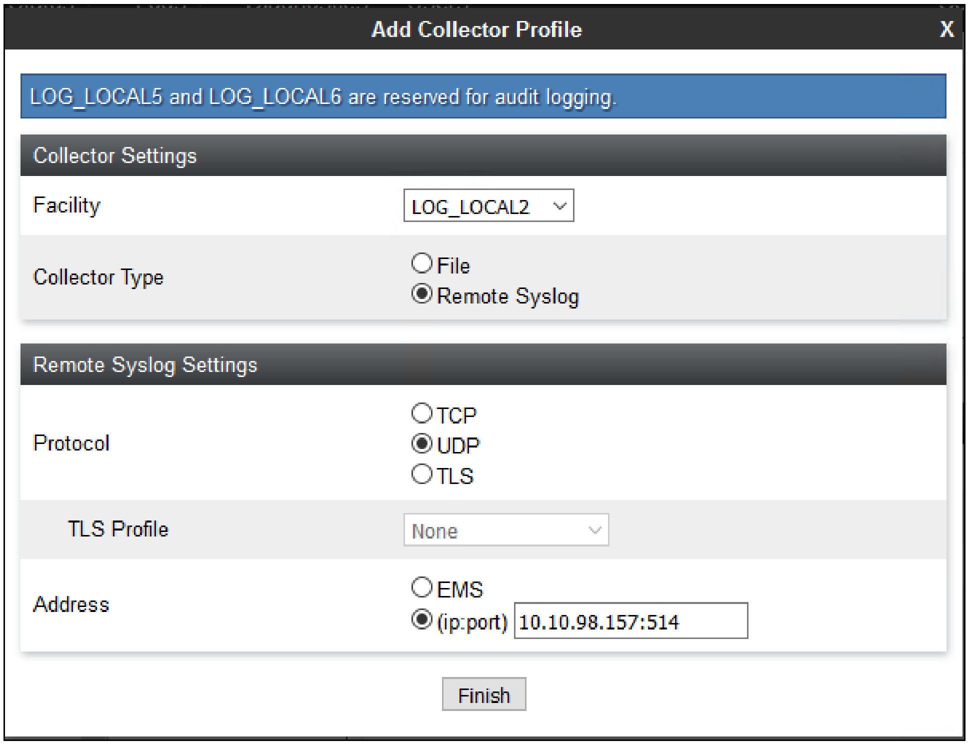
To setup syslog output from Avaya SBCE to VSM, navigate to **Device Specific Settings → Syslog Management** from the dashboard shown below. The **Syslog Management: SBCE100** page is seen. Under **Devices**, **SBCE100** is seen. Select **SBCE100** and then select **Collectors** tab. Click on the **Add** button.



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

- **Facility**: A collector suffix that is not being used is selected. During compliance testing **LOG_LOCAL2** was selected.
- **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 probe and the port as **514**.

Click on the **Finish** button.



Add Collector Profile

LOG_LOCAL5 and LOG_LOCAL6 are reserved for audit logging.

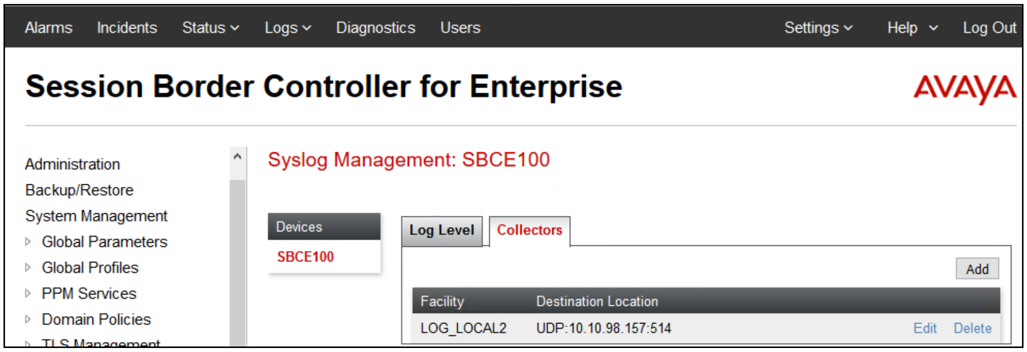
Collector Settings

| | |
|---|---|
| Facility | LOG_LOCAL2 |
| Collector Type | ○ File<br>● Remote Syslog |

Remote Syslog Settings

| | |
|---|---|
| Protocol | ○ TCP<br>● UDP<br>○ TLS |
| TLS Profile | None |
| Address | ○ EMS<br>● (ip:port) 10.10.98.157:514 |

Screen below shows the Collectors configured for SBCE100 device. Now select the **Log Level** tab.



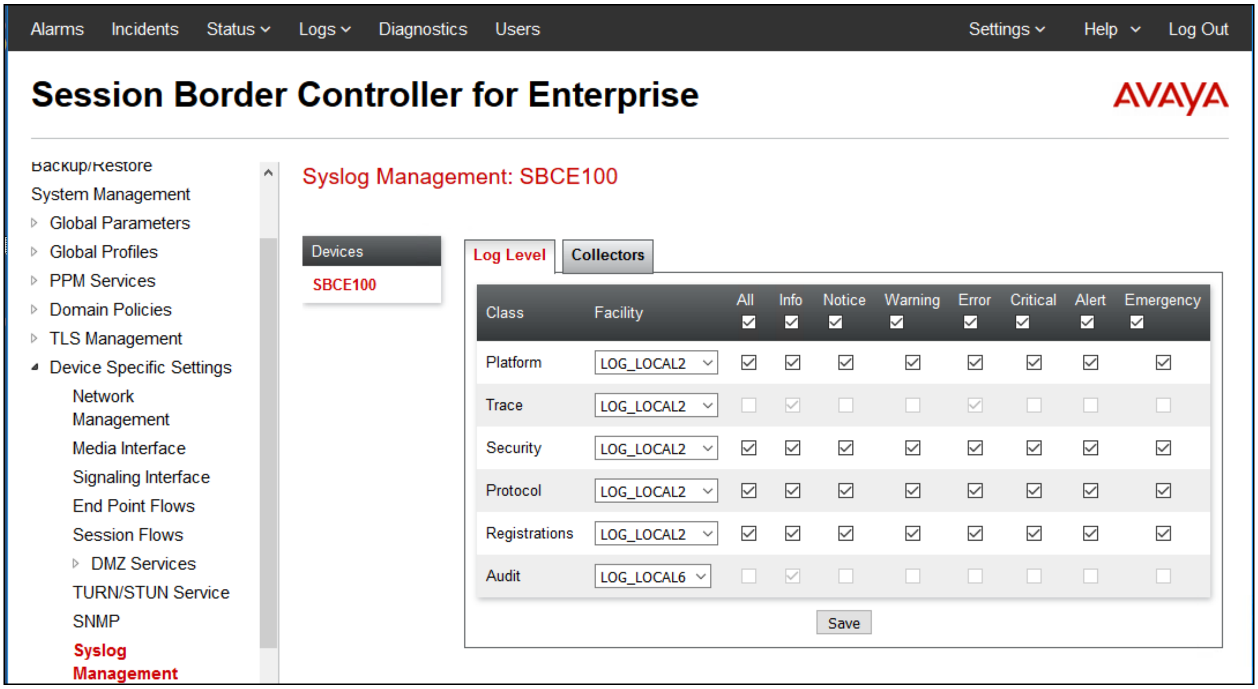
Session Border Controller for Enterprise

Syslog Management: SBCE100

Devices: SBCE100

| Facility | Destination Location | |
|---|---|---|
| LOG_LOCAL2 | UDP:10.10.98.157:514 | Edit Delete |

In the **Log Level** tab screen shown below, select the **Facility** configured above for the **Class Platform**, **Trace**, **Security**, **Protocol** and **Registrations**. During compliance testing, **All** levels of logs were selected. Click on the **Save** button.



Session Border Controller for Enterprise

Syslog Management: SBCE100

SBCE100

| Class | Facility | All<br>☑ | Info<br>☑ | Notice<br>☑ | Warning<br>☑ | Error<br>☑ | Critical<br>☑ | Alert<br>☑ | Emergency<br>☑ |
|---|---|---|---|---|---|---|---|---|---|
| Platform | LOG_LOCAL2 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| Trace | LOG_LOCAL2 | □ | ☑ | □ | □ | ☑ | □ | □ | □ |
| Security | LOG_LOCAL2 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| Protocol | LOG_LOCAL2 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| Registrations | LOG_LOCAL2 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| Audit | LOG_LOCAL6 | □ | ☑ | □ | □ | □ | □ | □ | □ |

# 6. Configure Virsae Service Management

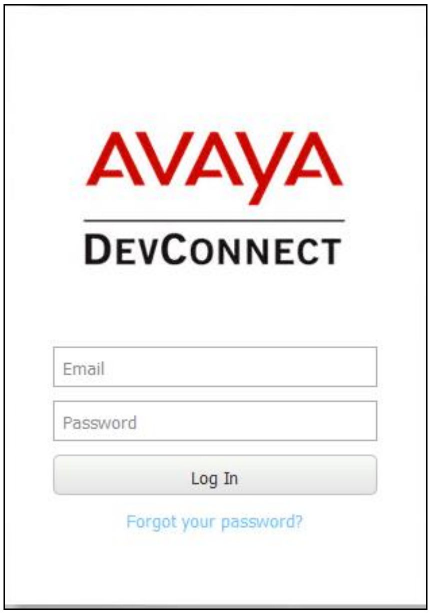
This section describes the configuration of VSM required to interoperate with Avaya SBCE.

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, supplied by Virsae, are provided only for reference. These represent only an example of the configuration GUI of VSM, available through the web Portal. Contact Virsae for details on how to configure VSM. The configuration operations described in this section can be summarized as follows:

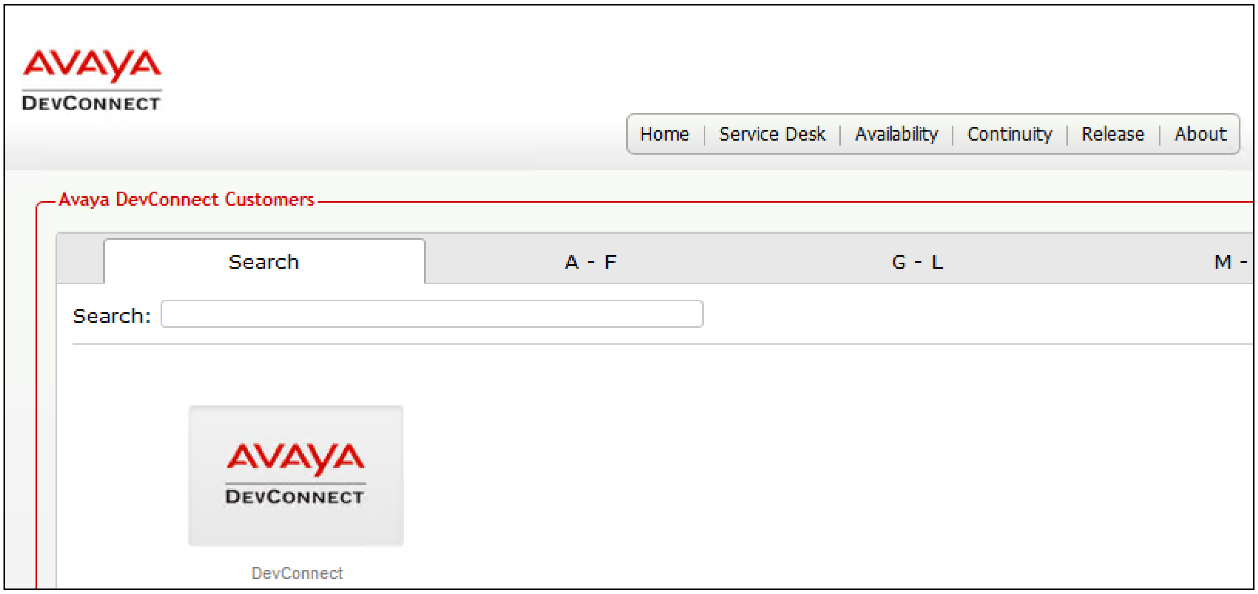
- Login to the Web Portal
- Configuring Avaya Session Border Controller for Enterprise
- Configure Dashboard

## 6.1. Login to the Web Portal

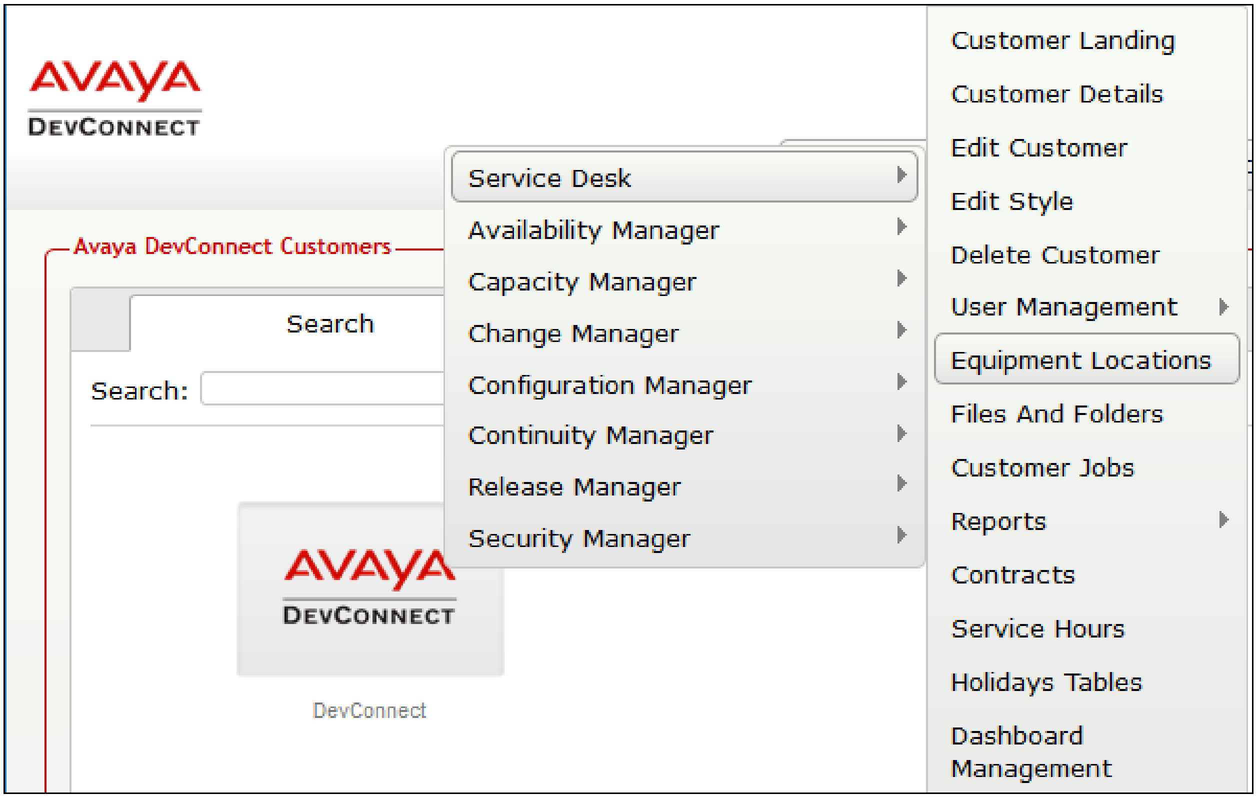
A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL *<business partner name>.virsae.com* in a web browser. During compliance testing the URL used was *devconnect.virsae.com*. The Login screen is shown as below. Enter the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



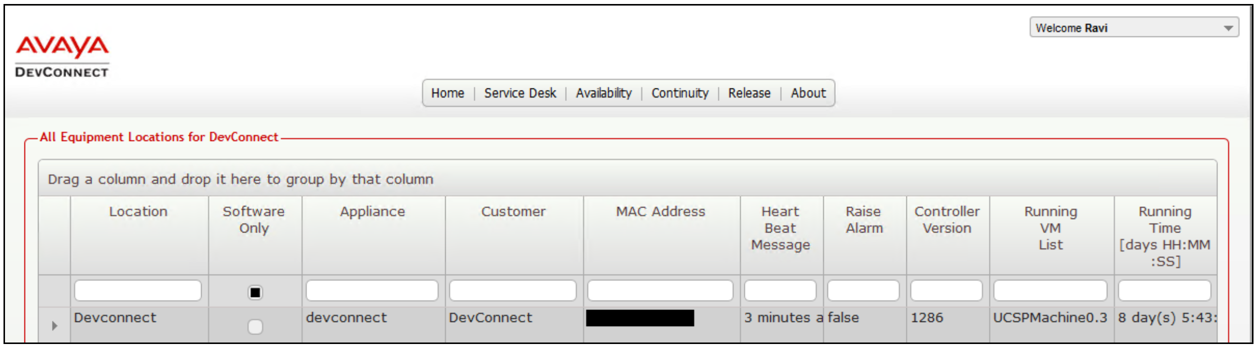
The customers belonging to a business partner screen is shown. During compliance testing, the customer created by Virsae is **DevConnect** which belongs to the business **Avaya DevConnect Customers**.


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

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



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


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

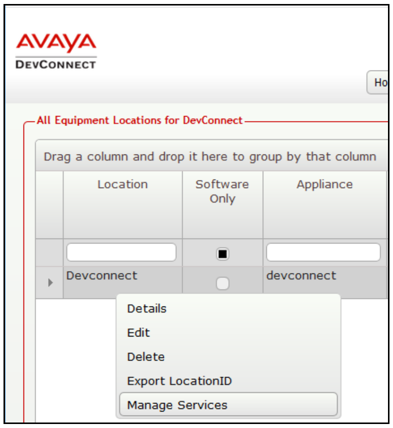
All Equipment Locations for DevConnect

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

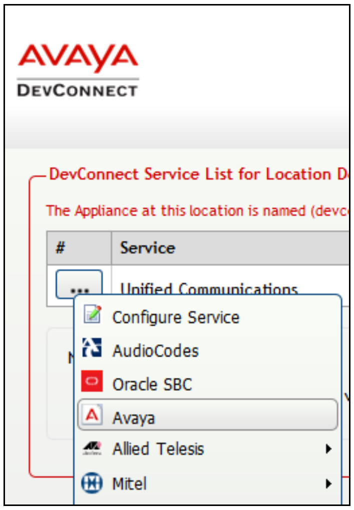
| Location | Software Only | Appliance | Customer | MAC Address | Heart Beat Message | Raise Alarm | Controller Version | Running VM List | Running Time [days HH:MM :SS] |
|---|---|---|---|---|---|---|---|---|---|
| Devconnect | ○ | devconnect | DevConnect | [redacted] | 3 minutes a | false | 1286 |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

## 6.2. Configuring Avaya Session Border Controller for Enterprise

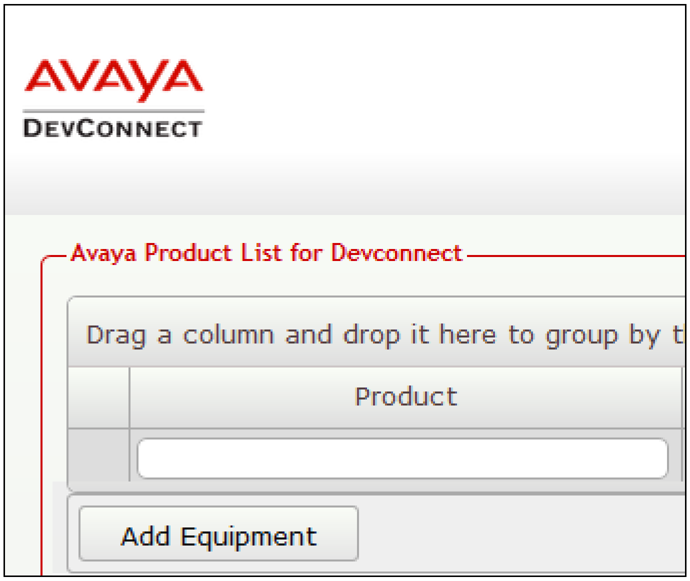
To add an Avaya SBCE to the Location created in **Section 6.1**, right click on the location **Devconnect** and select **Manage Services** as shown below.



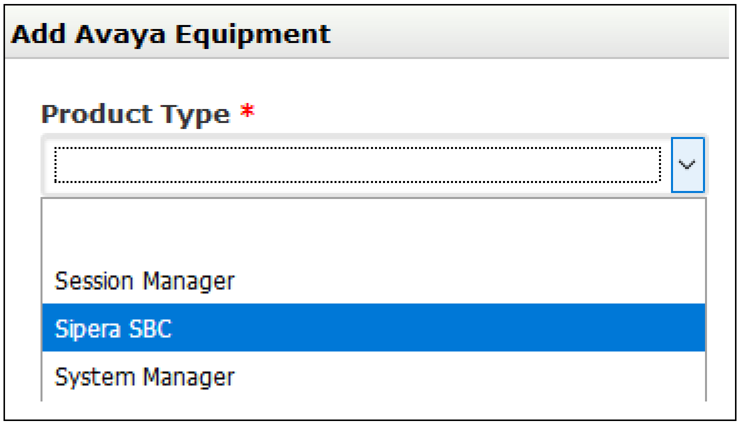
From the **Unified Communications** Service, select **Avaya**.



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

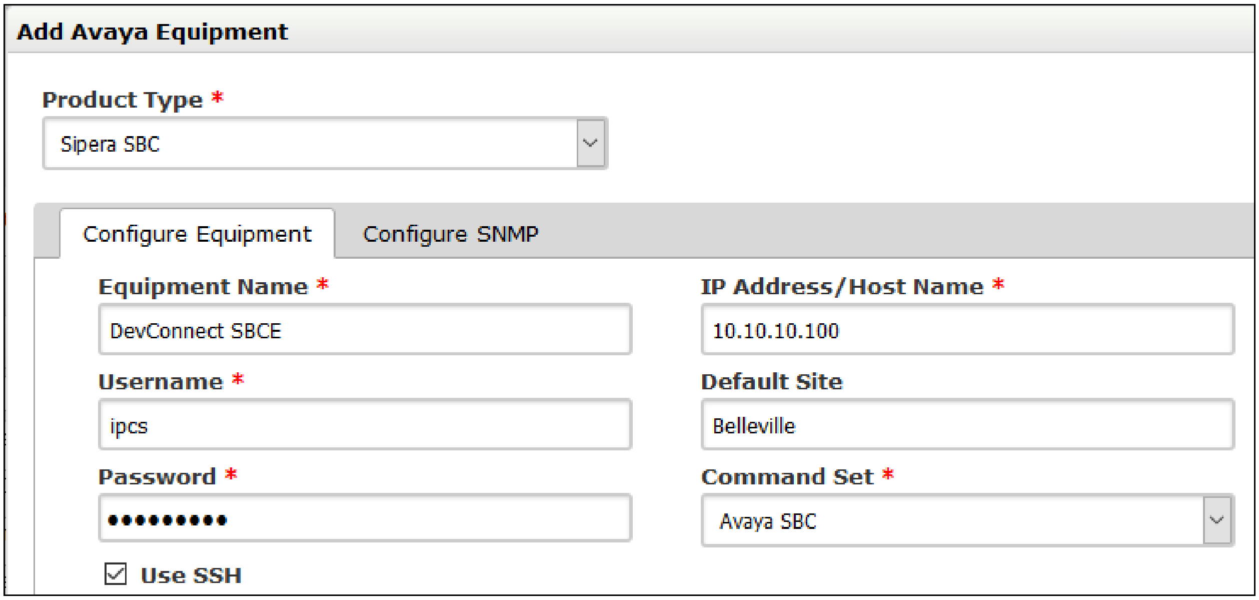

AVAYA
DEVCONNECT
Avaya Product List for Devconnect
Drag a column and drop it here to group by t
Product
Add Equipment

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



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



Add Avaya Equipment

Product Type * : Sipera SBC

Configure Equipment | Configure SNMP

Equipment Name * : DevConnect SBCE

IP Address/Host Name * : 10.10.10.100

Username * : ipcs

Default Site : Belleville

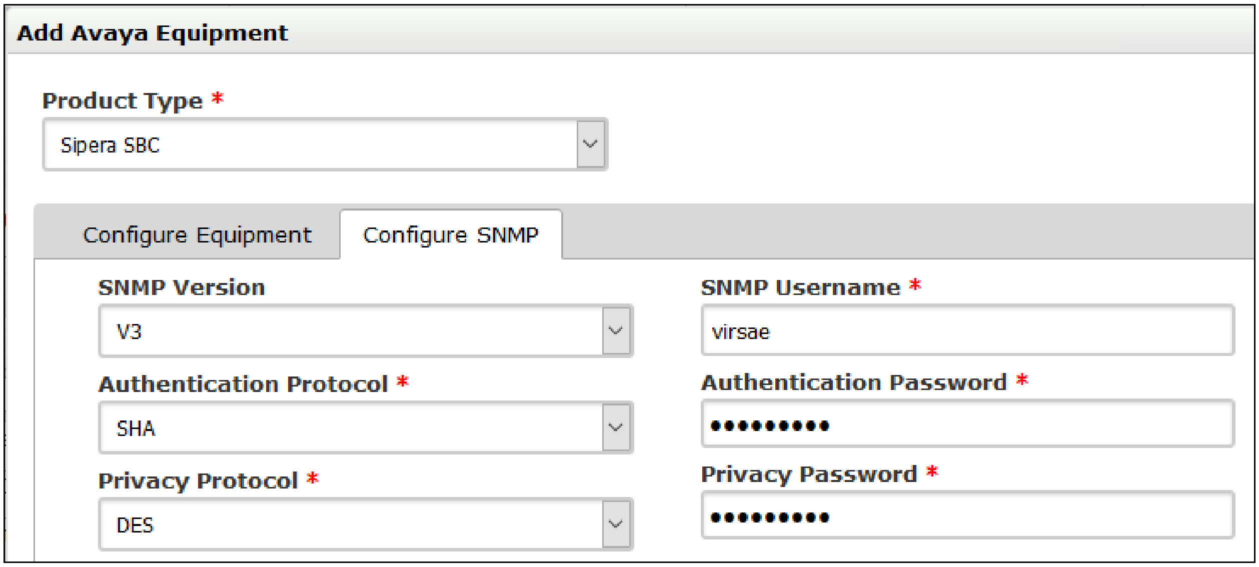
Password * : •••••••••

Command Set * : Avaya SBC

☑ Use SSH

In the **Configure SNMP** tab, select the **SNMP 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 **Add** (not shown) button to complete the configuration.



Add Avaya Equipment

Product Type *: Sipera SBC

SNMP Version: V3

SNMP Username *: virsae

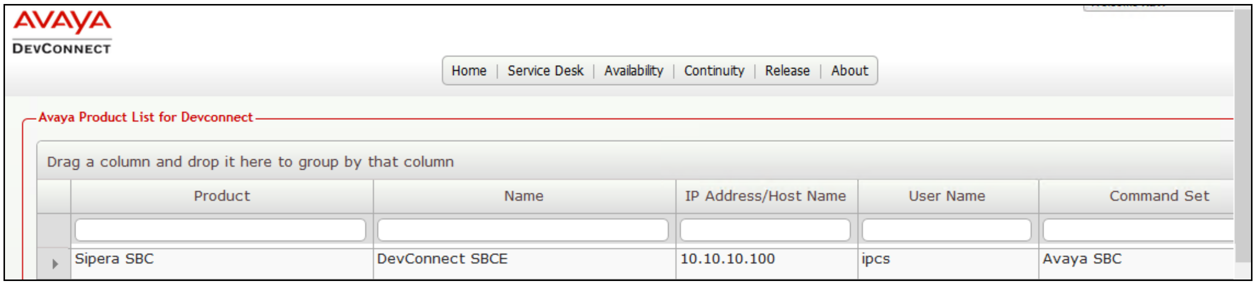
Authentication Protocol *: SHA

Authentication Password *: ●●●●●●●●●

Privacy Protocol *: DES

Privacy Password *: ●●●●●●●●●

The screen below shows the added Avaya SBCE equipment.



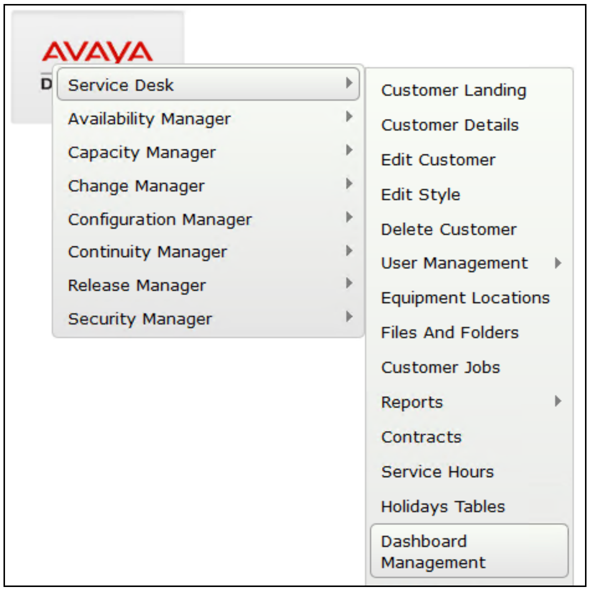
AVAYA
DEVCONNECT
Home | Service Desk | Availability | Continuity | Release | About
Avaya Product List for Devconnect
Drag a column and drop it here to group by that column

| Product | Name | IP Address/Host Name | User Name | Command Set |
|---|---|---|---|---|
| Sipera SBC | DevConnect SBCE | 10.10.10.100 | ipcs | Avaya SBC |

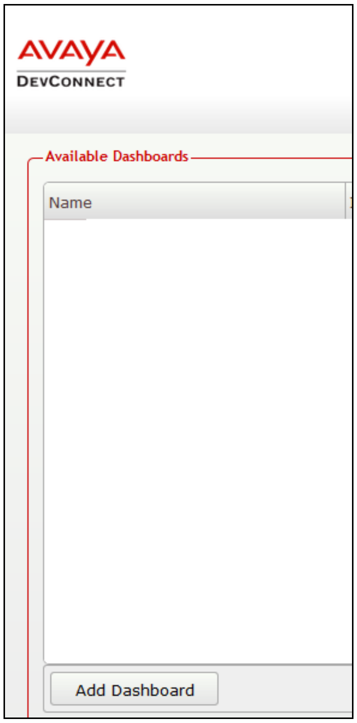
## 6.3. Configure Dashboard

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

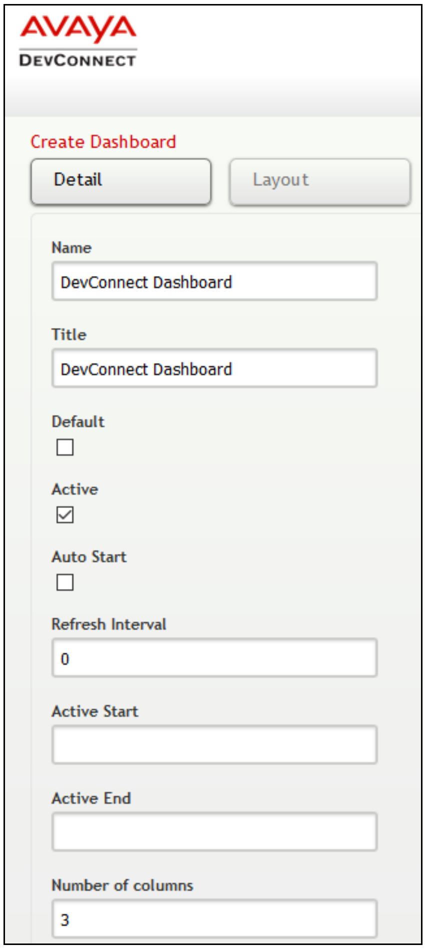
From the customer icon, navigate to **Service Desk → Dashboard Management** as shown below.



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



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



Name: DevConnect Dashboard

Title: DevConnect Dashboard

Default: □

Active: ☑

Auto Start: □

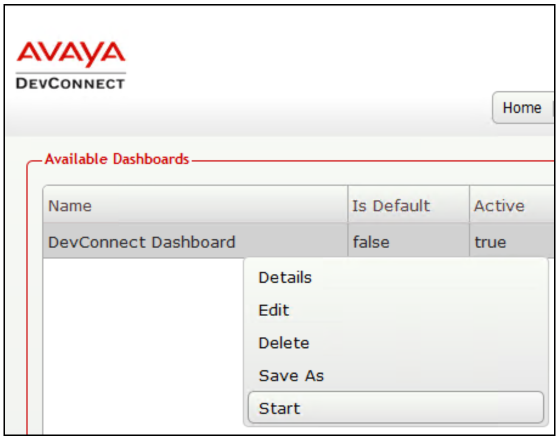
Refresh Interval: 0

Active Start:

Active End:

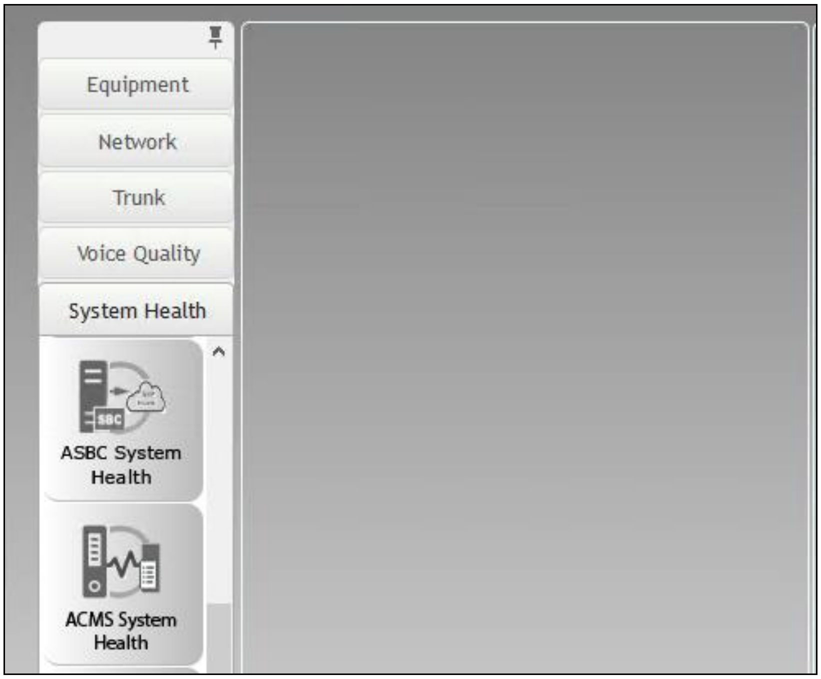
Number of columns: 3

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

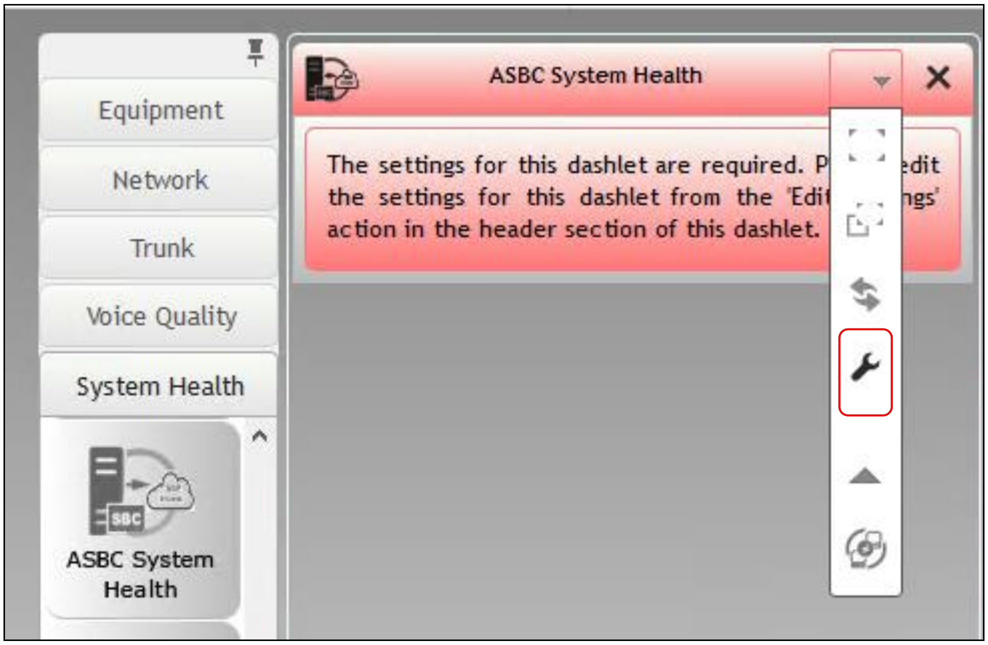


| Name | Is Default | Active |
|---|---|---|
| DevConnect Dashboard | false | true |

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

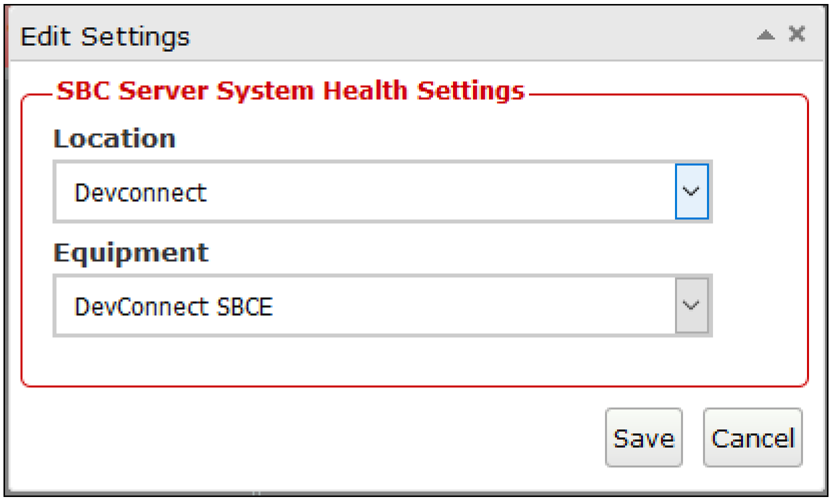


From the drop-down menu for **ASBC System Health** window, select the **Edit Settings** button as shown below.



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

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



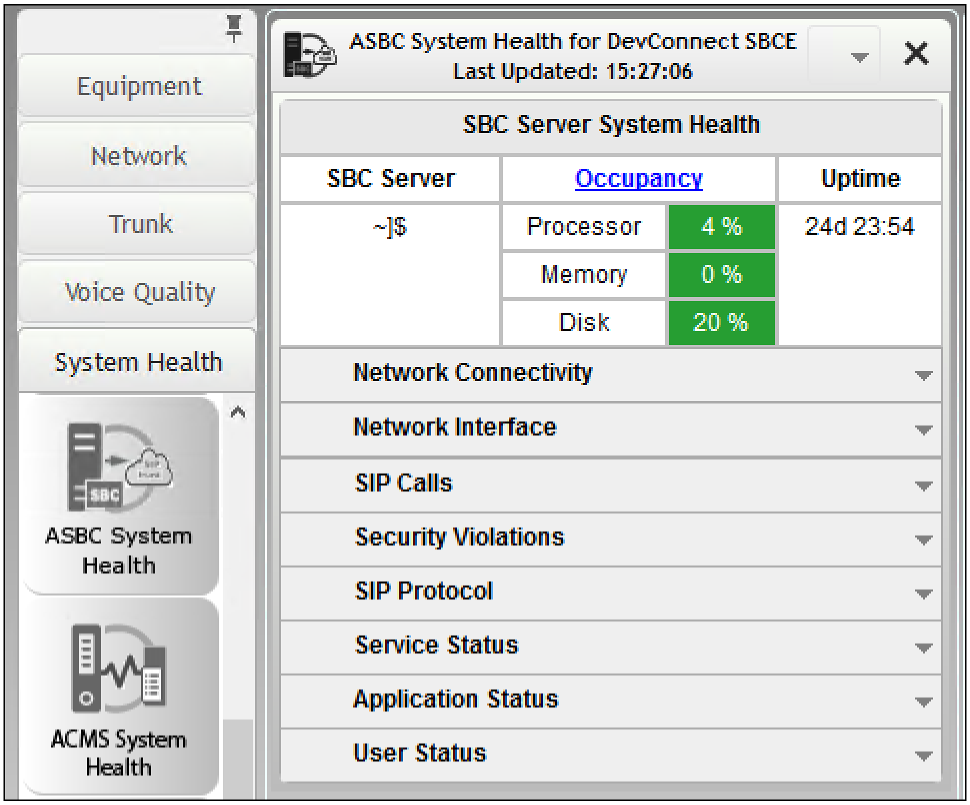
Edit Settings

SBC Server System Health Settings

Location: Devconnect

Equipment: DevConnect SBCE

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



ASBC System Health for DevConnect SBCE
Last Updated: 15:27:06

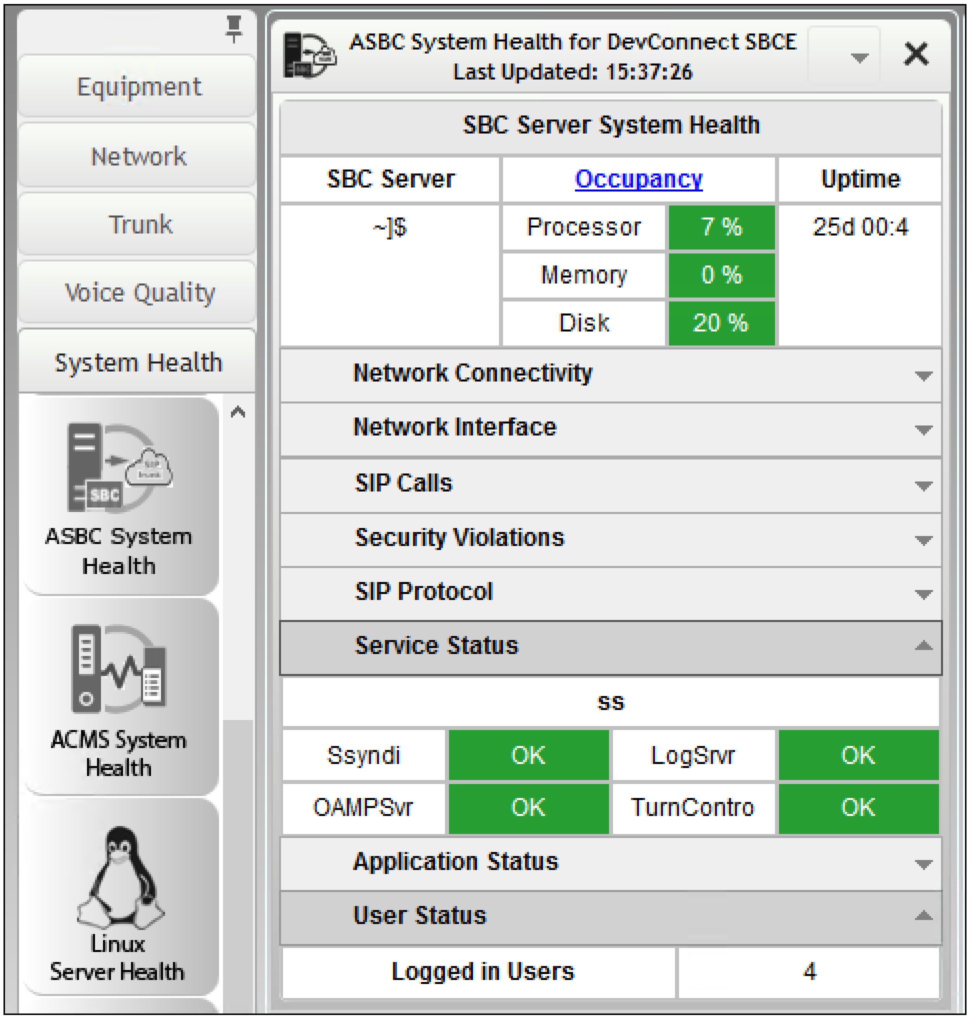
SBC Server System Health

| SBC Server | Occupancy | | Uptime |
|---|---|---|---|
| ~]$ | Processor | 4 % | 24d 23:54 |
| | Memory | 0 % | |
| | Disk | 20 % | |

# 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 logging into the web portal, navigate to **Service Desk → Dashboard Management** (not shown). Start the dashboard and the screen below shows the System Health of the already configured Avaya SBCE for various parameters.



ASBC System Health for DevConnect SBCE
Last Updated: 15:37:26

SBC Server System Health

| SBC Server | Occupancy | | Uptime |
|---|---|---|---|
| ~]$ | Processor | 7 % | 25d 00:4 |
| | Memory | 0 % | |
| | Disk | 20 % | |

Network Connectivity

Network Interface

SIP Calls

Security Violations

SIP Protocol

Service Status

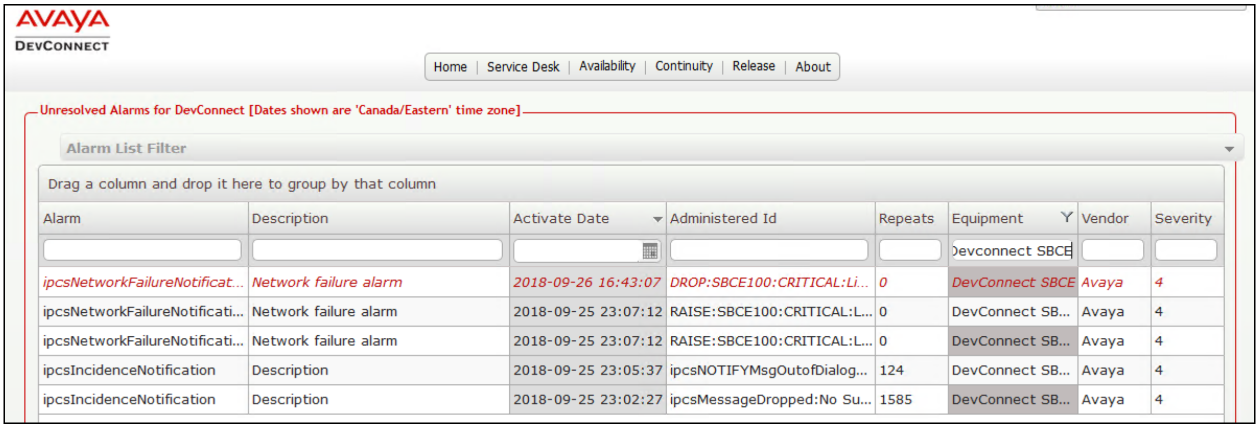
| ss | | | |
|---|---|---|---|
| Ssyndi | OK | LogSrvr | OK |
| OAMPSvr | OK | TurnContro | OK |

Application Status

User Status

| Logged in Users | 4 |
|---|---|

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


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

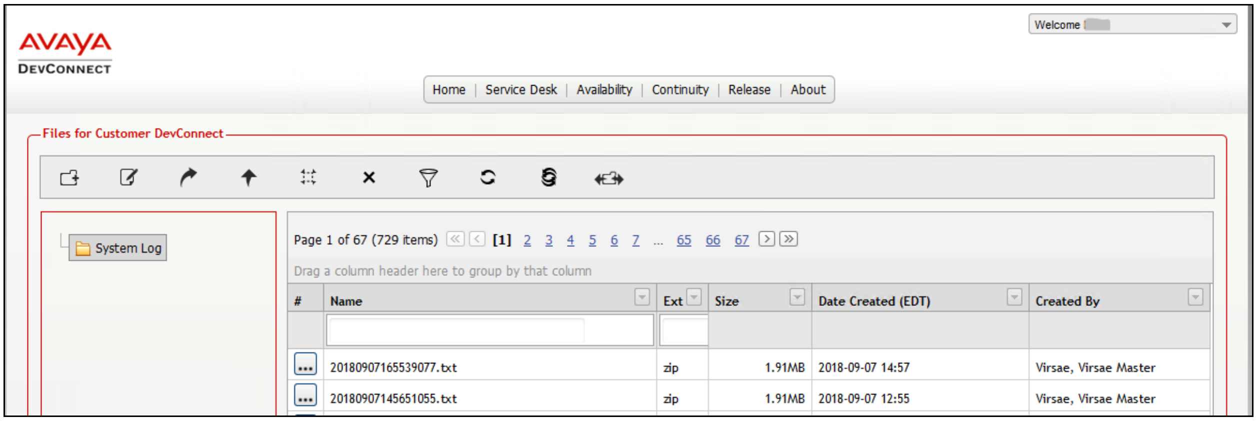
Unresolved Alarms for DevConnect [Dates shown are 'Canada/Eastern' time zone]

Alarm List Filter

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

| Alarm | Description | Activate Date | Administered Id | Repeats | Equipment | Vendor | Severity |
|---|---|---|---|---|---|---|---|
| | | | | | Jevconnect SBCE | | |
| *ipcsNetworkFailureNotificat...* | *Network failure alarm* | *2018-09-26 16:43:07* | *DROP:SBCE100:CRITICAL:Li...* | *0* | *DevConnect SBCE* | *Avaya* | *4* |
| ipcsNetworkFailureNotificati... | Network failure alarm | 2018-09-25 23:07:12 | RAISE:SBCE100:CRITICAL:L... | 0 | DevConnect SB... | Avaya | 4 |
| ipcsNetworkFailureNotificati... | Network failure alarm | 2018-09-25 23:07:12 | RAISE:SBCE100:CRITICAL:L... | 0 | DevConnect SB... | Avaya | 4 |
| ipcsIncidenceNotification | Description | 2018-09-25 23:05:37 | ipcsNOTIFYMsgOutofDialog... | 124 | DevConnect SB... | Avaya | 4 |
| ipcsIncidenceNotification | Description | 2018-09-25 23:02:27 | ipcsMessageDropped:No Su... | 1585 | DevConnect SB... | Avaya | 4 |

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


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

Files for Customer DevConnect

Page 1 of 67 (729 items) « ‹ [1] 2 3 4 5 6 7 ... 65 66 67 › »

Drag a column header here to group by that column

| # | Name | Ext | Size | Date Created (EDT) | Created By |
|---|---|---|---|---|---|
| ... | 20180907165539077.txt | zip | 1.91MB | 2018-09-07 14:57 | Virsae, Virsae Master |
| ... | 20180907145651055.txt | zip | 1.91MB | 2018-09-07 12:55 | Virsae, Virsae Master |

# 8. Conclusion

These Application Notes describe the procedures for configuring the Virsae Service Management to interoperate with Avaya Session Border Controller for Enterprise. During compliance testing, all test cases were completed successfully with observations if any noted in **Section 2.2**.

# 9. Additional References

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

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

1. *Deploying Avaya Aura® Session Manager*, Release 7.1.3. Issue 5. May 2018.
2. *Administering Avaya Aura® Session Manager*, Release 7.1.3. Issue 5. May 2018.
3. *Deploying Avaya Aura® System Manager*, 7.1.3. Issue 8. July 2018.
4. *Administering Avaya Aura® System Manager for Release 7.1.3*, Release 7.1.3. Issue 15. July 2018.
5. *Deploying Avaya Aura® Communication Manager*, Release 7.1.3. Issue 5. May 2018.
6. *Administering Avaya Aura® Communication Manager*, Release 7.1.3. Issue 7. May 2018.
7. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.3. Issue 6. May 2018.
8. *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.2.2. Issue 7. July 2018.
9. *Administering Avaya Session Border Controller for Enterprise*, Release 7.2.2. Issue 10. June 2018.

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

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

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.