Avaya Solution & Interoperability Test Lab

Application Notes for Virsae Service Management for Unified Communications with Avaya IP Office Server Edition - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management for Unified Communication to interoperate with Avaya IP Office Server Edition. Virsae Service Management provides real-time monitoring and displays Avaya IP Office Server Edition information regarding Voice Quality, Syslog, Call Details, Alarms, Ping test results and Protocol validation using Simple Network Management Protocol (SNMP), Real Time Transport Control Protocol (RTCP) connections and Call Detail Records (SMDR).

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.

©2018 Avaya Inc. All Rights Reserved.

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 IP Office Server Edition (herein after referred to as IP Office). Test configuration included deploying Avaya IP Office on a Primary Linux Server and on a 500 V2 Expansion server.

During compliance test, one VSM server managed a Primary IP Office Server Edition and an IP Office 500 V2 Expansion as separate system; one instance of each must be added on VSM. VSM uses SNMP Version 1c connection to monitor Primary Linux Server and 500 V2 Expansion server.

VSM uses SNMP messages received from IP Office systems to monitor events and displays them on web-based interface. VSM collects RTCP packets from H.323 and SIP phones and displays detailed call traffic. VSM also collects the CDR details of internal and external, and inbound and outbound calls.

2. General Test Approach and Test Results

The feature test cases were performed manually. Manually make calls using H.323 and SIP phones, which register to Primary Server as well as H.323 and SIP phones which register to 500 V2 Expansion server to verify the proper call traffic detail is displayed. Verify Voice Quality, Syslog, Call Details, Alarms, Ping test results and Protocol validation details are displayed correctly.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to 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.

©2018 Avaya Inc. All Rights Reserved.

For the testing associated with these Application Notes, the interface between Avaya systems and VSM utilized capabilities of 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

2.1. Interoperability Compliance Testing

The compliance testing verified the use of the VSM web interface to display correct information of the IP Office configuration.

- Verify IP Office is successfully configured to be monitored by VSM.
- Verify SNMP traps received from IP Office such as Alarms (Critical, Major, Minor and Warning), SNMP Availability and VSM raised Alerts.
- Verify IP Office call traffic detail information such as Time Start/End of Call, Local/Remote PBX, Phone Type, Mean Opinion Score (MOS) Cost and Quality of Service.
- Verify CDR for internal and external calls, and inbound and outbound calls.

©2018 Avaya Inc. All Rights Reserved.

2.2. Test Results

All test cases passed successfully with the following observation.

- Avaya H.323 Phones will get the RTCP collector information as part of registration to the IP Office. Changing the setting will require re-registration of the phones for the change to take effect. Other phone types, if they support dual unicast of RTCP data, will need manual configuration. Refer to **Section 5.1** for further details.

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

©2018 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify the VSM application with Avaya IP Office Server Edition including a Primary Linux Server and a 500 V2 Expansion server. Each system has its own SNMP/RTCP/SMDR connection to VSM. 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 probe service of the VSM server communicates with IP Office. 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.

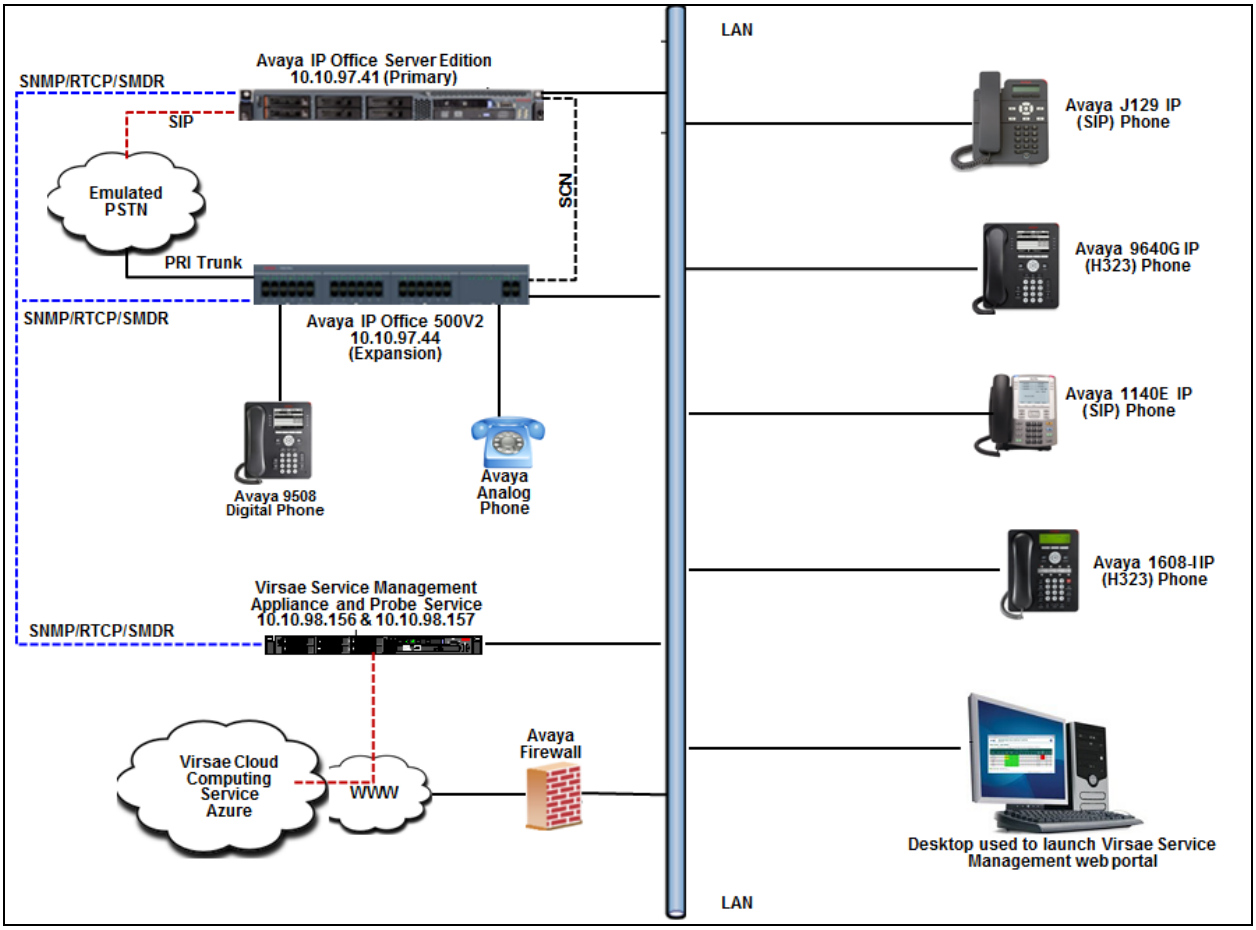


Figure 1: Test Configuration Diagram

©2018 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

The following equipment and software were used for the compliance test provided:

Equipment/Software	Release/Version
Avaya IP Office Server Edition on Primary Linux server	11.0.0.0.0 build 849
Avaya IP Office 500 V2 Expansion	11.0.0.0.0 build 849
Avaya IP Phones: - 1140E (SIP) - J129 (SIP) -9641G (H.323) -1608-I (H.323)	 4.4.23 2.0.0.0.45 6.6506 1.3110
Avaya 9508 Digital Phone	0.60
Virsae Service Management running on Windows 2012 R2 SP1	R79

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and when deployed with IP Office Server Edition in all configurations.

©2018 Avaya Inc. All Rights Reserved.

5. Configure Avaya IP Office Server Edition

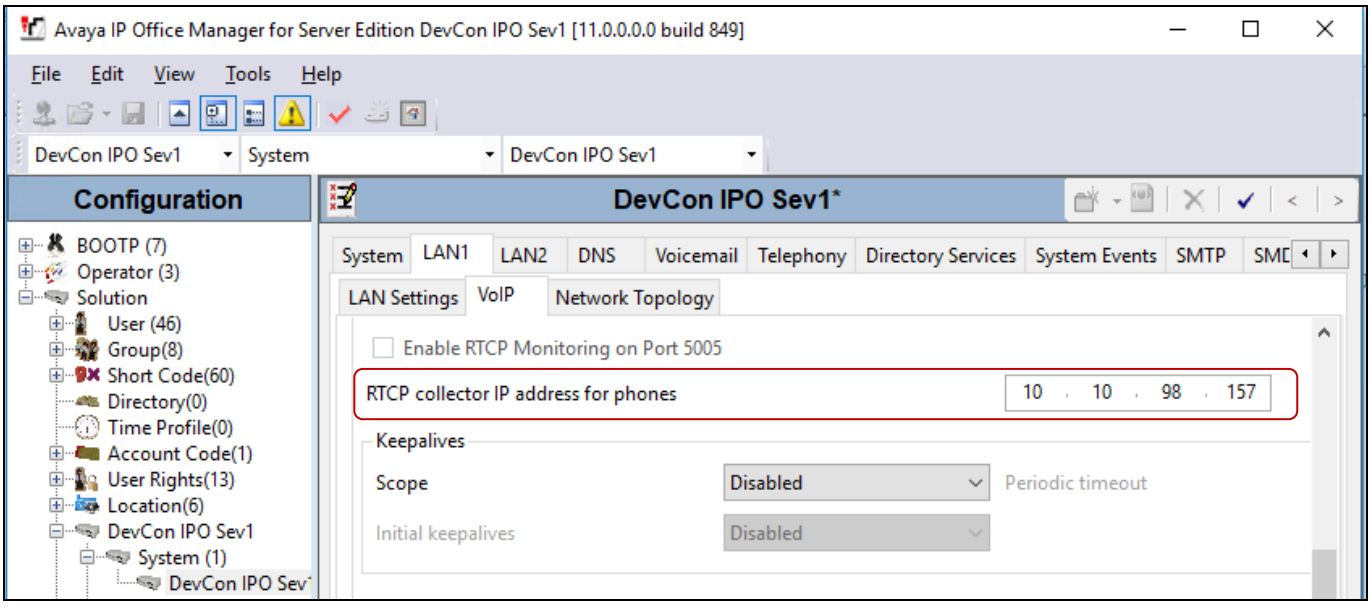
Configuration and verification operations on the Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. This section only covers the following configuration that is required for administering connectivity to VSM. It is implied a working system is already in place with the necessary licensing. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Configure RTCP
- Configure SNMP
- Configure SMDR
- Save Configuration

5.1. Configure RTCP

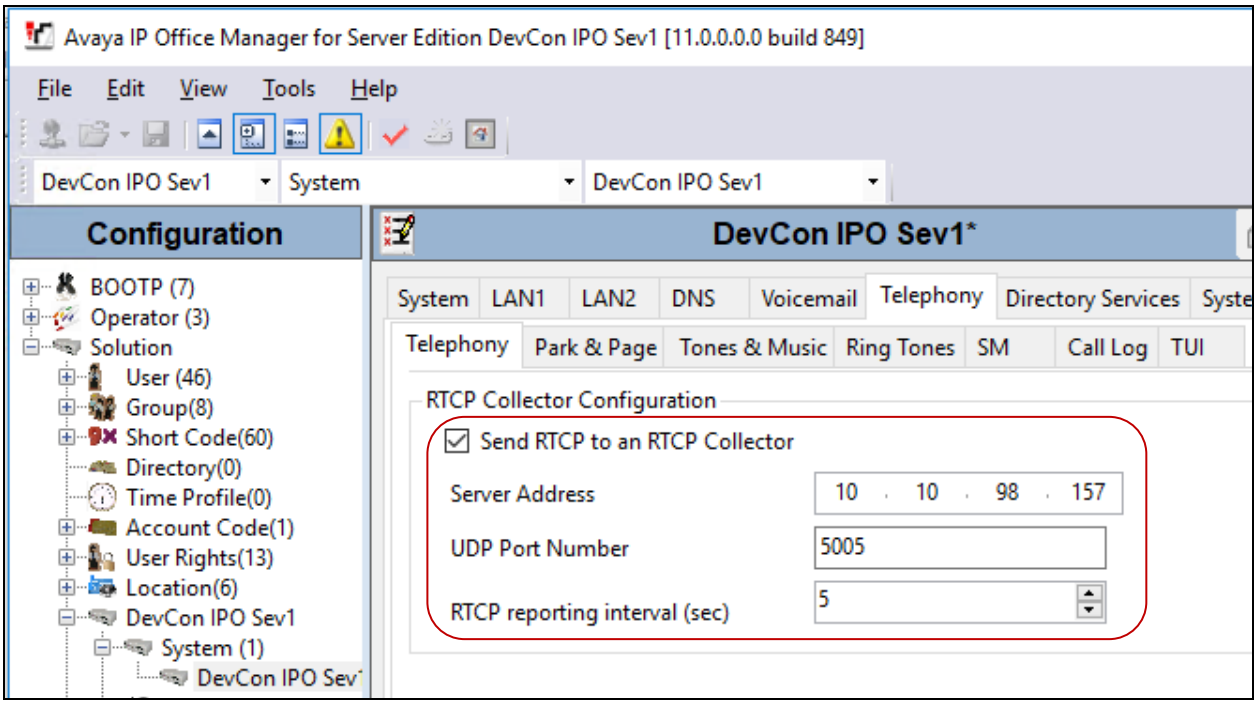
This section describes steps to configure the dual-unicast functionality to send RTCP packets to VSM.

On system window, click **LAN1 → VoIP**. In the **RTCP collector IP Address for phones** section, enter VSM probe IP address, in this example it is: **10.10.98.157**. This will instruct Avaya H.323 phones during registration to send RTCP to VSM. Click **OK** (not shown) to save changes.



©2018 Avaya Inc. All Rights Reserved.

On system window, click **Telephony → Telephony**. In the **RTCP Collector Configuration** section, check the box for **Send RTCP to an RTCP Collector**. When the check box is selected, system RTCP reporting is enabled. In addition to having the individual phones send RTCP call quality reports, the system can also send RTCP reports for calls. In the **Server Address** field, enter the VSM probe IP address, in this example it is: **10.10.98.157**. This sets the address of the third-party QoS monitoring application to which the system sends RTCP reports. Retain default values for all other fields.



©2018 Avaya Inc. All Rights Reserved.

In case of SIP phones, the configuration needs to be done on the 46xxsettings file. Screen below shows the changes made to the 46xxsettings file that was used by the Avaya J129 IP (SIP) phone.

```
##################  RTCP MONITORING  ######################
##
## The RTCP monitor
##   One RTCP monitor (VMM server) IP address in
##   dotted-decimal format or DNS name format (0 to 15
##   characters). Note that for H.323 telephones only this
##   parameter may be changed via signaling from Avaya
##   Communication Manager. For 96xx/J100 SIP models in Avaya Aura
##   environments, this parameter is set via the PPM server.
##   Note : This setting is supported by J129  SIP  R1.0.0.0 (or R1.1.0.0), J169/J179
SIP R1.5.0, J100 SIP R2.0.0.0 and later, H1xx SIP R1.0 and later
##   for non-Aura environment (For example: IP Office, etc).
SET RTCPMON 10.10.98.157 ◄── This is the IP address of the VSM probe
##
## RTCPMONPORT sets the port used to send RTCP information
## to the IP address specified in the RTCPMON parameter.
## RTCPMONPORT is only supported on 96xx/J100 in non-Avaya environments.  For
96xx/J100 SIP
## models in Avaya environments, this parameter is set via the PPM server. The default
value is 5005.
##   Note : This setting is supported by H1xx SIP R1.0 and later and J129  SIP
R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   for non-Aura environment (For example: IP Office, etc).
SET RTCPMONPORT 5005
##
## RTCP Monitor Report Period
##   Specifies the interval for sending out RTCP monitoring
##   reports (5-30 seconds).  Default is 5 seconds. This
##   parameter applies only to 96xx/J100 SIP telephones.
##   Note : This setting is supported by J129  SIP  R1.0.0.0 (or R1.1.0.0), J169/J179
SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   for non-Aura environment (For example: IP Office, etc).
SET RTCPMONPERIOD 5
##
```

Repeat the above steps on the 500 V2 Expansion server also.

©2018 Avaya Inc. All Rights Reserved.

5.2. Configure SNMP

This section describes steps to configure SNMP Agent and to configure IP Office to send traps to VSM.

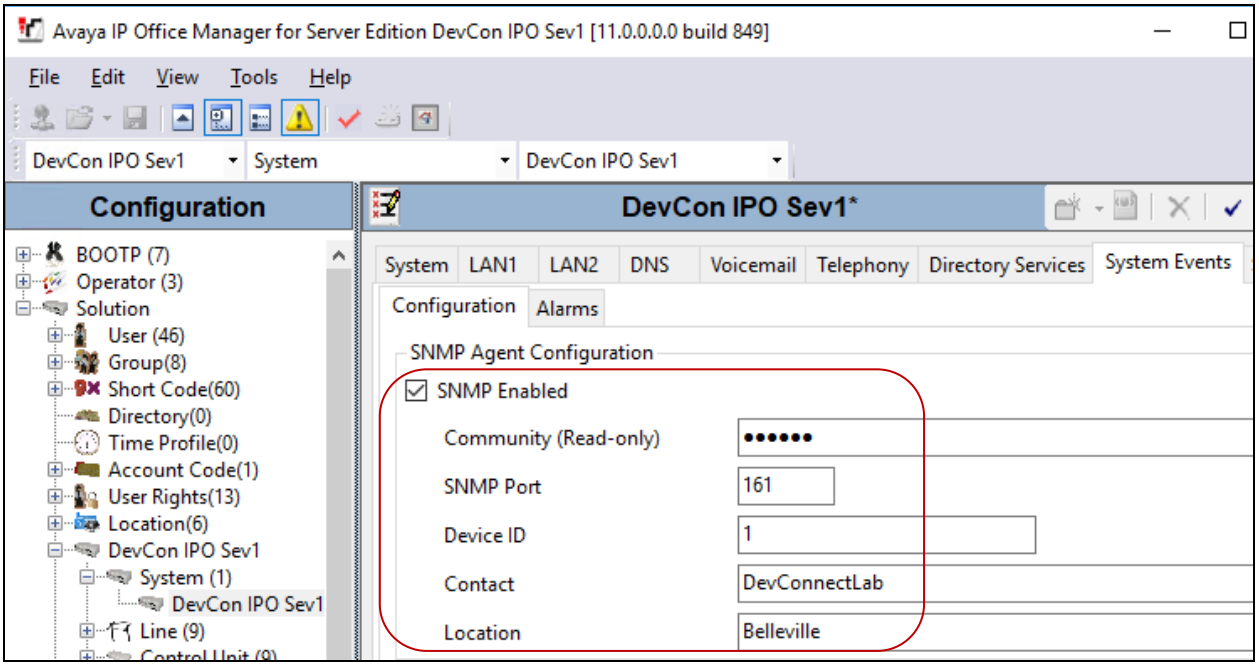
5.2.1. Configure SNMP Agent

On system window, click on **System Events → Configuration**, check **SNMP Enabled** checkbox. Enter the following information:

- **Community (Read-only):** Enter community string, example: **public**.
- **SNMP Port:** Use default port **161**.
- **Device ID:** Use default value.
- **Contact:** Enter any descriptive name, example: **DevConnectLab.**
- **Location:** Enter any descriptive name for location, example: **Belleville.**

Click **OK** (not shown) and save the configuration to apply the change.

Repeat same steps on the 500 V2 Expansion.



©2018 Avaya Inc. All Rights Reserved.

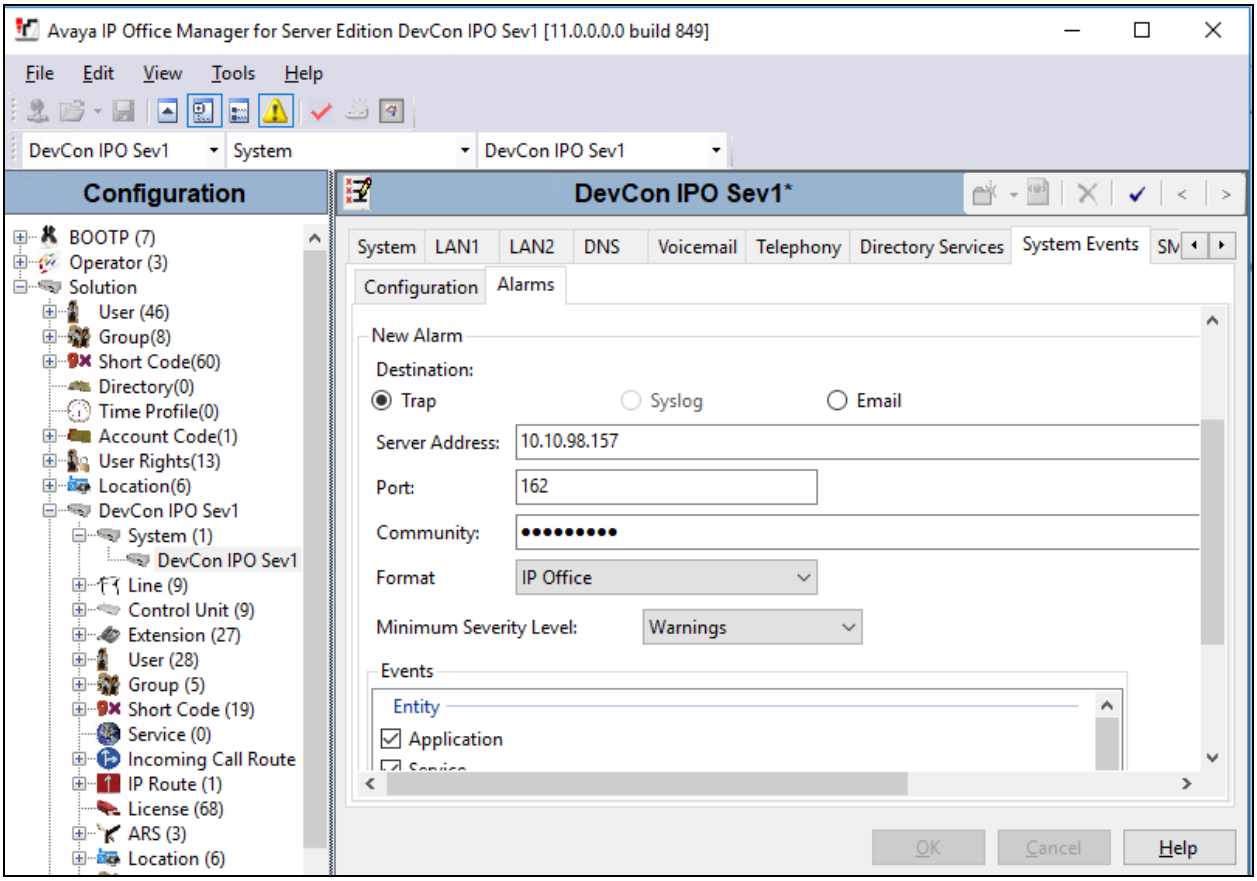
5.2.2. Configure Avaya IP Office to send SNMP traps to VSM

On system window, click **System Events → Alarms**, click on **Add …** button (not shown) to add new trap. Enter the following detail for alarm:

- **Destination:** Select type **Trap**.
- **Server Address:** Enter the IP address of the VSM probe
- **Port:** Use default value **162**.
- **Community**: Enter string configured from previous section, ex: **public**.
- **Format**: Retain default **IP Office**.
- **Minimum Severity Level:** Select **Warnings**. The events with severity level lower than this will not be collected and sent.
- **Events**: Select types of system events that should be collected and sent, example: all events are selected during compliance testing.

To activate the new trap, make sure that the configuration is saved (**File → Save Configuration** or **Ctr + S**) and choose the option to reboot the physical box immediately.

Repeat same steps on the 500 V2 Expansion.



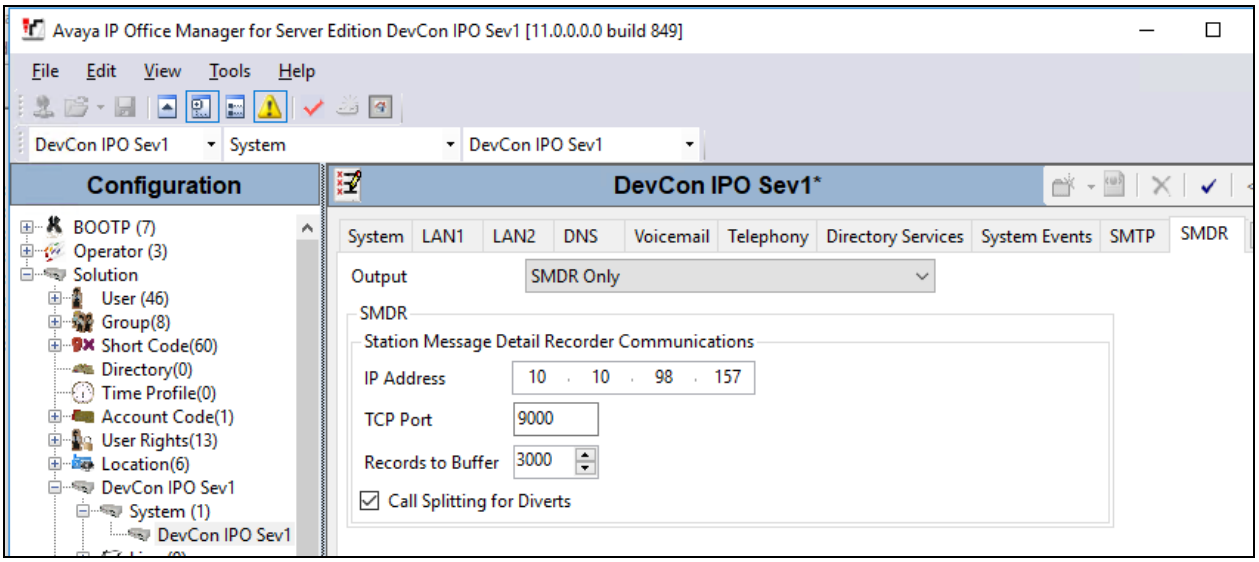
©2018 Avaya Inc. All Rights Reserved.

5.3. Configure SMDR

This section describes steps to configure SMDR so that IP Office can send CDR to VSM.

On system window, click on **SMDR** and enter the following information:

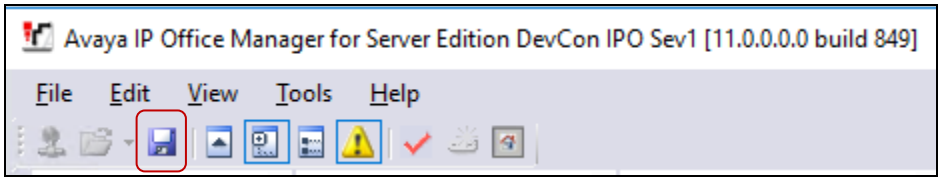
- **Output:** Select **SMDR Only** from the drop-down menu.
- **IP Address:** Enter the IP Address of the VSM probe.
- **TCP Port:** During compliance testing **9000** was used.
- **Records to Buffer:** Used the default value of **3000**
- Check the box for **Call Splitting for Diverts**



Click **OK** (not shown) and save the configuration to apply the change. Repeat same steps on the 500 V2 Expansion.

5.4. Save Configuration

Once all the configurations are complete, the changes need to be saved on the IP Office System. To achieve this, click on the Save Icon as shown in the screen below. A subsequent window will appear (not shown) asking the user to proceed with the changes made to the IP Office system/s or not. Click on the **OK** button to confirm.



©2018 Avaya Inc. All Rights Reserved.

6. Configure Virsae Service Management

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

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:

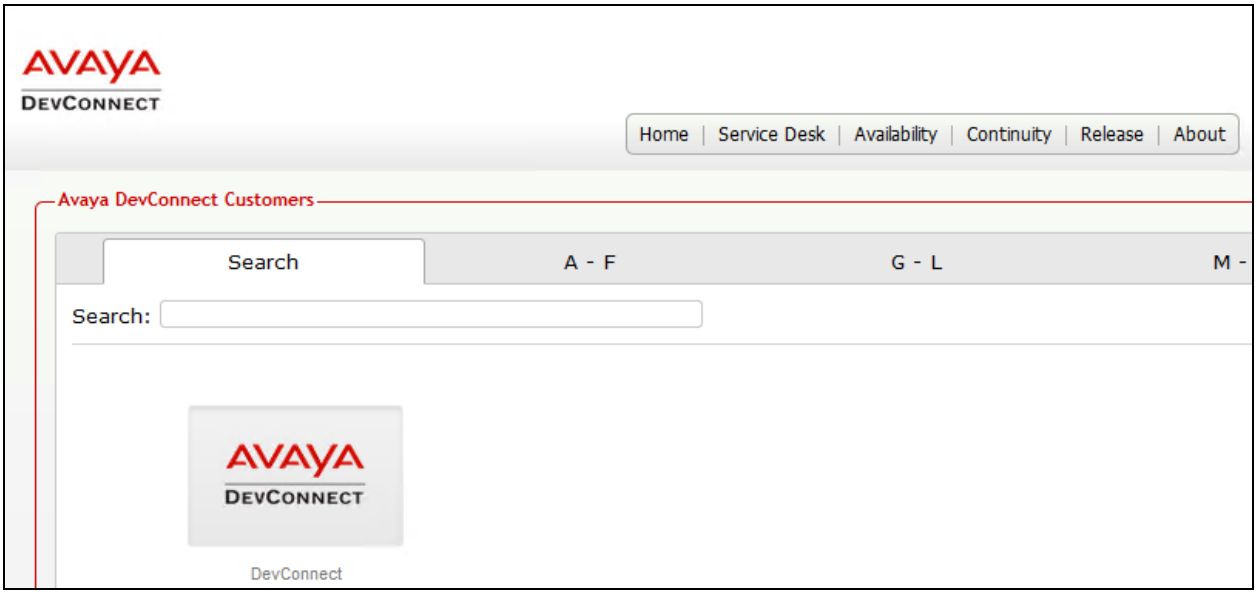
- Login to the Web Portal
- Configuring Avaya IP Office
- Configure Dashboard

6.1. Login to the Web Portal

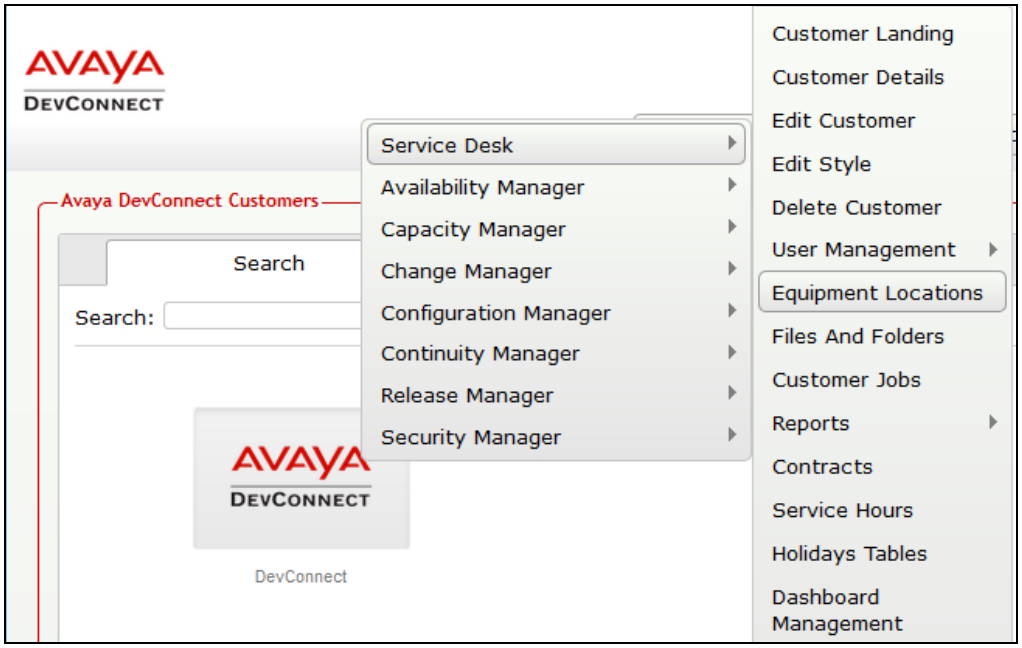
A portal for business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL, *<business partner name>.virsae.com* in a web browser. During compliance testing the URL used was *devconnect.virsae.com*. The Login screen is shown as below. Enter the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

©2018 Avaya Inc. All Rights Reserved.

The customers belonging to the business partner screen is shown. During compliance testing the customer created by Virsae was **Devconnect**.

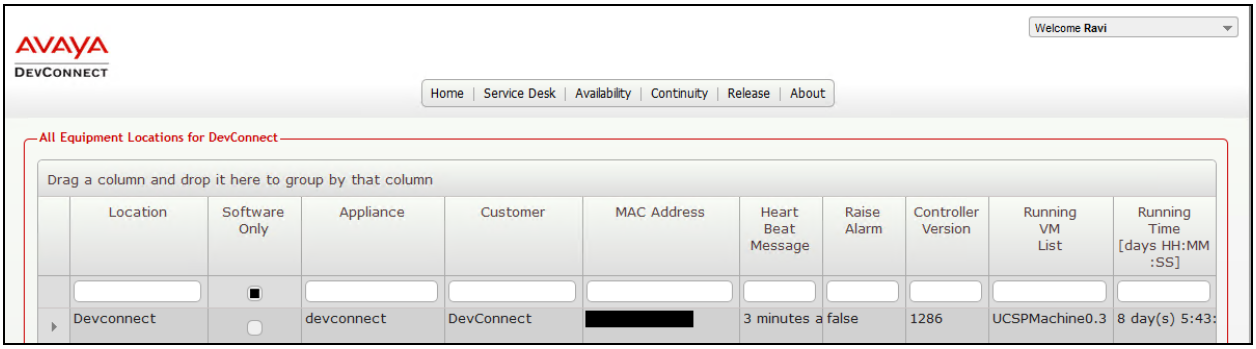


Click on the customer icon and navigate to **Service Desk → Equipment Locations** as shown below.



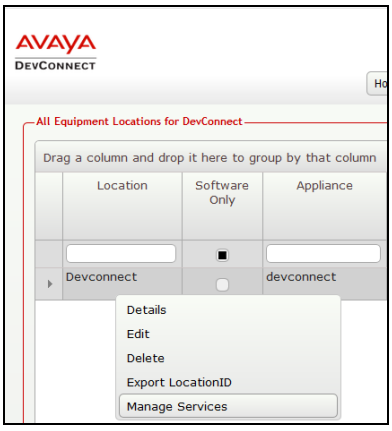
©2018 Avaya Inc. All Rights Reserved.

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

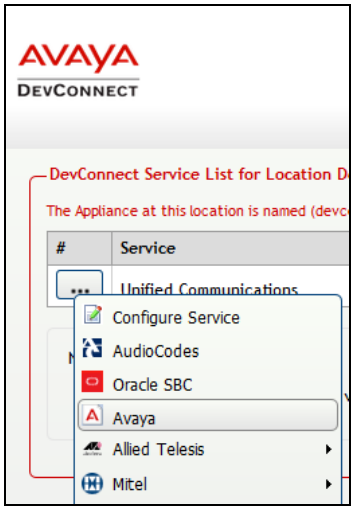


6.2. Configuring Avaya IP Office

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



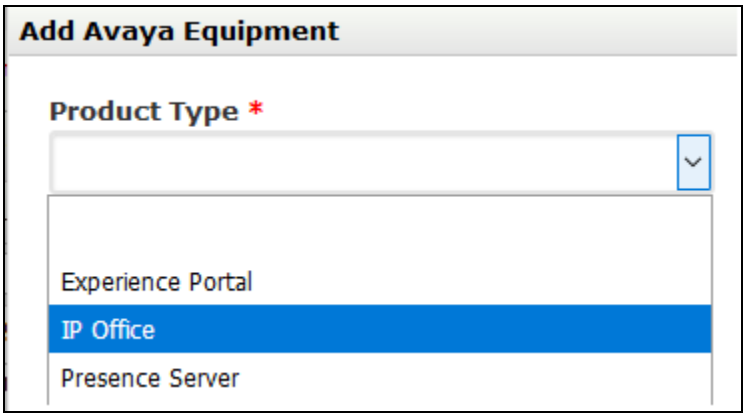
From the **Unified Communications** Service, select **Avaya**.



©2018 Avaya Inc. All Rights Reserved.

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

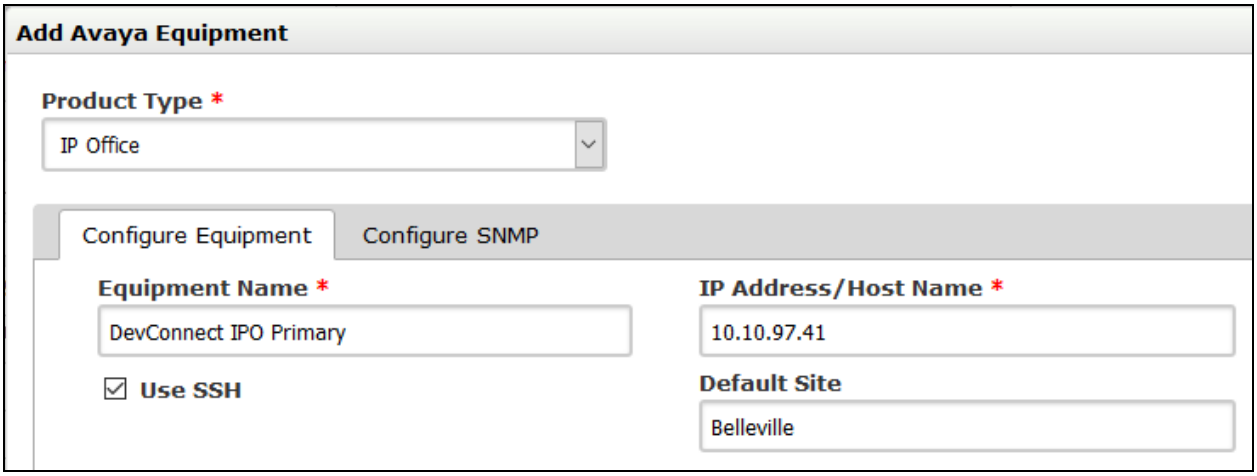
From the **Add Avaya Equipment** window, select **IP Office** from the **Product Type** drop-down menu.



©2018 Avaya Inc. All Rights Reserved.

In the **Configure Equipment** tab, configure the following values.

- **Equipment Name:** A descriptive name
- Check the **Use SSH** box
- **IP Address/Host Name:** IP address of IP Office Primary Server
- **Default Site:** A descriptive site name

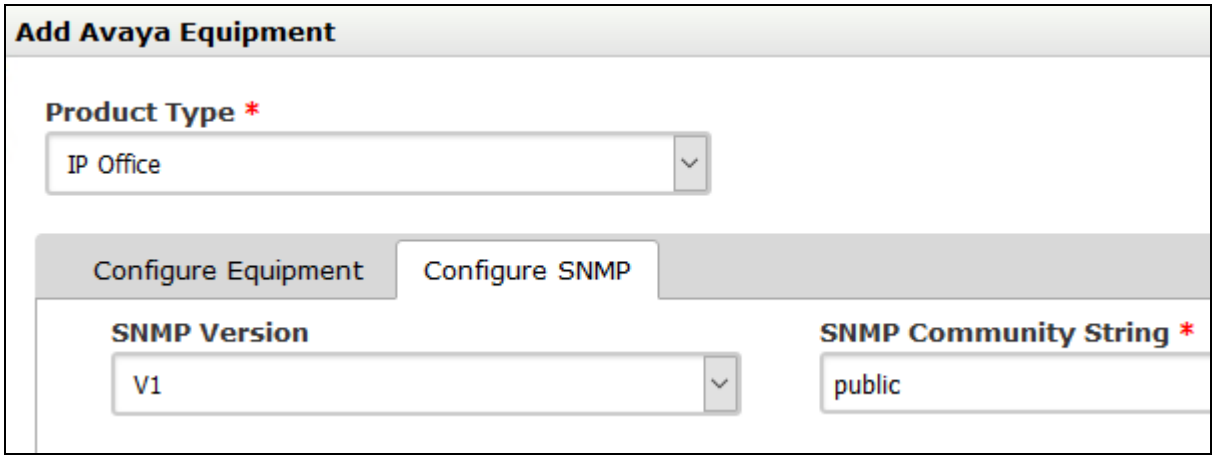


©2018 Avaya Inc. All Rights Reserved.

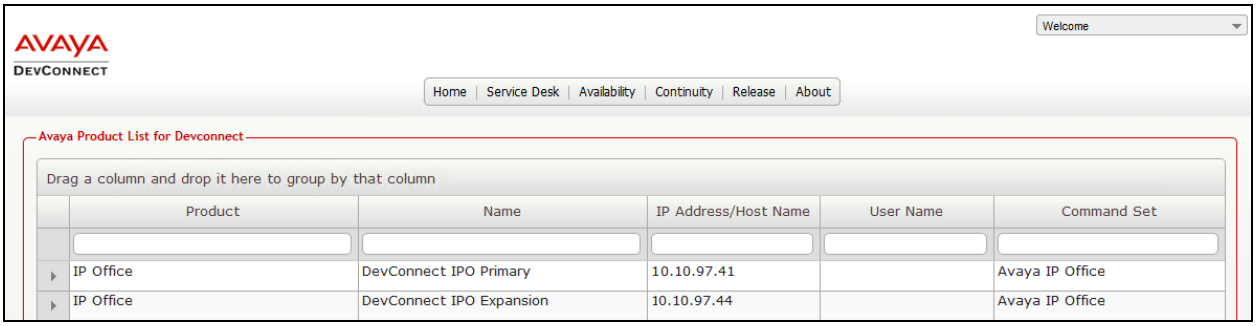
In the **Configure SNMP** tab, configure the following values.

- **SNMP Version:** Select **V1** from the drop-down menu
- **SNMP Community String:** Enter the value configured in **Section 5.2.2**

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



Repeat the above section to add an IP Office Expansion System too. The screen below shows both the IP Office Primary Server and Expansion System added.



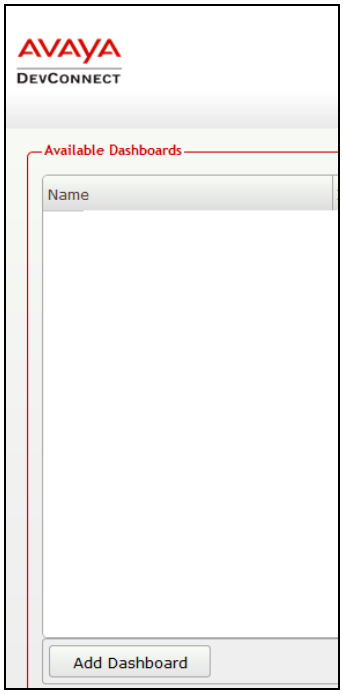
©2018 Avaya Inc. All Rights Reserved.

6.3. Configure Dashboard

This section shows the steps to configure IP Office on the dashboard.

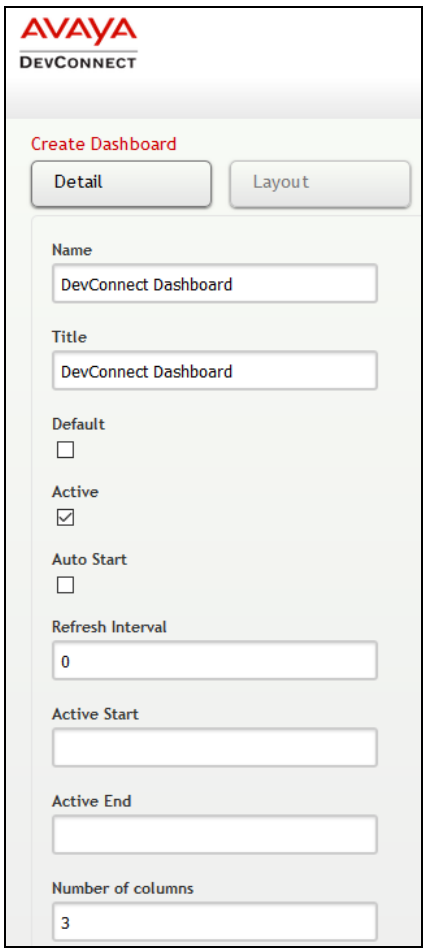
From the customer icon, navigate to **Service Desk → Dashboard Management** as shown below.

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

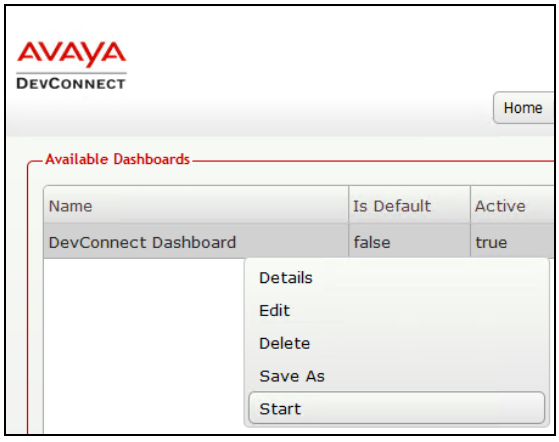


©2018 Avaya Inc. All Rights Reserved.

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.



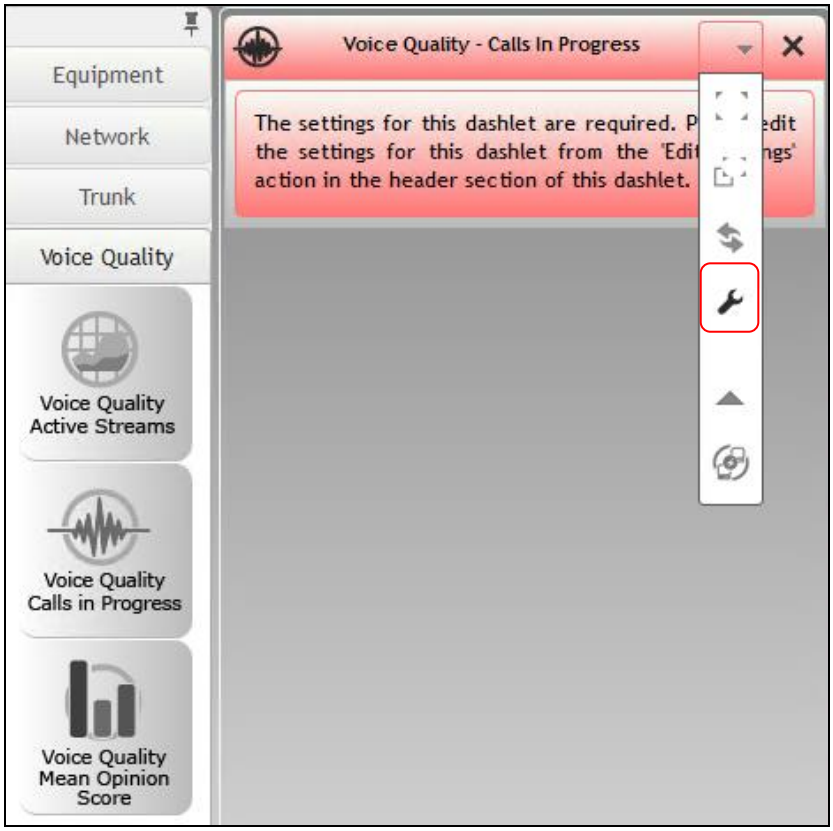
Screen below shows the above created Dashboard. Right click on it and select **Start**.



©2018 Avaya Inc. All Rights Reserved.

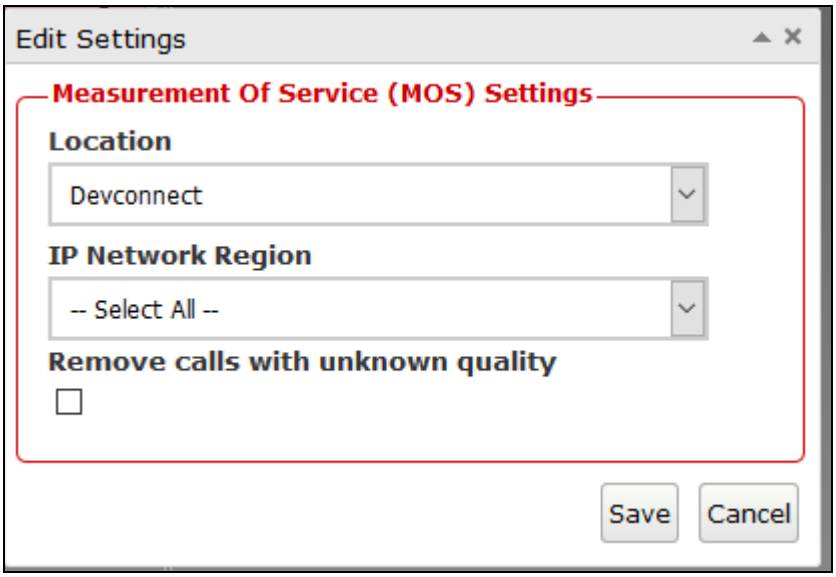
In the dashboard window shown below, click on **Voice Quality** and drag the **Voice Quality Calls in Progress** icon from the left to the right column.

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

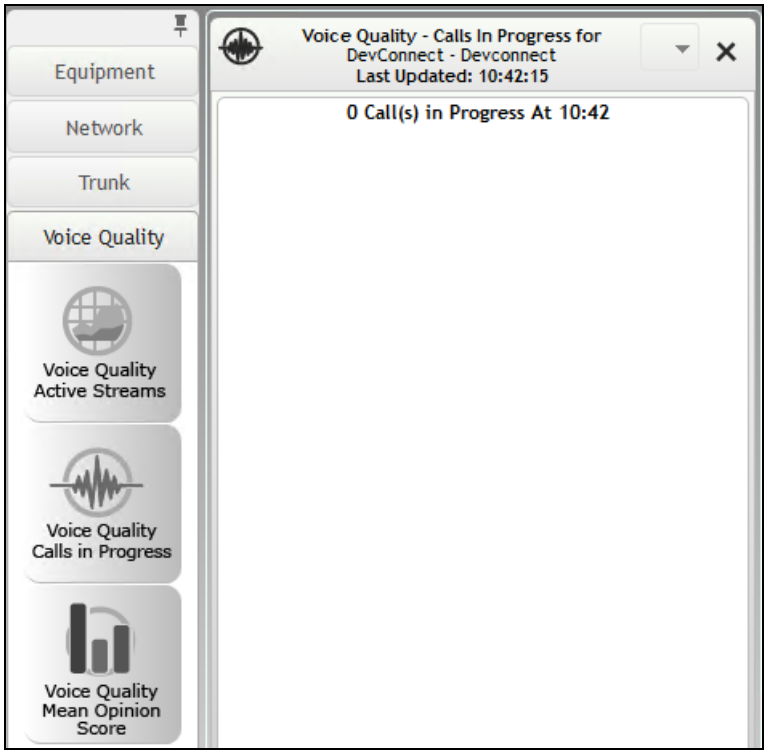


©2018 Avaya Inc. All Rights Reserved.

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



The dashboard with the configured voice quality window is shown below.

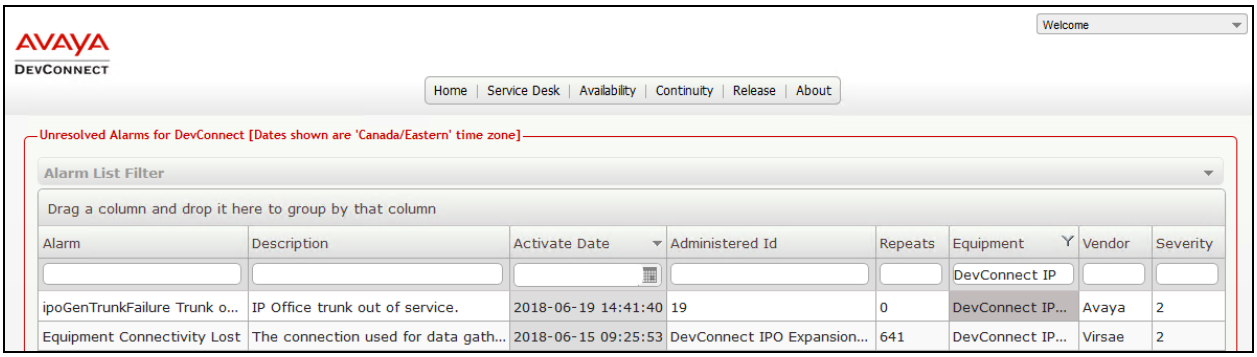


©2018 Avaya Inc. All Rights Reserved.

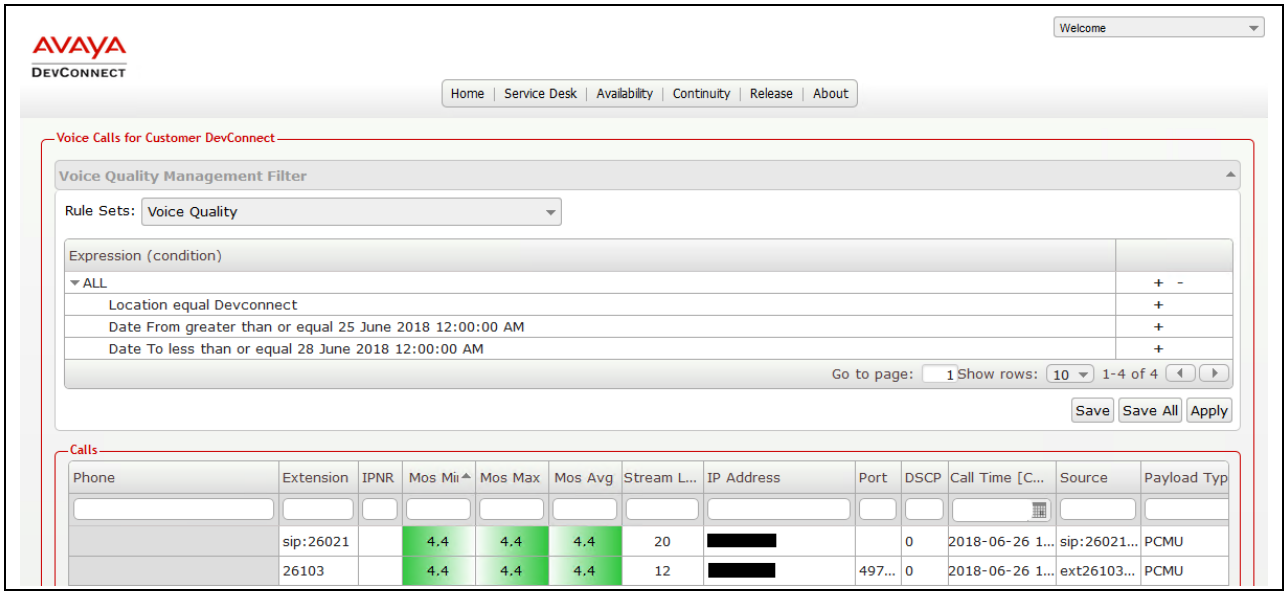
7. Verification Steps

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

To view alarms using historical reporting, navigate to **Availability Manager → Manage Alarms** (not shown). A list of all unresolved alarms for all equipment is shown. Screen below shows the alarms by filtering for IP Office equipment

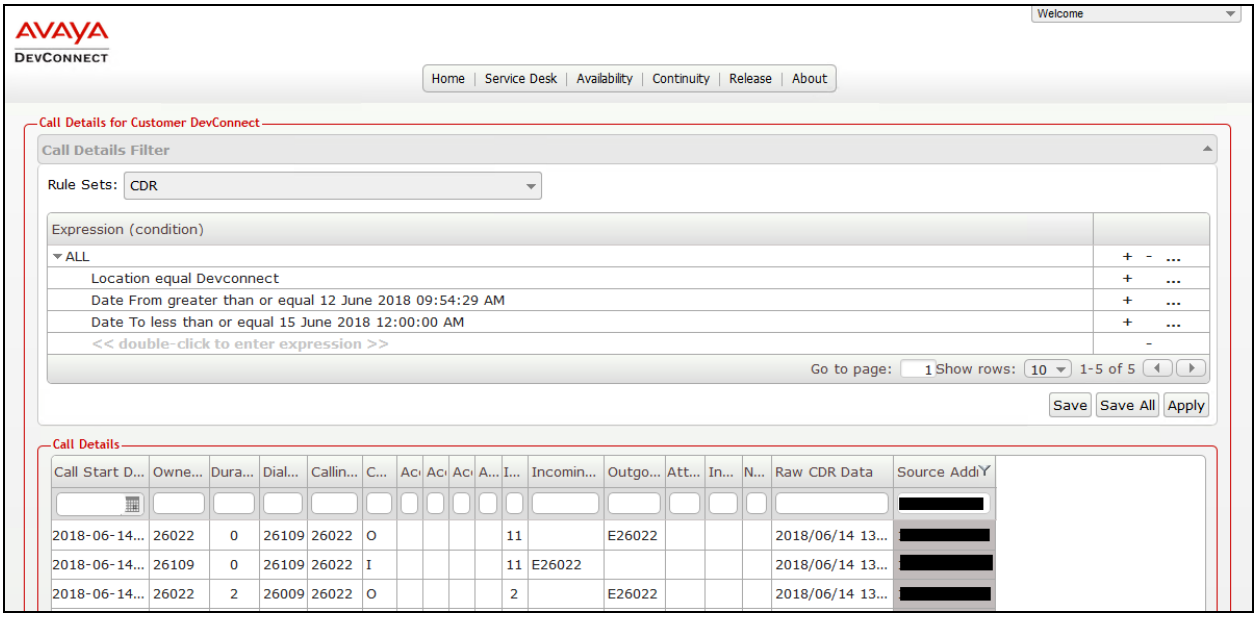


To view voice quality using historical reporting, navigate to **Availability Manager → Voice Quality Management** (not shown). Create a rule set and apply the rule. Screen below shows a few examples of voice quality for extensions on both Primary and Expansion IP Office Systems. Real time voice quality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



©2018 Avaya Inc. All Rights Reserved.

To view CDR using historical reporting, navigate to **Service Desk → Call Details** (not shown). Create a rule set and apply the rule. Screen below shows a few examples of CDR collected from IP Office by using filters at Source Address.



©2018 Avaya Inc. All Rights Reserved.

8. Conclusion

These Application Notes describe the configuration steps required for Virsae Service Management for Unified Communications to successfully interoperate with Avaya IP Office Server Edition. All feature and serviceability test cases were completed with any observations noted in **Section 2.2**.

9. Additional References

This section references the Avaya documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com.

1. IP Office™ Platform 11.0 Installing and Maintaining the IP Office Application Server, 15-601011 Issue 13c - (Tuesday, May 22, 2018).
2. IP Office™ Platform 11.0 Deploying IP Office Basic Edition, 15-601042 Issue 33g - (Tuesday, May 22, 2018).
3. Administering Avaya IP Office™ Platform with Manager, Release 11.0 May 2018.

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

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

©2018 Avaya Inc. All Rights Reserved.

©2018 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.