Avaya Solution & Interoperability Test Lab

Application Notes for Service Pilot 9.0 and Avaya Aura® Communication Manager 7.1 and Avaya Aura® Session Manager 7.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Service Pilot 9.0 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Session Manager 7.1.

Service Pilot is a performance monitoring solution for multi-vendor infrastructure and unified communications. Service Pilot provides visibility of Avaya and other vendor's IP Telephony solutions from a single console. Targeted at multi-site enterprises and managed service providers of IP telephony solutions, Service Pilot monitoring solution is non-intrusive as there is no need to install any agent on the communication servers or their infrastructure and can be installed in a virtualized environment.

Service Pilot integrates directly to Communication Manager using Secure Shell (SSH) or Telnet. At the same time, it processes Simple Network Management Protocol (SNMP), Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Communication Manager, Gateways and Avaya Endpoints.

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 ServicePilot 9.0 with Avaya Aura® Communication Manager, G450 Media Gateway, Avaya Aura® Media Server, Avaya Aura® Session Manager, Avaya Aura® System Manager and Avaya Aura® Application Enablement Services. ServicePilot provides enterprises and Managed Service Providers with the following capabilities:

- Monitoring
- Troubleshooting
- Reporting

ServicePilot uses four methods to monitor a Communication Manager system.

- System Access Terminal (SAT) – ServicePilot uses telnet/SSH connections to the SAT using the IP address of Communication Manager. By default, the solution establishes 2 concurrent SAT connections to the Communication Manager system and uses the connections to execute SAT commands.

- Real Time Transport Control Protocol (RTCP) Collection - ServicePilot collects RTCP information sent by the Communication Manager, System Manager, media gateways, and IP/SIP Telephones. The call quality metrics including packet loss, latency, and jitter are collected and from these metrics, the MOS (mean opinion score) is computed, which measures overall call quality.

- Simple Network Management Protocol (SNMP) Collection – ServicePilot uses SNMP to collect configuration and status information and SNMP traps from Communication Manager, Media Gateways, Session Manager, System Manager and Application Enablement Services.

- Call Detail Recording (CDR) Collection – ServicePilot collects CDR information sent by Communication Manager and Session Manager.

2. General Test Approach and Test Results

The general test approach was to configure the Avaya equipment and verify ServicePilot interoperability as on a customer site. The interoperability compliance test included both feature and functionality testing.

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 the ServicePilot did not include use of any specific encryption features as requested by ServicePilot Technologies. Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

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

2.1. Interoperability Compliance Testing

For feature testing, ServicePilot web interface was used to view the configurations of Communication Manager, G450 Media Gateway, Media Server, Session Manager, System Manager and Application Enablement Services, trunk groups, route patterns, IP network regions, stations, processor occupancy, SNMP alarm and error information. For the collection of RTCP and CDR information, the endpoints included Avaya H.323, SIP, digital and analog telephones. CDR information was collected from both Communication Manager and Session Manager. The types of calls made included intra-switch calls, inbound/outbound PSTN calls, inbound/outbound inter-switch IP trunk calls, transfer and conference calls.

For serviceability testing, reboots were applied to the ServicePilot ISM Server and Avaya Servers to simulate system unavailability.

2.2. Test Results

The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with the following observation.

- The iddetail in the Media stream record log sometimes switches extension between caller and called number.
- The Live Calls does not show the status of Quality and MOS information for H.323 endpoint for internal call between SIP endpoint and H.323 endpoint
- The iddetail in the Media Stream record log intermittently shows blank information for call record. These issues are current investigated by ServicePilot

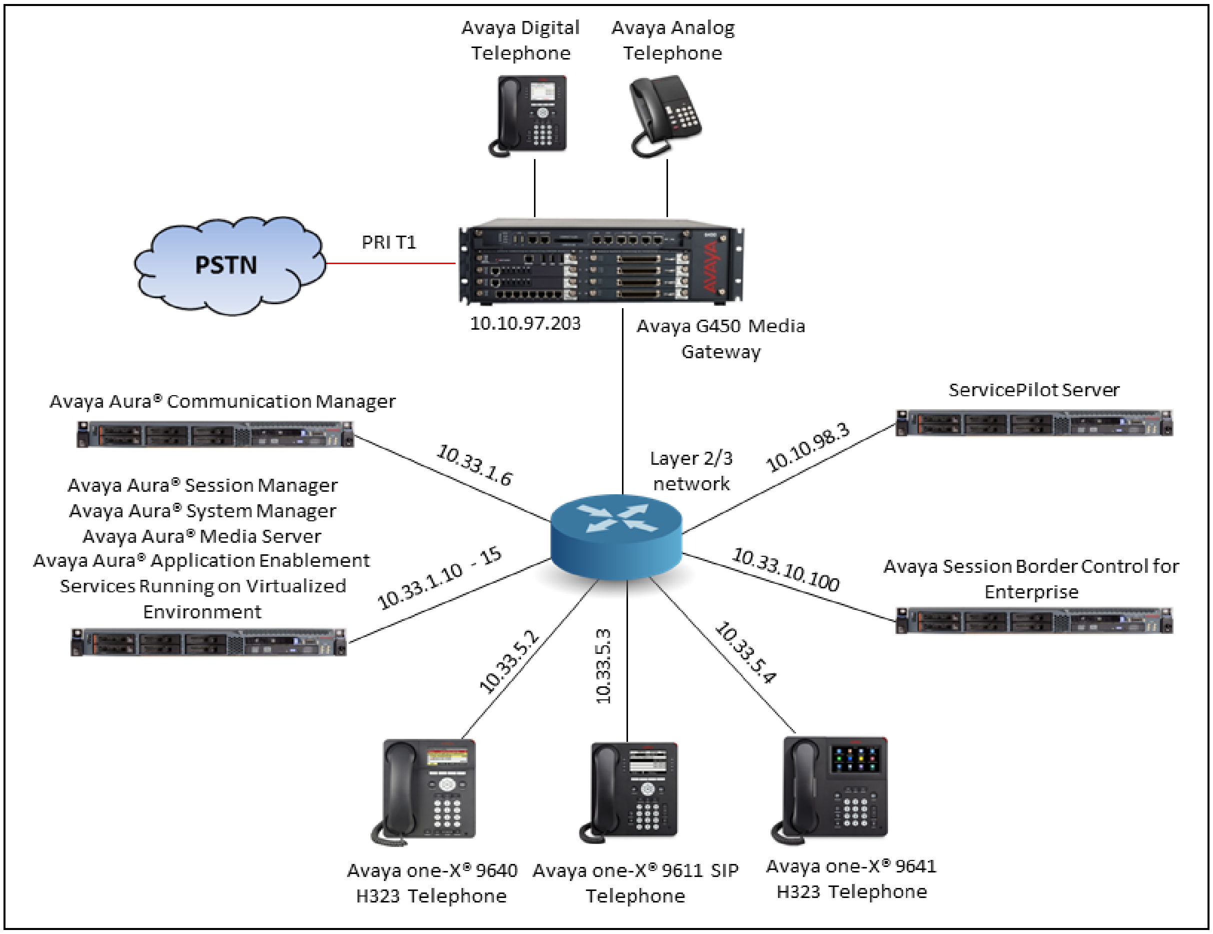
2.3. Support

For technical support on ServicePilot, contact the ServicePilot Support Team at:

- Hotline: +33 2 4060-8052
- Email: support@servicepilot.com.

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify ServicePilot interoperability with Communication Manager, G450 Media Gateway, Media Server, Session Manager, System Manager and Application Enablement Services. ServicePilot connected on the same LAN as the Avaya equipment and collects relevant information using SNMP and collects CDR data from both Communication Manager and Session Manager. ServicePilot also monitors RTCP. A verity of Avaya telephones were configured and used to make calls to be monitored and produce CDR data. A simulated PSTN was also configured to allow incoming and outgoing calls.



Avaya Digital Telephone
Avaya Analog Telephone
PSTN
PRI T1
10.10.97.203
Avaya G450 Media Gateway
Avaya Aura® Communication Manager
ServicePilot Server
10.33.1.6
Layer 2/3 network
10.10.98.3
Avaya Aura® Session Manager
Avaya Aura® System Manager
Avaya Aura® Media Server
Avaya Aura® Application Enablement Services Running on Virtualized Environment
10.33.1.10 - 15
10.33.10.100
Avaya Session Border Control for Enterprise
10.33.5.2
10.33.5.3
10.33.5.4
Avaya one-X® 9640 H323 Telephone
Avaya one-X® 9611 SIP Telephone
Avaya one-X® 9641 H323 Telephone

Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Environment	7.1.2.0 (7.1.2.0.0.532.24184)
Avaya Aura® Session Manager running on Virtual Environment	7.1.2.0 (7.1.2.0.712004)
Avaya Aura® System Manager running on Virtual Environment	7.1.2.0 (7.1.2.0.057353)
Avaya Aura® Application Enablement Services running on Virtual Environment	7.1.2.0.0.3
Avaya Aura® Media Server running on Virtual Environment	7.8.0.333
Avaya G450 Media Gateway	38.21.0
Avaya Session Border Controller for Enterprise	7.2.1.0-05-14222
Avaya Telephones 9641GS (H323) 9611G (H323) 9608G (SIP) 9641G (SIP) Avaya Digital 1416 Telephone	 6.6506 6.6506 7.1.1.0.9 7.1.1.0.9 FW1
ServicePilot running on Windows 2012	9.0

5. Configuration pre-requisites

Make sure that all Avaya Aura® Communication Manager and Avaya Aura® Session Manager elements are configured to keep time using NTP. CDR records received by ServicePilot will therefore be properly time-stamped.

6. Configure Avaya Aura® Communication Manager

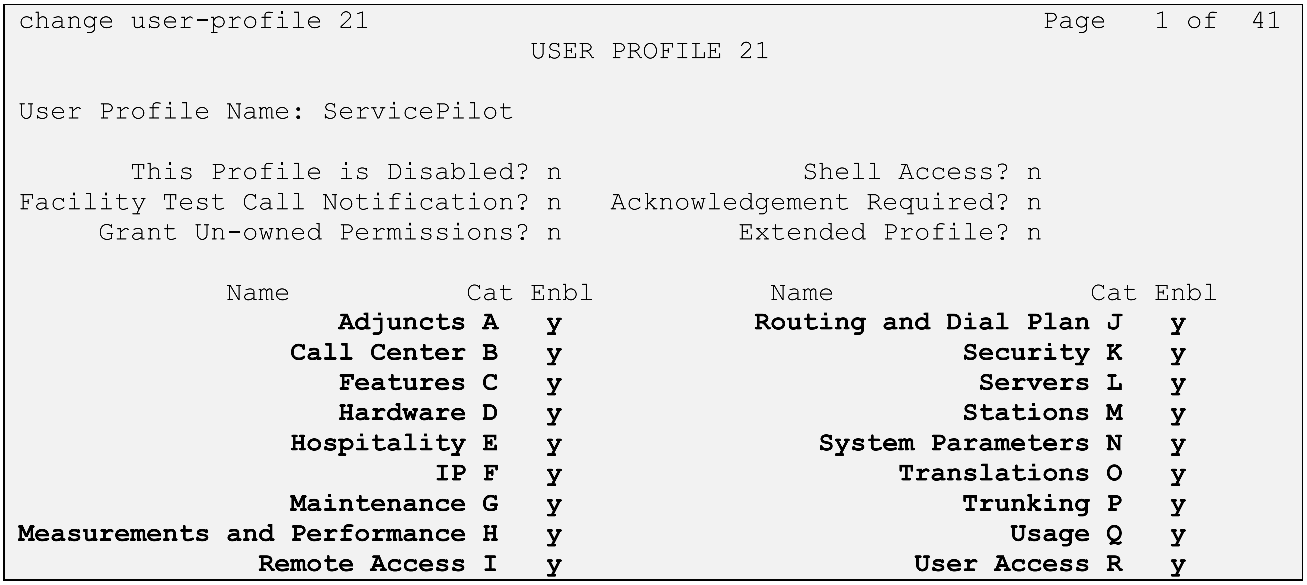
Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 12**. The configuration described in this section can be summarized as follows:

- Configure SAT User Profile
- Configure Login Group
- Configure SNMP on Avaya Aura® Communication Manager
- Configure RTCP Monitoring
- Configure CDR Monitoring

6.1. Configure SAT User Profile

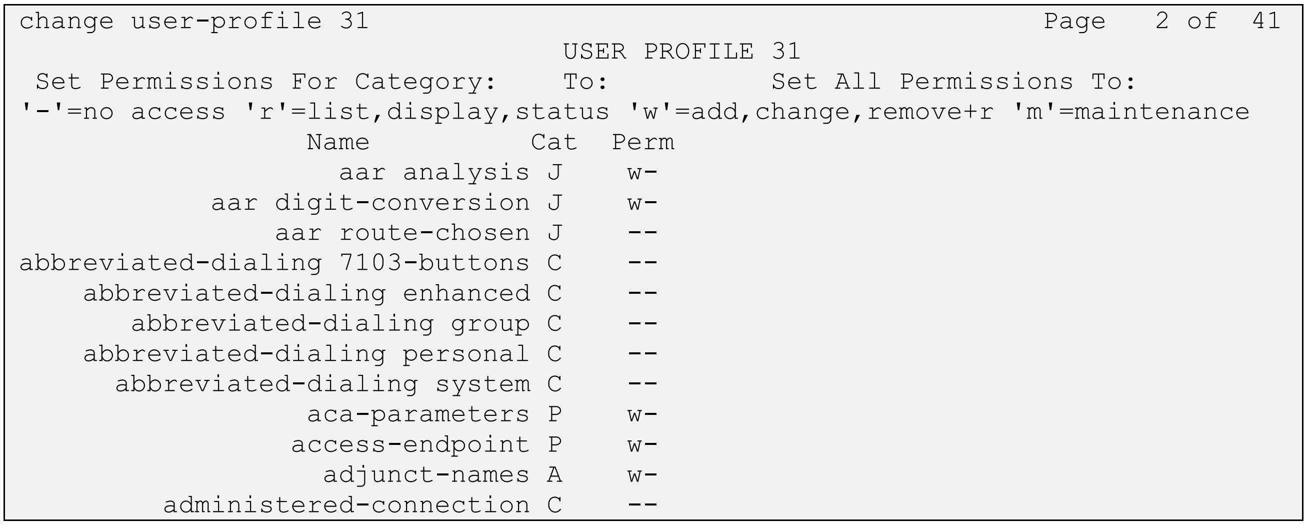
A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As ServicePilot does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the ServicePilot login account.

Use the **add user-profile *n*** command, where ***n*** is the next unused profile number. Enter a descriptive name for **User Profile Name** and enable all categories by setting the **Enbl** field to **y**. In this test configuration, the user profile 21 is created.



```
change user-profile 21                                          Page   1 of  41
                                USER PROFILE 21

User Profile Name: ServicePilot

       This Profile is Disabled? n               Shell Access? n
Facility Test Call Notification? n   Acknowledgement Required? n
     Grant Un-owned Permissions? n           Extended Profile? n

             Name           Cat Enbl           Name                Cat Enbl
                    Adjuncts A   y            Routing and Dial Plan J   y
                 Call Center B   y                         Security K   y
                    Features C   y                          Servers L   y
                    Hardware D   y                         Stations M   y
                 Hospitality E   y                System Parameters N   y
                          IP F   y                     Translations O   y
                 Maintenance G   y                         Trunking P   y
Measurements and Performance H   y                            Usage Q   y
               Remote Access I   y                      User Access R   y
```

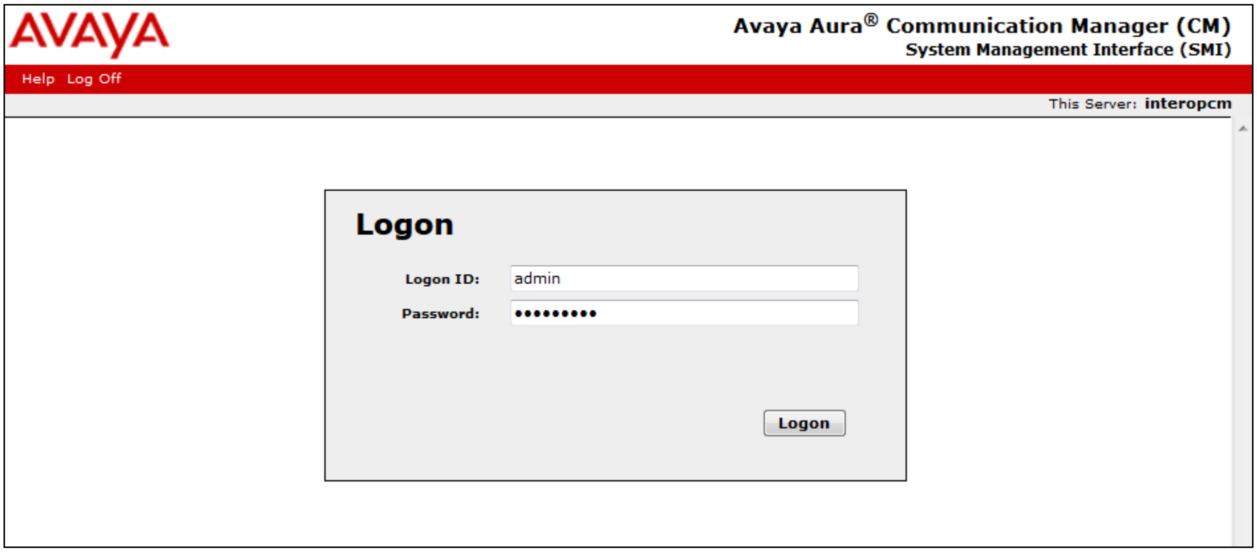
On **Pages 2** to **41** of the USER PROFILE forms, set the permissions of all objects to proper permission as shown in the table below. Submit the form to create the user profile.



```
change user-profile 31                                          Page   2 of  41
                                  USER PROFILE 31
 Set Permissions For Category:    To:          Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                    aar analysis J    w-
            aar digit-conversion J    w-
                aar route-chosen J    --
abbreviated-dialing 7103-buttons C    --
    abbreviated-dialing enhanced C    --
       abbreviated-dialing group C    --
    abbreviated-dialing personal C    --
      abbreviated-dialing system C    --
                  aca-parameters P    w-
                 access-endpoint P    w-
                   adjunct-names A    w-
         administered-connection C    --
```

6.2. Configure Login Group

Create an Access-Profile Group on Communication Manager System Management Interface (SMI) to correspond to the SAT User Profile created in **Section 6.1**. Using a web browser, enter **https://<IP address of Communication Manager>** to connect to the Communication Manager Server being configured and log in using appropriate credentials.



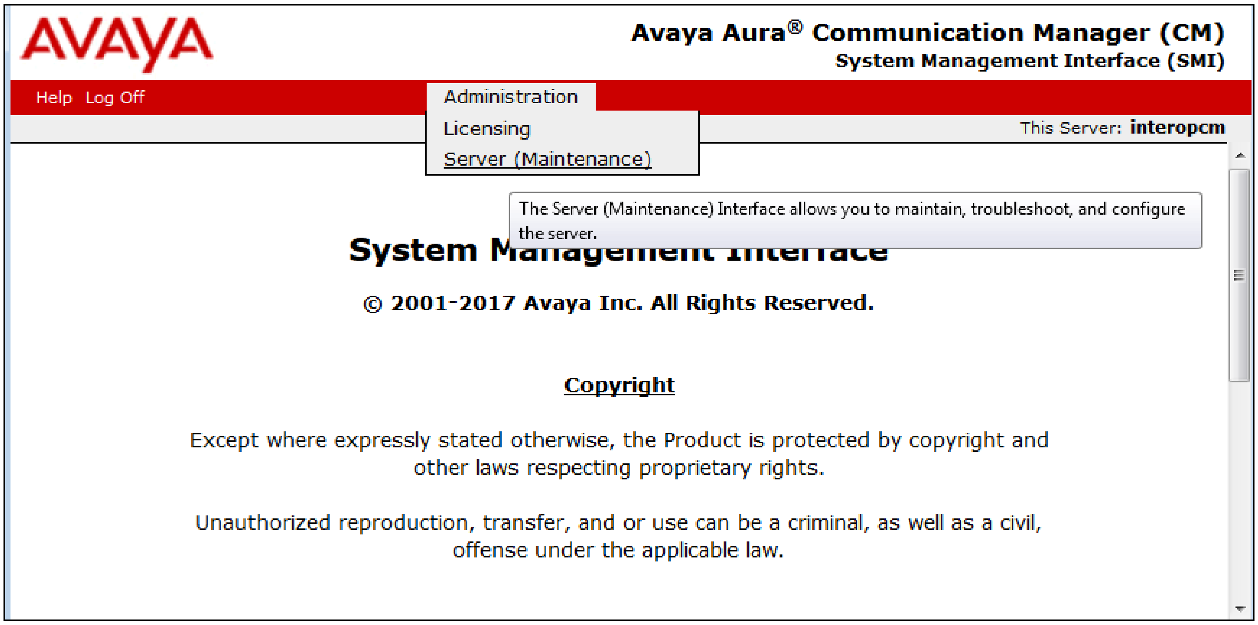
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

This Server: interopcm

Logon

Logon ID: admin
Password: •••••••••

Click **Administration → Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow the user to complete the configuration process.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

This Server: interopcm

The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.

System Management Interface

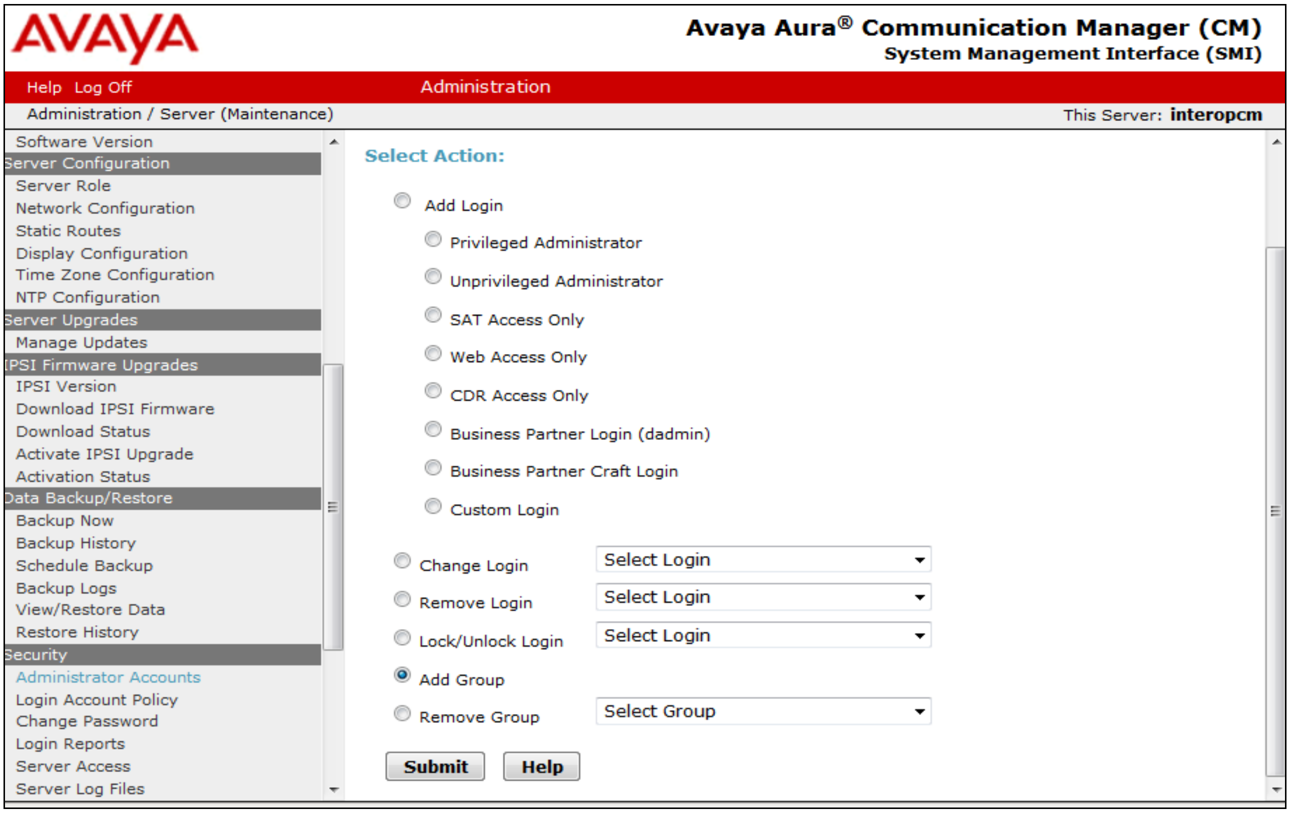
© 2001-2017 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Group** and click **Submit**.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Administration / Server (Maintenance) — This Server: **interopcm**

Select Action:

○ Add Login
- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

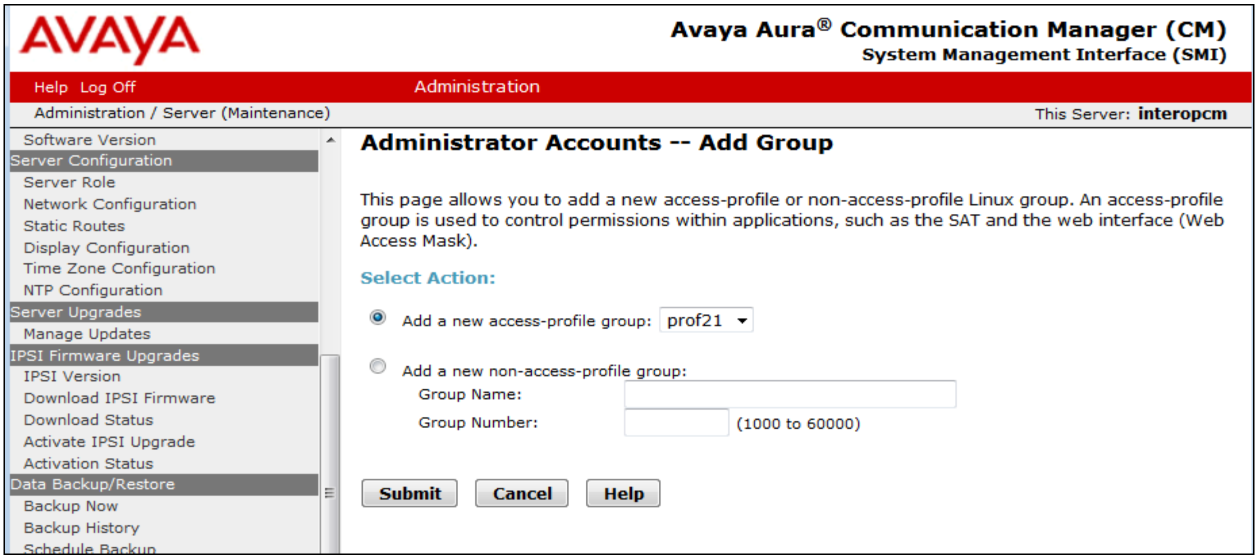
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

● Add Group

○ Remove Group — Select Group

Select **Add a new access-profile group** and select **prof21** from the drop-down list to correspond to the user-profile created in **Section 6.1**. Click **Submit**. This completes the creation of the login group.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Administration / Server (Maintenance) — This Server: **interopcm**

Administrator Accounts -- Add Group

This page allows you to add a new access-profile or non-access-profile Linux group. An access-profile group is used to control permissions within applications, such as the SAT and the web interface (Web Access Mask).

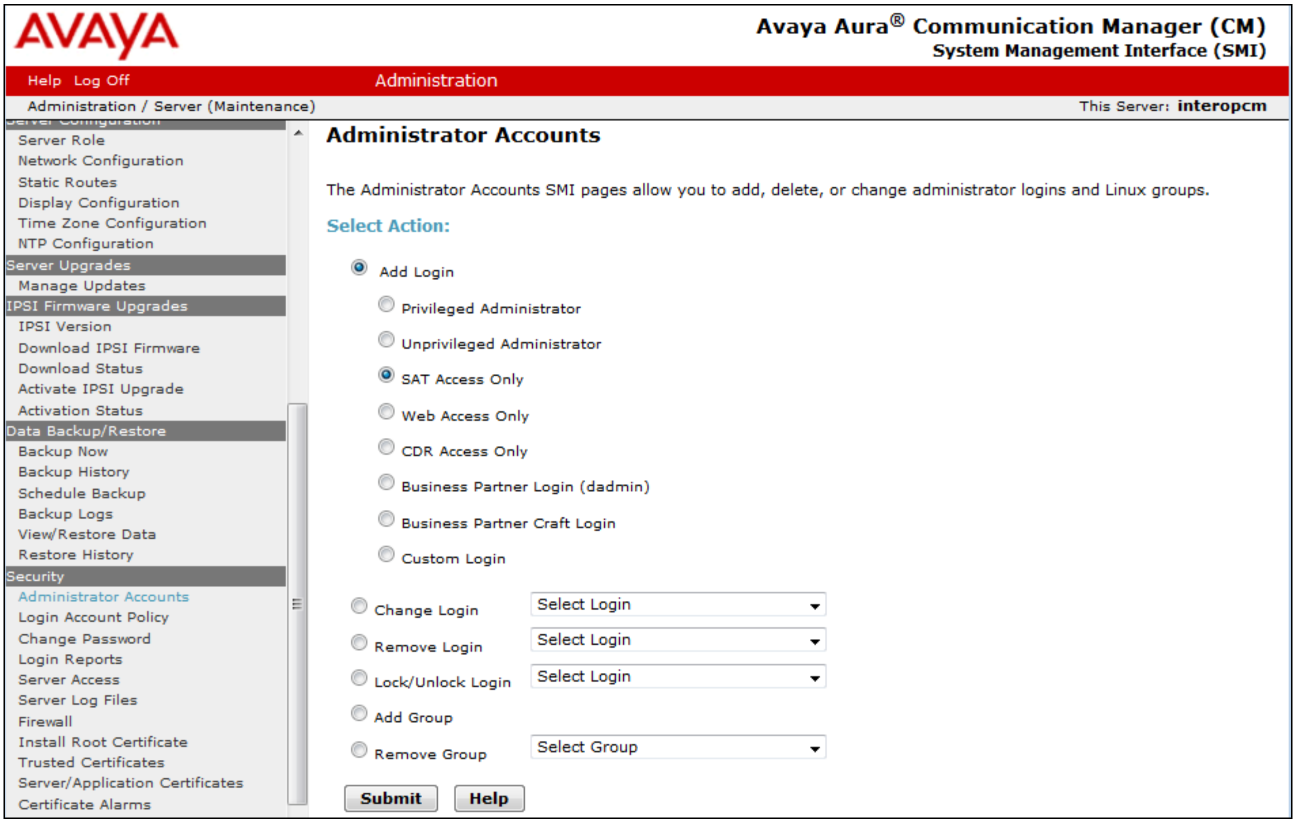
Select Action:

● Add a new access-profile group: prof21

○ Add a new non-access-profile group:
Group Name:
Group Number: (1000 to 60000)

6.3. Configure Login User

Create a login account for ServicePilot to access the Communication Manager SAT. From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Login** and **SAT Access Only** to create a new login account with SAT access privileges only. Click **Submit**.



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

● Add Login

○ Privileged Administrator

○ Unprivileged Administrator

● SAT Access Only

○ Web Access Only

○ CDR Access Only

○ Business Partner Login (dadmin)

○ Business Partner Craft Login

○ Custom Login

○ Change Login — Select Login

○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

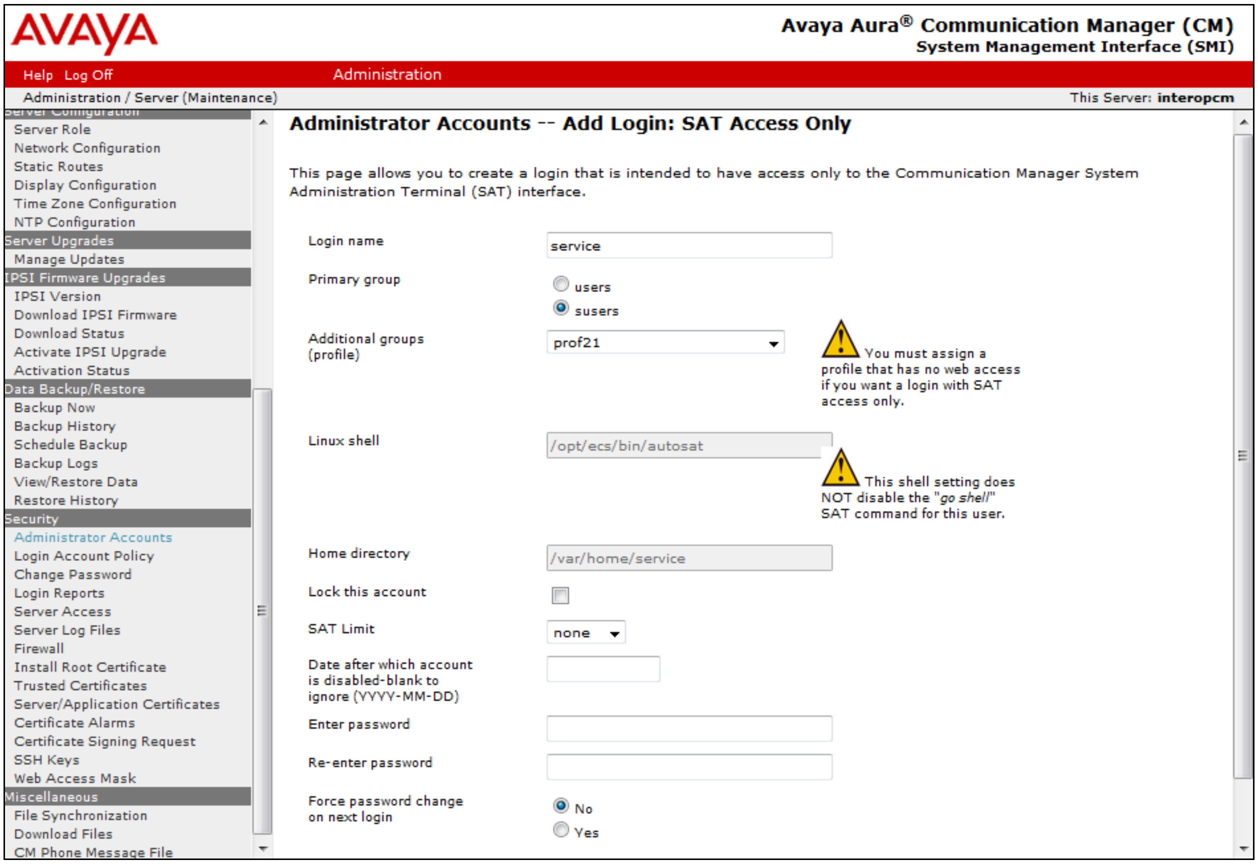
○ Add Group

○ Remove Group — Select Group

In the subsequent page enter the following:

- **Login name** Enter an informative name (i.e., SPISM)
- **Primary group** Click on the **susers** radio button
- **Additional groups (profile)** Select **prof21** from the drop-down list (the **login group** created in **Section 5.2**)
- **Sat Limit** Select **None** from the drop down list
- **Enter password** Enter a password (used by ServicePilot in **Section 11.3**)
- **Re-enter password** Re-enter the password
- **Force password change on next login** Click on the **No** radio button

Click **Submit** (not shown) to continue. This completes the configuration of the login.



Administrator Accounts -- Add Login: SAT Access Only

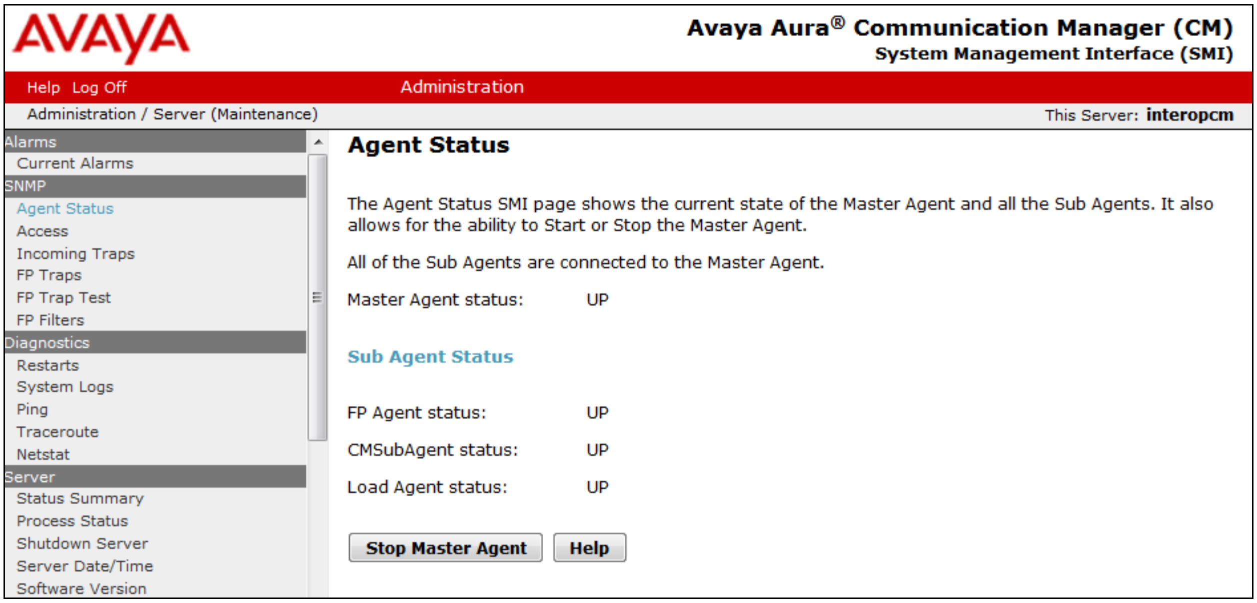
This page allows you to create a login that is intended to have access only to the Communication Manager System Administration Terminal (SAT) interface.

Login name	service
Primary group	○ users ● susers
Additional groups (profile)	prof21 You must assign a profile that has no web access if you want a login with SAT access only.
Linux shell	/opt/ecs/bin/autosat This shell setting does NOT disable the "*go shell*" SAT command for this user.
Home directory	/var/home/service
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Enter password	
Re-enter password	
Force password change on next login	● No ○ Yes

6.4. Configure SNMP on Communication Manager

Note that the following needs to be configured per Communication Manager node. If a duplex system is to be configured, complete these steps on each side of the Communication Manager.

To configure SNMP on Communication Manager, navigate to **Administration → Server Administration** (not shown) and select **Agent Status**. Click **Stop Master Agent** if the **Master Agent status** is **UP** to allow setup of the SNMP Agent.



Agent Status

The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

All of the Sub Agents are connected to the Master Agent.

Master Agent status: UP

Sub Agent Status

FP Agent status: UP

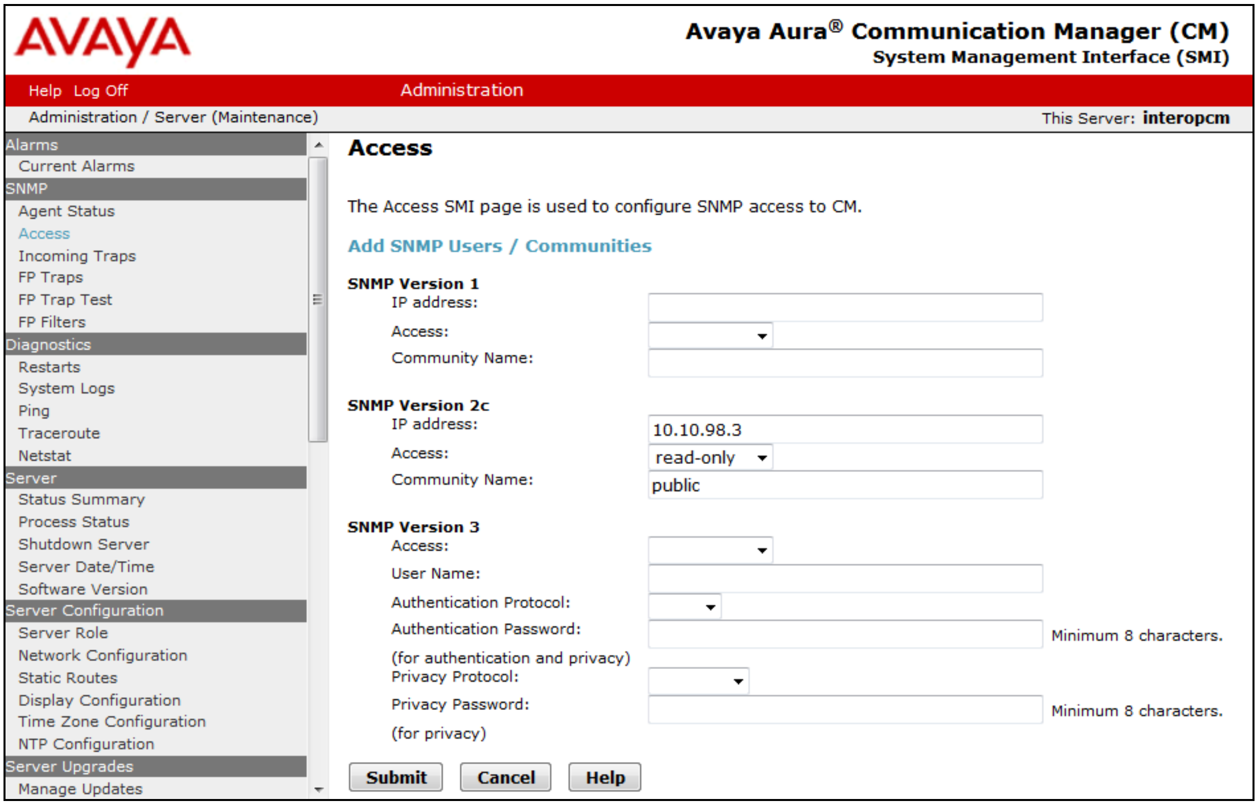
CMSubAgent status: UP

Load Agent status: UP

To allow ServicePilot to use SNMP to collect configuration and status information from Communication Manager, Select **Access** in the left pane and enter the following in the **SNMP Version 2c** section.

- **IP address** Enter the ServicePilot IP address 10.10.98.3
- **Access** Select "read-only" from the list
- **Community Name** Enter a name, e.g., "public"

Click the **Submit** button at the bottom of the page.



Access

The Access SMI page is used to configure SNMP access to CM.

Add SNMP Users / Communities

SNMP Version 1

IP address:

Access:

Community Name:

SNMP Version 2c

IP address: 10.10.98.3

Access: read-only

Community Name: public

SNMP Version 3

Access:

User Name:

Authentication Protocol:

Authentication Password: Minimum 8 characters.

(for authentication and privacy)

Privacy Protocol:

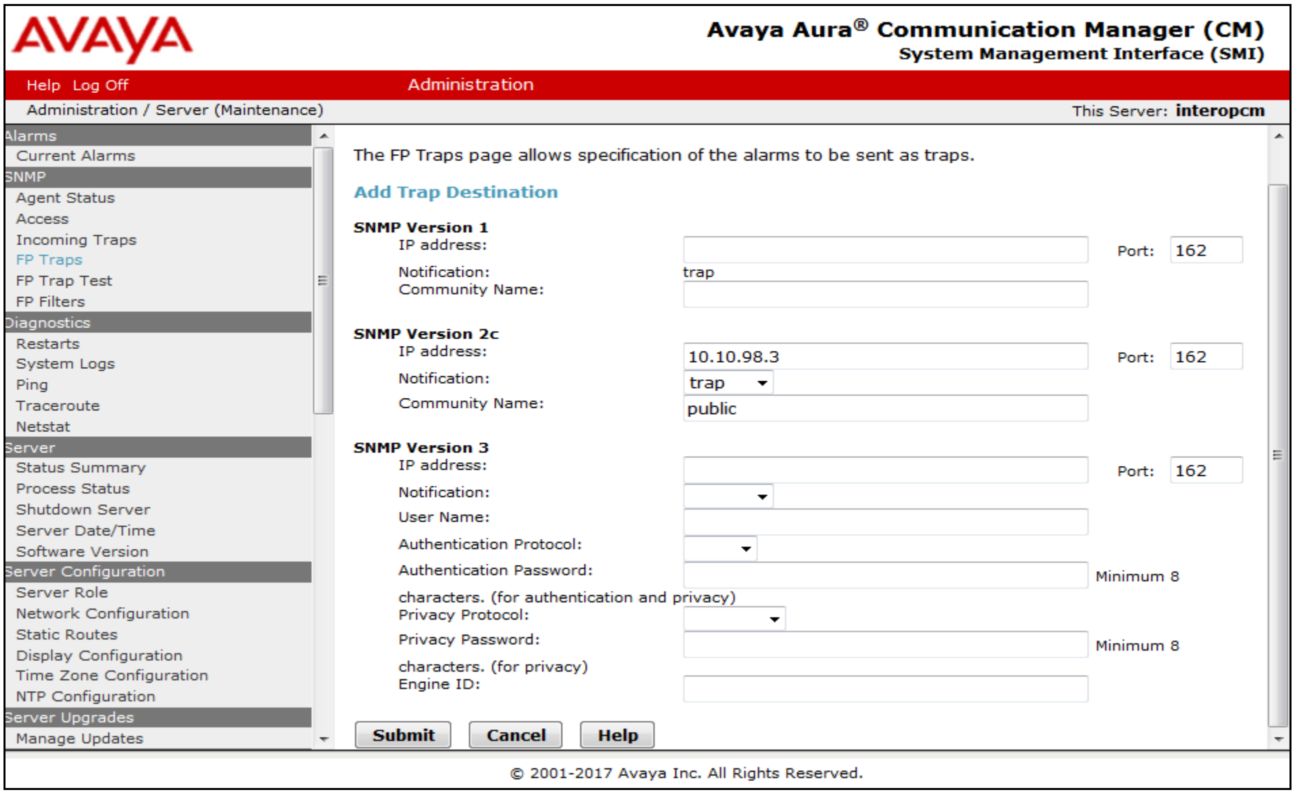
Privacy Password: Minimum 8 characters.

(for privacy)

Select **FP Traps** in navigation panel on the left side and click the **Add/Change** button (not shown). In the subsequent page enter the following in the **SNMP Version 2c**:

- **IP address** Enter the IP address of ServicePilot e.g., **10.10.98.3**
- **Notification** Select **trap** from the drop down list
- **Community Name** Enter **public**

Click the **Submit** button at the bottom of the page.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Administration / Server (Maintenance) This Server: **interopcm**

The FP Traps page allows specification of the alarms to be sent as traps.

Add Trap Destination

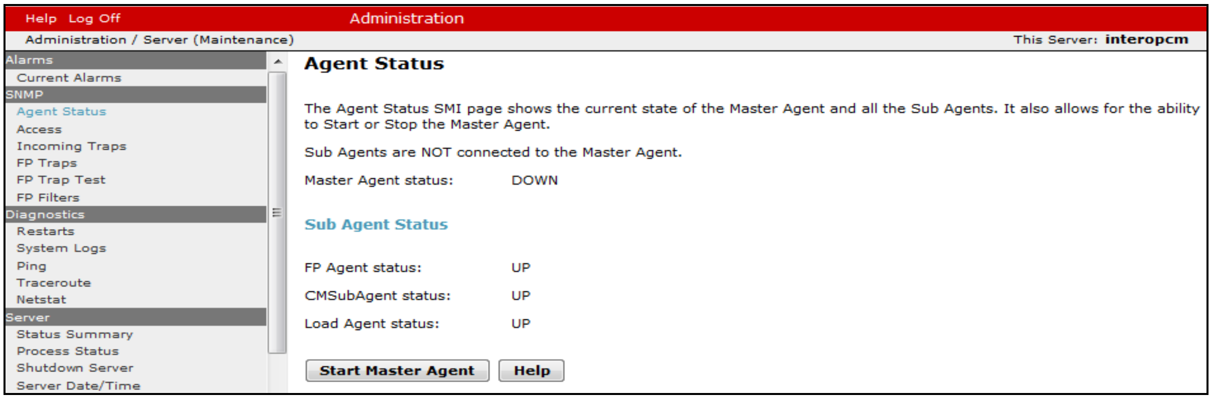
SNMP Version 1
IP address: Port: 162
Notification: trap
Community Name:

SNMP Version 2c
IP address: 10.10.98.3 Port: 162
Notification: trap
Community Name: public

SNMP Version 3
IP address: Port: 162
Notification:
User Name:
Authentication Protocol:
Authentication Password: Minimum 8 characters. (for authentication and privacy)
Privacy Protocol:
Privacy Password: Minimum 8 characters. (for privacy)
Engine ID:

© 2001-2017 Avaya Inc. All Rights Reserved.

To start the SNMP agent, select **Agent Status** in navigation panel on the left side. If the **Master Agent status** is **Down,** then click the **Start Master Agent** button. If the **Master Agent status** is **Up**, then the agent must be stopped and restarted.



Administration / Server (Maintenance) This Server: **interopcm**

Agent Status

The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

Sub Agents are NOT connected to the Master Agent.

Master Agent status: DOWN

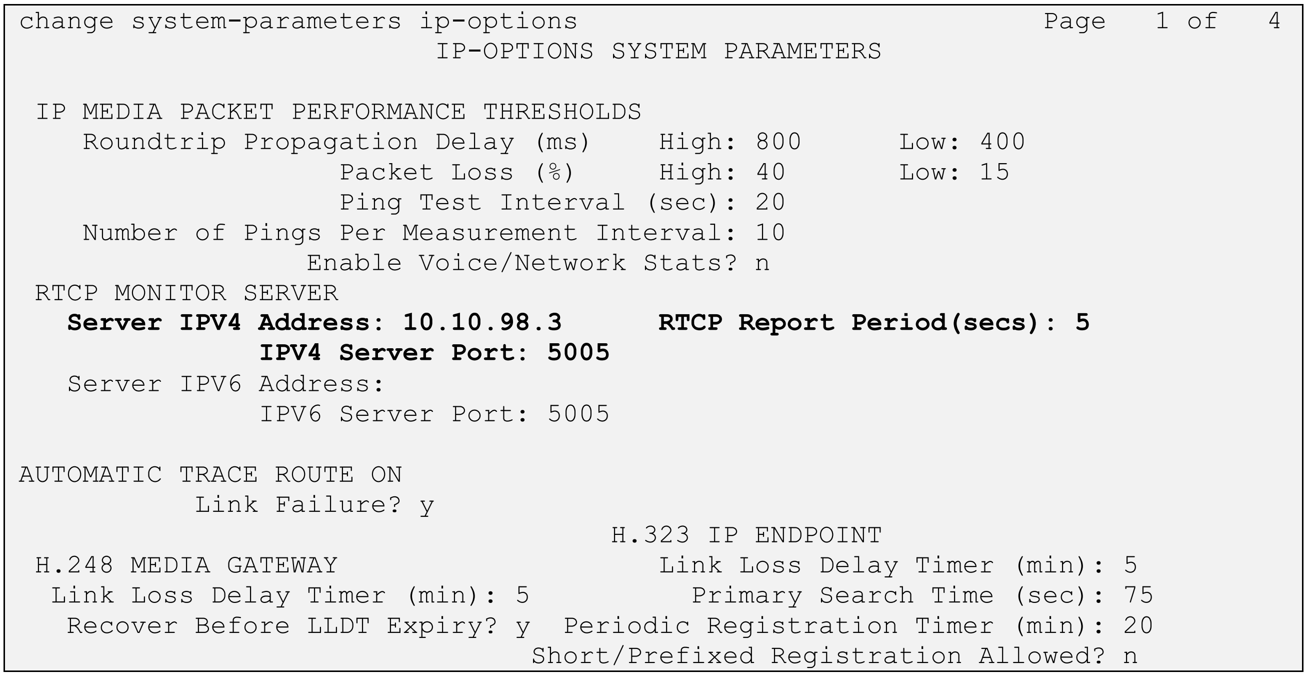
Sub Agent Status

FP Agent status: UP
CMSubAgent status: UP
Load Agent status: UP

6.5. Configure RTCP Monitoring

To allow ServicePilot to monitor the quality of IP calls, configure Communication Manager to send RTCP reporting to the IP address of the ServicePilot server. This is done through the SAT interface. Use the **change system-parameters ip-options** command and enter the following:

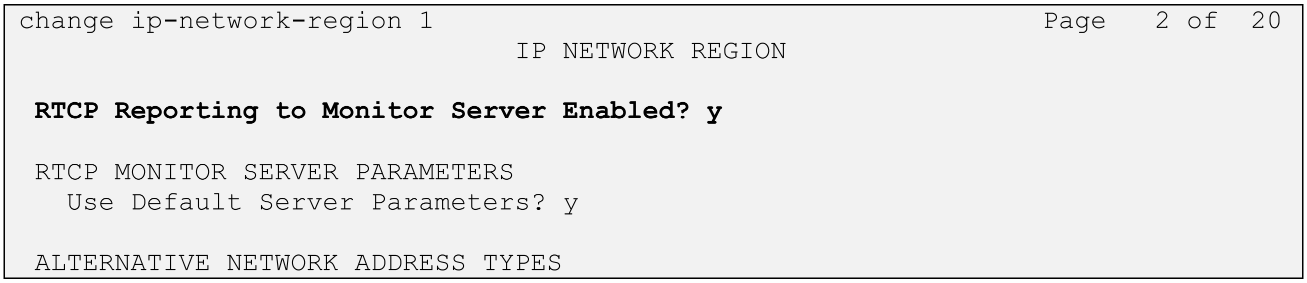
Server IPV4 Address	Enter the IP address of the ServicePilot server **10.10.98.3**
RTCP Report Period (secs)	Enter **5**
IPV4 Server Port	Enter **5005**



```
change system-parameters ip-options                             Page   1 of   4
                          IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                    Packet Loss (%)     High: 40       Low: 15
                    Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10
                  Enable Voice/Network Stats? n
 RTCP MONITOR SERVER
   Server IPV4 Address: 10.10.98.3      RTCP Report Period(secs): 5
               IPV4 Server Port: 5005
   Server IPV6 Address:
               IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                     H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY                    Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5          Primary Search Time (sec): 75
   Recover Before LLDT Expiry? y  Periodic Registration Timer (min): 20
                                Short/Prefixed Registration Allowed? n
```

Enter the **change ip-network-region *n*** command, where ***n*** is IP network region number to be monitored. On **Page 2**, set **RTCP Reporting to Monitor Server Enabled** to **y** and **Use Default Server Parameters** to **y**.

Note: Only one RTCP MONITOR SERVER can be configured per IP network region. Repeat this step for all IP network regions that are required to be monitored.



```
change ip-network-region 1                                      Page   2 of  20
                               IP NETWORK REGION

 RTCP Reporting to Monitor Server Enabled? y

 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? y

 ALTERNATIVE NETWORK ADDRESS TYPES
```

6.6. Configure CDR Monitoring

Use the **change node-names ip** command to add a new node name for the ISM server. In this configuration, the name **SPISM** is added with the IP address specified as **10.10.98.3.**

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AMS1                10.33.1.30
CMS18               10.33.1.20
SPISM               10.10.98.3
RDTT                10.10.98.86
```

A CDR link needs to be defined between Communication Manager and the ISM Server. Use the **change ip-services** command to configure the following:

- **Service Type** Enter **CDR2**
- **Local Node** Enter **procr**
- **Remote Node** Enter **SPISM**
- **Remote Port** Enter **50000**

Note: The ServicePilot is not a billing system they utilize the call detail recording to monitor calls in and out from Communication Manager therefore the CDR link should be configured as secondary link.

```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
CDR1                 procr            0       RDTT            9000
CDR2                 procr            0       SPISM           50000
```

Navigate to **Page 3** and set the **Reliable Protocol** field to **n**. This will disable Reliable Session Protocol (RSP) for CDR transmission. In this case, the CDR link will use TCP without RSP.

```
change ip-services                                              Page   3 of   4

                              SESSION LAYER TIMERS
  Service     Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type       Protocol     Timer       Message Cntr    Cntr     Timer

 CDR1            y         30                3          3         60
 CDR2            n         30                3          3         60
```

Use the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance testing.

- **CDR Date Format** Select **month/day** (day/month Date Format is also supported)
- **Primary Output Format** Select **unformatted**
- **Primary Output Endpoint** Select **CDR2** (CDR1 is usually used for billing applications)

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. The test configuration used some of the more common fields described below.

- **Intra-switch CDR** Select **y** (Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH-CDR form)
- **Record Outgoing Calls Only?** Select **n** (Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls)
- **Outg Trk Call Splitting?** Select **y** (Allows a separate call record for any portion of an outgoing call that is transferred or conferenced)
- **Inc Trk Call Splitting?** Select **y** (Allows a separate call record for any portion of an incoming call that is transferred or conferenced)

```
change system-parameters cdr                                    Page   1 of   1
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID):                       CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format: unformatted Secondary Output Endpoint: CDR2
           Use ISDN Layouts? n                 Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? n                Remove # From Called Number? n
Modified Circuit ID Display? n                            Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? y      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? y
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                    Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 5
Remove '+' from SIP Numbers? y
```

If the **Intra-switch CDR** field is set to **y** on **Page 1** of the SYSTEM-PARAMETERS CDR form, then use the **change intra-switch-cdr** command to define the extensions that will be subjected to call detail recording. In the **Assigned Members** field, enter the specific extensions whose usage will be tracked with CDR records.

```
change intra-switch-cdr                                         Page   1 of   3
                           INTRA-SWITCH CDR

                                Assigned Members:   17   of 5000   administered
   Extension          Extension          Extension          Extension
   3300
   3301
   3302
   3303
   3304
   3306
   3309
   3314
   3315
   3400
   3401
   3402
   3403
   3404
   3406
Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add
new members and 'change intra-switch-cdr <ext>' to change/remove other members
```

7. Configure SNMP for Media Gateway

This section provides the procedures for configuring SNMP on the Avaya G450 Media Gateway and Avaya Media Server. The procedures include the following areas. Repeat these procedures for any Media Gateway and Media Server in the network.

- Administer community string
- Administer SNMP traps
- Show SNMP

7.1. Configure SNMP for Media Gateway G450

Using SSH use the **snmp-server community** command shown below to set the desired community strings for read-only and read-write access, where *public* and *private* can be any desired community string.

```
G450-002(super)#
G450-002(super)# snmp-server community read-only public read-write public
Done!
```

Use the **snmp-server host** command shown below to enable SNMP traps to ServicePilot ISM, where **10.10.98.3** is the IP address of the ServicePilot server, and **public** is the read-only community string.

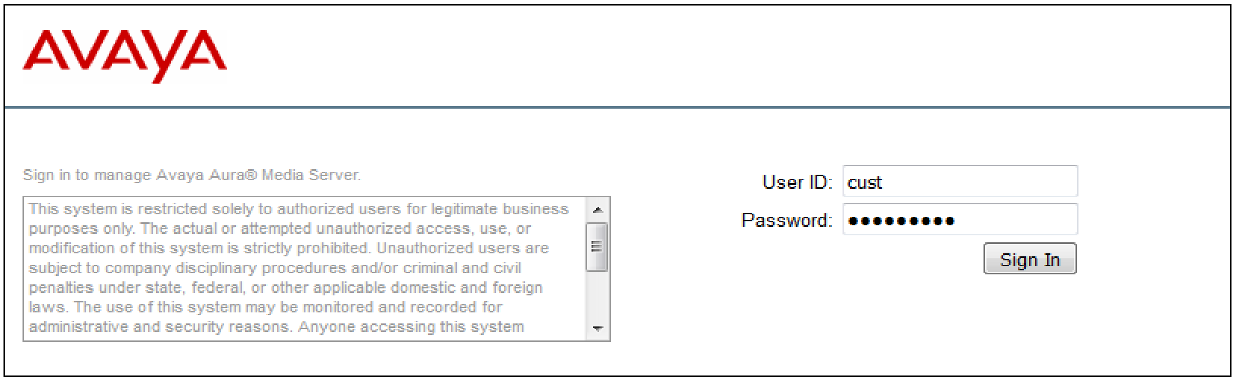
```
G450-002(super)# snmp-server host 10.10.98.3 traps v2c public
Done!
G450-002(super)#
```

The **show snmp** command can be used to display the list of SNMP receivers as shown below.

```
G450-002(super)# show snmp

Authentication trap disabled

Community-Access     Community-String
----------------     ----------------
read-only            *****
read-write           *****


SNMPv3 Notifications Status
-----------------------------
Traps:  Enabled
Informs:  Enabled         Retries: 3   Timeout: 3 seconds


SNMP-Rec-Address                              Model   Notification
Trap/InformUDP port                                      Level
User name
--------------------------------------------- ------- -------------- --------
---
10.33.1.6                                       v1    all            trap
162 - Dynamic Trap Manager                    noauth
ReadCommN


10.10.98.3                                      v2c   all            trap
162                                           noauth
WriteCommN

G450-002(super)#
```

7.2. Configure SNMP for Media Server

Using a web browser, access Element Manager of Media Server **https://<ip-addr of media server>:8443/em**. Login Element Manager by using proper credentials and click on **Sign In** button to login.



Sign in to manage Avaya Aura® Media Server.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system

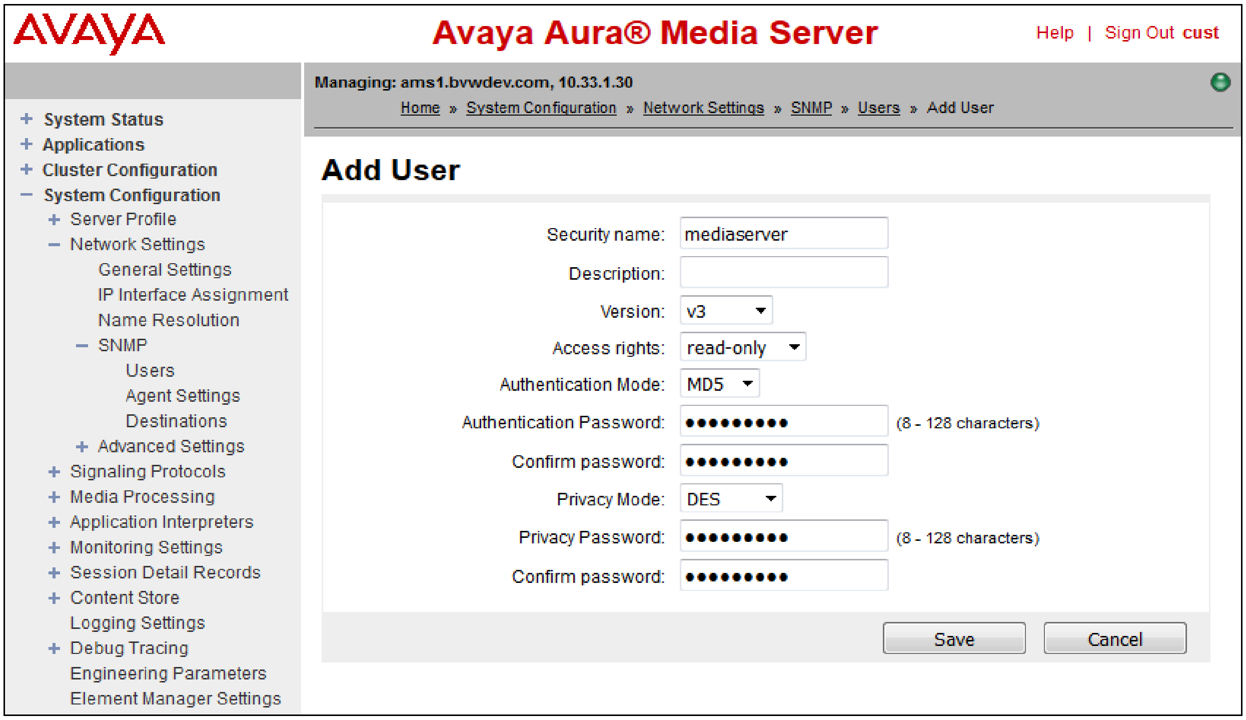
User ID: cust

Password: ●●●●●●●●●

To configure SNMP for Media Server, navigate to **Home → System Configuration → Network Settings → SNMP**. Select **User** (not shown) to add a new SNMP user. Provide the following values for the new user.

- **Security name**: Enter a username e.g., "mediaserver"
- **Version**: Select **v3** from the drop down list
- **Access rights**: Select **read-only** from the drop down list
- **Authenticate Mode**: Select **MD5**
- **Authentication Password** and **Confirm Password**: Enter a password for the Authentication mode
- **Privacy Mode**: Select **DES** from the list
- **Privacy Password** and **Confirm Password**: Enter a password for the privacy mode

On completion, select **Save** button.



Managing: ams1.bvwdev.com, 10.33.1.30

Home » System Configuration » Network Settings » SNMP » Users » Add User

Add User

Security name: mediaserver

Description:

Version: v3

Access rights: read-only

Authentication Mode: MD5

Authentication Password: ●●●●●●●●● (8 - 128 characters)

Confirm password: ●●●●●●●●●

Privacy Mode: DES

Privacy Password: ●●●●●●●●● (8 - 128 characters)

Confirm password: ●●●●●●●●●

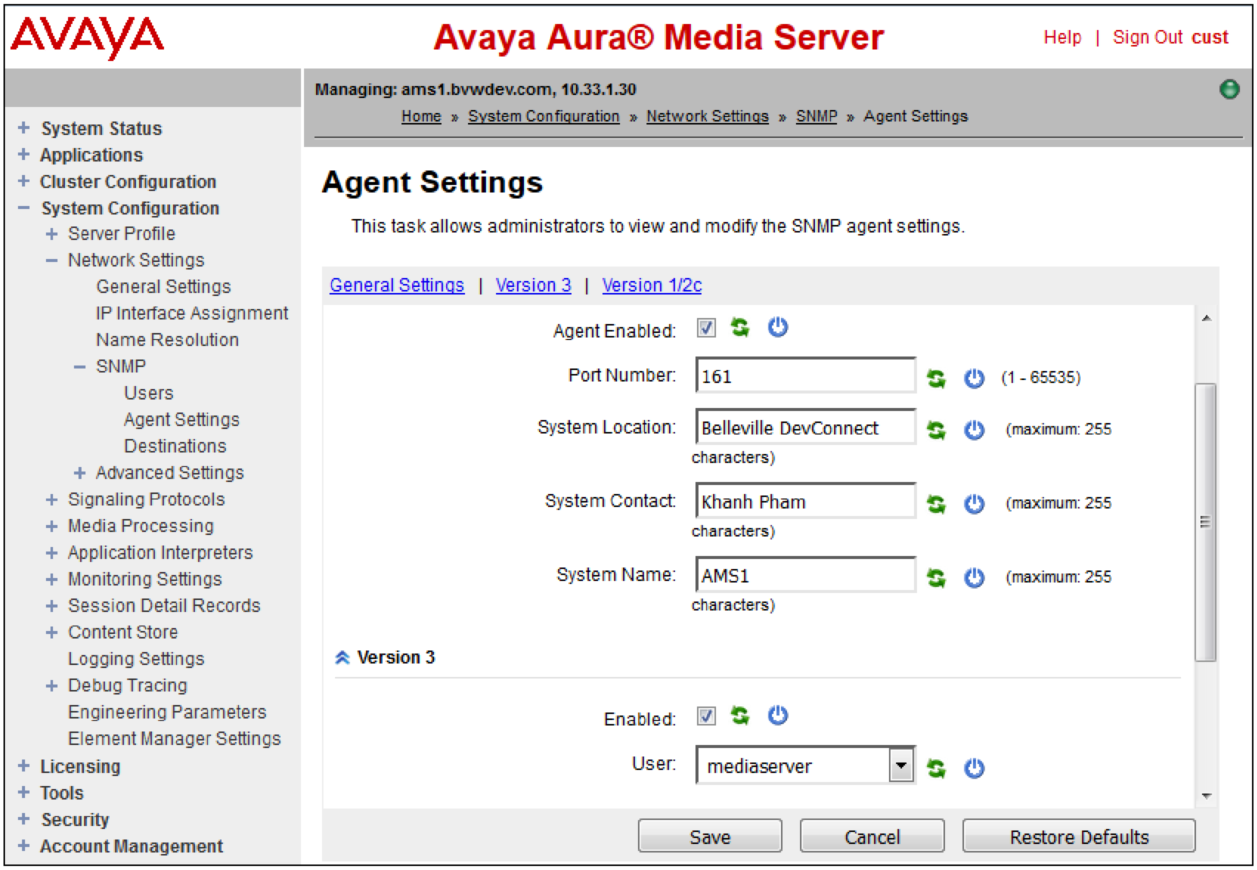
Select **Agent Settings** to administer SNMP agent settings.

In the **General Settings** section:

- **Agent Enabled**: Check on the checkbox to enable
- **Port Number**: Enter port **161**
- **System Location**: Enter location e.g., "Belleville DevConnect"
- **System Contact**: Enter a contact name
- **System Name**: Enter a name of the system

In the **Version 3** section, select **Enabled** checkbox and select "mediaserver" user from the drop down list as configured above.

On completion, select **Save** button.



Managing: ams1.bvwdev.com, 10.33.1.30

Home » System Configuration » Network Settings » SNMP » Agent Settings

Agent Settings

This task allows administrators to view and modify the SNMP agent settings.

General Settings | Version 3 | Version 1/2c

Agent Enabled: ☑

Port Number: 161 (1 - 65535)

System Location: Belleville DevConnect (maximum: 255 characters)

System Contact: Khanh Pham (maximum: 255 characters)

System Name: AMS1 (maximum: 255 characters)

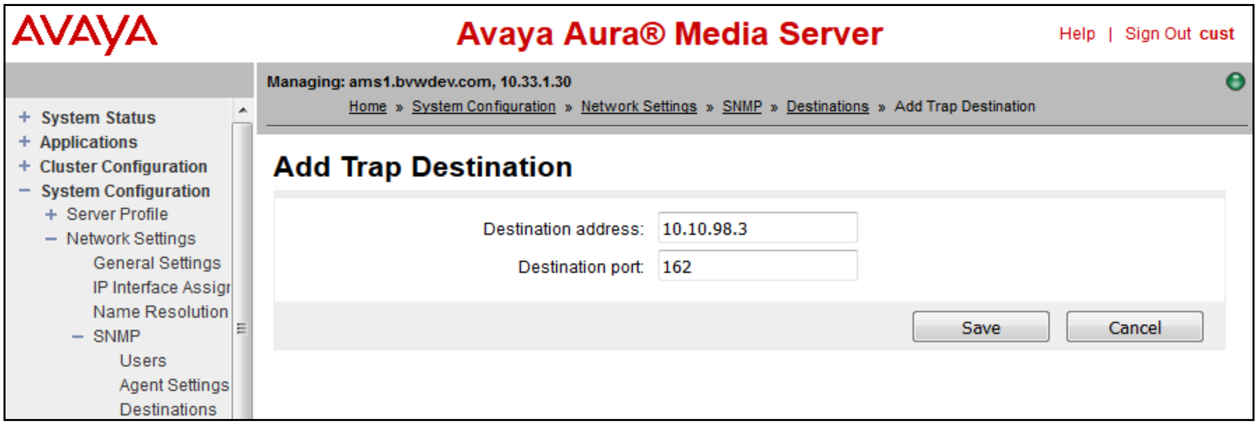
Version 3

Enabled: ☑

User: mediaserver

The Traps destination needs to be configured to send the traps to the ServicePilot server. Select **Destinations**, the Traps Destinations page is displayed in the right hand select **Add** button (not shown) and enter the IP address of ServicePilot **10.10.98.3** in the **Destination address** and port **162** in the **Destination port**.

On completion, select **Save** button.



Add Trap Destination

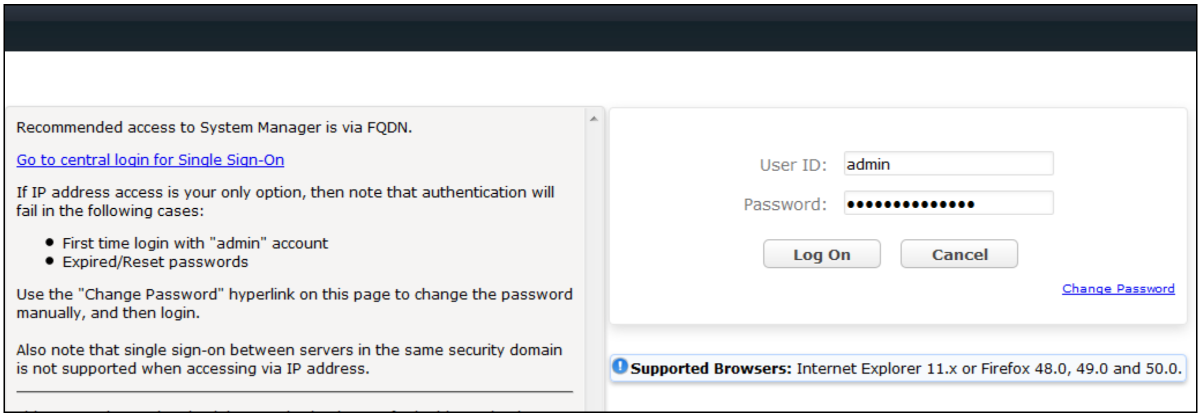
Destination address: 10.10.98.3

Destination port: 162

8. Configure Avaya Aura® System Manager

ServicePilot monitors and collects data from System Manager and Session Manager, a number of configurations are required and can be summarized as follows:

Configuration changes are required on these devices to allow monitoring. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and click the **Log On** button.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

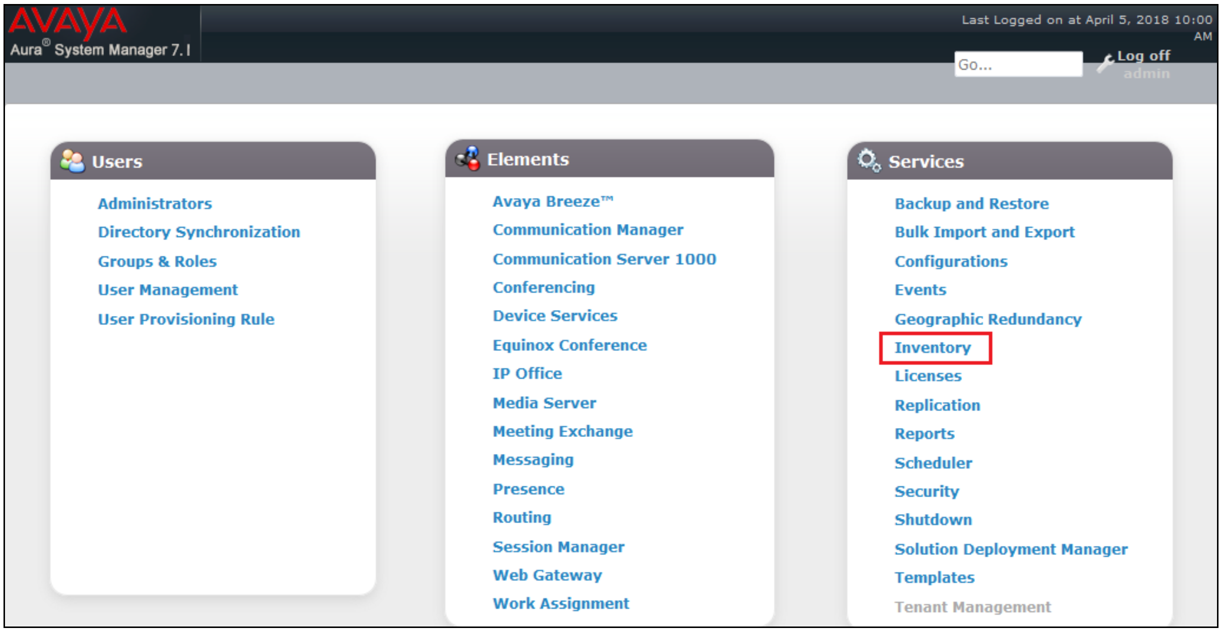
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID: admin

Password: ••••••••••••••

Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

On the subsequent page**,** select **Inventory** in the **Services** section.



Last Logged on at April 5, 2018 10:00 AM

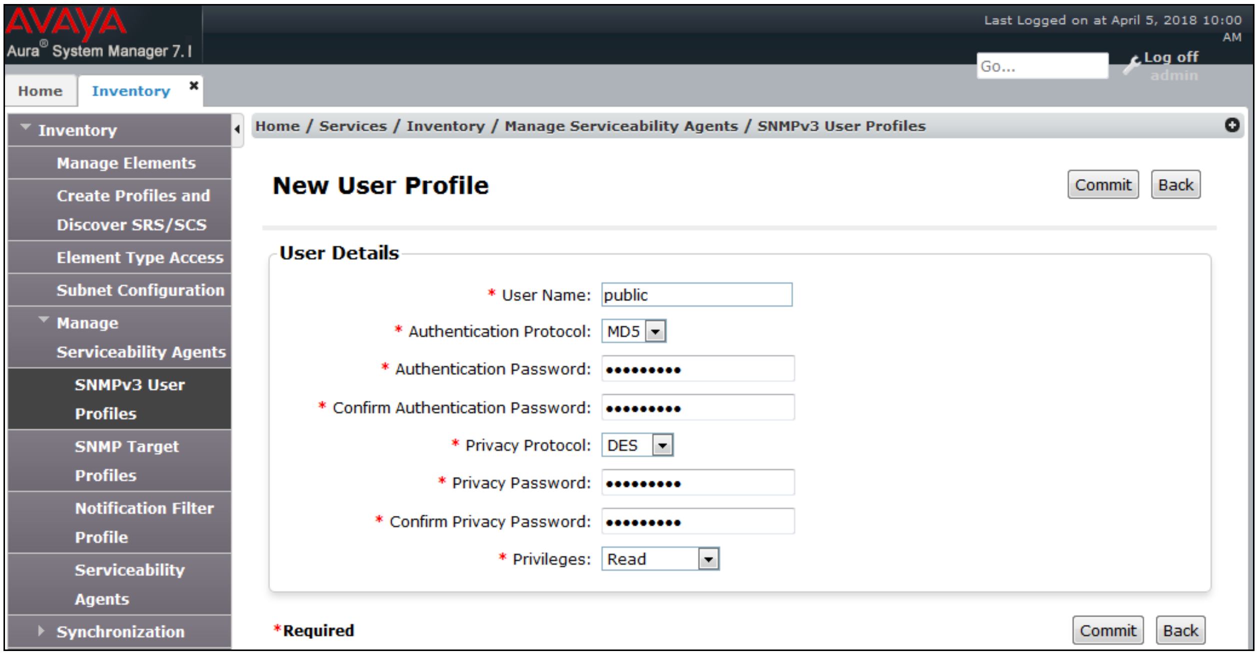
Select **Manage Serviceability Agents → SNMPv3 User Profiles** in the navigation panel on the left and click the **New** button to add a new user profile.

On the subsequent page enter the following details for the User Profile:

- **User Name** Enter a username e.g., **public**
- **Authentication Protocol** Select **MD5** from the drop down list
- **Authentication Password** Enter an appropriate password and confirm
- **Privacy Protocol** Enter **DES**
- **Privacy Password** Enter an appropriate password and confirm
- **Privileges** Select **Read** from the drop down list

Click **Commit** to submit.

Note: The user profile will be defined in the ServicePilot configuration **Section 11.5**.


AVAYA
Aura® System Manager 7.1
Last Logged on at April 5, 2018 10:00 AM
Go...
Log off admin
Home
Inventory
Inventory
Manage Elements
Create Profiles and Discover SRS/SCS
Element Type Access
Subnet Configuration
Manage Serviceability Agents
SNMPv3 User Profiles
SNMP Target Profiles
Notification Filter Profile
Serviceability Agents
Synchronization
Home / Services / Inventory / Manage Serviceability Agents / SNMPv3 User Profiles
Commit
Back

New User Profile

User Details

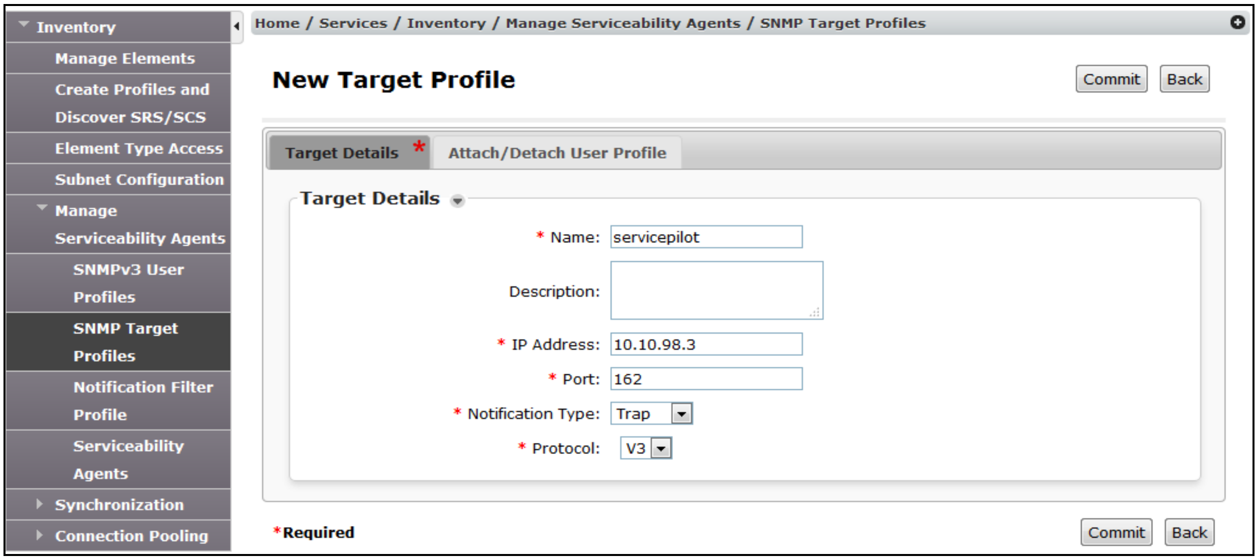
* User Name:	public
* Authentication Protocol:	MD5
* Authentication Password:	•••••••••
* Confirm Authentication Password:	•••••••••
* Privacy Protocol:	DES
* Privacy Password:	•••••••••
* Confirm Privacy Password:	•••••••••
* Privileges:	Read

*Required

Select **Manage Serviceability Agents → SNMPv3 Target Profiles** in the navigation panel on the left and click the **New** button (not shown) to add a new target profile.

On the subsequent page enter the following details for the User Profile:

- **Name** Enter a name e.g., **servicepilot**
- **Description** This field is optional
- **IP Address** Enter the IP address of ServicePilot server
- **Port** Enter the port **162**
- **Notification Type** Select **Trap** from the drop down list
- **Protocol** Select **V3** from the drop down list



Inventory
Manage Elements
Create Profiles and Discover SRS/SCS
Element Type Access
Subnet Configuration
Manage Serviceability Agents
SNMPv3 User Profiles
SNMP Target Profiles
Notification Filter Profile
Serviceability Agents
Synchronization
Connection Pooling
Home / Services / Inventory / Manage Serviceability Agents / SNMP Target Profiles
Commit
Back
Target Details *
Attach/Detach User Profile

New Target Profile

Target Details

* Name: servicepilot

Description:

* IP Address: 10.10.98.3

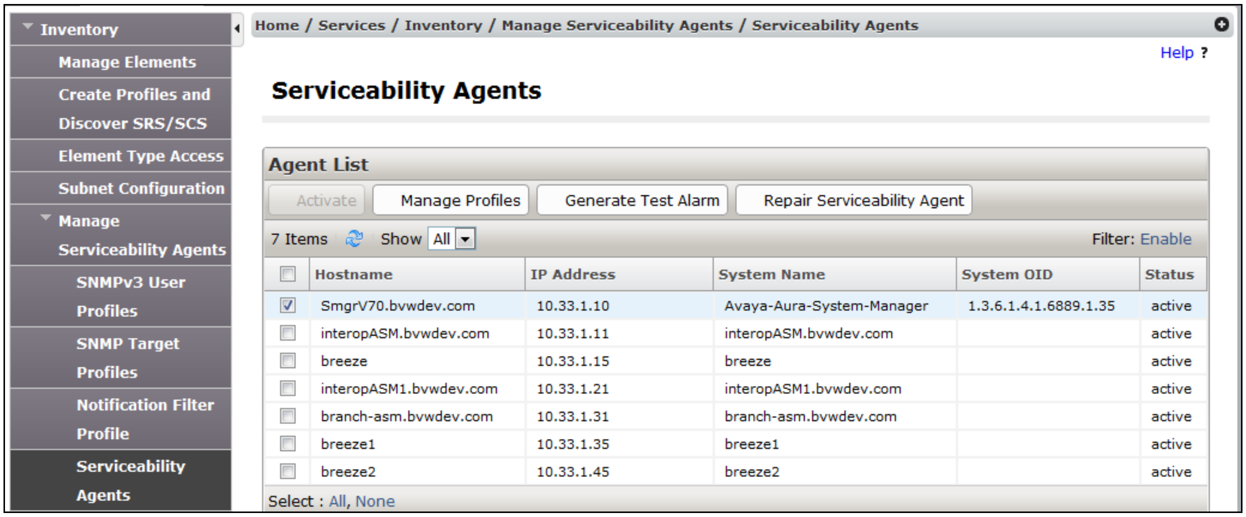
* Port: 162

* Notification Type: Trap

* Protocol: V3

*Required

Navigate to **Manage Serviceability Agents → Serviceability Agents** in the panel on the left. Check that the System Manager Agent Status is active. Select System Manager (SMGRV70.bvwdev.com.) and click **Manage Profiles**.



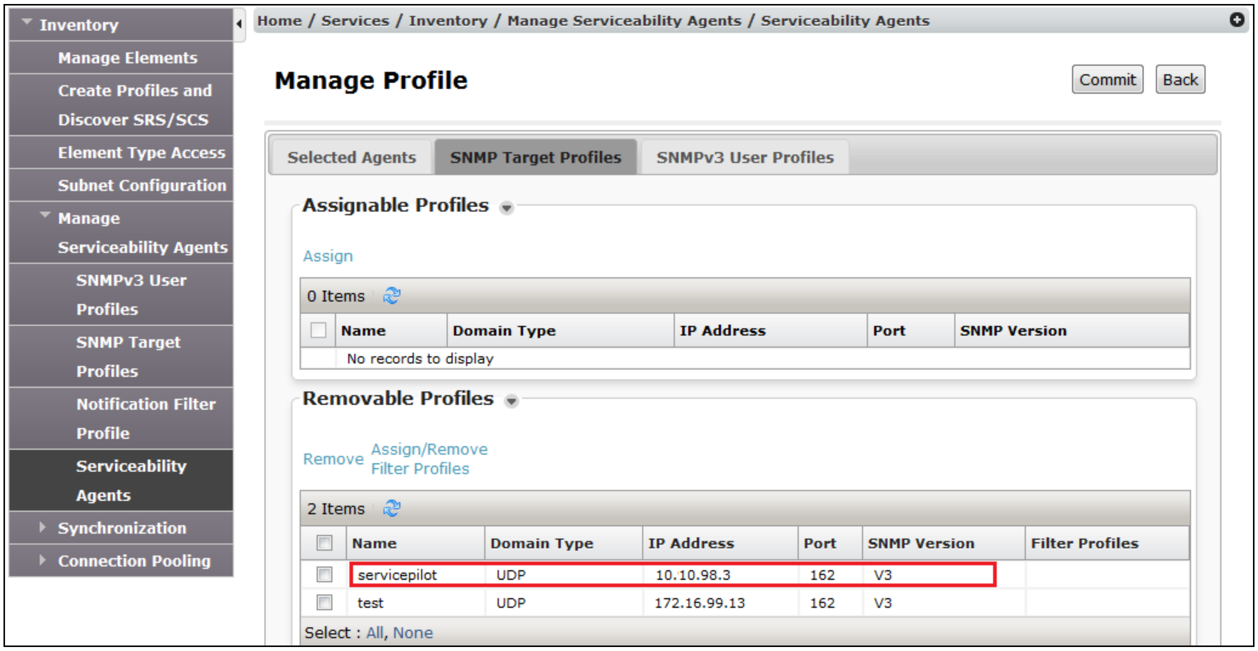
Serviceability Agents

Agent List

7 Items Show All

□	Hostname	IP Address	System Name	System OID	Status
☑	SmgrV70.bvwdev.com	10.33.1.10	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
□	interopASM.bvwdev.com	10.33.1.11	interopASM.bvwdev.com		active
□	breeze	10.33.1.15	breeze		active
□	interopASM1.bvwdev.com	10.33.1.21	interopASM1.bvwdev.com		active
□	branch-asm.bvwdev.com	10.33.1.31	branch-asm.bvwdev.com		active
□	breeze1	10.33.1.35	breeze1		active
□	breeze2	10.33.1.45	breeze2		active

On the subsequent page, select **SNMP Target Profiles**. Click down arrow beside **Assignable Profiles** section if not expanded. Click **Assign** to assign it to System Manager. The target profile is moved to the **Removable Profiles** section as below. The target profile has been assigned to System Manager. Click **Commit** to submit the changes.



Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

Manage Profile

Assignable Profiles

0 Items

□	Name	Domain Type	IP Address	Port	SNMP Version
	No records to display				

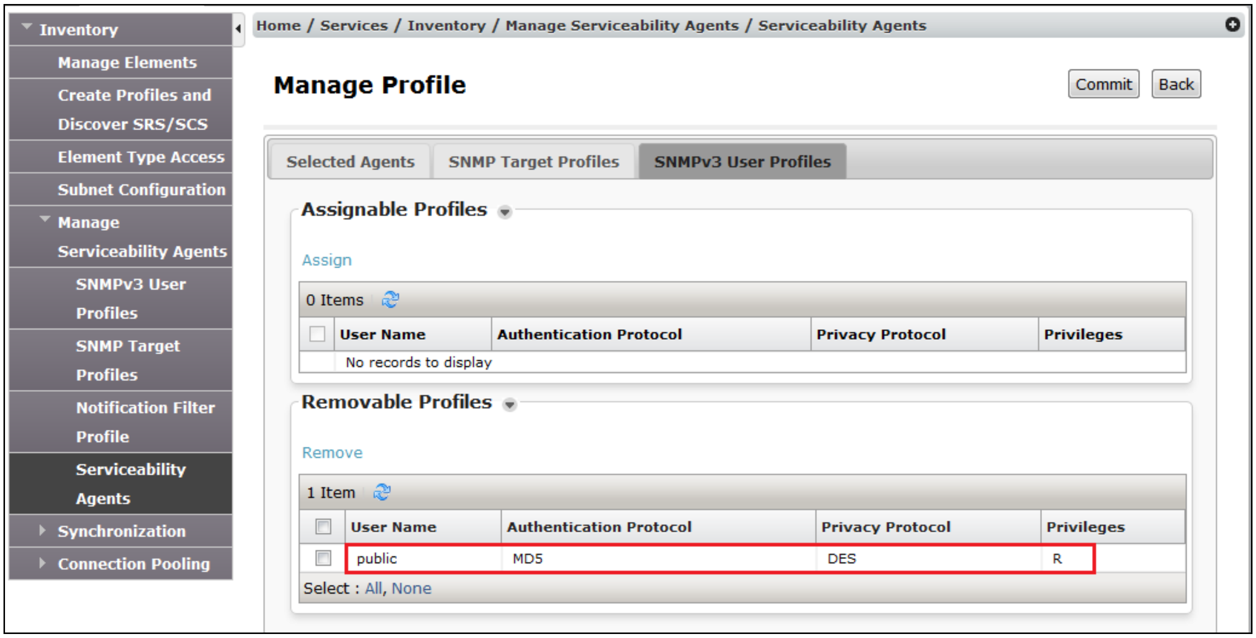
Removable Profiles

2 Items

□	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
□	servicepilot	UDP	10.10.98.3	162	V3	
□	test	UDP	172.16.99.13	162	V3	

Select : All, None

Repeat the same step above for **SNMPv3 User Profiles**. The user profile **public** is assigned to System Manager. Click **Commit** button to save the change.



Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

Manage Profile

Assignable Profiles

0 Items

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
	No records to display			

Removable Profiles

1 Item

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
□	public	MD5	DES	R

Select : All, None

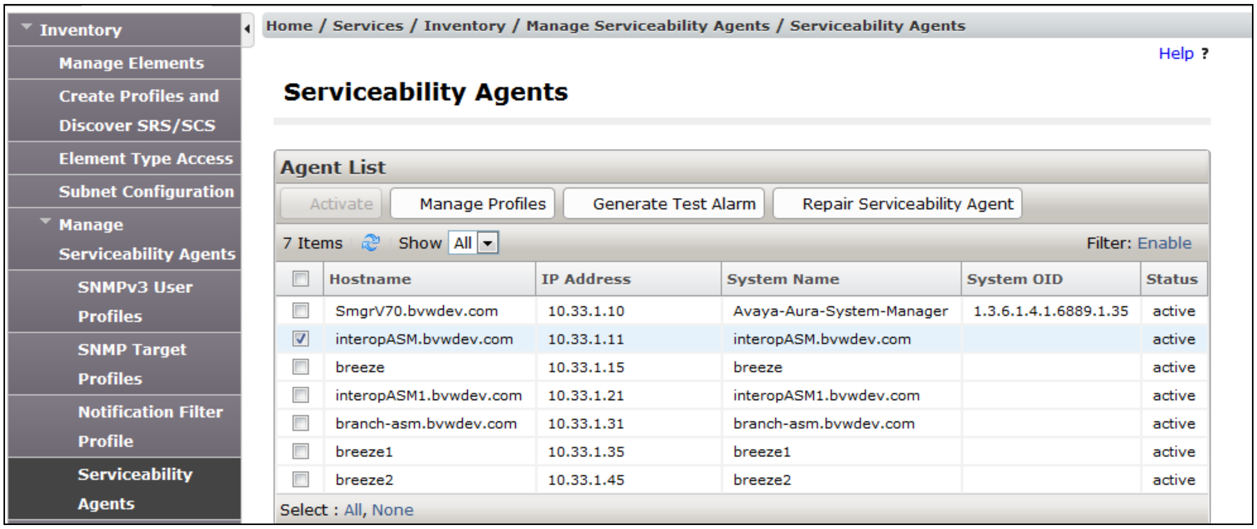
9. Configure Avaya Aura® Session Manager

ServicePilot monitors and collects data from Session Manager; a number of configurations are required and can be summarized as follows:

- Configure SNMP for Session Manager
- Configure RTCP
- Configure CDR

9.1. Configure SNMP for Session Manager

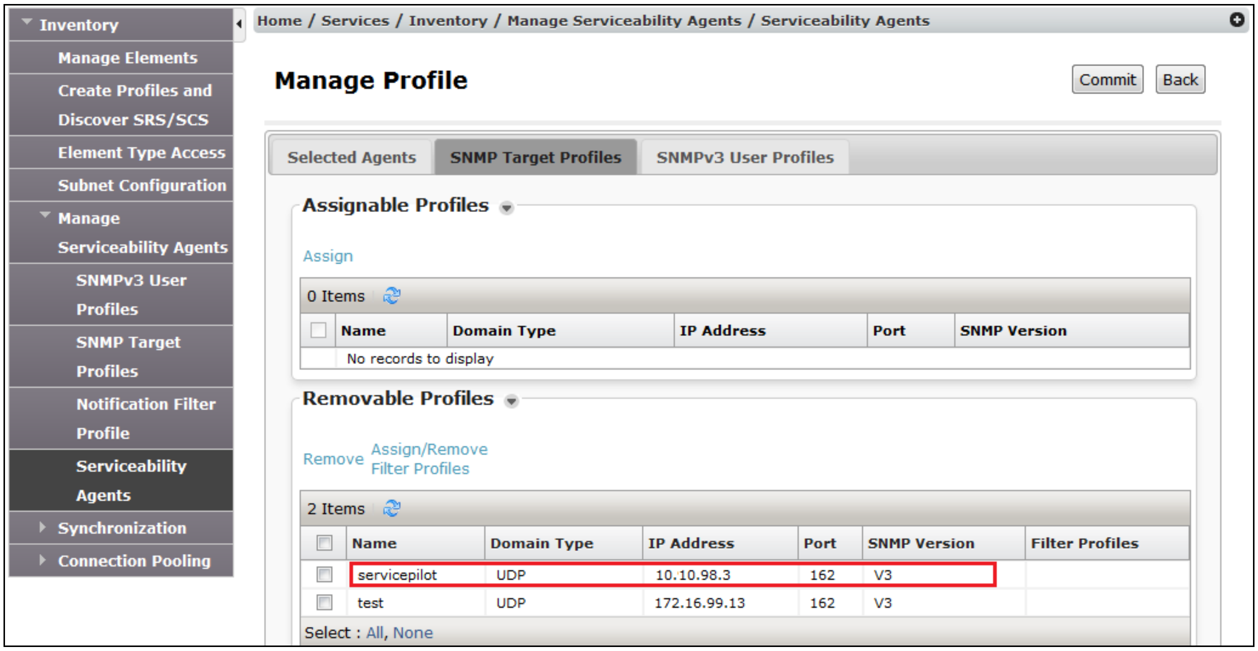
Use the same **SNMPv3 User Profiles** and **SNMPv3 Target Profiles** in **Section 8** above to configure SNMP for Session Manger. Navigate to **Manage Serviceability Agents → Serviceability Agents** in the panel on the left. Check that the System Manager Agent Status is active. Select Session Manager (**interopASM.bvwdev.com**) and click **Manage Profiles**.



□	Hostname	IP Address	System Name	System OID	Status
□	SmgrV70.bvwdev.com	10.33.1.10	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
☑	interopASM.bvwdev.com	10.33.1.11	interopASM.bvwdev.com		active
□	breeze	10.33.1.15	breeze		active
□	interopASM1.bvwdev.com	10.33.1.21	interopASM1.bvwdev.com		active
□	branch-asm.bvwdev.com	10.33.1.31	branch-asm.bvwdev.com		active
□	breeze1	10.33.1.35	breeze1		active
□	breeze2	10.33.1.45	breeze2		active

Select : All, None

On the subsequent page select **SNMP Target Profiles**. Click down arrow beside **Assignable Profiles** section if not expanded. Click **Assign** to assign it to System Manager. The target profile is moved to the **Removable Profiles** section as below. The target profile has been assigned to System Manager. Click **Commit** to submit the changes.



Manage Profile

Assignable Profiles

0 Items

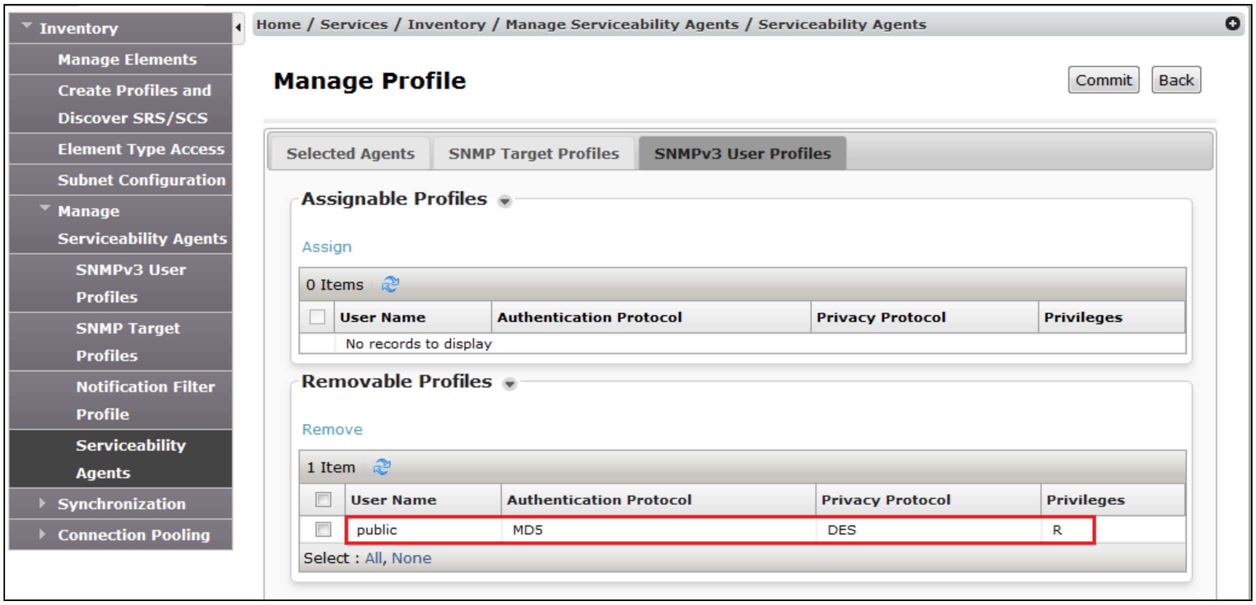
□	Name	Domain Type	IP Address	Port	SNMP Version
	No records to display				

Removable Profiles

2 Items

□	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
□	servicepilot	UDP	10.10.98.3	162	V3	
□	test	UDP	172.16.99.13	162	V3	

Repeat the same step above for **SNMPv3 User Profiles**. The user profile **public** is assigned to System Manager. Click **Commit** button to save the change.



Manage Profile

Assignable Profiles

0 Items

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
	No records to display			

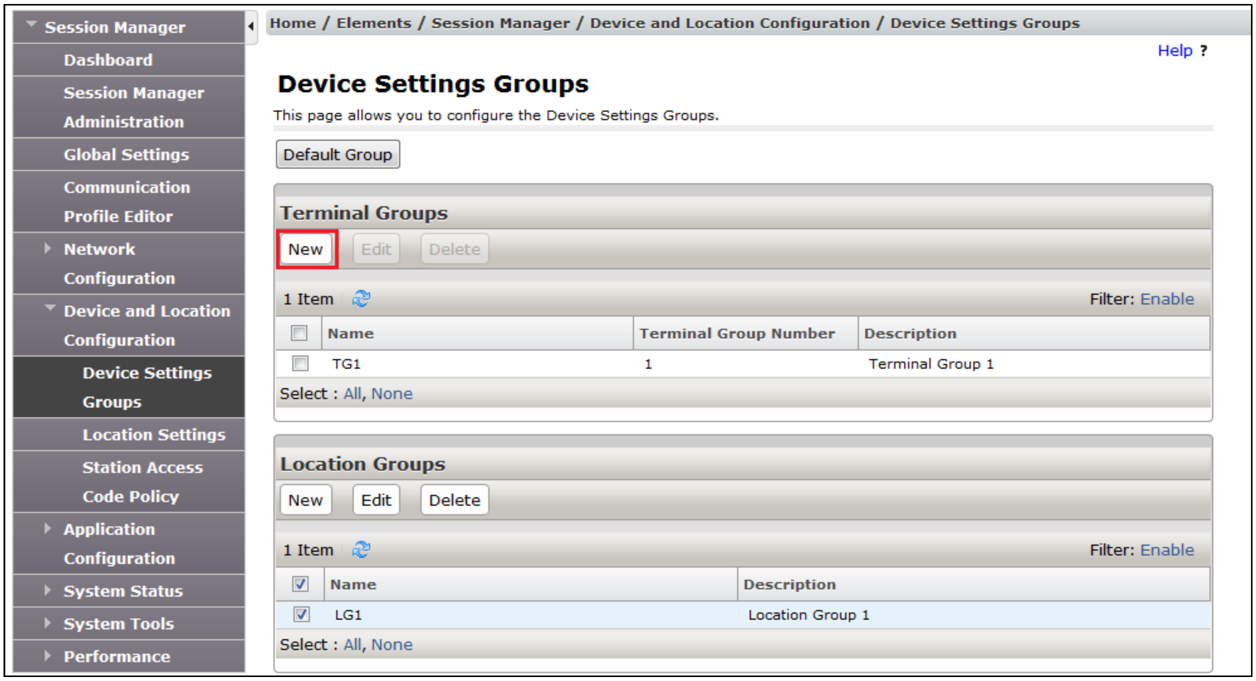
Removable Profiles

1 Item

□	User Name	Authentication Protocol	Privacy Protocol	Privileges
□	public	MD5	DES	R

9.2. Configure RTCP

Select **Session Manager** from the **Elements** section (not shown) and navigate to **Device and Location Configuration → Device Settings Groups** in the navigation panel on the left and click the **New** button to add a **Terminal Group**.


Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Device Settings Groups
Location Settings
Station Access Code Policy
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Device and Location Configuration / Device Settings Groups
Help ?
Default Group
New
Edit
Delete
Filter: Enable

Device Settings Groups

This page allows you to configure the Device Settings Groups.

Terminal Groups

1 Item

□	Name	Terminal Group Number	Description
□	TG1	1	Terminal Group 1

Select : All, None

Location Groups

1 Item

☑	Name	Description
☑	LG1	Location Group 1

Select : All, None

On the subsequent page enter the following:

General Section

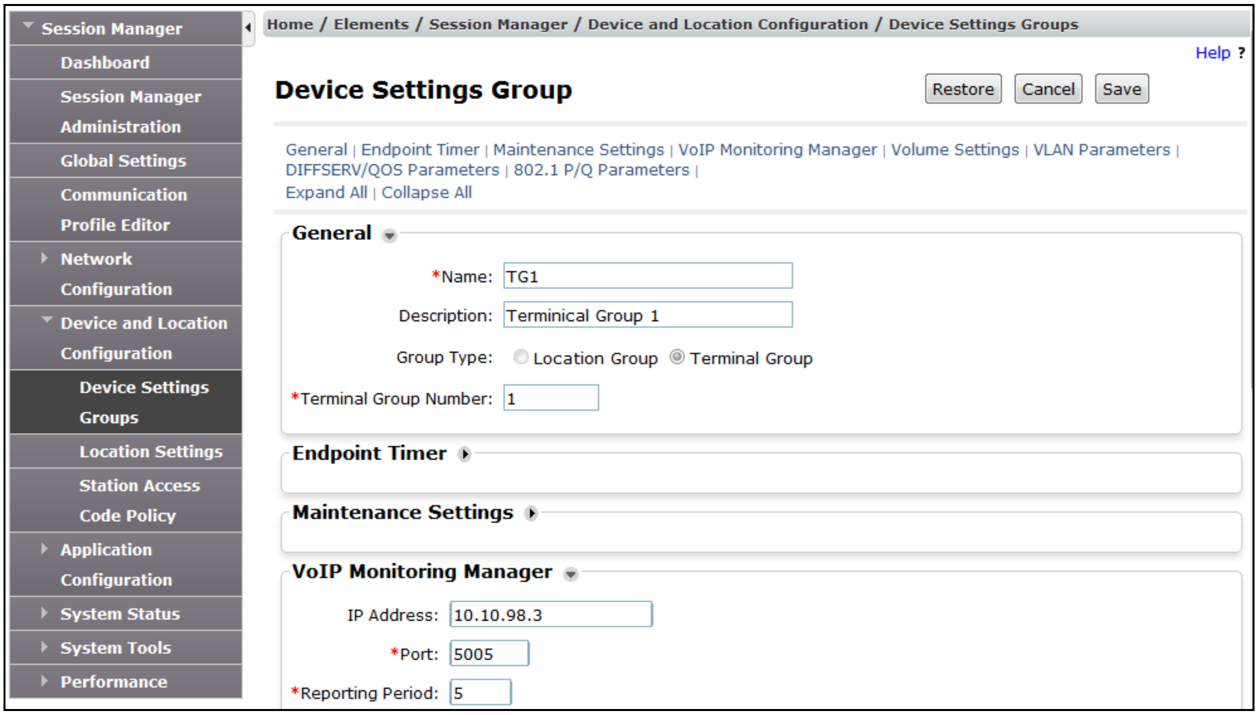
- **Name** Enter an appropriate name
- **Terminal Group** Click the radio button
- **Terminal Group Number** Enter an appropriate Terminal Group Number

Note: The Terminal group number needs to be configured on each telephone to be monitored using the **Group procedure**. The actual procedure is outside the scope of these Application Notes.

VoIP Monitoring Manager Section

- **IP Address** Enter he IP address of the ServicePilot Server **10.10.98.3**
- **Port** Enter **5005**
- **Reporting Period** Enter **5**

Click **Save** to submit the changes.



Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Device Settings Groups
Location Settings
Station Access Code Policy
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Device and Location Configuration / Device Settings Groups
Help ?
Restore
Cancel
Save
General | Endpoint Timer | Maintenance Settings | VoIP Monitoring Manager | Volume Settings | VLAN Parameters | DIFFSERV/QOS Parameters | 802.1 P/Q Parameters |
Expand All | Collapse All
Endpoint Timer
Maintenance Settings

Device Settings Group

General

*Name: TG1

Description: Terminical Group 1

Group Type: ○ Location Group ● Terminal Group

*Terminal Group Number: 1

VoIP Monitoring Manager

IP Address: 10.10.98.3

*Port: 5005

*Reporting Period: 5

In the **Device Settings Groups**, click **New** button in the **Location Groups** to add a new location group.

On the subsequent page enter the following:

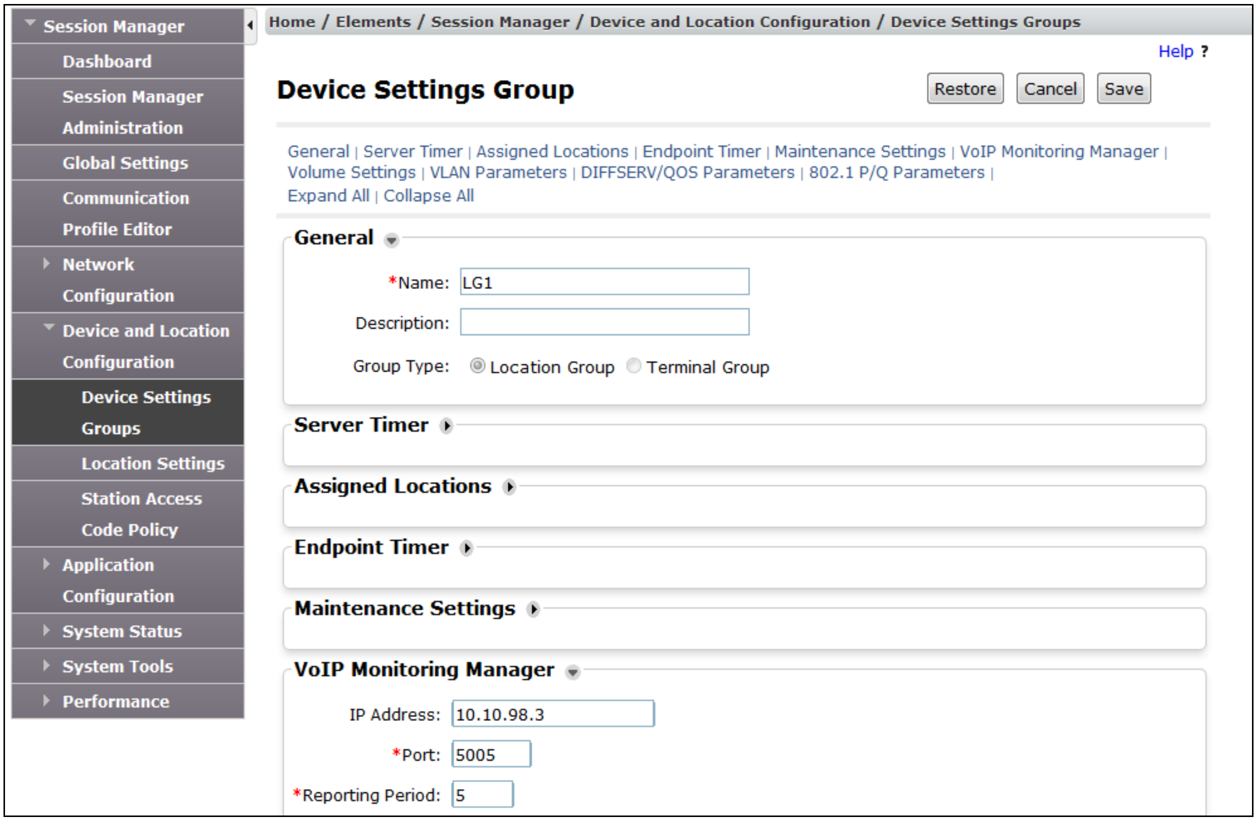
General Section

- **Name** Enter an appropriate name
- **Group Type** Select radio button **Location Group**

VoIP Monitoring Manager Section

- **IP Address** Enter he IP address of the ServicePilot Server **10.10.98.3**
- **Port** Enter **5005**
- **Reporting Period** Enter **5**

Click **Save** to submit the changes.


Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Device Settings Groups
Location Settings
Station Access Code Policy
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Device and Location Configuration / Device Settings Groups
Help ?
Restore
Cancel
Save
General | Server Timer | Assigned Locations | Endpoint Timer | Maintenance Settings | VoIP Monitoring Manager | Volume Settings | VLAN Parameters | DIFFSERV/QOS Parameters | 802.1 P/Q Parameters |
Expand All | Collapse All
Server Timer
Assigned Locations
Endpoint Timer
Maintenance Settings

Device Settings Group

General

*Name: LG1

Description:

Group Type: ● Location Group ○ Terminal Group

VoIP Monitoring Manager

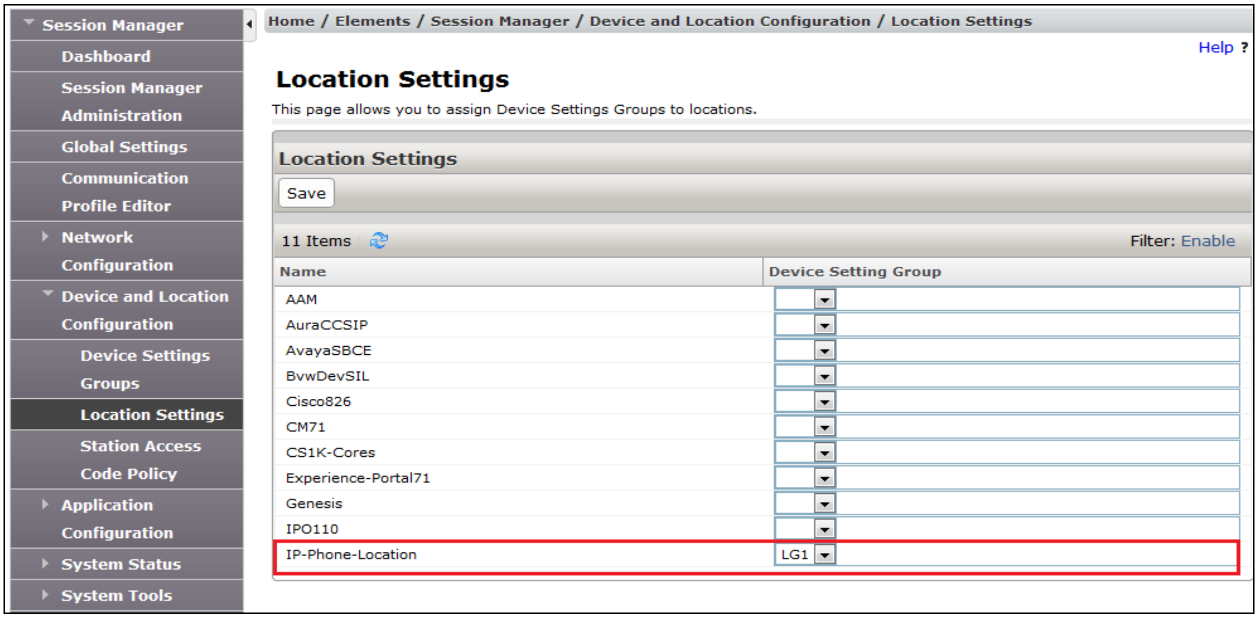
IP Address: 10.10.98.3

*Port: 5005

*Reporting Period: 5

Navigate to **Device and Location Configuration → Location Settings** in the navigation panel on the left and the **Location Settings** is displayed in the right hand side. In the list of Location Settings, select the location group **LG1** configured above in the **IP-Phone-Location** to assign the location group LG1to this location. Note that the **IP-Phone-Location** is previously configured in **Locations** section of **Routing**.

Click on **Save** button to save the change.



Home / Elements / Session Manager / Device and Location Configuration / Location Settings

Location Settings

This page allows you to assign Device Settings Groups to locations.

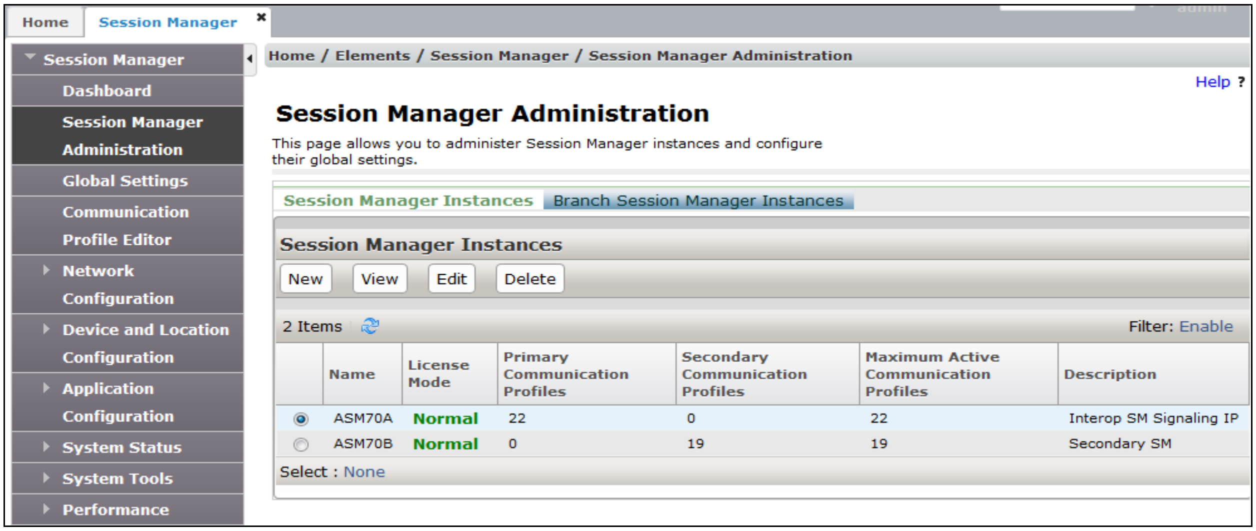
Location Settings

11 Items

Name	Device Setting Group
AAM	
AuraCCSIP	
AvayaSBCE	
BvwDevSIL	
Cisco826	
CM71	
CS1K-Cores	
Experience-Portal71	
Genesis	
IPO110	
IP-Phone-Location	LG1

9.3. Configure CDR

Navigate to **Session Manager → Session Manager Administration** in the navigation panel on the left. Scroll down to **Session Manager Instances** section, click the appropriate Session Manager radio button and then click the **Edit** button.


Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Help ?
Session Manager Instances
Branch Session Manager Instances
New
View
Edit
Delete
Filter: Enable

Home / Elements / Session Manager / Session Manager Administration

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

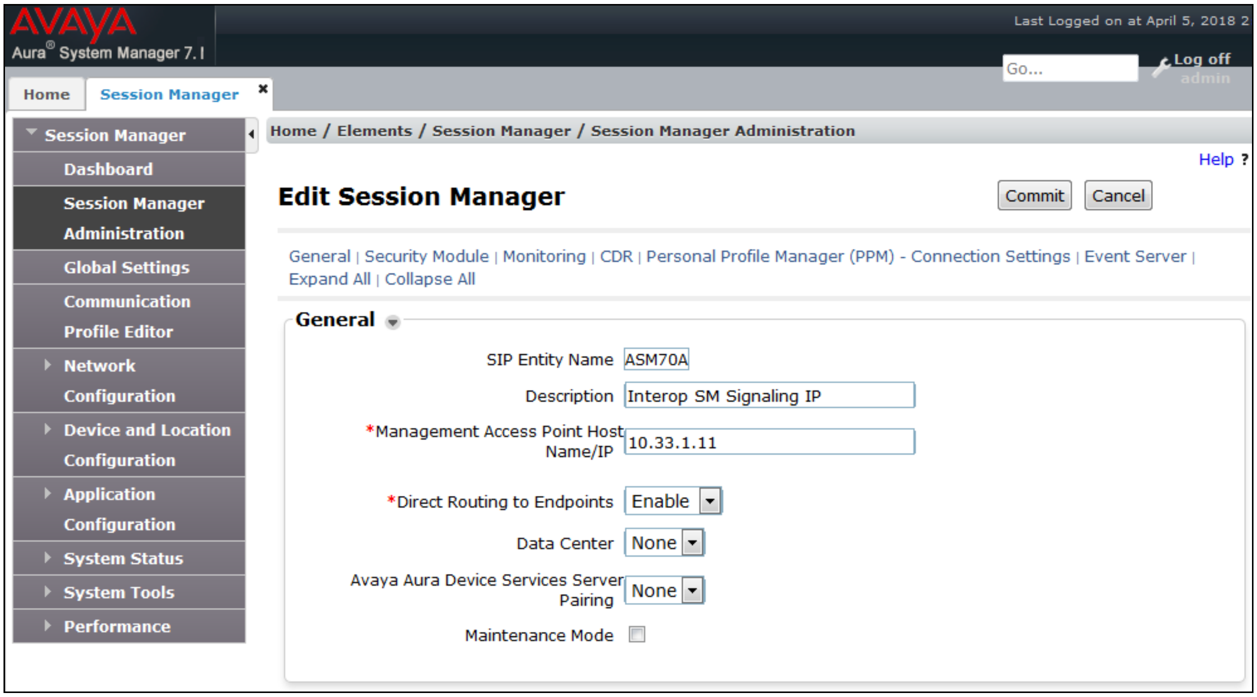
Session Manager Instances

2 Items

	Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
●	ASM70A	Normal	22	0	22	Interop SM Signaling IP
○	ASM70B	Normal	0	19	19	Secondary SM

Select : None

The **Edit Session Manager** is displayed in the right hand as shown in the picture below. Click on **CDR** link to jump to the CDR section.


AVAYA
Aura® System Manager 7.1
Last Logged on at April 5, 2018 2
Go...
Log off admin
Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Session Manager Administration
Help ?
Commit
Cancel
General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

Edit Session Manager

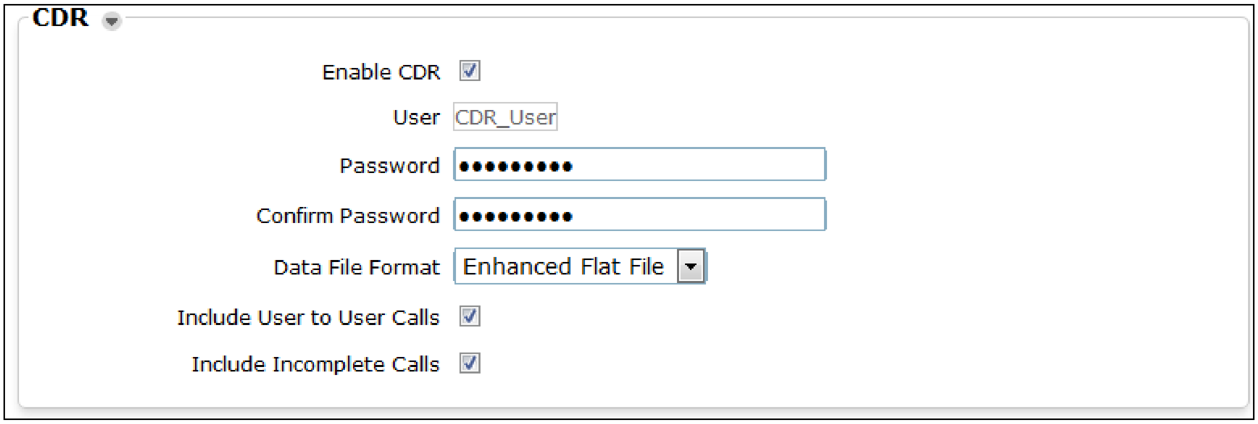
General

SIP Entity Name	ASM70A
Description	Interop SM Signaling IP
*Management Access Point Host Name/IP	10.33.1.11
*Direct Routing to Endpoints	Enable
Data Center	None
Avaya Aura Device Services Server Pairing	None
Maintenance Mode	□

In the CDR section, enter the following values.

Enable CDR	Select the checkbox to enable CDR
Password and **Confirm Password**	Enter a password for **CDR_User**
Data File Format	Select **Enhanced Flat File** from the drop down list
Include User to User Calls	Check the checkbox to include the user to user calls
Include Incomplete Calls	Check the checkbox to include the incomplete calls

Select **Commit** button to save the change.



CDR

Enable CDR	☑
User	CDR_User
Password	●●●●●●●●●
Confirm Password	●●●●●●●●●
Data File Format	Enhanced Flat File
Include User to User Calls	☑
Include Incomplete Calls	☑

10. Configure ServicePilot

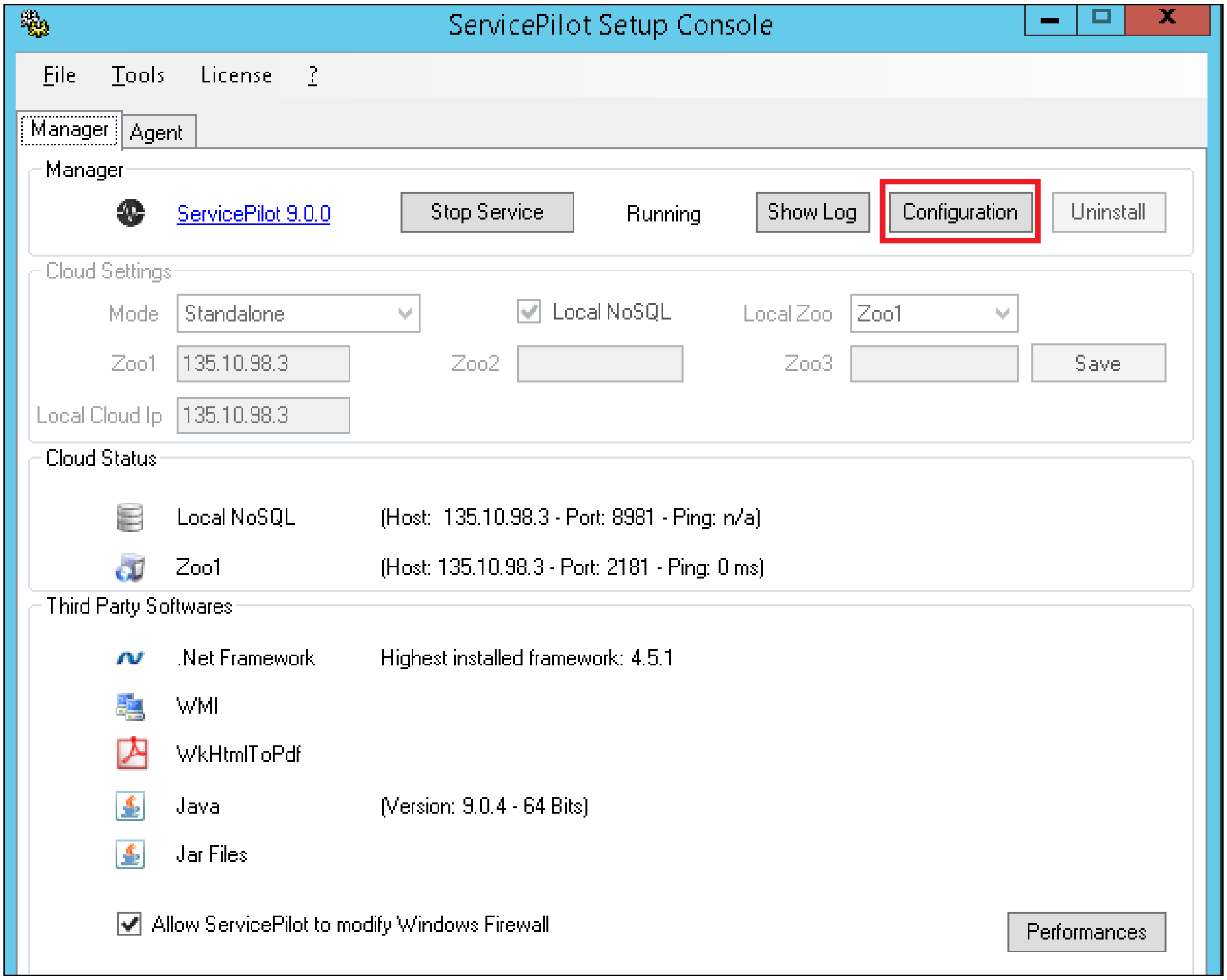
This section describes the configuration required for ServicePilot to interoperate with Communication Manager. It assumes that the application and all required software components have been installed and properly licensed.

Note: The installation and configuration of ServicePilot is carried out by ServicePilot or ServicePilot approved partner personnel and the following section only details a summary of the configuration used during compliance testing

10.1. Launch ServicePilot console

ServicePilot ISM is initially configured using the **Administration Console**. Launch **ServicePilot Setup Console** on the ServicePilot ISM server. When the **ServicePilot Setup Console** window opens, click on the **Configuration** button.

Note: The **ServicePilot ISM Administration Console** is located at **C:\Program Files (x86)\ServicePilot\ServicePilot ISM Enterprise\console.exe** and must be run as Administrator.



Mode: Standalone

☑ Local NoSQL

Local Zoo: Zoo1

Zoo1: 135.10.98.3

Zoo2:

Zoo3:

Local Cloud Ip: 135.10.98.3

Local NoSQL (Host: 135.10.98.3 - Port: 8981 - Ping: n/a)

Zoo1 (Host: 135.10.98.3 - Port: 2181 - Ping: 0 ms)

.Net Framework Highest installed framework: 4.5.1

WMI

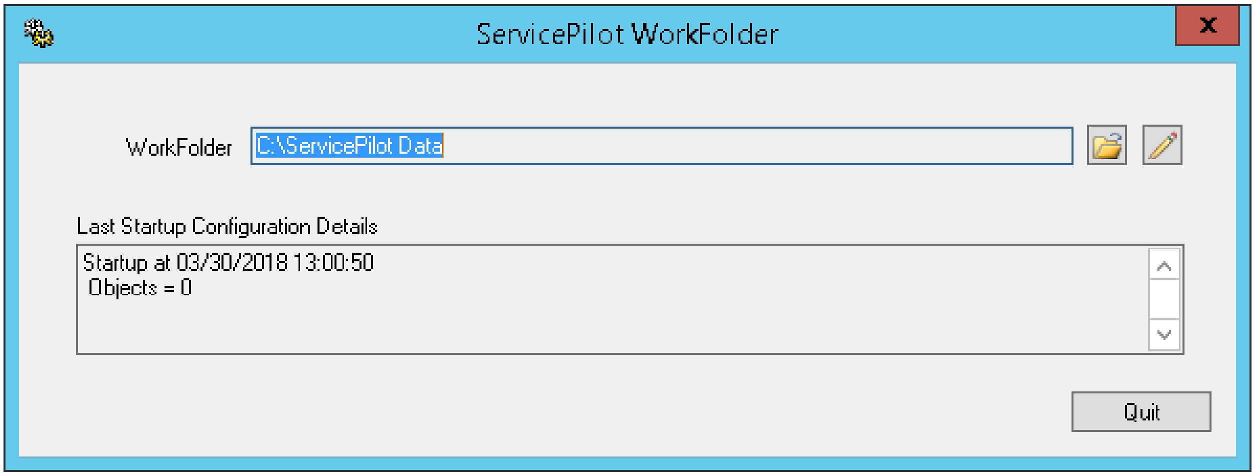
WkHtmlToPdf

Java (Version: 9.0.4 - 64 Bits)

Jar Files

☑ Allow ServicePilot to modify Windows Firewall

When the **ServicePilot WorkFolder** window opens, browser to a folder location on a data drive where configuration data will be stored (not shown). Click on the **Quit** button to continue.



ServicePilot WorkFolder

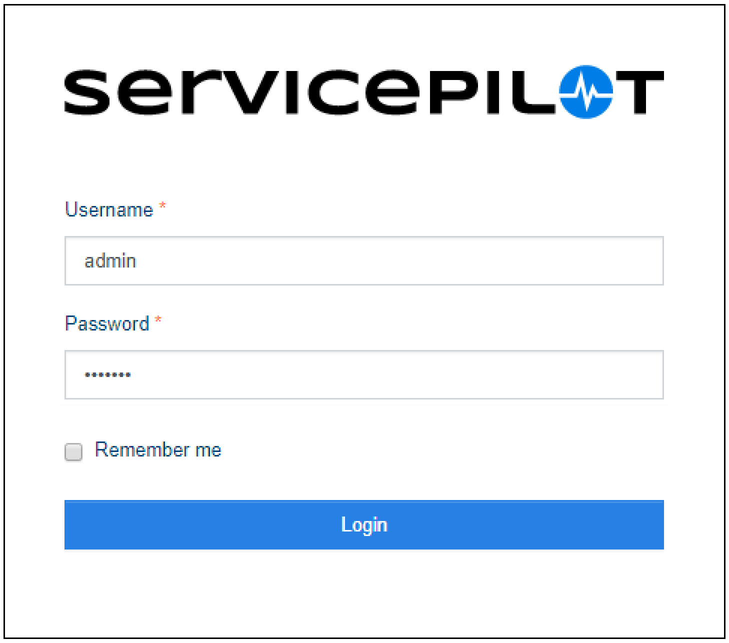
WorkFolder: C:\ServicePilot Data

Last Startup Configuration Details

```
Startup at 03/30/2018 13:00:50
 Objects = 0
```

10.2. Login to the ServicePilot web interface

When making changes to ServicePilot configuration, log in to the ServicePilot web interface using a username that has administrative privileges.



Username *: admin

Password *: •••••••

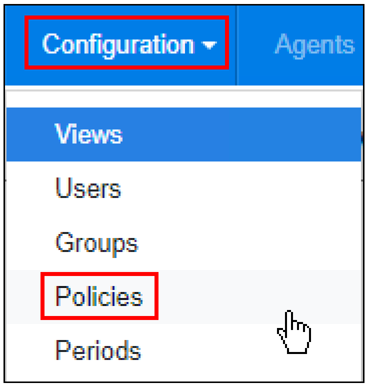
□ Remember me

Navigate to **Administration** by clicking on the ⚙ link (not shown).

10.3. Create SNMP credential profiles

ServicePilot requires SNMP credential profiles that match the SNMP credentials used by Avaya equipment to be polled. In this configuration, the Communication Manager and G450 Media Gateway have been configured with identical SNMP v2c credentials and the System Manager, Session Manager and Media Server have been configured with identical SNMP v3 credentials.

Select **Policies** from the **Configuration** Administration menu.

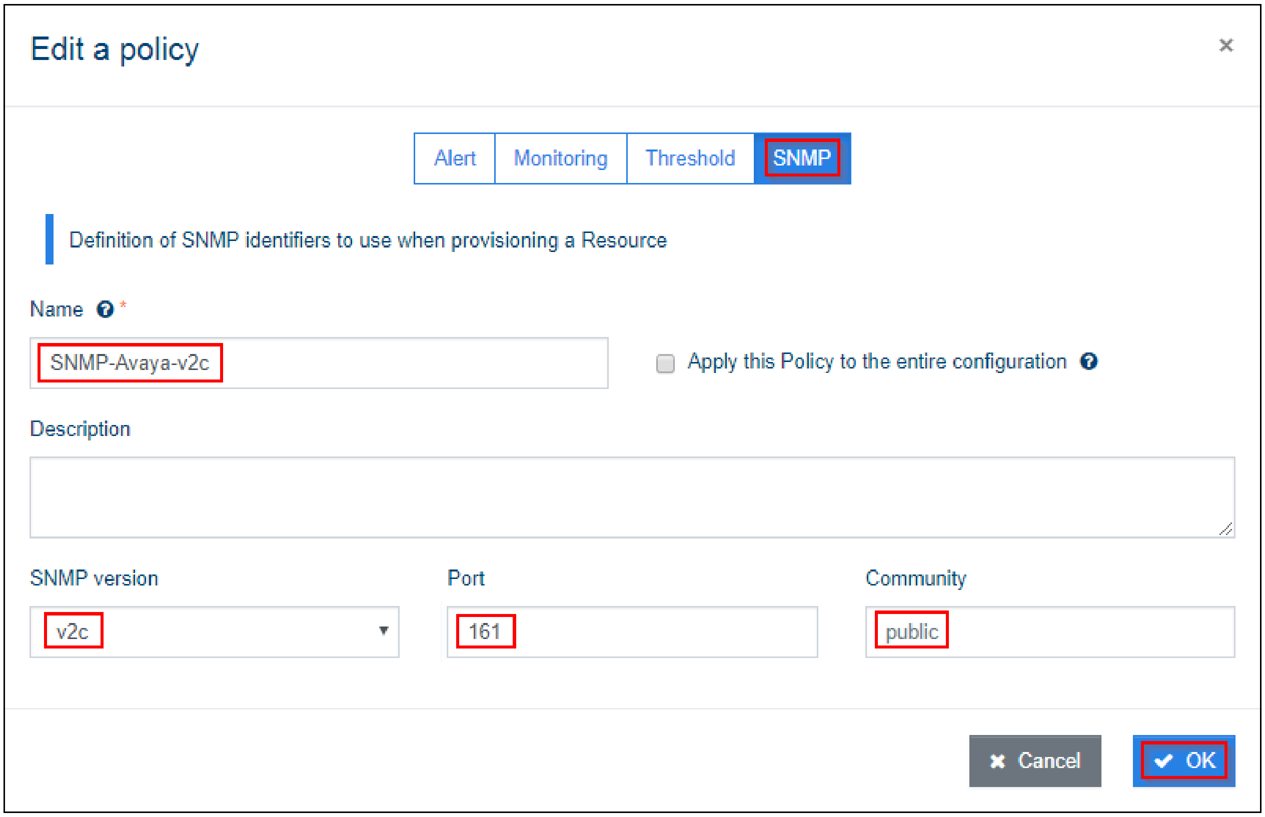


Start adding a new policy with the button.

Select the SNMP policy type and complete the form with the following details:

- **Name** Enter a policy name e.g., **SNMP-Avaya-v2c**
- **SNMP Version** Select **v2c** from the drop down list
- **Port** Enter the SNMP Agent listening port e.g., **161**
- **Community** Enter the community string as configured on the Avaya e.g., **public**

Click **OK** when done.



Edit a policy

Definition of SNMP identifiers to use when provisioning a Resource

Name * : SNMP-Avaya-v2c

□ Apply this Policy to the entire configuration

Description

SNMP version: v2c

Port: 161

Community: public

Click **Save** to add this new policy to the ServicePilot configuration.

Follow the same process to add SNMP v3 credentials.

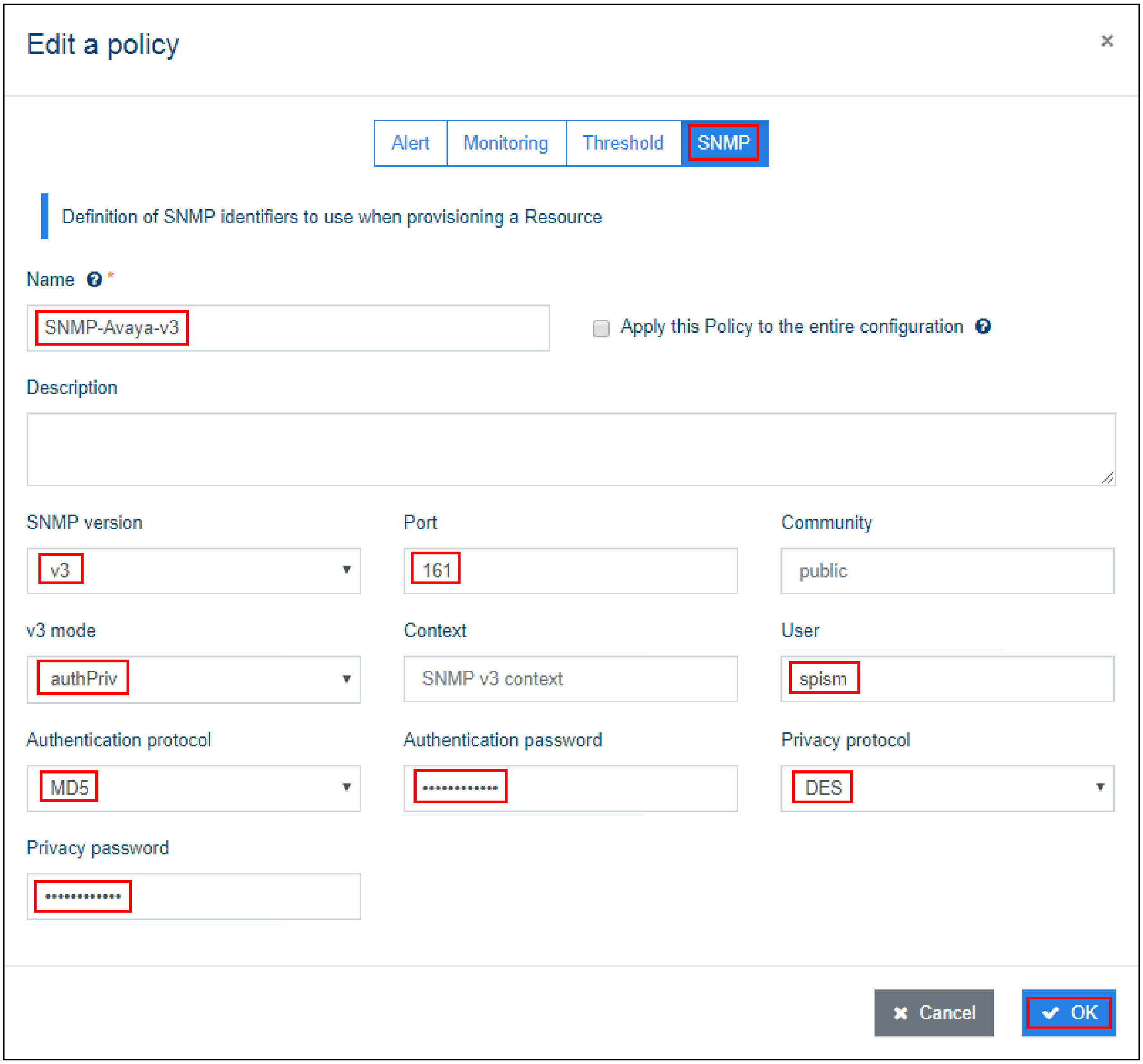
Start adding a new policy with the **+ Add a policy** button.

Select the SNMP policy type and complete the form with the following details:

- **Name** Enter a policy name e.g., **SNMP-Avaya-v3**
- **SNMP Version** Select **v3** from the drop down list
- **Port** Enter the SNMP Agent listening port e.g., **161**
- **v3mode** Select **authPriv** from the drop down list
- **User** Enter the user as set in Avaya configuration e.g., **spism**
- **Authentication protocol** Enter the authentication protocol as set in Avaya configuration e.g., **MD5**
- **Authentication password** Enter the authentication password as set in Avaya configuration
- **Privacy protocol** Enter the privacy protocol as set in Avaya configuration e.g., **DES**

- **Privacy password** Enter the privacy password as set in Avaya configuration

Click **OK** when done.



Edit a policy

Definition of SNMP identifiers to use when provisioning a Resource

Name *: SNMP-Avaya-v3

□ Apply this Policy to the entire configuration

Description:

SNMP version: v3

Port: 161

Community: public

v3 mode: authPriv

Context: SNMP v3 context

User: spism

Authentication protocol: MD5

Authentication password: ••••••••••••

Privacy protocol: DES

Privacy password: ••••••••••••

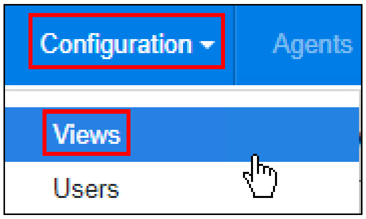
Click **Save** to add this new policy to the ServicePilot configuration.

10.4. Configure ServicePilot VoIP Agent

ServicePilot has a VoIP Agent that will process VoIP data from different sources. Basic configuration is required per ServicePilot VoIP Agent before monitoring particular VoIP components. Add one instance of each of the following two packages as described below:

- **voip-call-quality-by-zone-or-network** Configure network zones to categorize call data received
- **voip-call-quality-by-network-view** Provide view in which Avaya call quality will be stored

Select **Views** from the **Configuration** Administration menu.

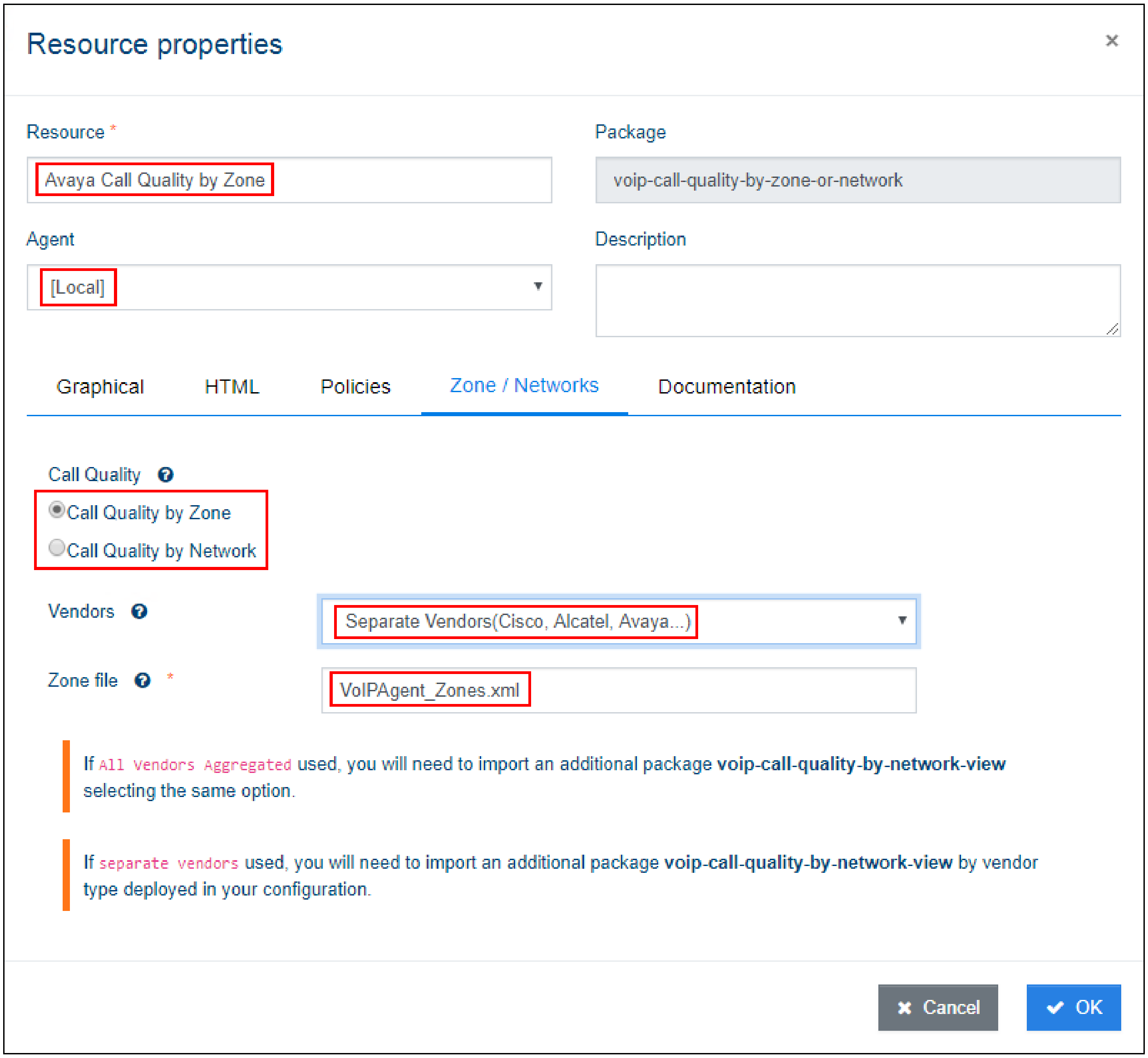


From the **Packages** list drag-and-drop the **voip-call-quality-by-zone-or-network** on to the **View editor**. A configuration dialog will open.

Complete the fields as shown:

- **Resource** Enter a unique resource name e.g., **Avaya Call Quality by Zone**
- **Agent** Select a ServicePilot Agent to act as VoIP Agent e.g., **[Local]**
- **Call Quality** Specify the way in which call quality statistics will be sub-divided e.g., **Call Quality by Zone**
- **Vendors** Specify if call quality will be merged or separated by vendor e.g., **SeparateVendors**
- **Zone file** Indicate the name of the zone XML file the Agent will use to define network zones

See the package **Documentation** tab for further details and example zone XML file along with instructions on where this file is to be placed. A zone XML file could be similarly provisioned to Avaya Network Region definitions.



Resource properties

Resource *: Avaya Call Quality by Zone

Package: voip-call-quality-by-zone-or-network

Agent: [Local]

Description:

Call Quality

● Call Quality by Zone

○ Call Quality by Network

Vendors: Separate Vendors(Cisco, Alcatel, Avaya...)

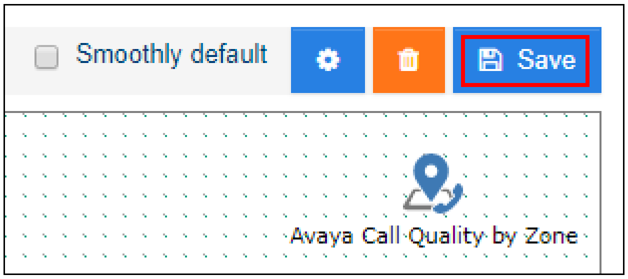
Zone file *: VoIPAgent_Zones.xml

If `All vendors Aggregated` used, you will need to import an additional package **voip-call-quality-by-network-view** selecting the same option.

If `separate vendors` used, you will need to import an additional package **voip-call-quality-by-network-view** by vendor type deployed in your configuration.

Click **OK** when done.

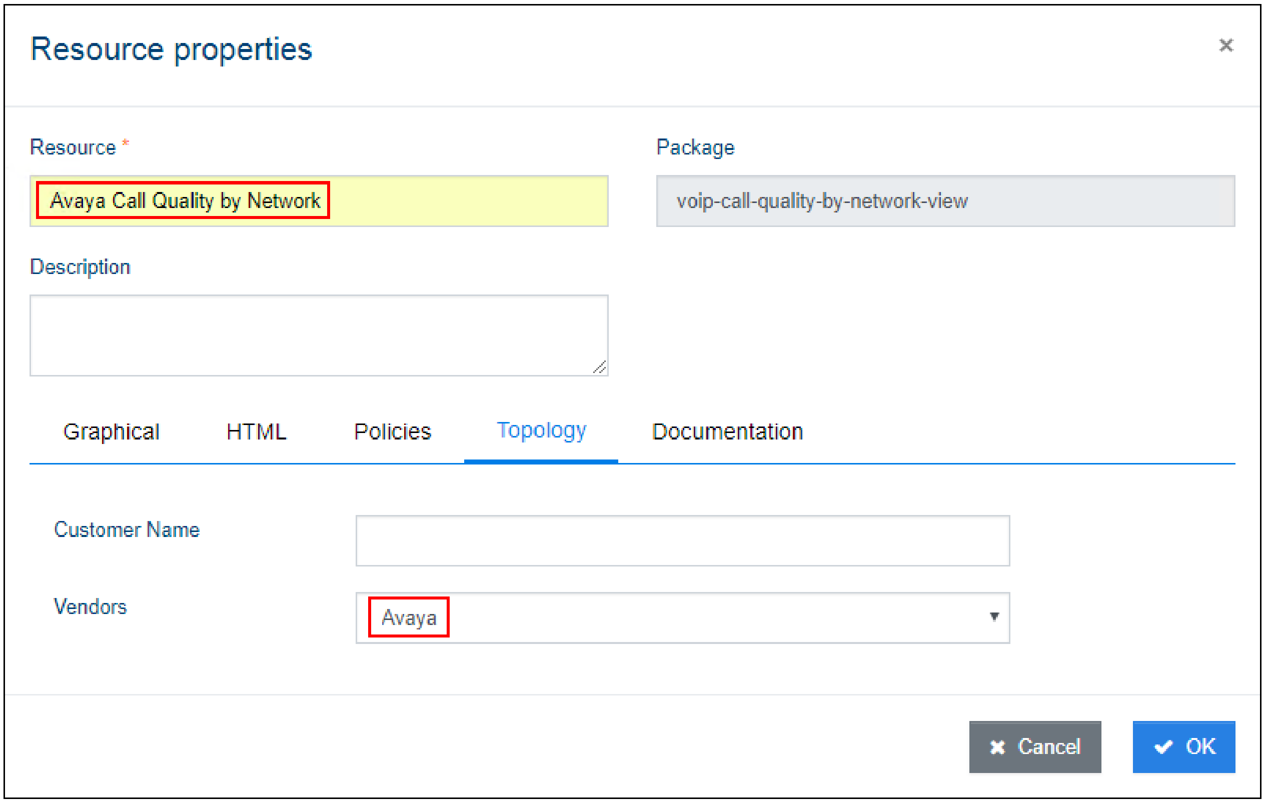
Click **Save** to add this new resource to the ServicePilot configuration.



From the **Packages** list drag-and-drop the **voip-call-quality-by-network-view** on to the **View editor**. A configuration dialog will open.

Complete the fields as shown:

- **Resource** Enter a unique resource name e.g., **Avaya Call Quality by Network**
- **Vendors** Select **Avaya** from the drop down list



Resource properties

Resource * Avaya Call Quality by Network

Package voip-call-quality-by-network-view

Description

Customer Name

Vendors Avaya

Click **OK** when done.

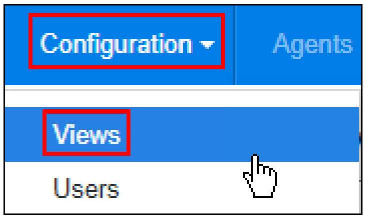
Click **Save** to add this new resource to the ServicePilot configuration.

10.5. Configure Avaya RTCP receipt

ServicePilot presents Avaya media quality when it receives RTCP from Avaya media endpoints. A ServicePilot VoIP Agent needs to be configured to expect these packets using of the following package as described below:

- **voip-avaya-rtcp-media-quality** Receive Avaya media quality RTCP packets

Select **Views** from the **Configuration** Administration menu.

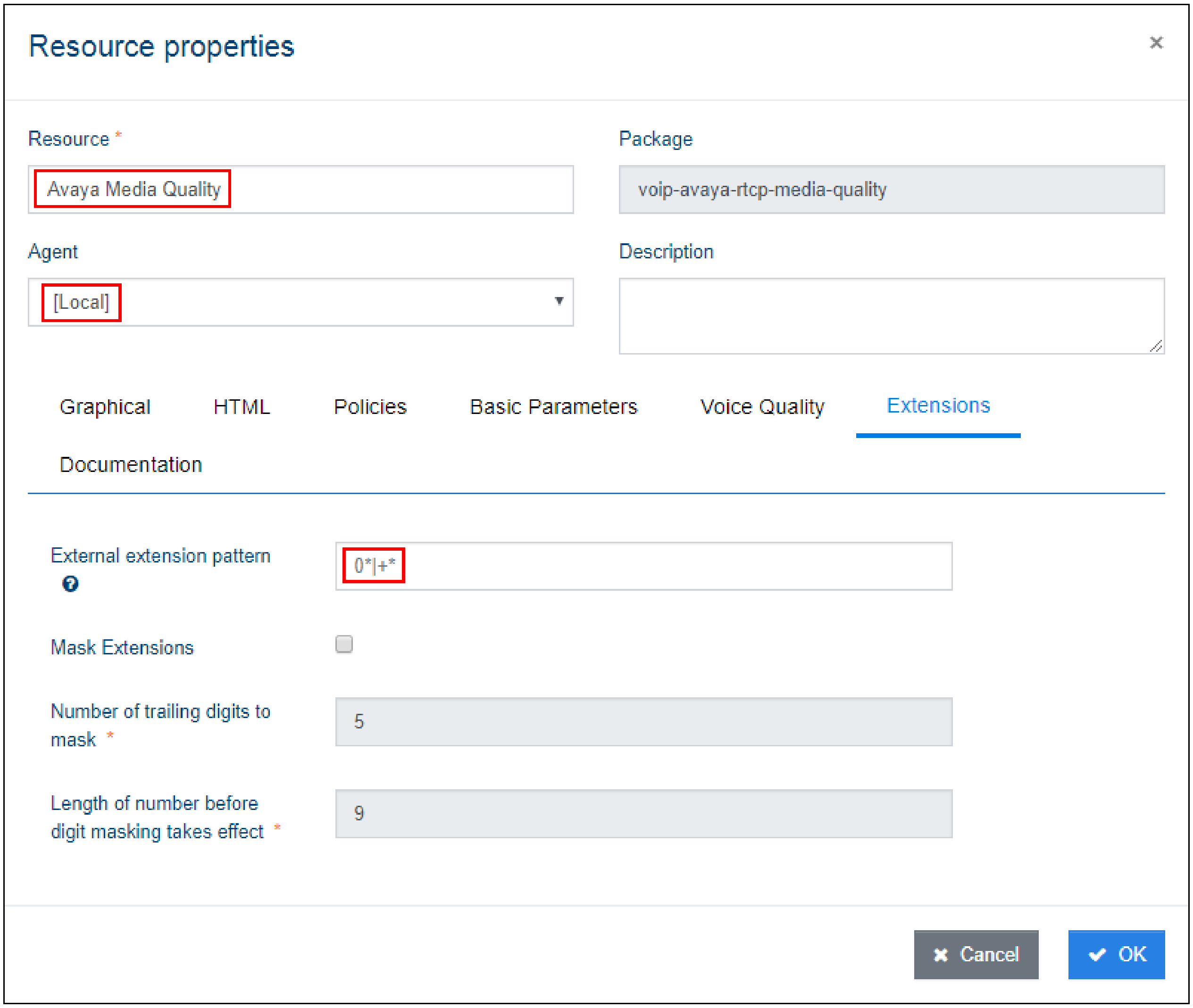


From the **Packages** list drag-and-drop the **voip-avaya-rtcp-media-quality** on to the **View editor**. A configuration dialog will open.

Complete the fields as needed:

- **Resource** Enter a unique resource name e.g., **Avaya Call Quality by Zone**
- **Agent** Select a ServicePilot Agent to act as VoIP Agent e.g., **[Local]**
- **External extension pattern** Set a pattern to differentiate between internal phone numbers and numbers outside the system e.g., **0*|+***

See the package **Documentation** tab for further details.



Resource properties

Resource * Avaya Media Quality

Package voip-avaya-rtcp-media-quality

Agent [Local]

Description

External extension pattern 0*|+*

Mask Extensions □

Number of trailing digits to mask * 5

Length of number before digit masking takes effect * 9

Click **OK** when done.

Click **Save** to add this new resource to the ServicePilot configuration.

10.6. Configure other Avaya resources

ServicePilot can be configured to monitor specific Avaya elements based on built-in package templates. Depending on the equipment to be monitored, select the template required:

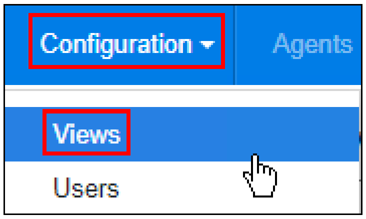
- **voip-avaya-aes** Avaya Application Enablement Services
- **voip-avaya-communication-manager** Avaya Communication manager and associated ESS
- **voip-avaya-gateway** Avaya Media Gateway
- **voip-avaya-session-manager** Avaya Session Manager

Other Avaya equipment might be monitored using generic ServicePilot packages. For example:

server-linux-snmp	Linux Server
network-ping	ICMP Ping an IP address
application-webcheck	HTTP(S) web page check

Follow this procedure for each element to be monitored:

Select **Views** from the **Configuration** Administration menu.

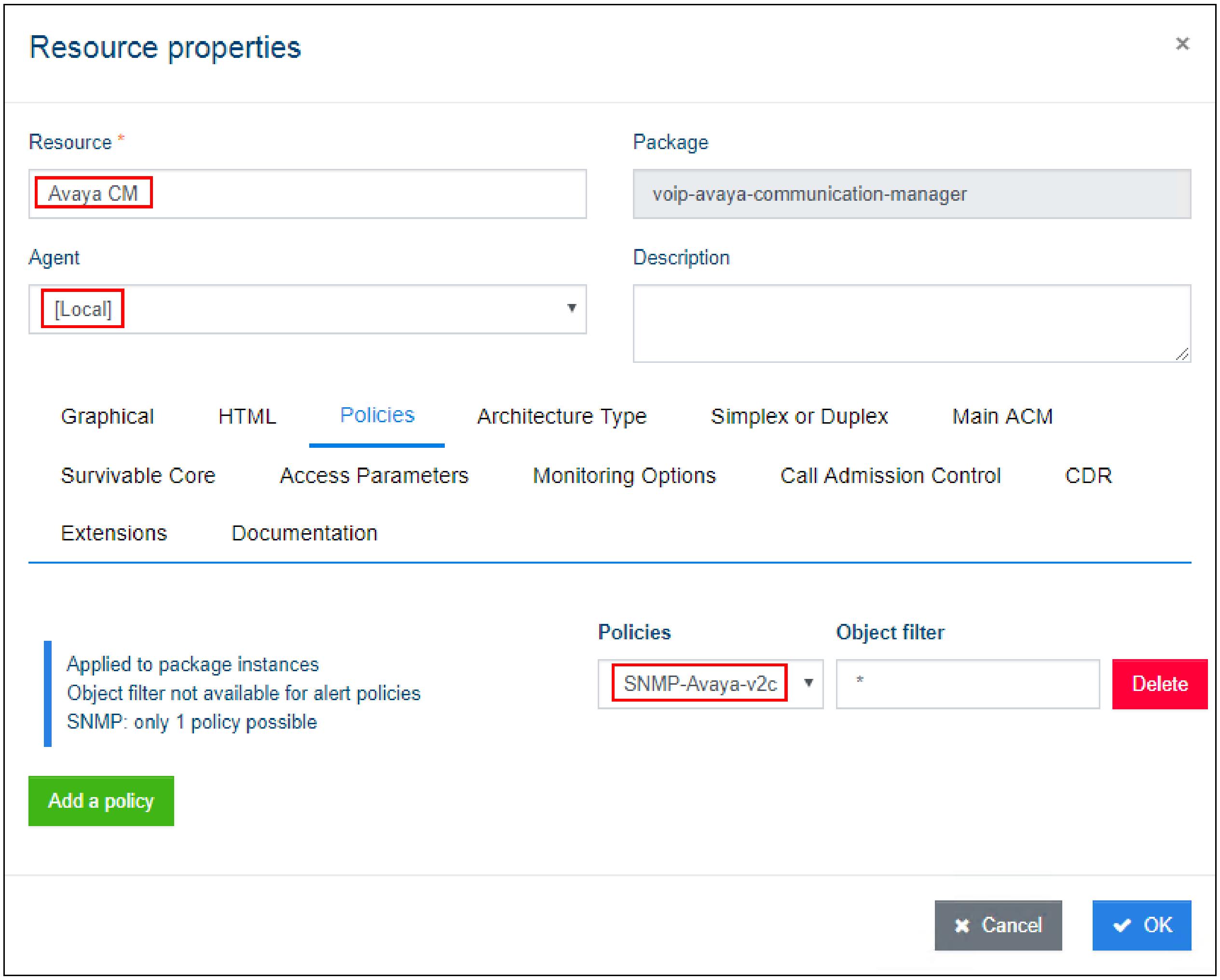


From the **Packages** list drag-and-drop the required package type depending on the equipment to be monitored on to the **View editor**. A configuration dialog will open.

Complete the fields as shown:

- **Resource** Enter a unique resource name e.g., **Avaya CM**
- **Agent** (If required) Select a ServicePilot Agent to act as VoIP Agent e.g., **[Local]**
- **Policies** Add a policy to specify the correct SNMP credentials matching the SNMP credentials set on the equipment to be monitored e.g., **SNMP-Avaya-v2c**

See the package **Documentation** tab for further details. Each type of package has different parameters depending on the equipment to be monitored.



Resource properties

Resource *: Avaya CM

Package: voip-avaya-communication-manager

Agent: [Local]

Description:

Applied to package instances
Object filter not available for alert policies
SNMP: only 1 policy possible

Policies	Object filter
SNMP-Avaya-v2c	*

Click **OK** when done.

Click **Save** to add this new resource to the ServicePilot configuration.

11. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya and ServicePilot solution.

11.1. Verify Communication Manager

Verify ServicePilot ISM has established two concurrent connections to the SAT by using the **status logins** command.

```
status logins

                    COMMUNICATION MANAGER LOGIN INFORMATION

Login     Profile   User's Address       Active Command              Session

 service     18                                                          1
                     10.10.98.3
 service     18                                                          3
                     10.10.98.3
 acpsnmp     17                                                          4
                     127.0.0.1
*admin       18                        stat logins                       5
                     10.10.98.86
```

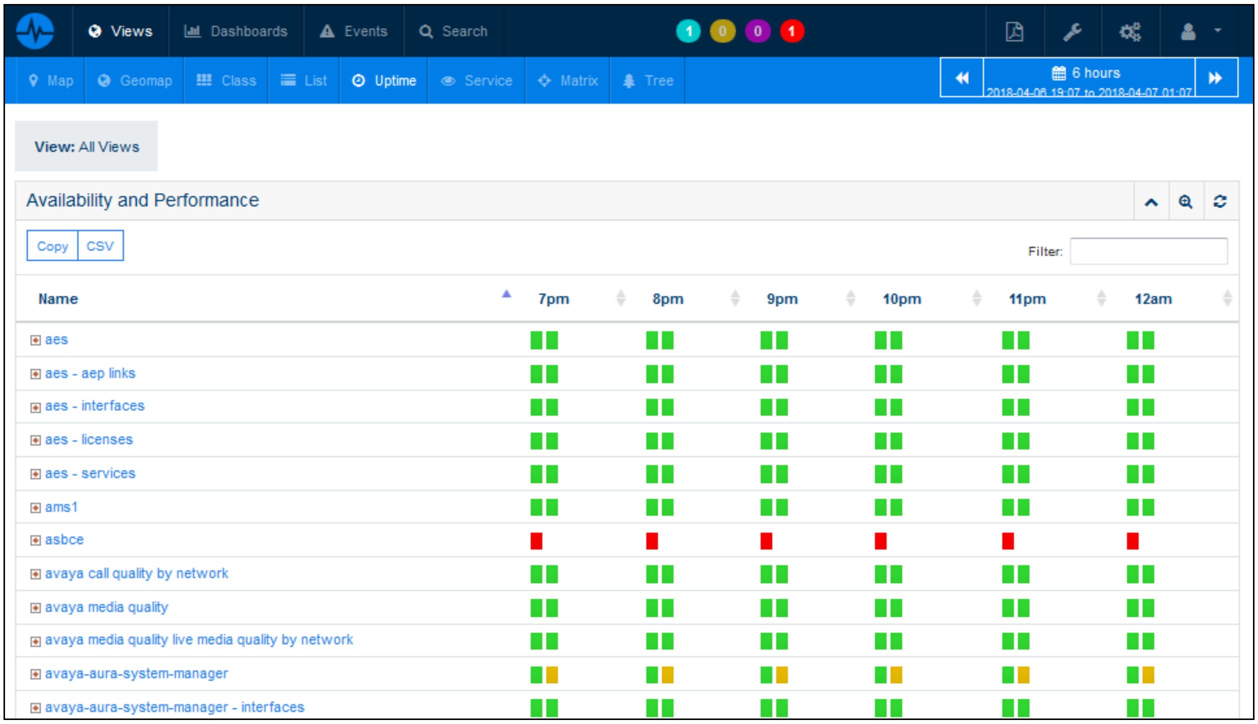
11.2. Verify Avaya Aura® Communication Manager CDR Link

Use the **status cdr-link** command to verify that the **Link State** is **up** and the **Reason Code** is **OK**.

```
status cdr-link
                                CDR LINK STATUS
                   Primary                        Secondary

       Link State: up                             up

      Date & Time: 2018/03/21 23:28:59            2018/03/30 13:01:42
  Forward Seq. No: 19                             0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                           0.00
      Reason Code: OK                             OK
```

11.3. Verify ServicePilot

On the ServicePilot web interface it is possible to verify the correct monitoring of Avaya components, it is recommended to look at the view Service level Report. Go to **Reports → View reports → Service level**. The report presented indicates the state of the all views by view type. It is expected that the Availability of all components is green as shown by the top row of coloured indicators per view type over time. The Performance of components should also show green if the system is idle. Other performance indicator colours show usage thresholds being passed or equipment under maintenance. If Availability statues show red then equipment is unreachable for monitoring purposes.

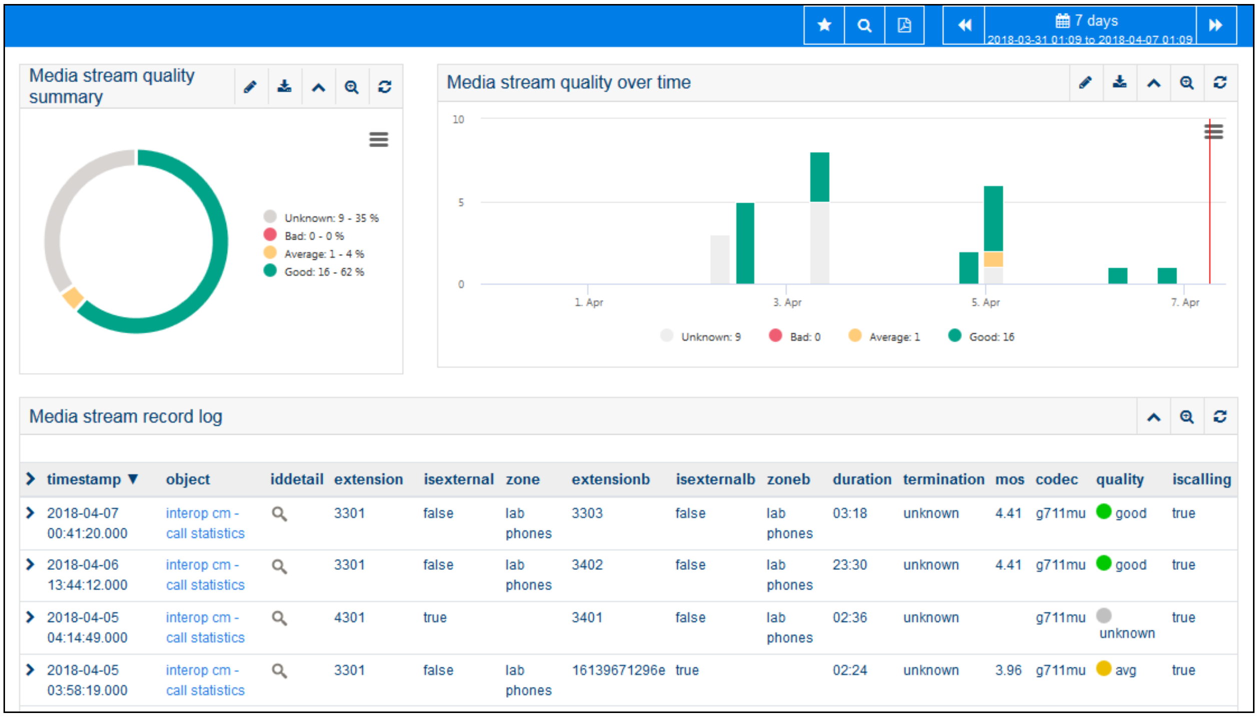


View: All Views

Availability and Performance

Name	7pm	8pm	9pm	10pm	11pm	12am
aes	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
aes - aep links	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
aes - interfaces	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
aes - licenses	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
aes - services	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
ams1	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
asbce	🟥	🟥	🟥	🟥	🟥	🟥
avaya call quality by network	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
avaya media quality	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
avaya media quality live media quality by network	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
avaya-aura-system-manager	🟩🟨	🟩🟨	🟩🟨	🟩🟨	🟩🟨	🟩🟨
avaya-aura-system-manager - interfaces	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩

In addition to ServicePilot monitoring views, verify CDR and call quality capture is operating correctly, by opening the Query VoIP event details. Go to **Query → VoIP** to show all received VoIP events. Selecting a call server call count will open a pop-up window showing call event details received. If call quality details are also being received then a magnifying glass icon indicates a link to call quality details for the call presented.



timestamp ▼	object	iddetail	extension	isexternal	zone	extensionb	isexternalb	zoneb	duration	termination	mos	codec	quality	iscalling
2018-04-07 00:41:20.000	interop cm - call statistics	🔍	3301	false	lab phones	3303	false	lab phones	03:18	unknown	4.41	g711mu	● good	true
2018-04-06 13:44:12.000	interop cm - call statistics	🔍	3301	false	lab phones	3402	false	lab phones	23:30	unknown	4.41	g711mu	● good	true
2018-04-05 04:14:49.000	interop cm - call statistics	🔍	4301	true		3401	false	lab phones	02:36	unknown		g711mu	● unknown	true
2018-04-05 03:58:19.000	interop cm - call statistics	🔍	3301	false	lab phones	16139671296e	true		02:24	unknown	3.96	g711mu	● avg	true

12. Conclusion

These Application Notes describe the steps required to configure ServicePilot to interoperate with Avaya Aura® Communication Manager, G450 Media Gateway, Avaya Aura®cSession Manager, Avaya Aura® System Manager and Avaya Aura® Application Enablement Services. All test cases have passed and met the objectives outlined in **Section 2.1**.

13. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from http://support.avaya.com or from your Avaya representative.

[1] *Administering Avaya Aura® Communication Manager (Release 7.1.2, Issue 5, February 2018)*

[2] *Administering Network Connectivity on Avaya Aura® Communication Manager (Release 7.1.1, Issue 2, August 2017), 555-233-504*

[3] *Avaya Aura® Communication Manager Feature Description and Implementation (Release 7.1.2, Issue 4, January 2018)*

[4] *Avaya Aura® Communication Manager Screen Reference (Release 7.1.1, Issue 2, August 2017), 03-602878*

[5] *Avaya Aura® Communication Manager SNMP Administration and Reference Guide (Release 7.1, Issue 1, May 2017), 03-602013*

[6] *Administering Avaya Aura® Session Manager (Release 7.1.2, Issue 3, December 2017)*

[7] *Implementing and Administering Avaya Aura® Media Server (Release 7.8, Issue 6, December 2017)*

[8] *Administering Avaya Session Border Controller for Enterprise (Release 7.2.1, Issue 7, January 2018)*

[9] *Deploying Avaya Aura® Session Manager (08 Dec 2017)*

[10] *Administering Avaya G450 Branch Gateway (Release 7.1.2, Issue 2, December 2017)*

[11] *Administering Avaya Aura® Session Manager (Release 7.1.2, Issue 3, December 2017)*

[12] *Administering and Maintaining Avaya Aura® Application Enablement Services (Release 7.1.2, Issue 4, December 2017)*

[13] *Administering Avaya Aura® System Manager for Release 7.1.2 (Release 7.1.2, Issue 10, January 2018)*

ServicePilot documentation can be obtained directly from the ServicePilot website http://www.servicepilot.com and ServicePilot help videos: https://www.servicepilot.com/en/video/

©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.