Avaya Solution & Interoperability Test Lab

Application Notes for ServicePilot ISM 8.5 with Avaya Aura® Communication Manager 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring ServicePilot ISM 8.5 to interoperate with Avaya Aura® Communication Manager 6.3.

ServicePilot ISM is a performance monitoring solution for multi-vendor infrastructure and unified communications. ServicePilot ISM 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, ServicePilot ISM 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.

ServicePilot ISM 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 ISM 8.5 with Avaya Aura® Communication Manager 6.3, Avaya G430 Media Gateway, Avaya Aura® Session Manager 6.3, Avaya Aura® System Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. ServicePilot ISM provides enterprises and Managed Service Providers with the following capabilities:

- Monitoring
- Troubleshooting
- Reporting

ServicePilot ISM uses four methods to monitor a Communication Manager system.

- System Access Terminal (SAT) – ServicePilot ISM 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 ISM 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 ISM 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 ISM 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 ISM 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 as a substitute for 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.

2.1. Interoperability Compliance Testing

For feature testing, ServicePilot ISM web interface was used to view the configurations of Communication Manager, G430 Media Gateway, Session Manager 6, 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 H323, 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

Tests were performed to verify interoperability of ServicePilot ISM to interoperate with Communication Manager, G430 Media Gateway, Session Manager, System Manager and Application Enablement Services. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

For technical support on ServicePilot ISM, 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 ISM interoperability with Communication Manager, G430 Media Gateway, Session Manager, System Manager and Application Enablement Services. ServicePilot ISM 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 ISM also monitors RTCP. A variety 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.

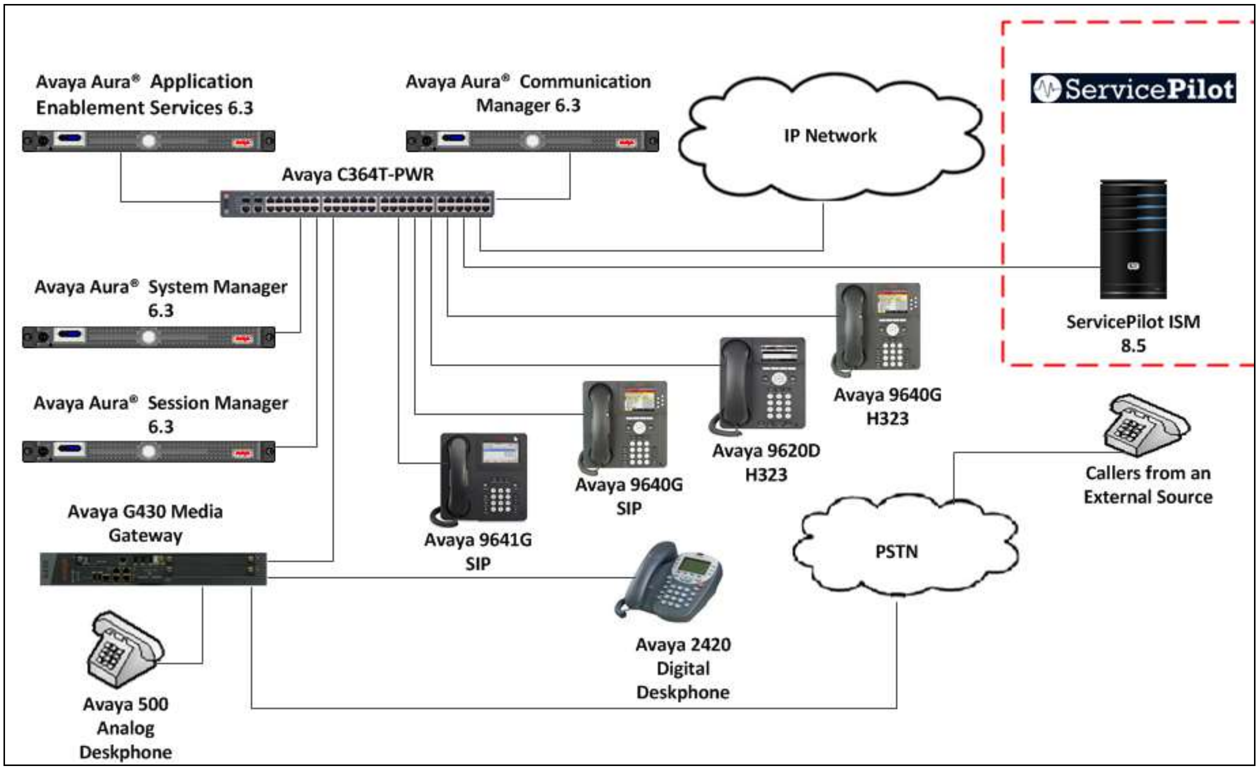

Avaya Aura® Application Enablement Services 6.3
Avaya Aura® Communication Manager 6.3
IP Network
ServicePilot
Avaya C364T-PWR
Avaya Aura® System Manager 6.3
ServicePilot ISM 8.5
Avaya 9640G H323
Avaya Aura® Session Manager 6.3
Avaya 9620D H323
Callers from an External Source
Avaya 9640G SIP
Avaya G430 Media Gateway
Avaya 9641G SIP
PSTN
Avaya 2420 Digital Deskphone
Avaya 500 Analog Deskphone

Figure 1: Test Configuration for Avaya and ServicePilot solution

4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on VMware	R6.3 Build R016x.03.0.124.0 S/W update 03.0.124.0-21591
Avaya Aura® Session Manager running on VMware	R6.3.11.0.631103
Avaya Aura® System Manager running on VMware	R6.3.11 Build No. 6.3.0.8.5682-6.3.8.4711 S/W update 6.3.11.8.2871
Avaya Aura® Application Enablement Services running on VMware	R6.3.01.212-0 Patch 1
Avaya G430 Media Gateway Module MM710 (DSP MP20) Avaya Media Gateway DSP module	Version 36.7.0/1 Version HW04 FW021 MP20 FW 132
Avaya Telephones phones 9640G (H.323) 9620D (H.323) 9640G (SIP) 9641G (SIP) Avaya 2420 Digital phone	 3.2.2A 3.1.1S SIP 96xx 2.6.13.1 S96x1 6.2.2r17.V4r70 Rel 6.0, FWV 6
Avaya Analog Phones	-
ServicePilot Equipment/Software	Release/Version
ServicePilot ISM running on a Dell PowerEdge R610 with Windows 2008 R2 (64 Bit)	8.5.0.2015_02_04
Microsoft .Net Framework	Version 4.5.2
Java	Version 8 Update 31

5. Configure Avaya solution

The configuration of the Avaya environment is quite complex for this solution and requires configuration changes to the following Avaya equipment:

- Avaya Aura® Communication Manager
- Avaya G430 Media Gateway
- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Application Enablement Services

An outline of the configuration of each piece of equipment will be detailed in a separate Section. For more comprehensive information relating to the configuration required for this solution please see the relevant documentation in **Section 14**.

Note: The configuration of network (including required ports) and firewalls settings are beyond the scope of these Application Notes. It is also recommended that Network Time Protocol (NTP) is configured for this solution, and this is also beyond the scope of these Application Notes.

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 necessary additional 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 14**. 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 ISM does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the ServicePilot ISM 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.

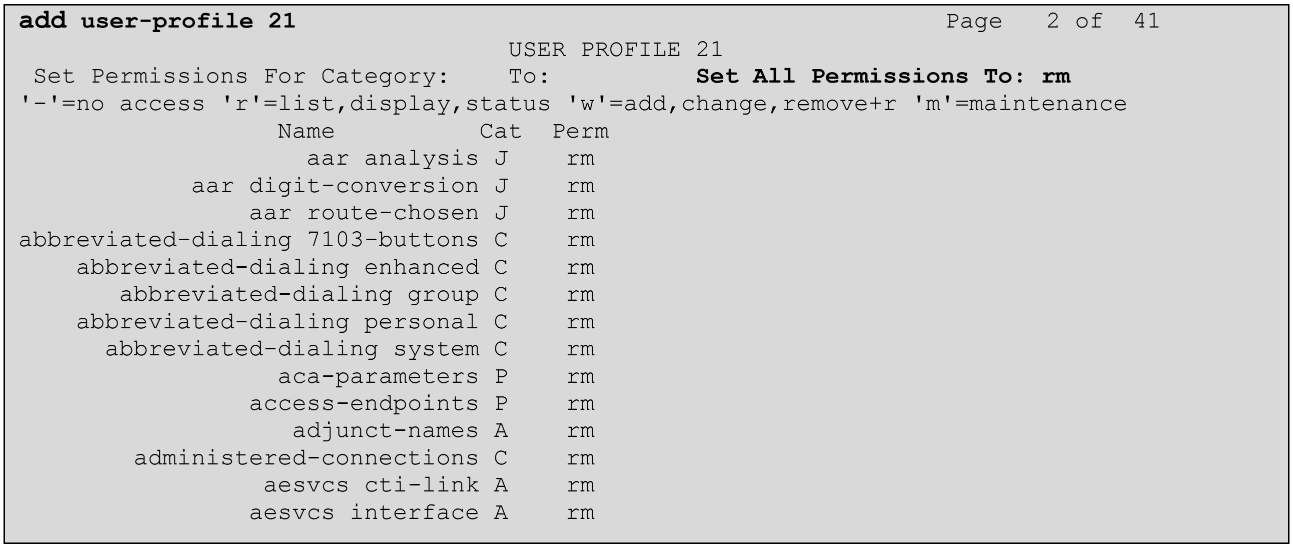
```
add user-profile 21                                          Page   1 of  41
                                USER PROFILE 23

User Profile Name: SPISM

       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
```

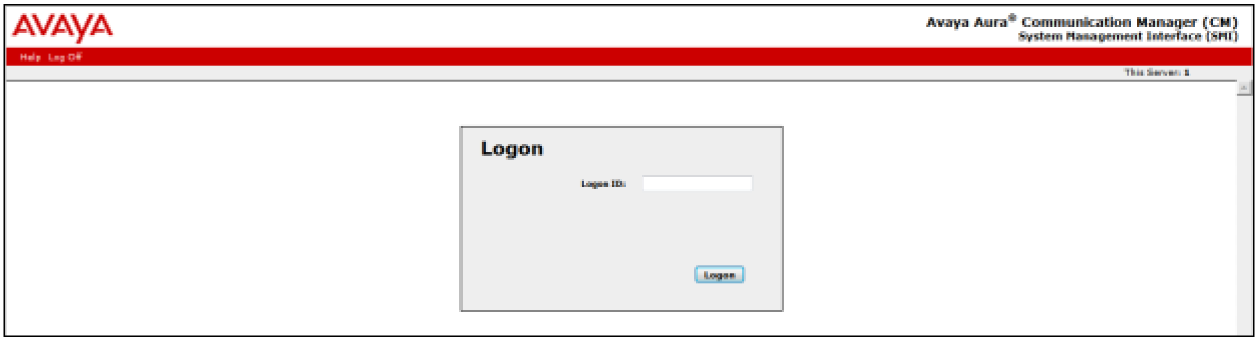
On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the field **Set All Permissions To**. Submit the form to create the user profile.



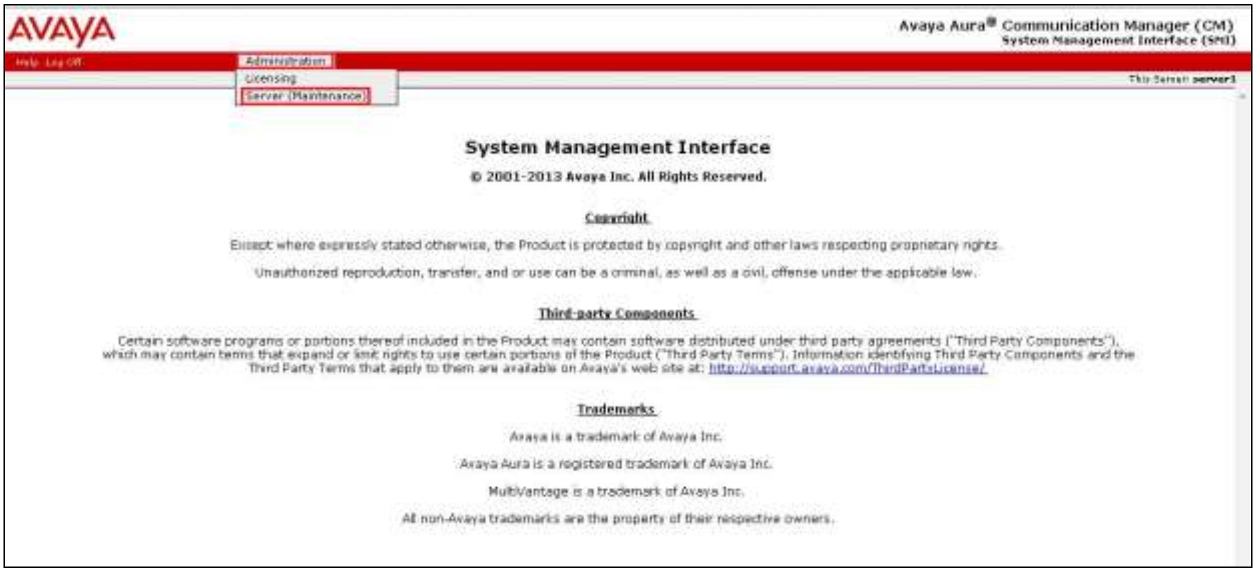
```
add user-profile 21                                             Page   2 of  41
                                  USER PROFILE 21
 Set Permissions For Category:    To:          Set All Permissions To: rm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                    aar analysis J    rm
            aar digit-conversion J    rm
                aar route-chosen J    rm
abbreviated-dialing 7103-buttons C    rm
    abbreviated-dialing enhanced C    rm
       abbreviated-dialing group C    rm
    abbreviated-dialing personal C    rm
      abbreviated-dialing system C    rm
                  aca-parameters P    rm
                access-endpoints P    rm
                   adjunct-names A    rm
        administered-connections C    rm
                 aesvcs cti-link A    rm
                aesvcs interface A    rm
```

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
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
This Server: 1
Logon
Logon ID:
Logon

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



System Management Interface

© 2001-2013 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.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

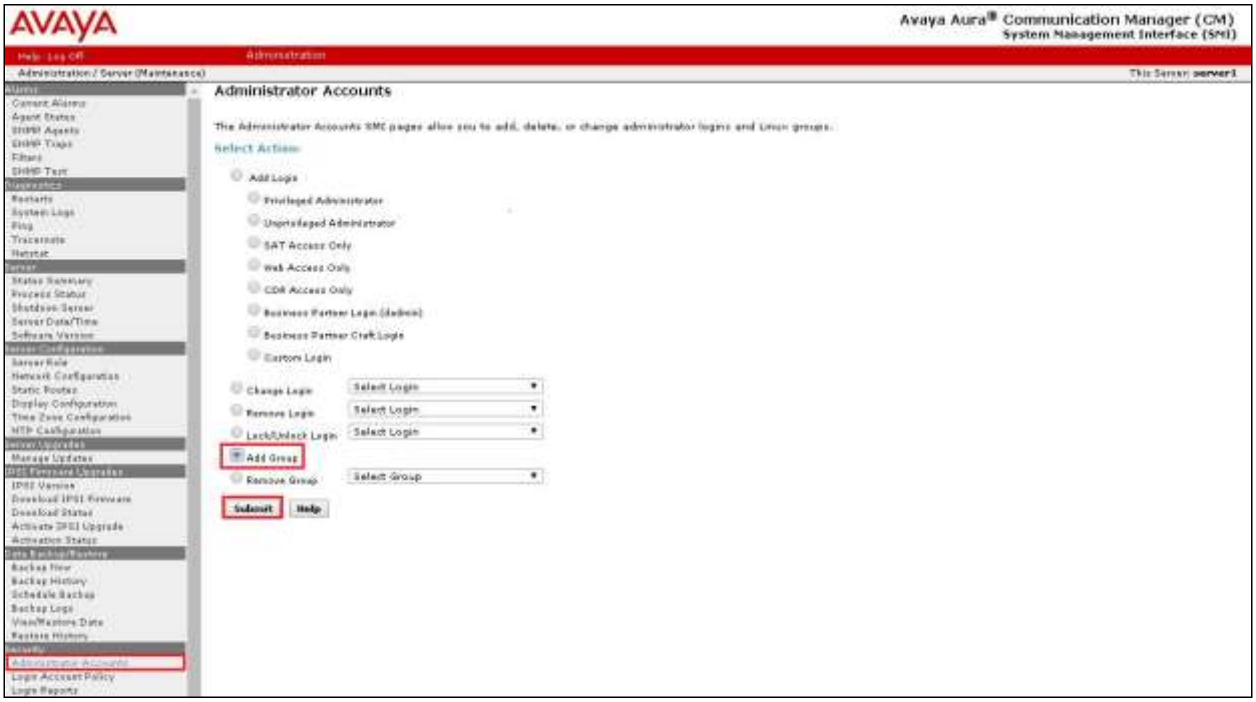
Avaya is a trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

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

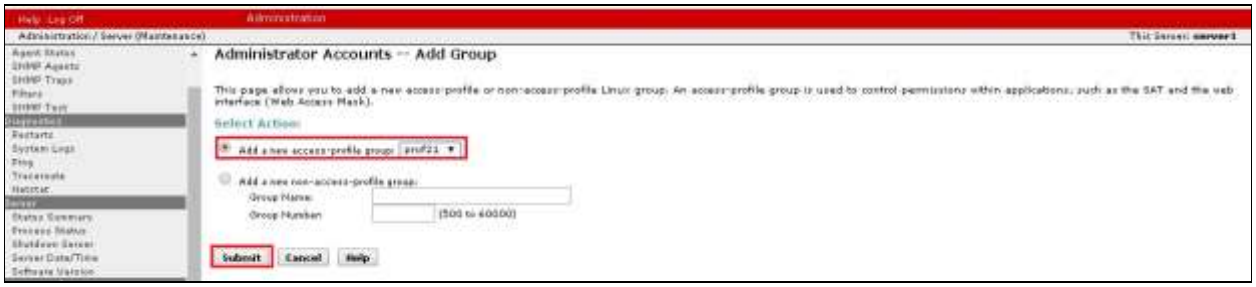
○ Lock/Unlock Login — Select Login ▾

● Add Group

○ Remove Group — Select Group ▾

Submit | Help

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.



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:

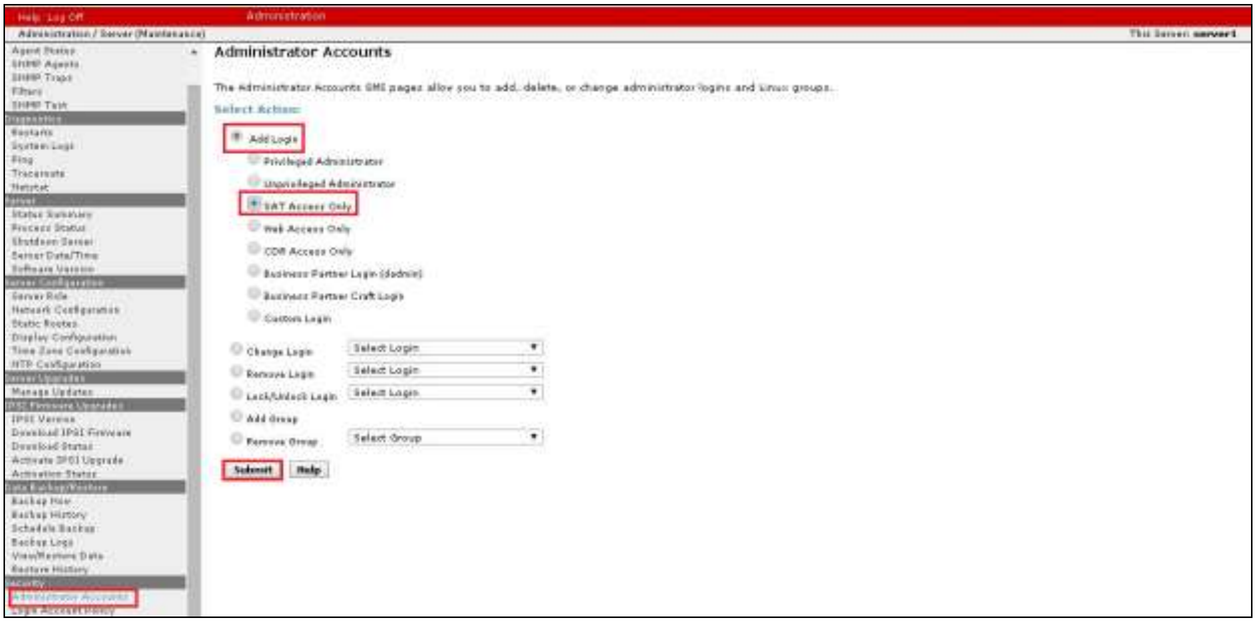
● Add a new access-profile group: prof21 ▾

○ Add a new non-access-profile group:
- Group Name:
- Group Number: (500 to 60000)

Submit | Cancel | Help

6.3. Configure Login

Create a login account for ServicePilot ISM 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:

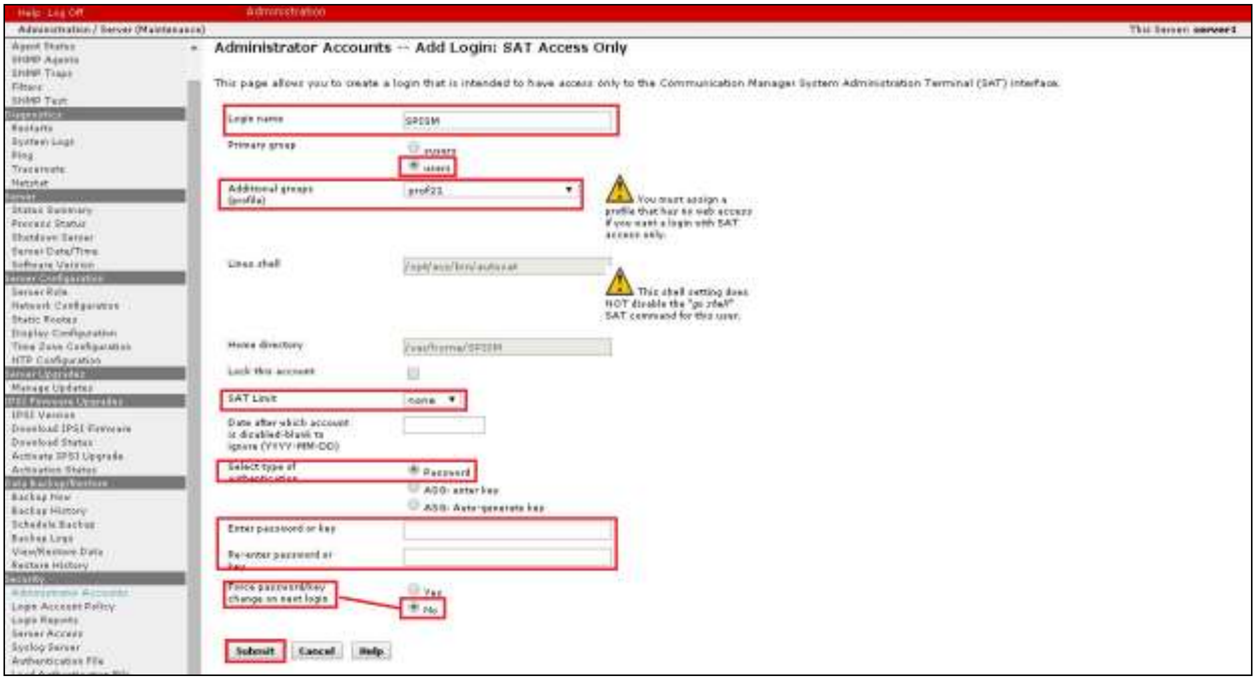
● Add Login
- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ● SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ 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 **users** 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
- **Select type of authentication** Click on the **Password** radio button
- **Enter password or key** Enter a password (used by ServicePilot in **Section 11.3**)
- **Re-enter password or key** Re-enter the password
- **Force password/Key change on next login** Click on the **No** radio button

Click **Submit** 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.

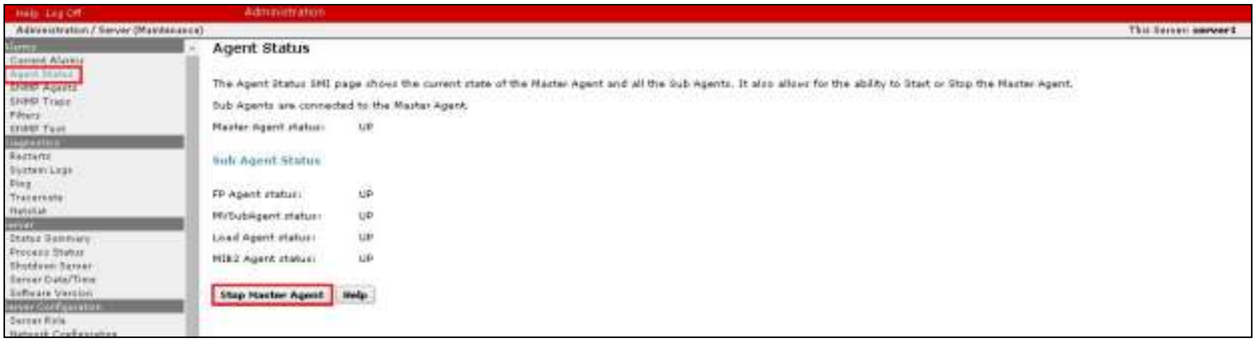
Login name	SPISM
Primary group	○ susers ● users
Additional groups (profile)	prof21 ▼
Linux shell	/opt/ecs/bin/autosat
Home directory	/var/home/SPISM
Lock this account	□
SAT Limit	none ▼
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Select type of authentication	● Password ○ ASG: enter key ○ ASG: Auto-generate key
Enter password or key	
Re-enter password or key	
Force password/key change on next login	○ Yes ● No

You must assign a profile that has no web access if you want a login with SAT access only.

This shell setting does NOT disable the "go shell" SAT command for this user.

6.4. Configure SNMP on Avaya Aura® 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.

Sub Agents are connected to the Master Agent.

Master Agent status: UP

Sub Agent Status

FP Agent status: UP

MVSubAgent status: UP

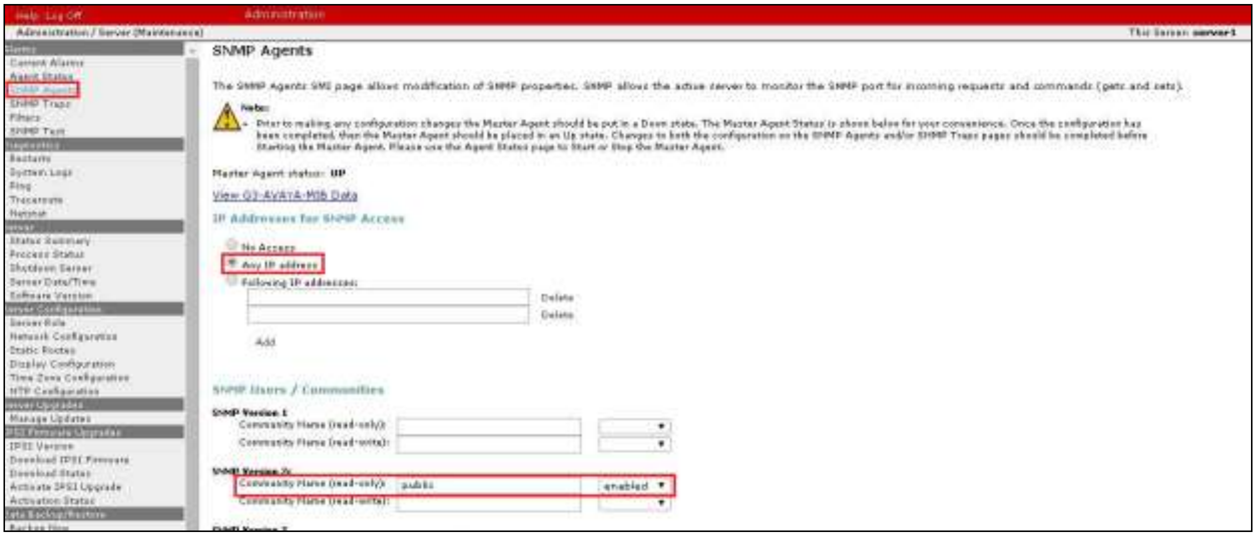
Load Agent status: UP

MIB2 Agent status: UP

To allow ServicePilot ISM to use SNMP to collect configuration and status information from Communication Manager, Select **SNMP Agents** in the left pane and enter the following:

- **Any IP address** Click on the radio button
- **SNMP Users / Communities**, In **SNMP Version 2c** in the **Community Name (read-only)** field enter **public** and the drop down list select **enabled**

Click the **Submit** button at the bottom of the page (not shown).



SNMP Agents

The SNMP Agents SMI page allows modification of SNMP properties. SNMP allows the active server to monitor the SNMP port for incoming requests and commands (gets and sets).

Note:

- Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

Master Agent status: **UP**

View G3-AVAYA-MIB Data

IP Addresses for SNMP Access

○ No Access

● Any IP address

○ Following IP addresses:

SNMP Users / Communities

SNMP Version 1

Community Name (read-only):

Community Name (read-write):

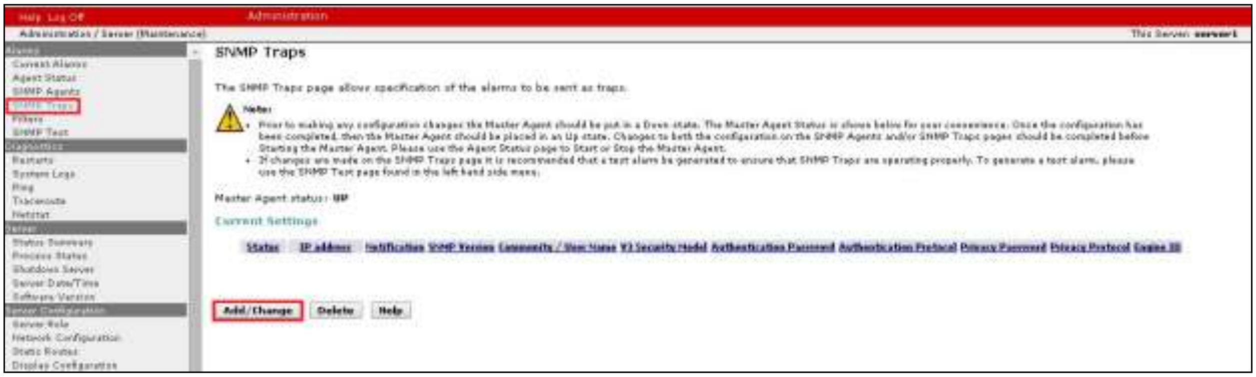
SNMP Version 2c

Community Name (read-only): public enabled

Community Name (read-write):

SNMP Version 3

Select **SNMP Traps** in navigation panel on the left side and click the **Add/**Change button.



SNMP Traps

The SNMP Traps page allow specification of the alarms to be sent as traps.

Note:

- Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.
- If changes are made on the SNMP Traps page it is recommended that a test alarm be generated to ensure that SNMP Traps are operating properly. To generate a test alarm, please use the SNMP Test page found in the left hand side menu.

Master Agent status: UP

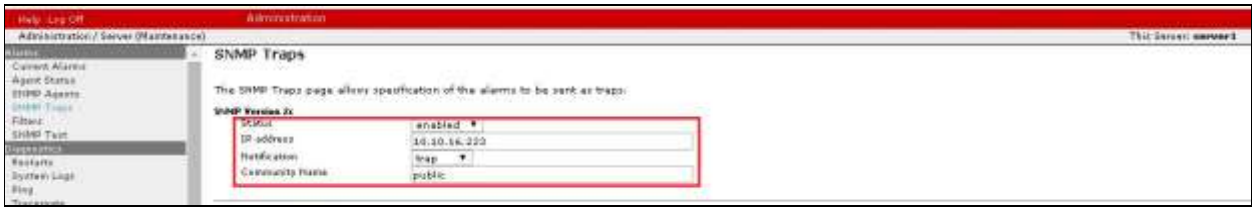
Current Settings

Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Authentication Protocol	Privacy Password	Privacy Protocol	Engine ID

In the subsequent page enter the following in the **SNMP Version 2c**:

- **Status** Select **enabled** from the drop down list
- **IP address** Enter the IP address of ServicePilot ISM (i.e. 10.10.16.223)
- **Notification** Select **trap** from the drop down list
- **Community Name** Enter **public**

Click the **Submit** button at the bottom of the page (not shown).



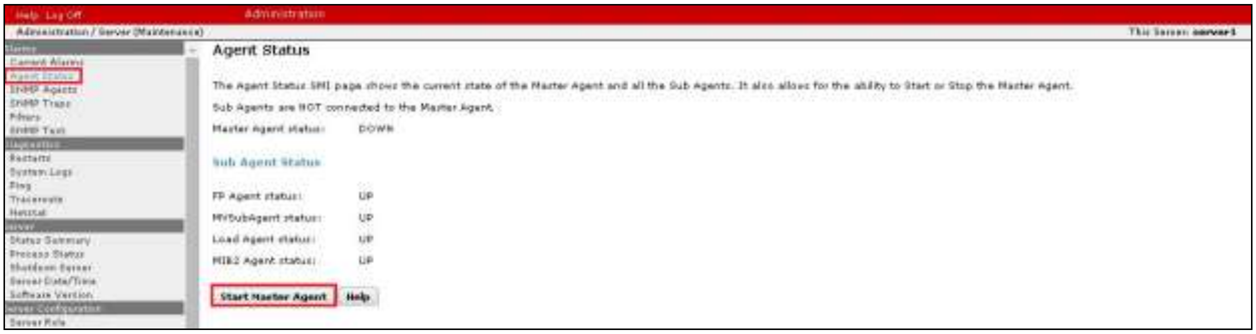
SNMP Traps

The SNMP Traps page allows specification of the alarms to be sent as traps:

SNMP Version 2c

Status	enabled
IP address	10.10.16.223
Notification	trap
Community Name	public

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.



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

MVSubAgent status: UP

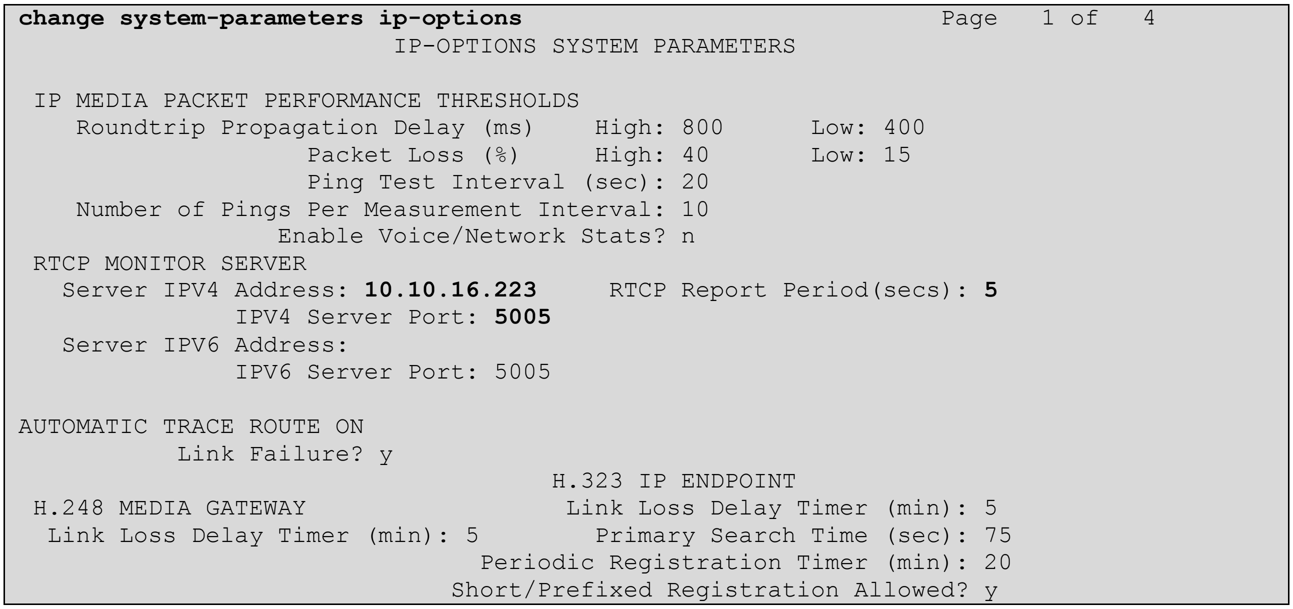
Load Agent status: UP

MIB2 Agent status: UP

6.5. Configure RTCP Monitoring

To allow ServicePilot ISM to monitor the quality of IP calls, configure Communication Manager to send RTCP reporting to the IP address of the ISM 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 ISM server (10.10.16.223)
- **RTCP Report Period (secs)** Enter **5**
- **IPV4 Server Port** Enter **5005**



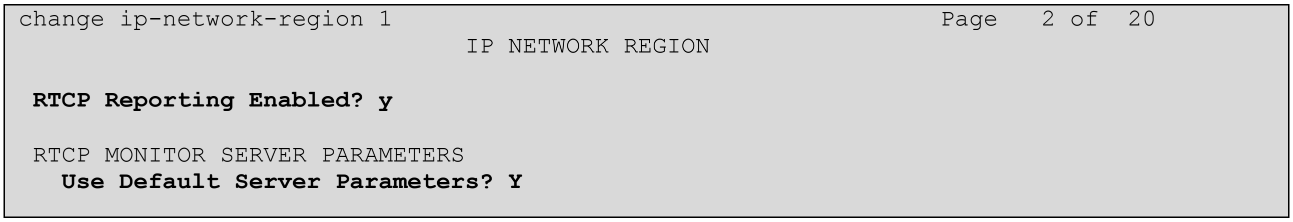
```
change system-parameters ip-options                            Page   1 of   4
                          IP-OPTIONS SYSTEM PARAMETERS

 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: 10.10.16.223     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
                               Periodic Registration Timer (min): 20
                             Short/Prefixed Registration Allowed? y
```

Enter the **change ip-network-region *n*** command, where ***n*** is IP network region number to be monitored. On Page 2, set **RTCP Reporting 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 Enabled? y

 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? Y
```

6.6. Configure CDR Monitoring

To allow ServicePilot ISM to monitor CDR information, configure Communication Manager to send CDR information to the IP address of the ISM server. Use the **change ip-interface procr** command to enable the processor-ethernet interface on Communication Manager. Set **Enable Interface** to **y**. This interface will be used by Communication Manager to send out CDR information.

```
change ip-interface procr                                    Page   1 of   2
                                  IP INTERFACES


                  Type: PROCR
                                                        Target socket load: 1700

      Enable Interface? y                            Allow H.323 Endpoints? y
                                                      Allow H.248 Gateways? y
        Network Region: 1                              Gatekeeper Priority: 5


                                 IPV4 PARAMETERS
             Node Name: procr                    IP Address: 10.1.10.230


           Subnet Mask: /24
```

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 **10.10.16.223**

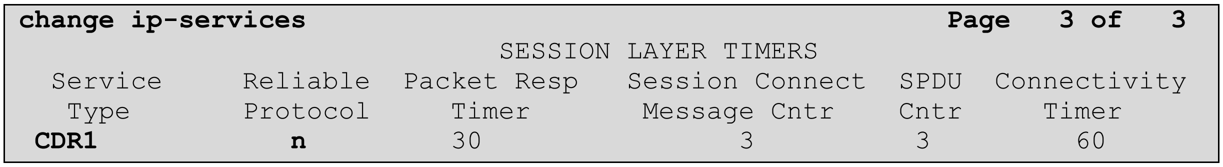
```
change node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SPISM              10.10.16.223
```

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 **CDR1**
- **Local Node** Enter **procr**
- **Remote Node** Enter **SPISM**
- **Remote Port** Enter **50000**

```
change ip-services                                           Page   1 of   3
                                  IP SERVICES
 Service     Enabled     Local        Local        Remote       Remote
  Type                   Node         Port         Node         Port
CDR1                   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.



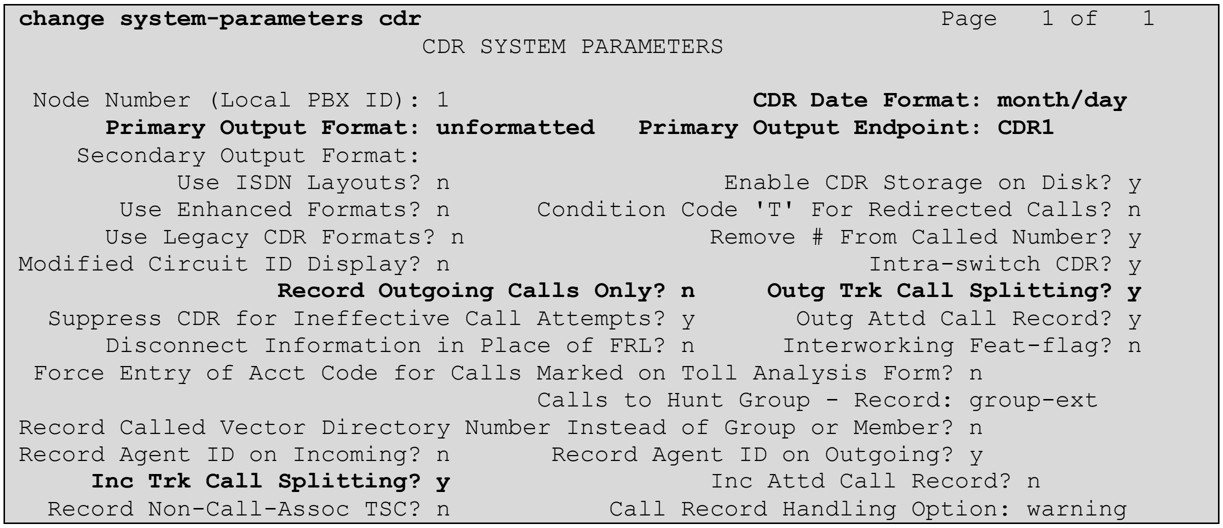
```
change ip-services                                         Page   3 of   3
                              SESSION LAYER TIMERS
  Service     Reliable  Packet Resp   Session Connect  SPDU Connectivity
   Type       Protocol     Timer       Message Cntr    Cntr    Timer
 CDR1            n         30                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 is also supported)
- **Primary Output Format** Select **unformatted**
- **Primary Output Endpoint** Select **CDR1**

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): 1                     CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format:
           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? y
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? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: group-ext
Record Called Vector Directory Number Instead of Group or Member? n
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: outpulsed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 7
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:   0    of 5000   administered
   Extension           Extension          Extension          Extension

   1000
   1001
   1002
   1004
   1008
   1009
...1015
   1016
   1026
```

7. Configure SNMP for Media Gateway

This section provides the procedures for configuring SNMP on the Avaya G430 Media Gateway. The procedures include the following areas. Repeat these procedures for every Media Gateway in the network.

- Administer community string
- Administer SNMP traps
- Show SNMP

7.1. Administer Community String

Using a SSH client and appropriate credentials logon to the G450 shell and 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.

```
G430-003(super)#
G430-003(super)# snmp-server community read-only public read-write public
Done!
G430-003(super)#
```

7.2. Administer SNMP Traps

Use the **snmp-server host** command shown below to enable SNMP traps to ServicePilot ISM, where **10.10.16.223** is the IP address of the ISM server, and **public** is the read-only community string.

```
G430-003(super)#
G430-003(super)# snmp-server host 10.10.16.223 traps v2c public
Done!
G430-003(super)#
```

7.3. Show SNMP

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

```
G430-003(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/Inform
UDP port                                      Level
User name
--------------------------------------------- ------- -------------- -----------
10.10.16.211                                     v1    all            trap
162 - Dynamic Trap Manager                    noauth
ReadCommN
10.10.16.223                                    v2c   all            trap
162                                           noauth
```

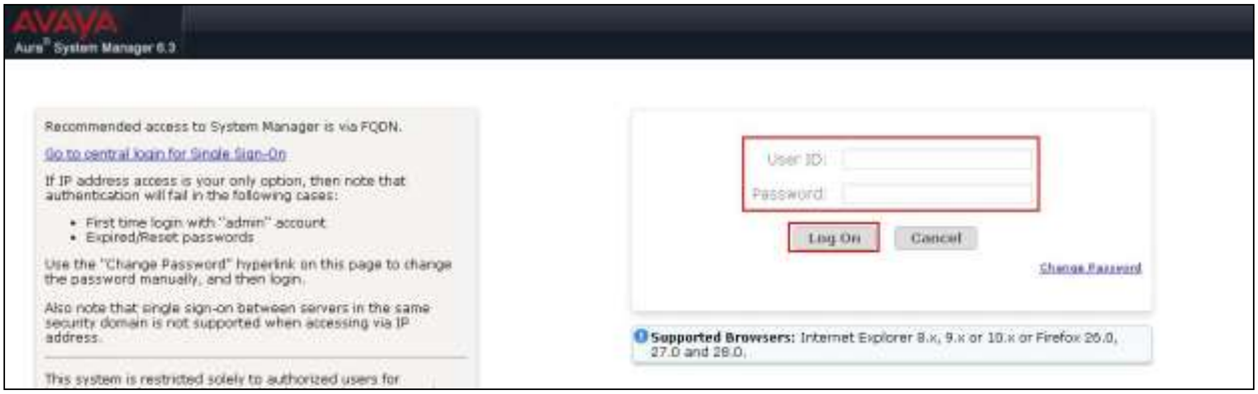
8. Configure Avaya Aura® System Manager

ServicePilot ISM monitors and collects data from System Managers; a number of configuration steps are required and can be summarized as follows:

- Configure Avaya Aura® System Manager for SNMP
- Configure Avaya Aura® System Manager for RTCP

8.1. Configure Avaya Aura® System Manager for SNMP

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

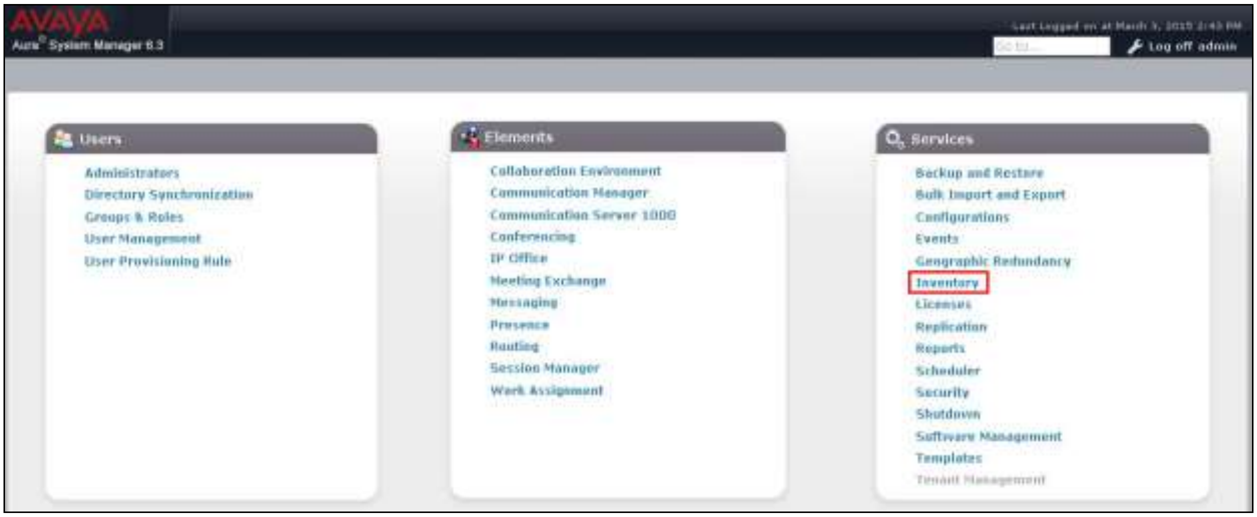
Use the "Change Password" hyperlink on this page to change the password manually, and then login.

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

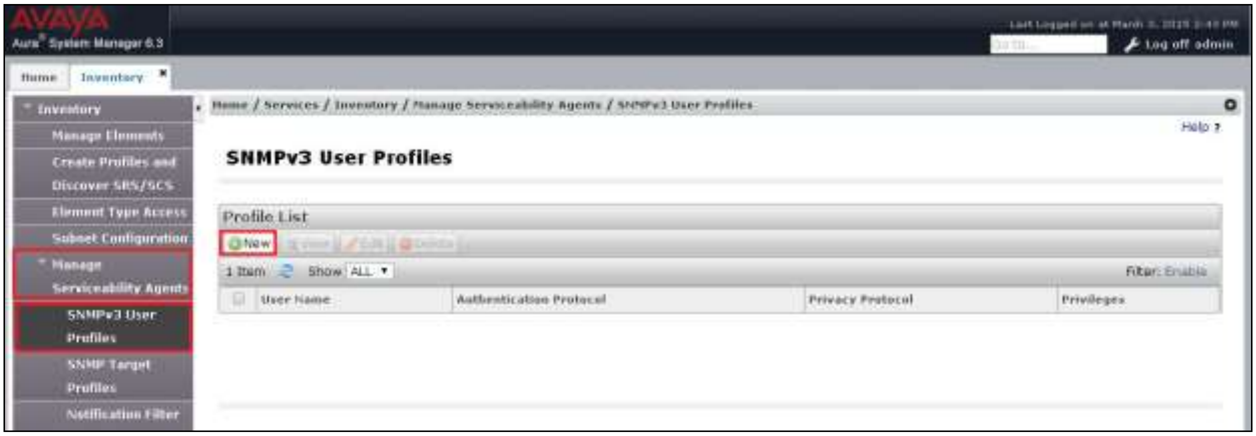
This system is restricted solely to authorized users for

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 26.0, 27.0 and 28.0.

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



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.

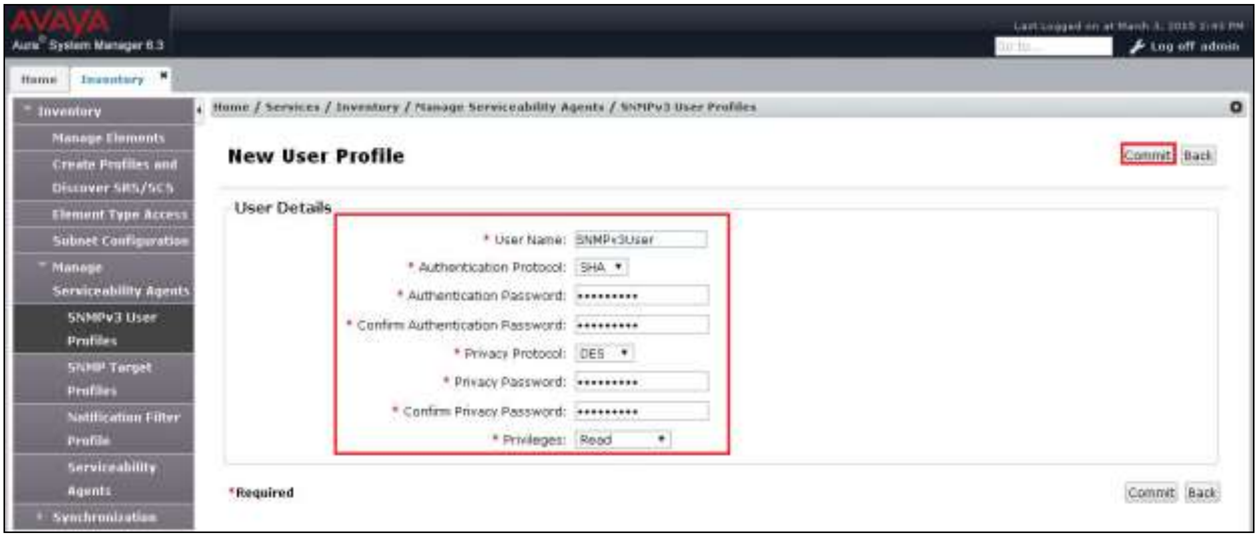


On the subsequent page enter the following details for the User Profile:

• User Name	Enter **SNMPv3User**
• Authentication Protocol	Select **SHA** 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 information will be required in the ServicePilot ISM configuration **Section 11.5**



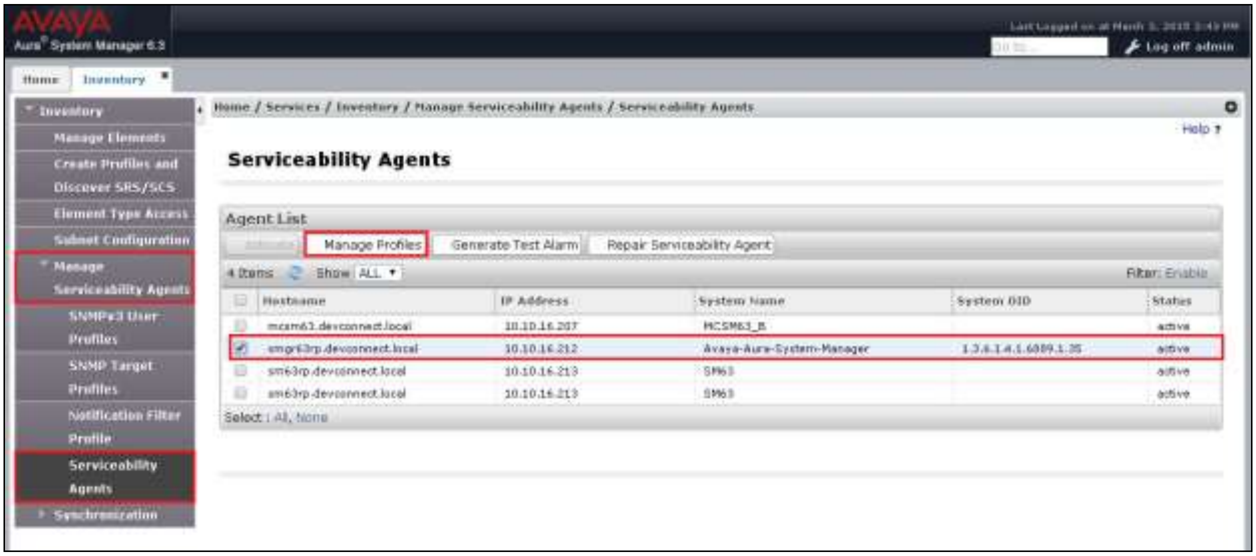
New User Profile

User Details

* User Name: SNMPv3User
* Authentication Protocol: SHA
* Authentication Password: ••••••••••
* Confirm Authentication Password: ••••••••••
* Privacy Protocol: DES
* Privacy Password: ••••••••••
* Confirm Privacy Password: ••••••••••
* Privileges: Read

*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 (smgr63rp.devconnect.local.) and click **Manage Profiles**.



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

Serviceability Agents

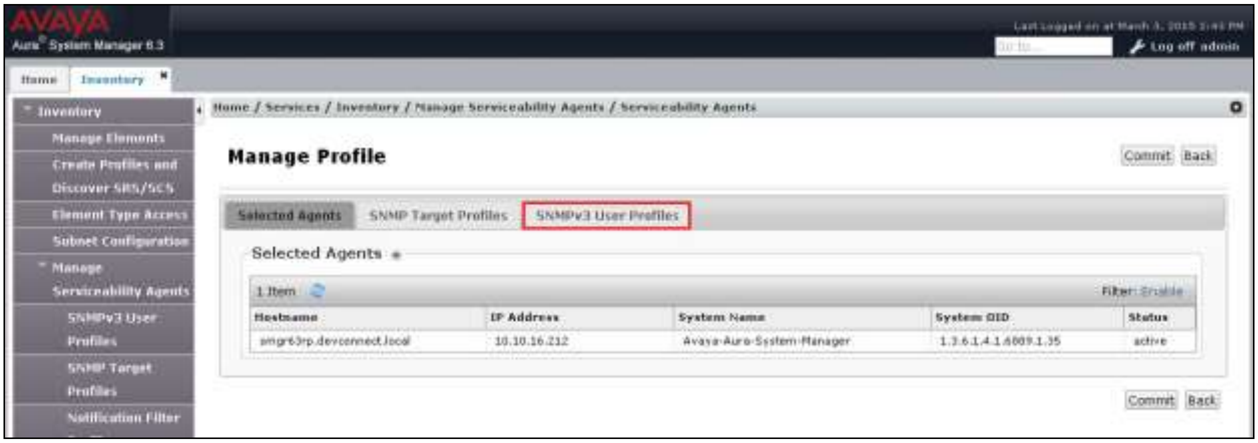
Agent List

4 Items Show ALL

	Hostname	IP Address	System Name	System OID	Status
□	mcsm63.devconnect.local	10.10.16.207	MCSM63_B		active
☑	smgr63rp.devconnect.local	10.10.16.212	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
□	sm63rp.devconnect.local	10.10.16.213	SM63		active
□	sm63rp.devconnect.local	10.10.16.213	SM63		active

Select : All, None

On the subsequent page select **SNMPv3User Profiles**.



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

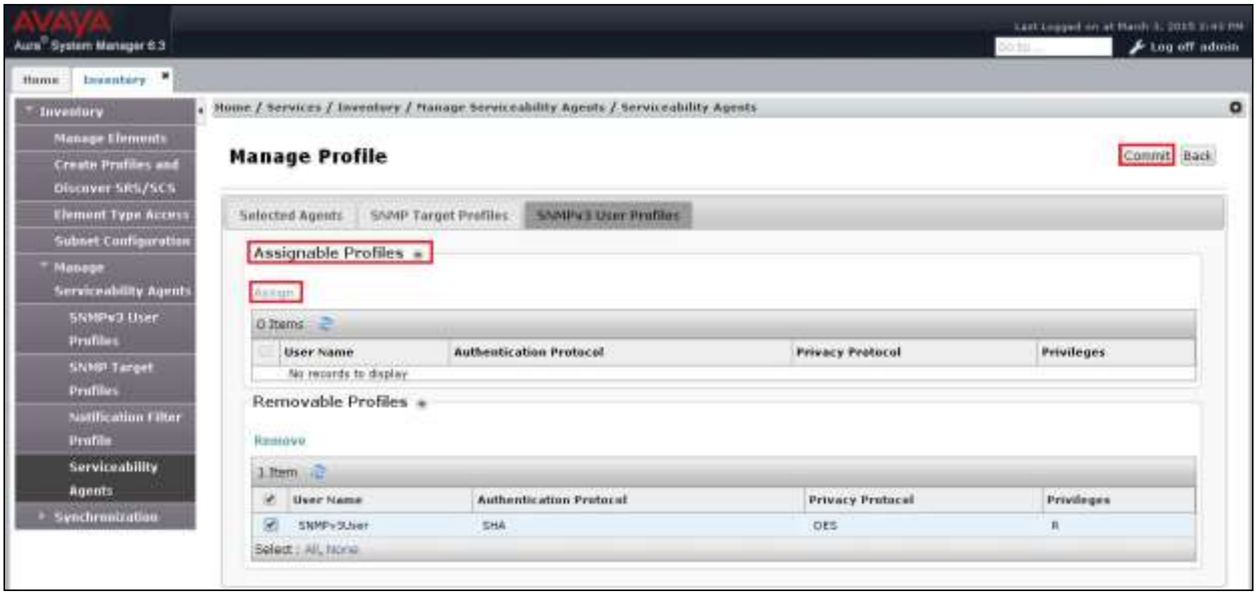
Manage Profile

Selected Agents

1 Item

Hostname	IP Address	System Name	System OID	Status
smgr63rp.devconnect.local	10.10.16.212	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active

Click down arrow beside **Assignable Profiles** section if not expanded. Click **Assign** to assign it to System Manager. The user profile is moved to the **Removable Profiles** section as below. The user profile has now been assigned to System Manager. Click **Commit** to submit the changes.



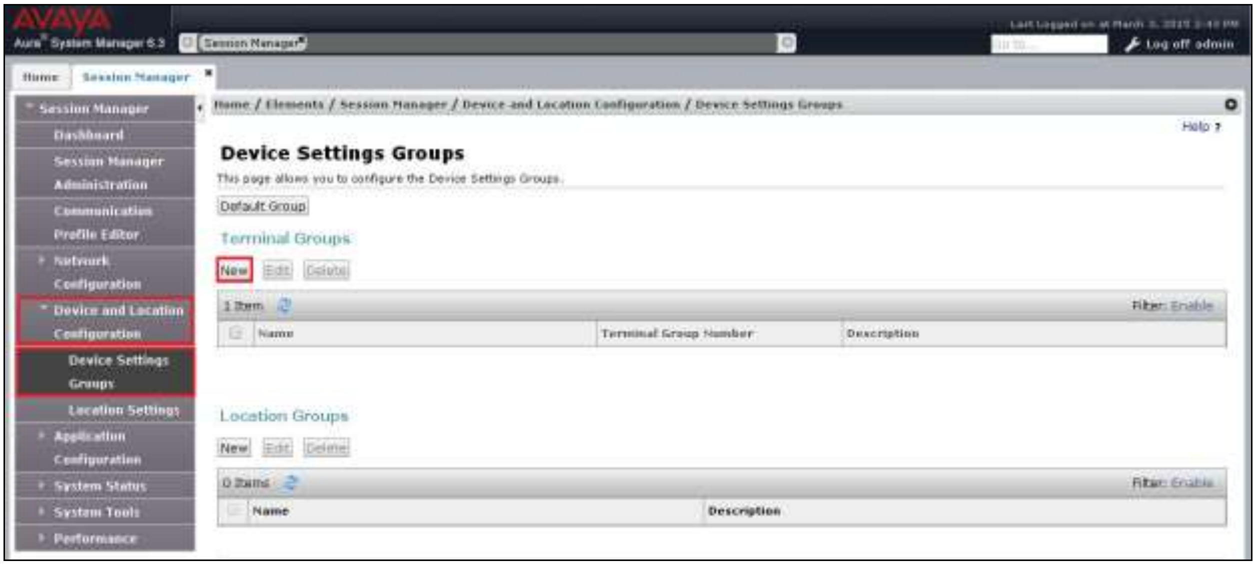
Manage Profile

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

✓	User Name	Authentication Protocol	Privacy Protocol	Privileges
☑	SNMPv3User	SHA	DES	R

8.2. Configure Avaya Aura® System Manager for 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**.



Device Settings Groups

This page allows you to configure the Device Settings Groups.

□	Name	Terminal Group Number	Description

□	Name	Description

On the subsequent page enter the following:

General Section

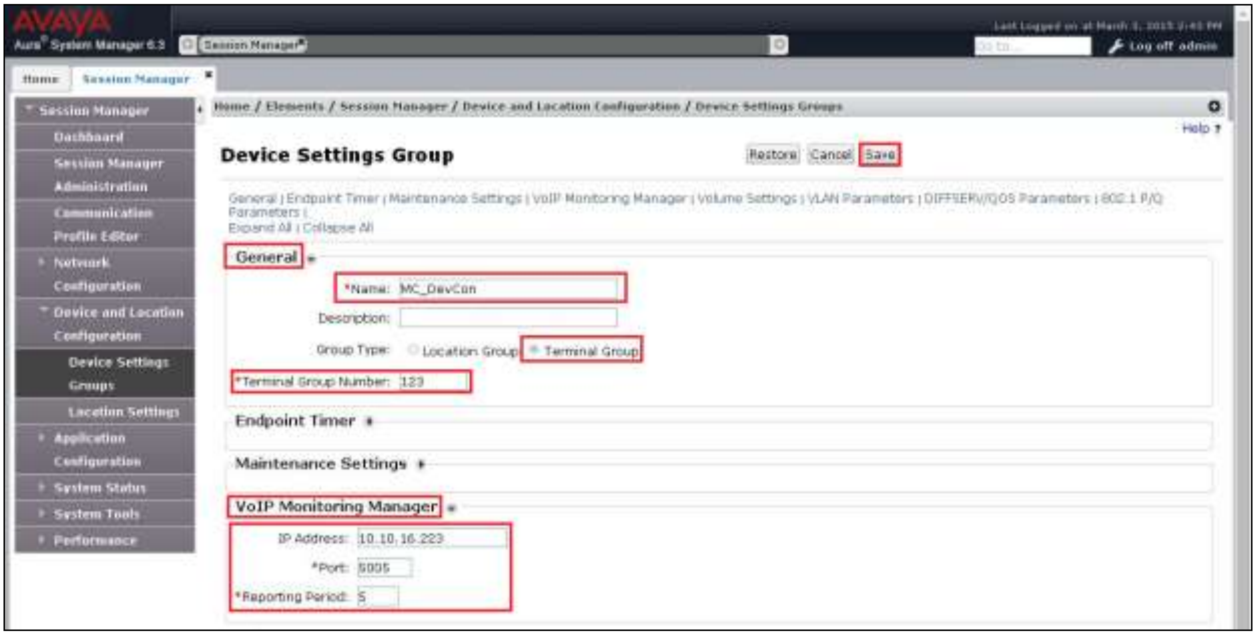
Name	Enter an appropriate name
Terminal Group	Click the radio button
Terminal Group Number	Enter an appropriate Terminal Group Number

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

VoIP Monitoring Manager Section

IP Address	Enter the IP address of the ISM Server
Port	Enter **5005**
Reporting Period	Enter **5**

Click **Save** to submit the changes.


AVAYA
Aura® System Manager 6.3
Session Manager
Last Logged on at March 3, 2015 2:43 PM
Go to...
Log off admin
Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Device Settings Groups
Location Settings
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: MC_DevCon

Description:

Group Type: ○ Location Group ● Terminal Group

*Terminal Group Number: 123

VoIP Monitoring Manager

IP Address: 10.10.16.223

*Port: 5005

*Reporting Period: 5

9. Configure Avaya Aura® Session Manager

ServicePilot ISM monitors and collects data from Session Managers, System Manager is used to configure Session Manager. A number of configurations are required and can be summarized as follows:

- Configure Avaya Aura® System Manager for SNMP
- Configure CDR user account for Avaya Aura® Session Manager

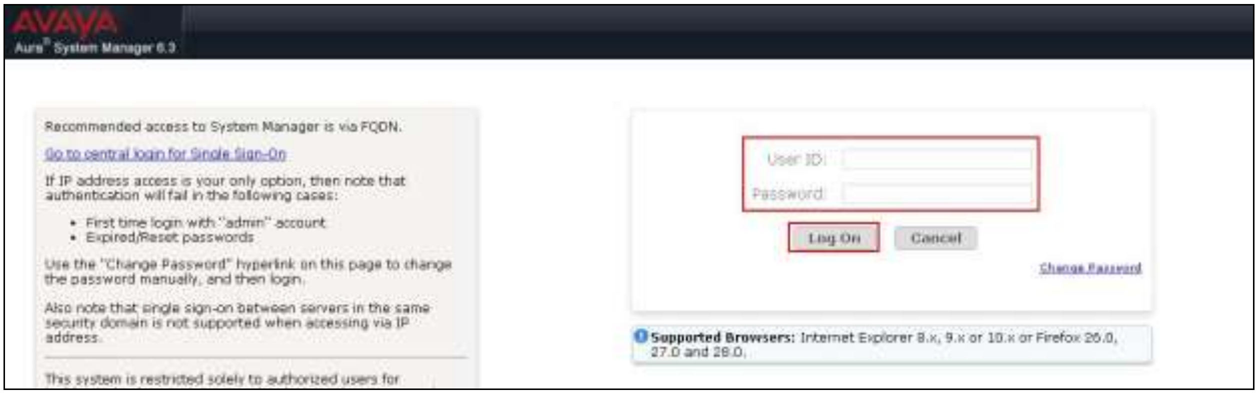
9.1. Configure Avaya Aura® System Manager for SNMP

Use the **SNMPv3 User Profile** as configured in **Section 8.1** and assign it to the appropriate Session Managers using the using the relevant steps in **Section 8.1**..

Configuration changes are required on these devices to allow monitoring.

9.2. Configure CDR user account for Avaya Aura® Session Manager

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

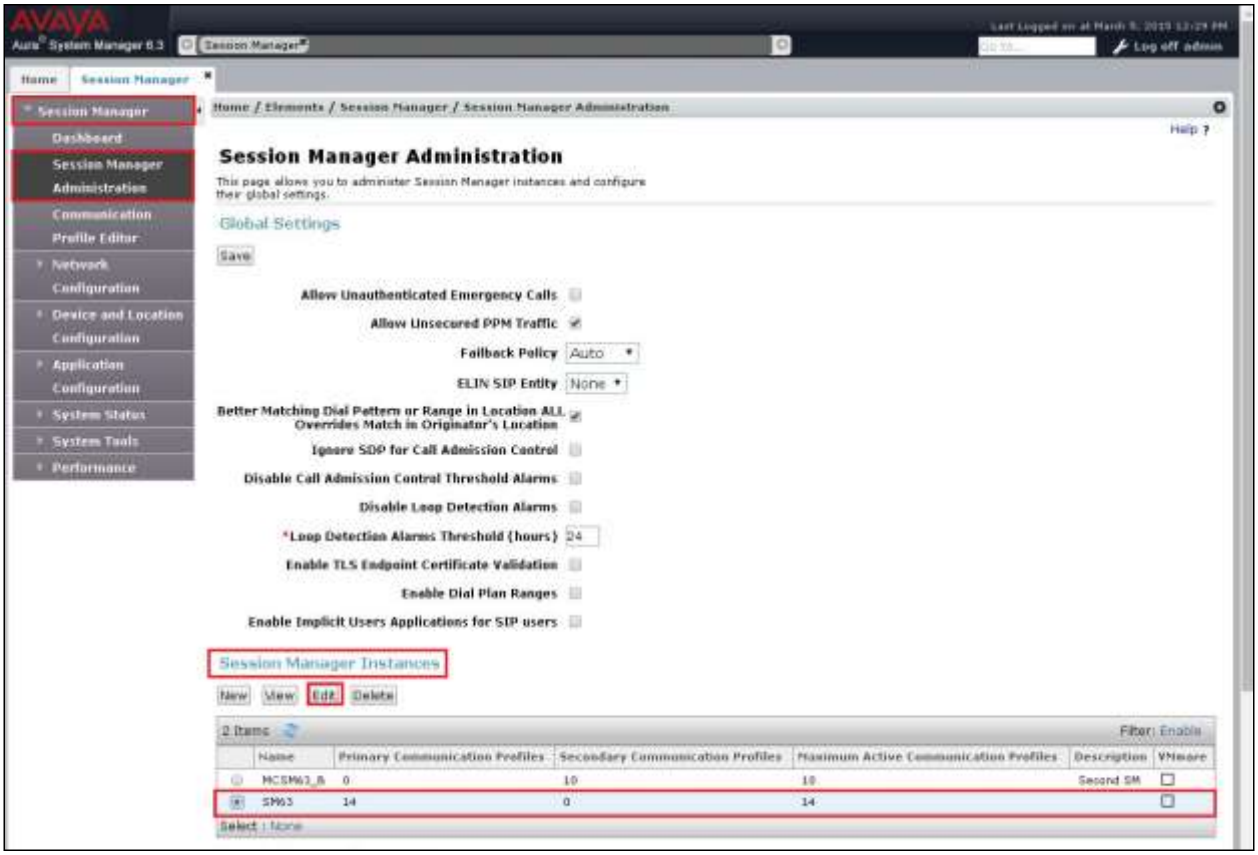
Use the "Change Password" hyperlink on this page to change the password manually, and then login.

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

This system is restricted solely to authorized users for

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 26.0, 27.0 and 28.0.

On the subsequent page select **Session Manager** in the **Elements** section (not shown) and 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.



Session Manager Administration

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

Global Settings

Allow Unauthenticated Emergency Calls □
Allow Unsecured PPM Traffic ☑
Failback Policy Auto
ELIN SIP Entity None
Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location ☑
Ignore SDP for Call Admission Control □
Disable Call Admission Control Threshold Alarms □
Disable Loop Detection Alarms □
*Loop Detection Alarms Threshold (hours) 24
Enable TLS Endpoint Certificate Validation □
Enable Dial Plan Ranges □
Enable Implicit Users Applications for SIP users □

Session Manager Instances

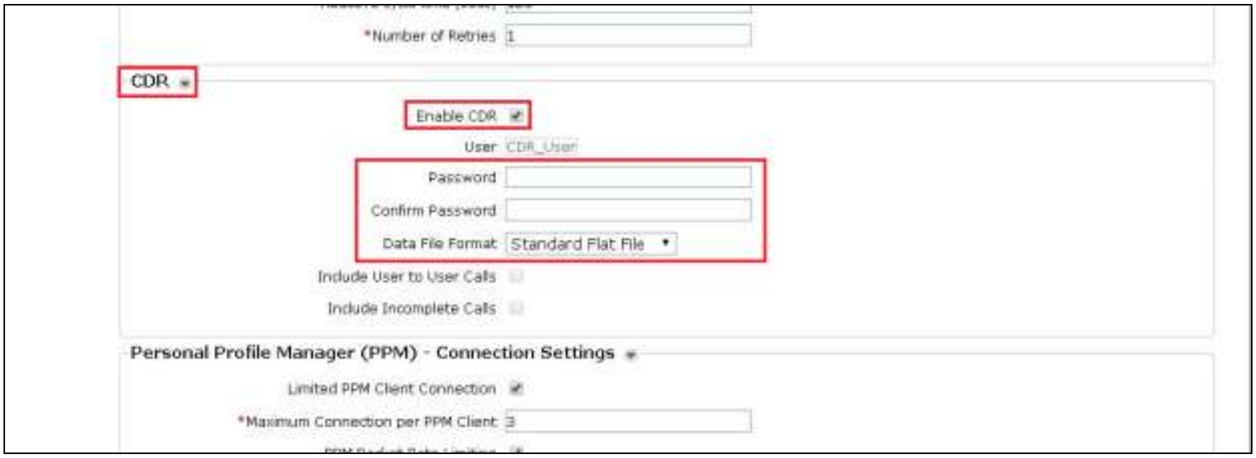
	Name	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description	VMware
○	MCSM63_B	0	10	10	Second SM	□
●	SM63	14	0	14		□

On the subsequent page scroll down to the **CDR** section and enter the following:

- **Enable CDR** Tick the check box
- **Password** Enter and re-enter an appropriate password
- **Data File Format** Select **Standard Flat File** from the drop down list

Click on the **Commit** button to submit (not shown).

Note: It is recommended that when the administrators are configuring trunks in Communication Manager that will talk to Session Manager, they set **CDR Reports** to **n** on the appropriate Trunk Group.



*Number of Retries 1

CDR

Enable CDR ☑

User CDR_User

Password

Confirm Password

Data File Format Standard Flat File

Include User to User Calls □

Include Incomplete Calls □

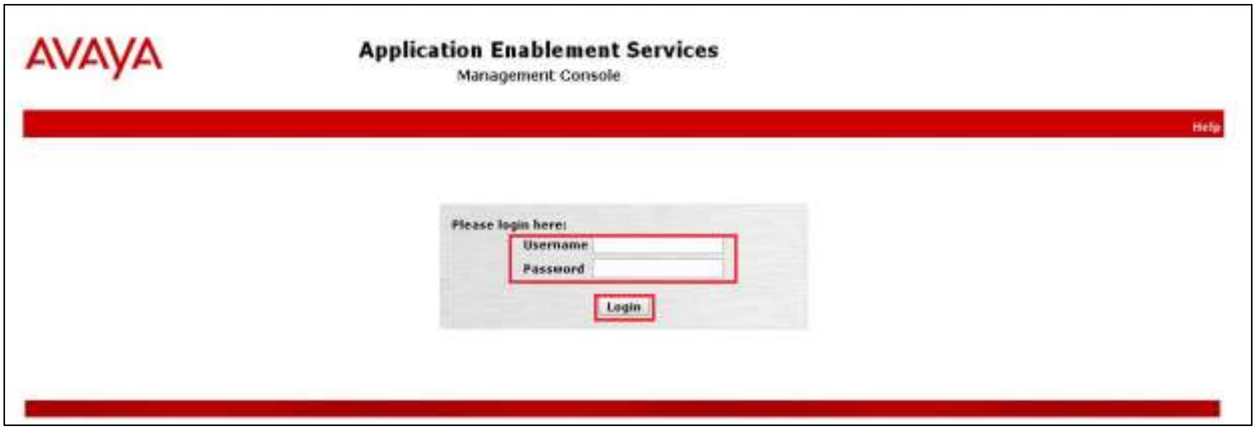
Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection ☑

*Maximum Connection per PPM Client 3

10. Configure Avaya Aura® Avaya Application Enablement Services for SNMP

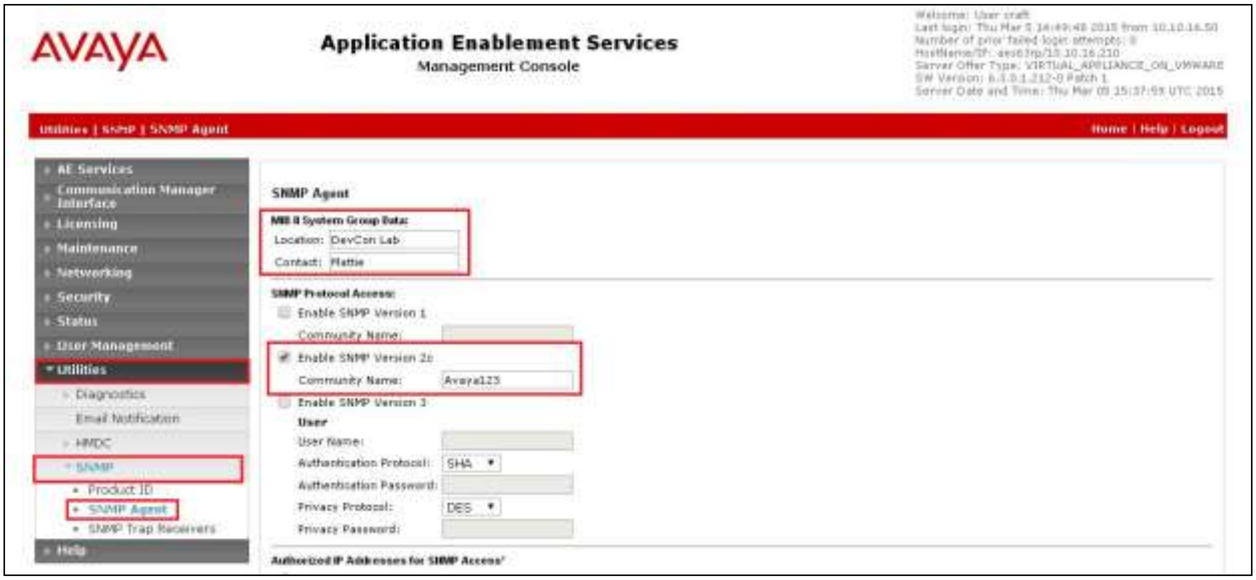
ServicePilot ISM monitors and collects data from AES. A number of configurations are required. To access the OAM web-based interface of the AES Server use the URL **http://x.x.x.x**, where **x. x. x. x** is the selected IP address of the AES. The **Management console** is displayed. Log in using the appropriate credentials.



After logging in, select **Utilities → SNMP → SNMP Agent** and enter the following:

Location	Enter an appropriate Location
Contact	Enter an appropriate Contact
Enable SNMP Version 2c	Tick the check box
Community Name	Enter an appropriate Community Name

Click on the **Apply Changes** button (not shown) to save.



Welcome: User craft
Last login: Thu Mar 5 14:49:48 2015 from 10.10.16.50
Number of prior failed login attempts: 0
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.212-0 Patch 1
Server Date and Time: Thu Mar 05 15:37:59 UTC 2015

SNMP Agent

MIB II System Group Data:
Location: DevCon Lab
Contact: Mattie

SNMP Protocol Access:
☐ Enable SNMP Version 1
Community Name:
☑ Enable SNMP Version 2c
Community Name: Avaya123
☐ Enable SNMP Version 3
User
User Name:
Authentication Protocol: SHA ▾
Authentication Password:
Privacy Protocol: DES ▾
Privacy Password:

Authorized IP Addresses for SNMP Access¹

11. Configure ServicePilot ISM

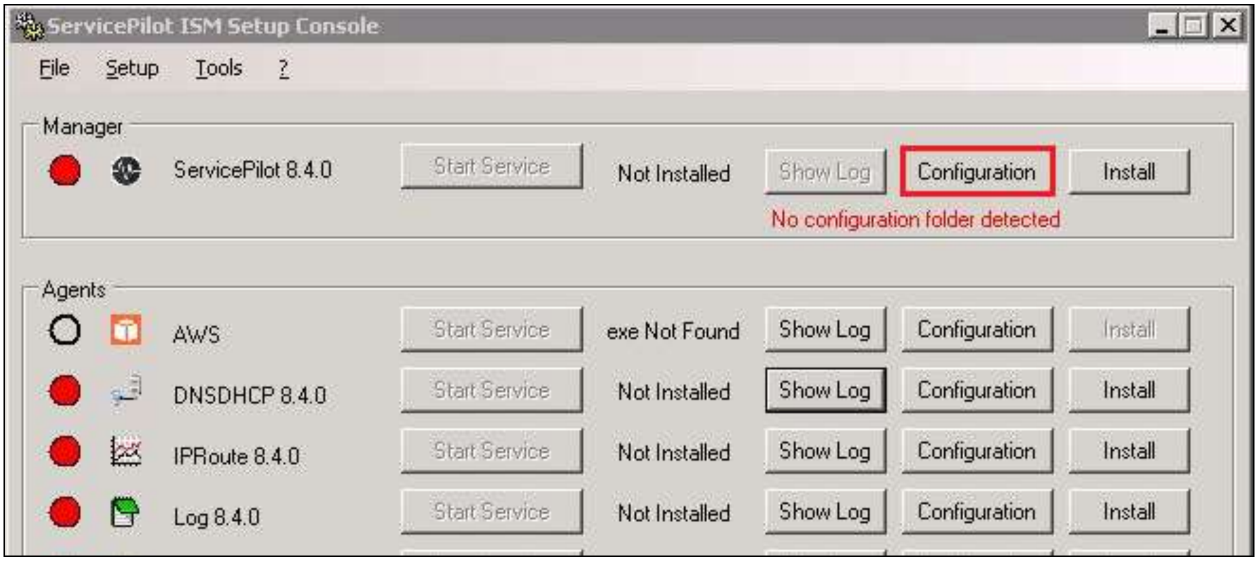
This section describes the configuration required for ServicePilot ISM to interoperate with Communication Manager. It assumes that the application and all required software components have been installed and properly licensed.

Note: The installation and configuration of ServicePilot ISM 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.

11.1. Launch ServicePilot ISM console

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

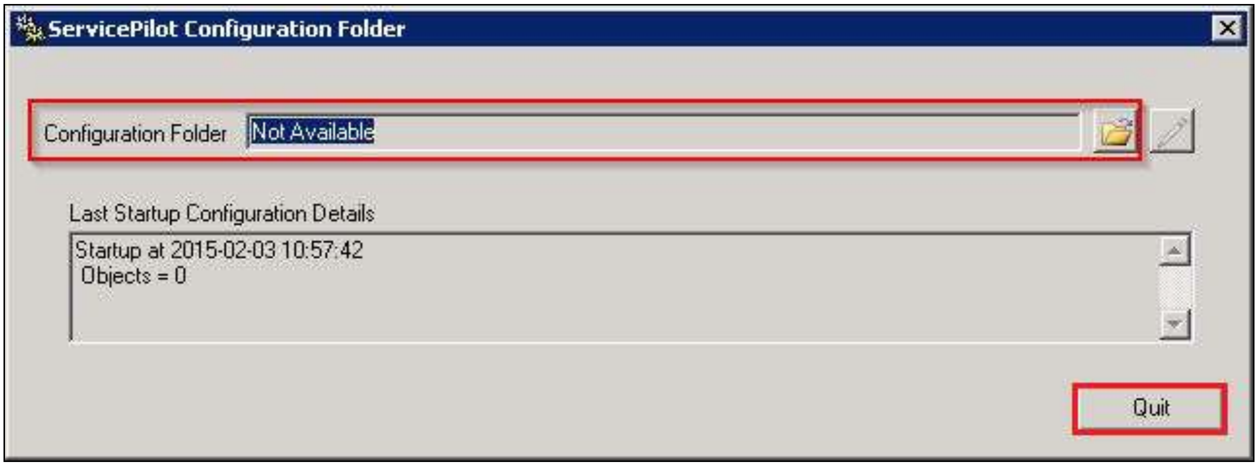
Note: The **ServicePilot ISM Administration Console** is located at **C:\Program Files (x86)\servicepilot\servicepilot ISM Enterprise\console.exe** and must be run as Administrator.



ServicePilot 8.4.0	Start Service	Not Installed	Show Log	Configuration	Install
AWS	Start Service	exe Not Found	Show Log	Configuration	Install
DNSDHCP 8.4.0	Start Service	Not Installed	Show Log	Configuration	Install
IPRoute 8.4.0	Start Service	Not Installed	Show Log	Configuration	Install
Log 8.4.0	Start Service	Not Installed	Show Log	Configuration	Install

No configuration folder detected

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

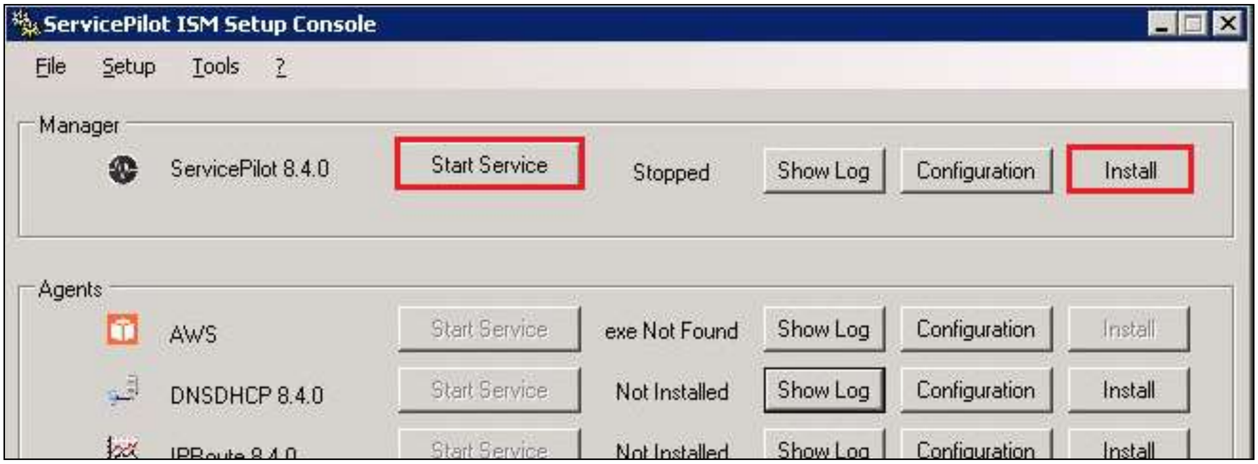


Configuration Folder: Not Available

Last Startup Configuration Details

```
Startup at 2015-02-03 10:57:42
 Objects = 0
```

After returning to the **ServicePilot ISM Setup Console** window click on the **Install** button followed by the **Start Service** button.

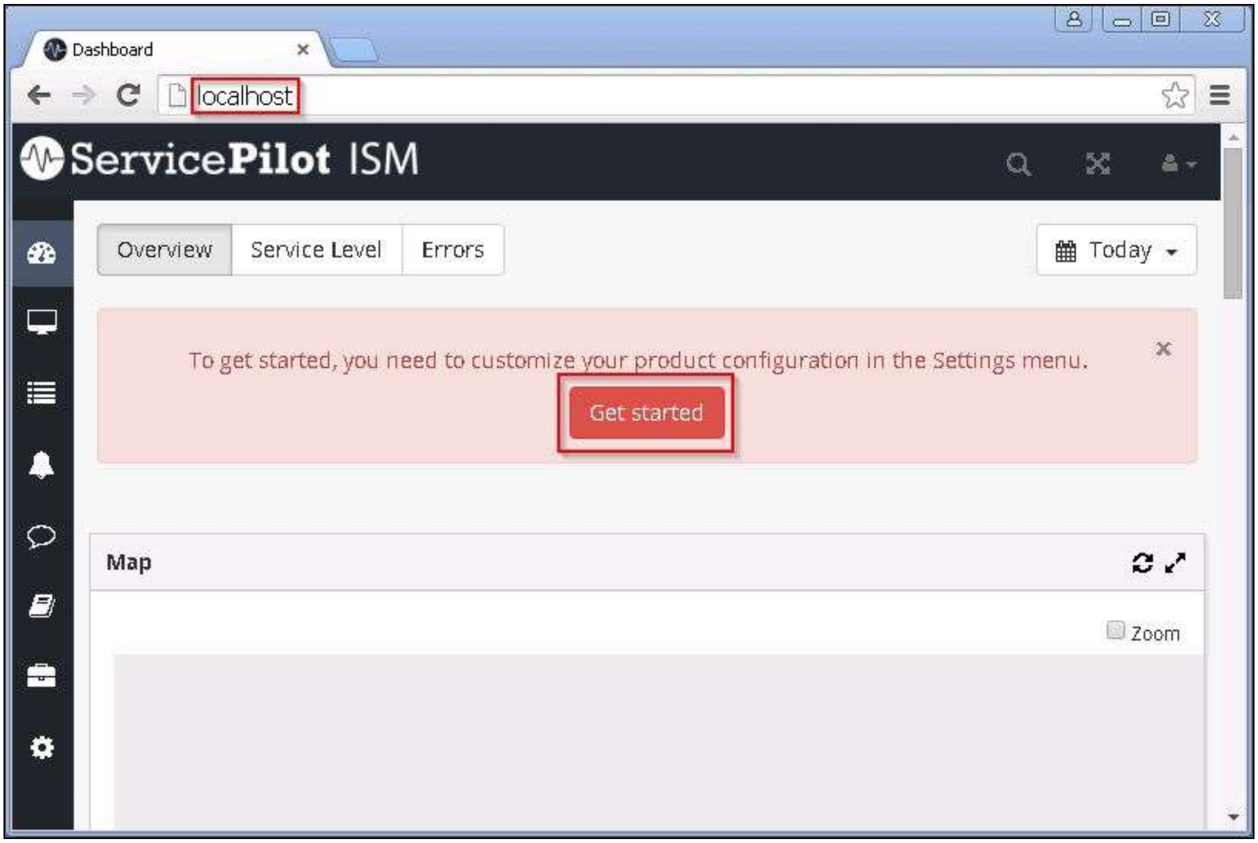


ServicePilot 8.4.0	Start Service	Stopped	Show Log	Configuration	Install
AWS	Start Service	exe Not Found	Show Log	Configuration	Install
DNSDHCP 8.4.0	Start Service	Not Installed	Show Log	Configuration	Install
IPRoute 8.4.0	Start Service	Not Installed	Show Log	Configuration	Install

11.2. Create ServicePilot ISM configuration

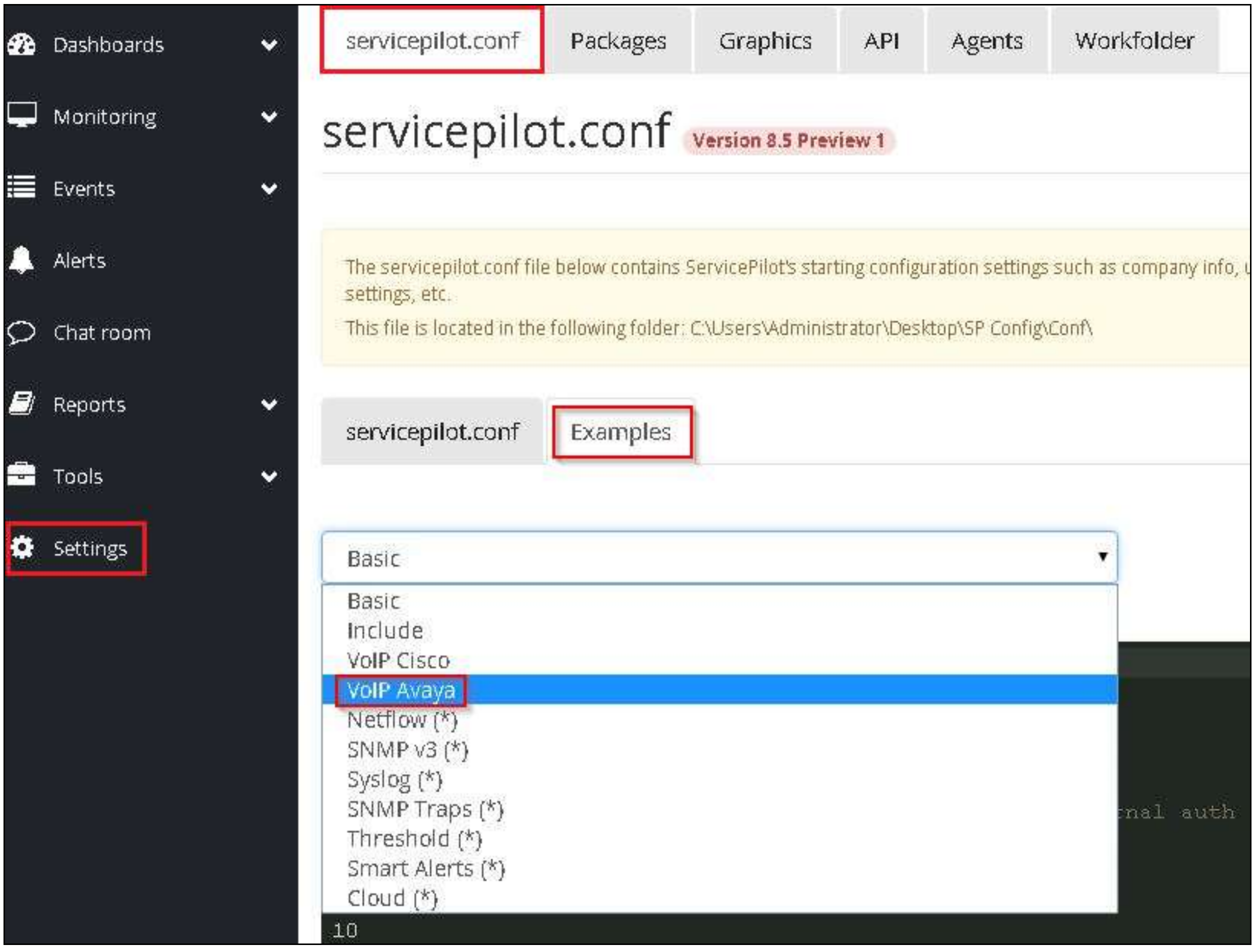
To create a new ServicePilot configuration use a Web Browser to browse to **localhost** and login with the appropriate credentials (not shown). When the Web page opens click on the **Get Started** button

Note: ServicePilot ISM supports Google Chrome and FireFox.



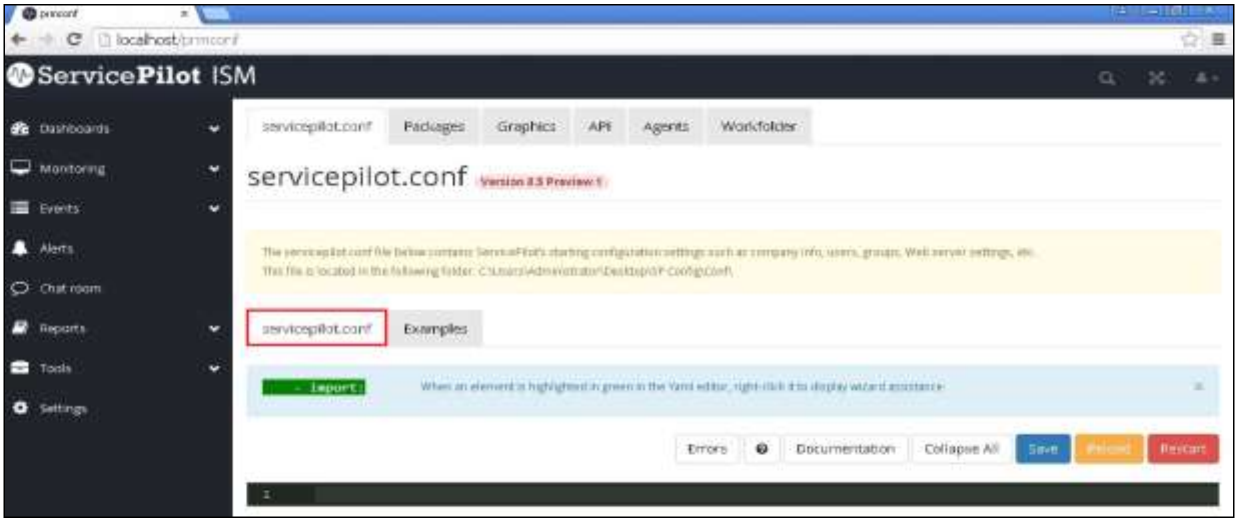
To get started, you need to customize your product configuration in the Settings menu.

When the new page opens click on **Settings** followed by the **servicepilot.conf** tab, then click on the **Examples** tab and select **VoIP Avaya** from the dropdown box.



The servicepilot.conf file below contains ServicePilot's starting configuration settings such as company info, u settings, etc.
This file is located in the following folder: C:\Users\Administrator\Desktop\SP Config\Conf\

In the example configuration for **VoIP Avaya,** use **Ctrl A** follow by **Ctrl C** to copy the configuration (not shown) from the built in configuration editor window, then click on the **servicepilot.conf** tab to the left of the **Examples** tab and paste the example configuration into the empty built-in configuration editor window.



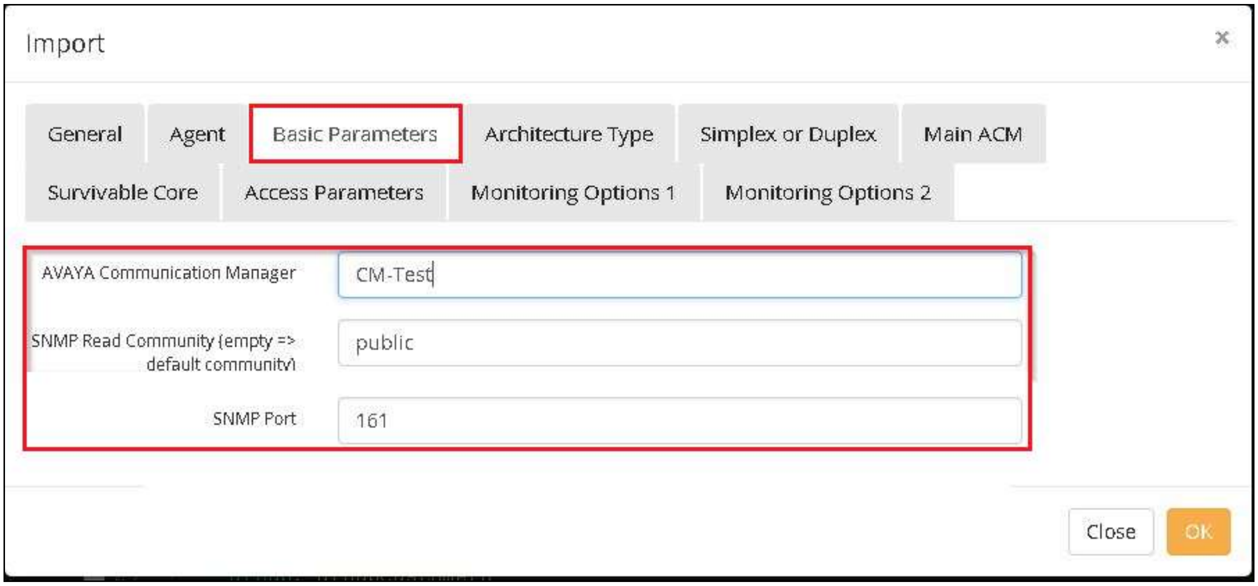
The servicepilot.conf file below contains ServicePilot's starting configuration settings such as company info, users, groups, Web server settings, etc.
This file is located in the following folder: C:\Users\Administrator\Desktop\SP-Config\Conf\

When an element is highlighted in green in the Yaml editor, right-click it to display wizard assistance

11.3. Configure Communication Manager PACKAGE

To configure the Communication PACKAGE scroll down in the built-in configuration editor window, and right click on the **import** button relating **to PACKAGE: CM-1** (not shown). When the **import** window opens click on the **Basic Parameters** tab and enter the following:

- **AVAYA communication Manager**	Enter an informative name
- **SNMP Read Community**	Enter **public**
- **SNMP Port**	Enter 161

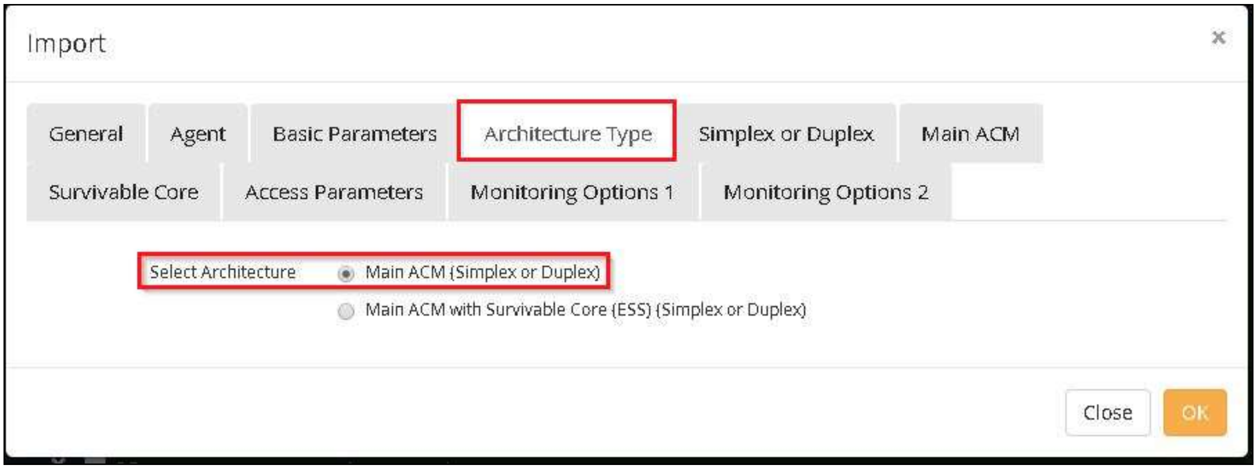


AVAYA Communication Manager: CM-Test

SNMP Read Community (empty => default community): public

SNMP Port: 161

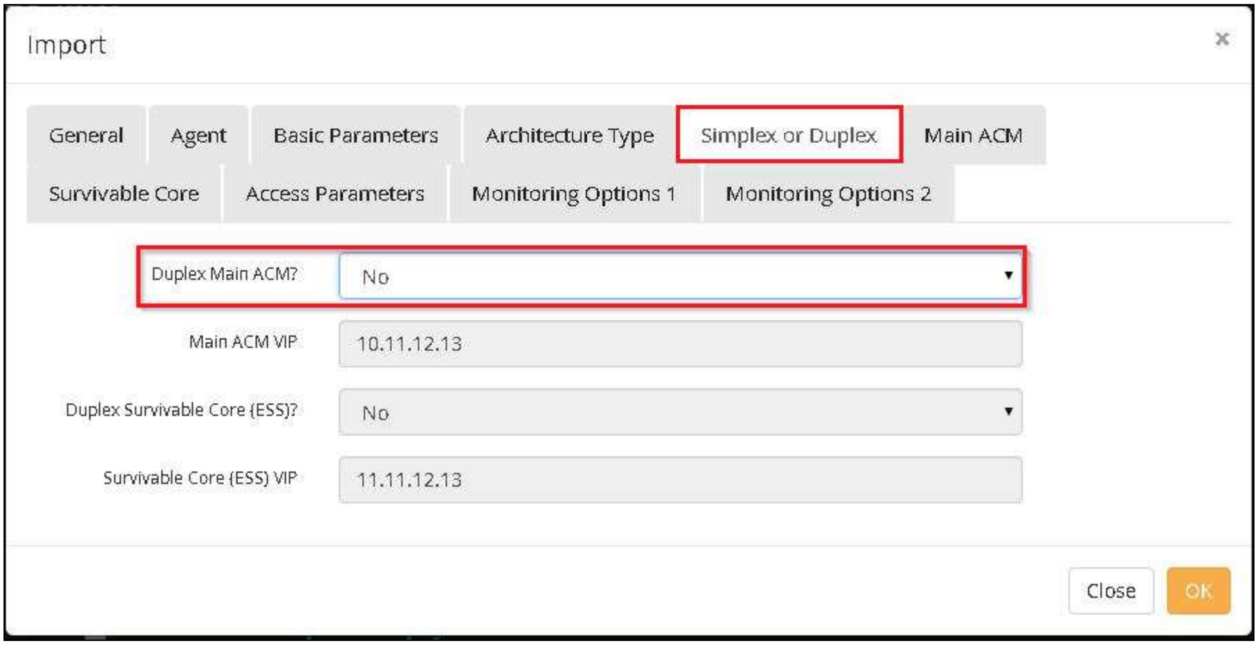
In the **Architecture Type** tab click on the **Main ACM** radio button for **Select Architecture**.



Select Architecture ● Main ACM (Simplex or Duplex)

○ Main ACM with Survivable Core (ESS) (Simplex or Duplex)

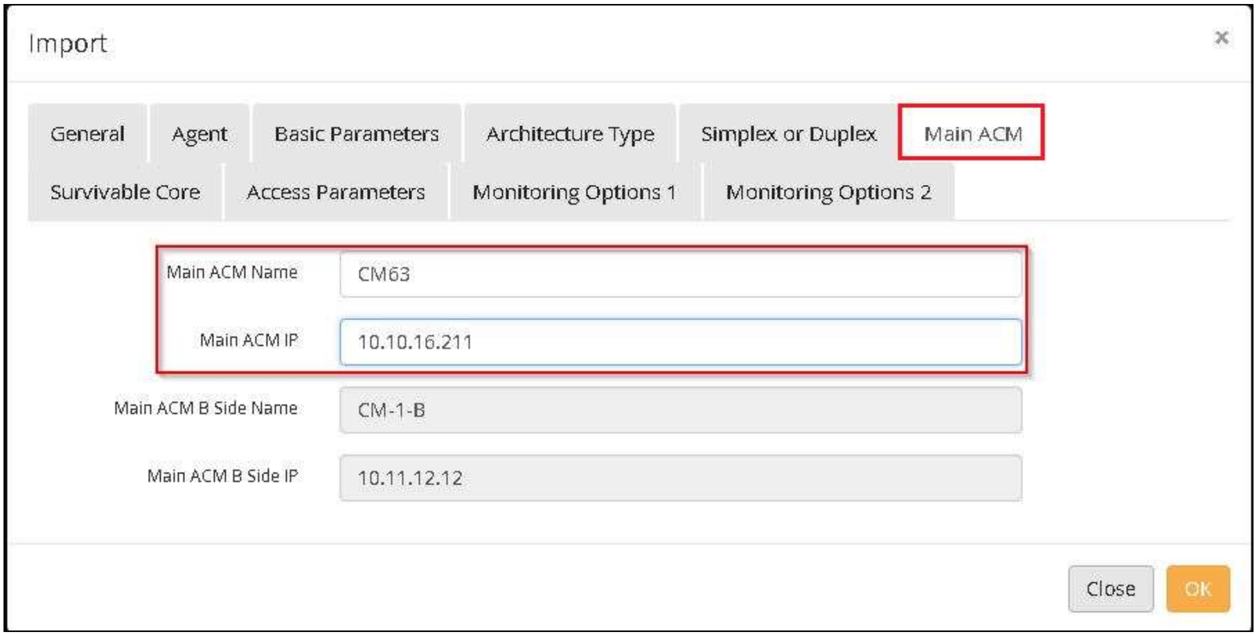
In the **Simplex or Duplex** tab select **No** from the **Duplex Main ACM?** Drop down list.



Duplex Main ACM?	No
Main ACM VIP	10.11.12.13
Duplex Survivable Core (ESS)?	No
Survivable Core (ESS) VIP	11.11.12.13

In the **Main ACM** tab enter the following:

- **Main ACM Name** Enter an informative name
- **Main ACM IP** Enter the IP address of Communication Manager



Main ACM Name: CM63

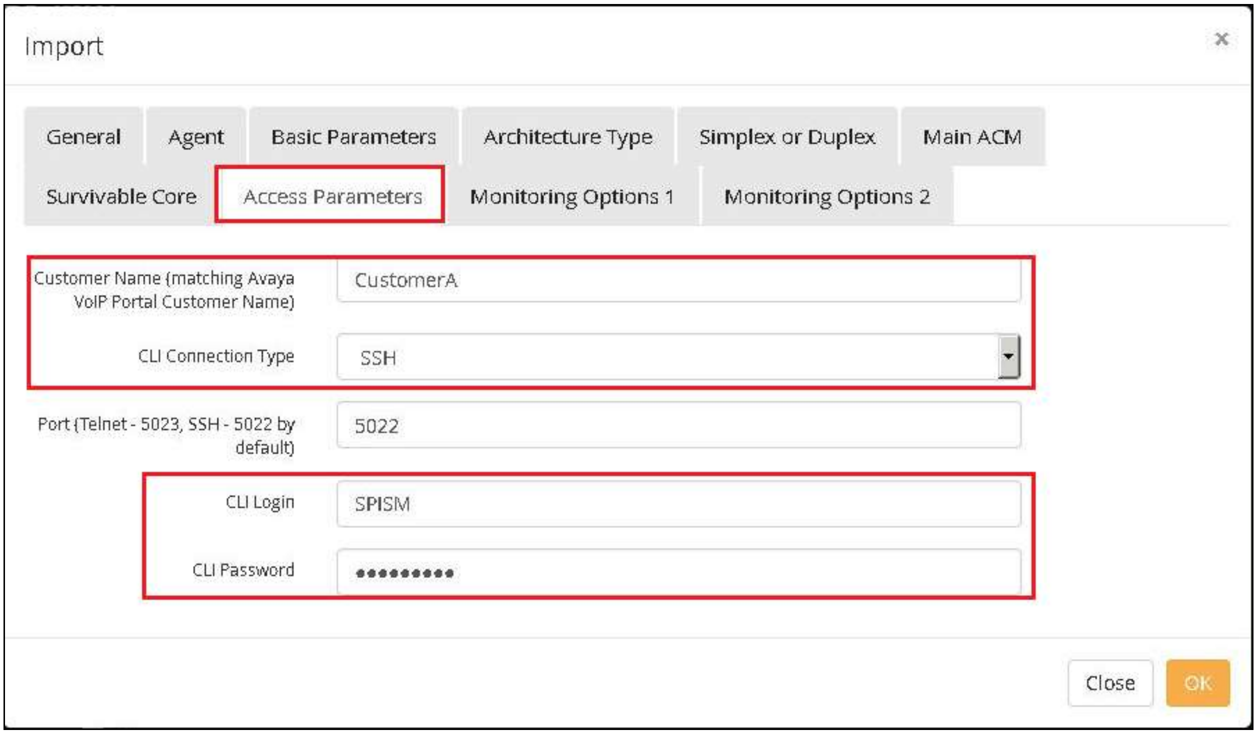
Main ACM IP: 10.10.16.211

Main ACM B Side Name: CM-1-B

Main ACM B Side IP: 10.11.12.12

In the **Access Parameters** tab enter the following:

• **Customer Name**	Enter an informative name
• **CLI Connection Type**	Select **SSH** from the drop down list
• **CLI Login**	Enter **SPISM** (as configured in **Section 6.3**)
• **CLI Password**	Enter the password as configured in **Section 6.3**



Customer Name (matching Avaya VoIP Portal Customer Name): CustomerA

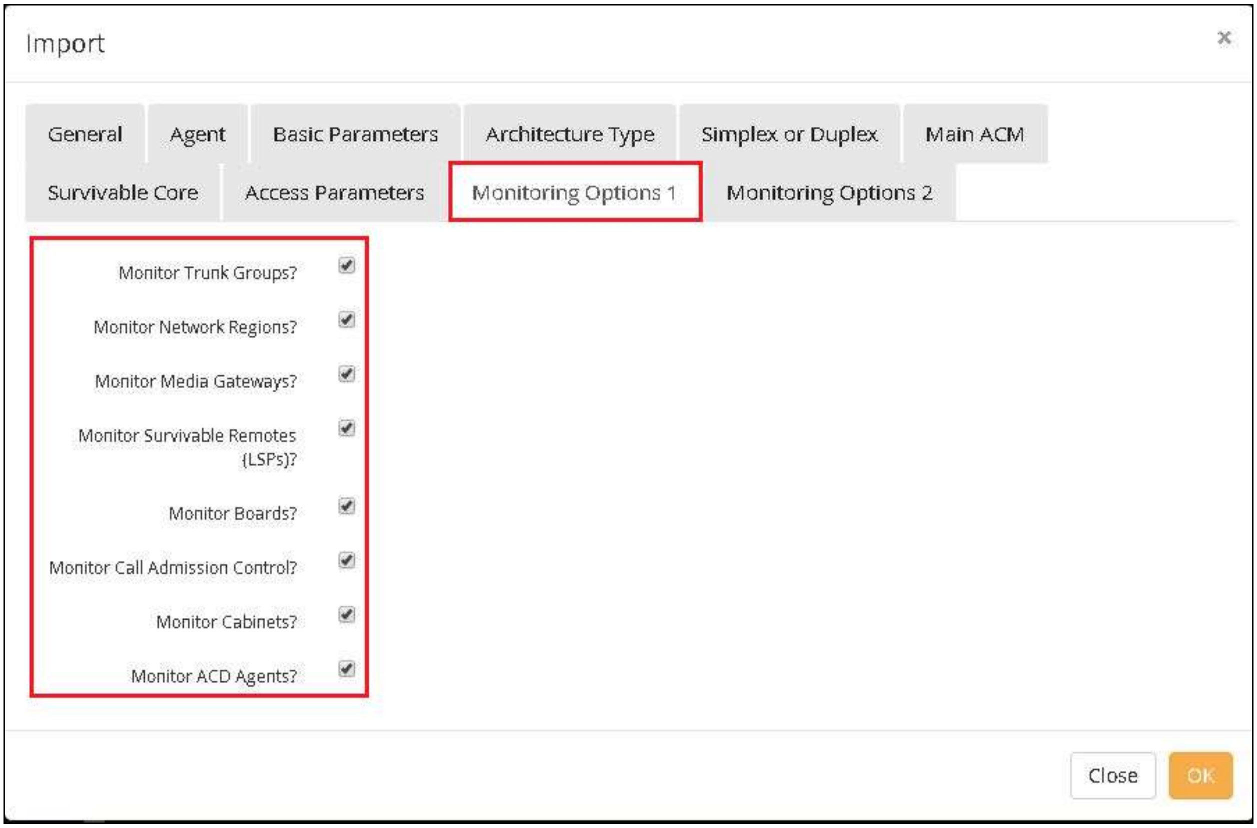
CLI Connection Type: SSH

Port (Telnet - 5023, SSH - 5022 by default): 5022

CLI Login: SPISM

CLI Password: ●●●●●●●●●

In the **Monitoring Options 1** tab, tick all the check boxes as shown below.



Monitor Trunk Groups? ☑

Monitor Network Regions? ☑

Monitor Media Gateways? ☑

Monitor Survivable Remotes (LSPs)? ☑

Monitor Boards? ☑

Monitor Call Admission Control? ☑

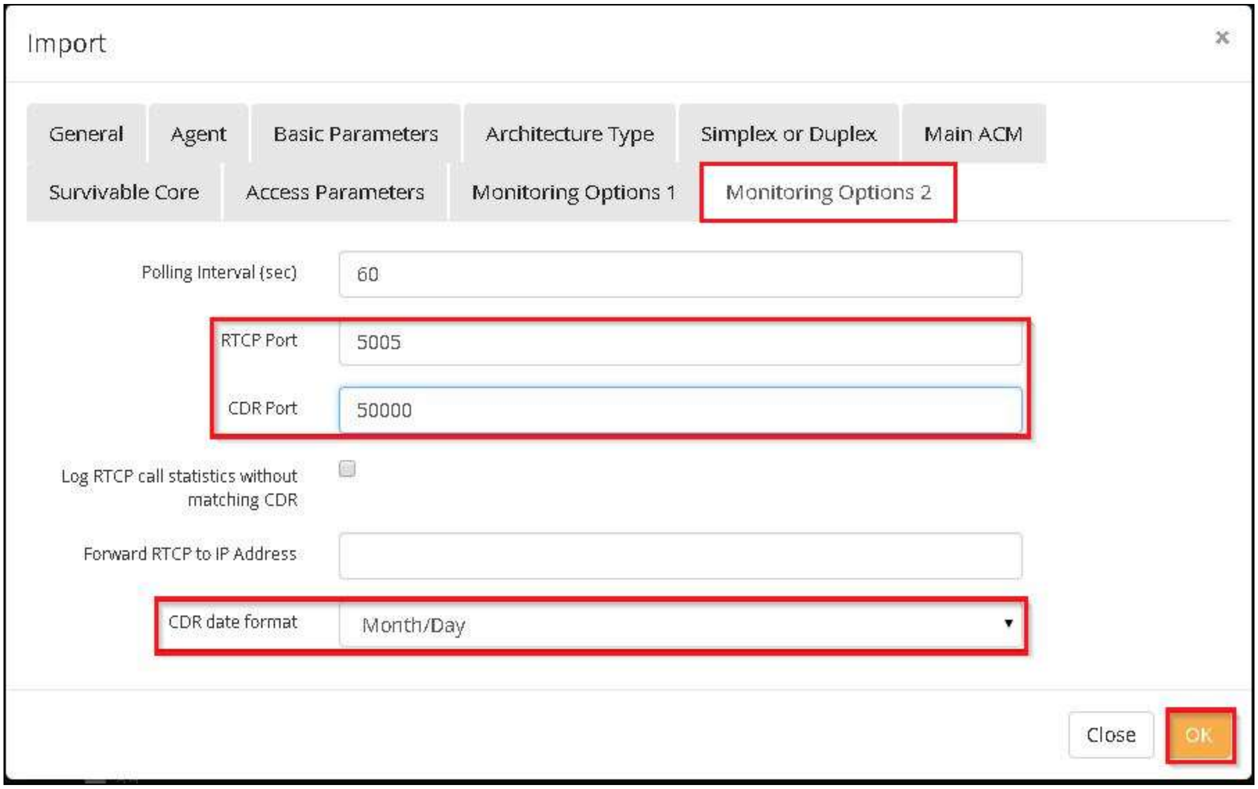
Monitor Cabinets? ☑

Monitor ACD Agents? ☑

In the **Monitoring Options 2** tab enter the following:

- **RTCP Port** Enter **5005** as configured in **Section 6.5**
- **CDR Port** Enter **50000** as configured in **Section 6.6**
- **CDR date format** select **month/Day** from the drop down list

Click on the **OK** button to save the configuration in the editor.



Import

Polling Interval (sec): 60

RTCP Port: 5005

CDR Port: 50000

Log RTCP call statistics without matching CDR: □

Forward RTCP to IP Address:

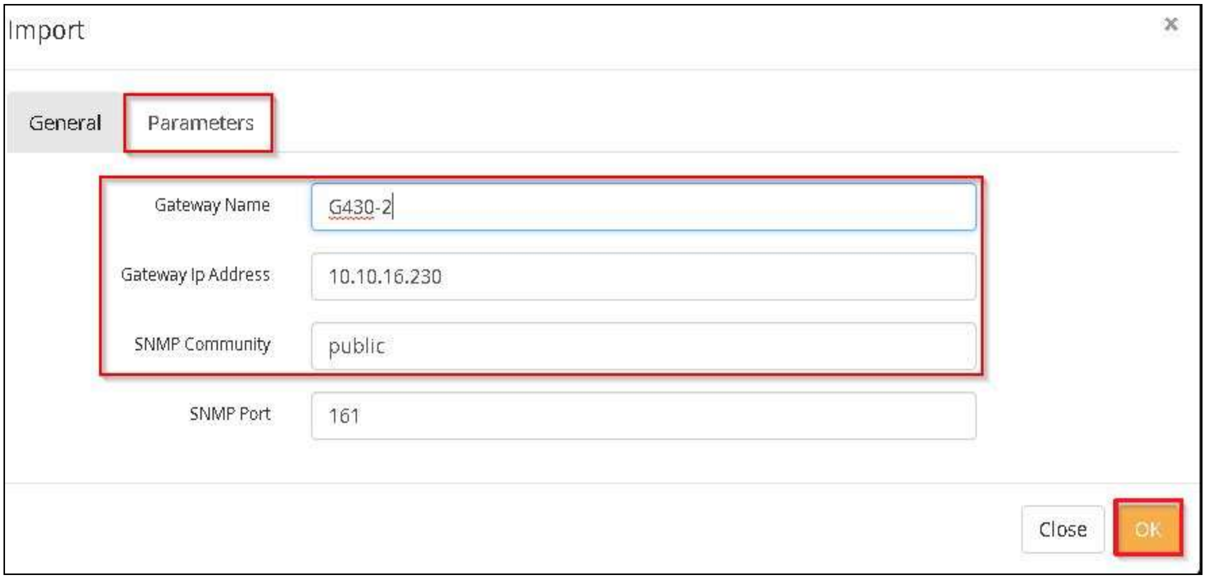
CDR date format: Month/Day

11.4. Configure Media Gateway PACKAGE

To configure the Media Gateway PACKAGE scroll down in the built in configuration editor window, and right click on the **import** button relating to **PACKAGE : MGW-1** (not shown). When the **import** window opens click on the **Parameters** tab and enter the following:

- **Gateway Name** Enter an informative name
- **Gateway Ip Address** Enter the IP address of the Media Gateway
- **SNMP Community** Enter **public** as configured in **Section 6.4**

Click on the **OK** button to save the configuration in the editor.


Import

Gateway Name: G430-2

Gateway Ip Address: 10.10.16.230

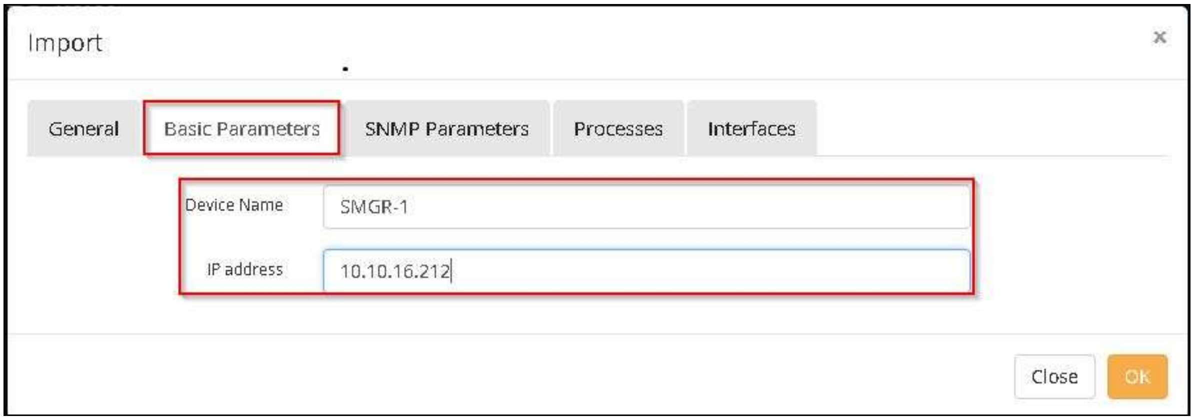
SNMP Community: public

SNMP Port: 161

11.5. Configure System Manager PACKAGE

To configure the System Manager PACKAGE scroll down in the built in configuration editor window, and right click on the **import** button relating to **PACKAGE : SMGR-1** (not shown). When the **import** window opens click on the **Basic Parameters** tab and enter the following:

• **Device Name**	Enter an informative name
• **IP Address**	Enter the IP address of the System Manager



Import

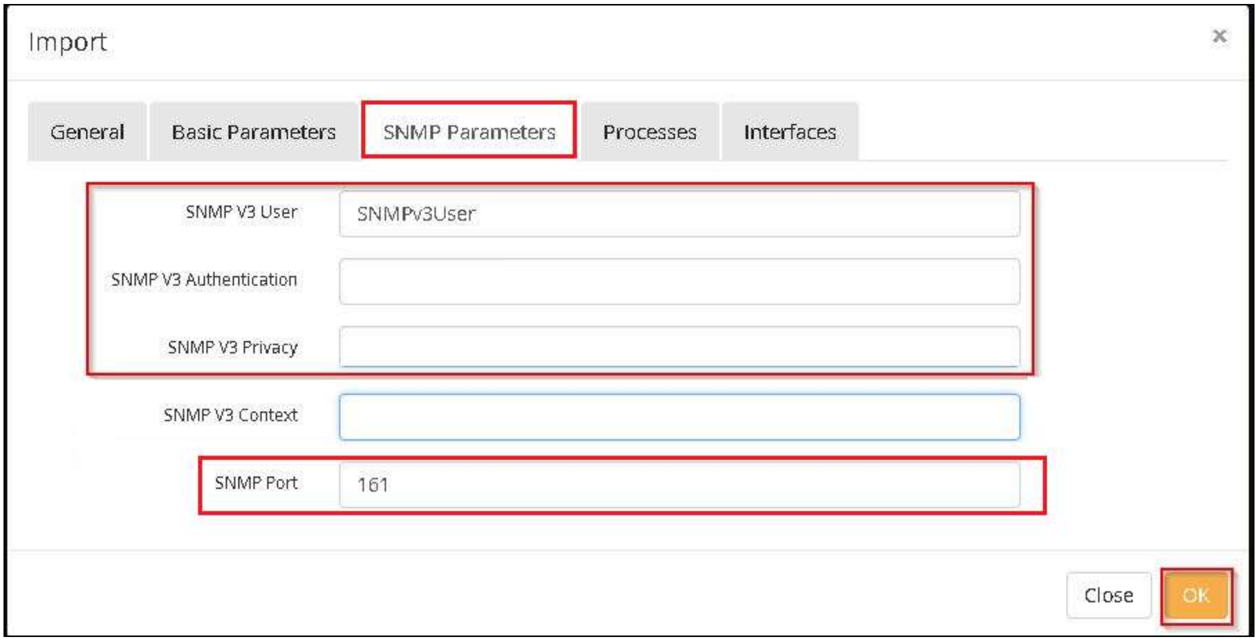
Device Name: SMGR-1

IP address: 10.10.16.212

In the **SNMP Parameters** tab enter the following:

- **SNMP V3 User** Enter **SNMPv3User** as configured in **Section 8.1**
- **SNMP V3 Authentication** Enter **Authentication** password as configured in **Section 8.1**
- **SNMP V3 Privacy** Enter the **Privacy** password as configured in **Section 8.1**
- **SNMP Port** Enter **161**

Click on the **OK** button to save the configuration in the editor.



SNMP V3 User: SNMPv3User

SNMP V3 Authentication:

SNMP V3 Privacy:

SNMP V3 Context:

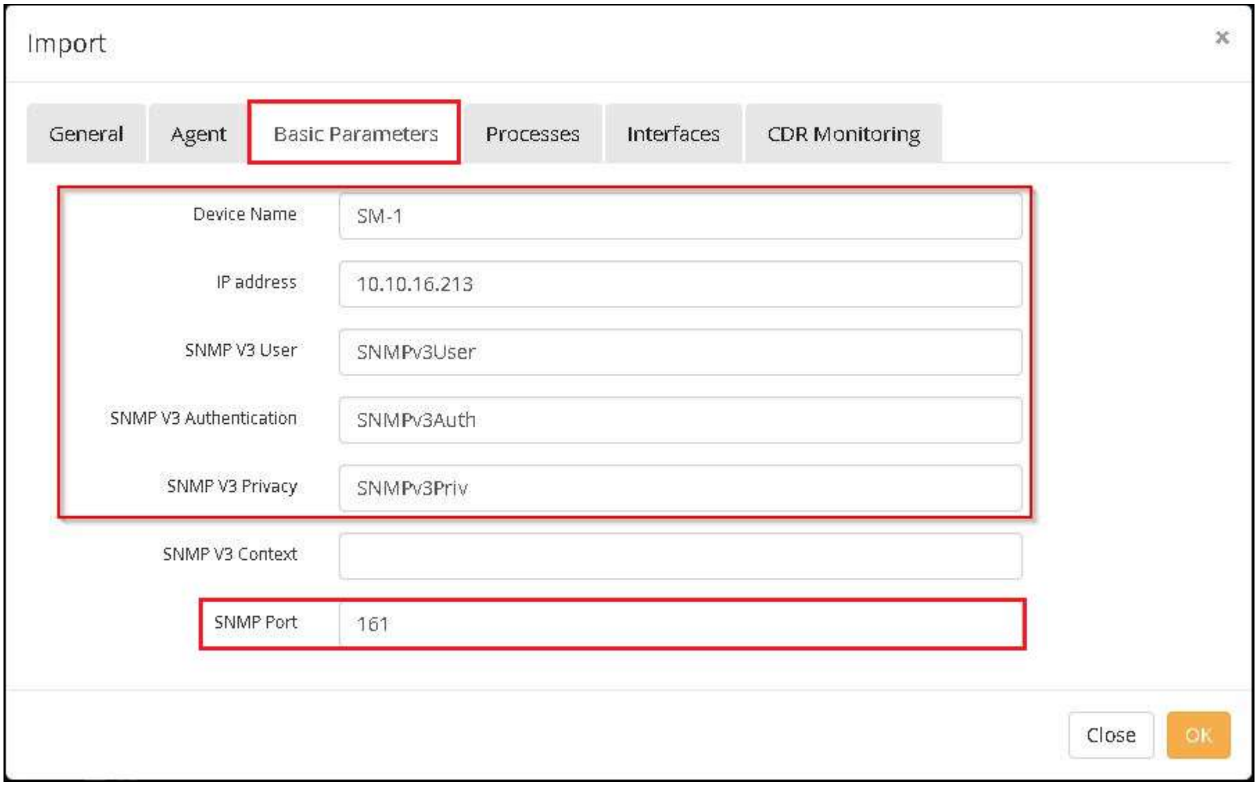
SNMP Port: 161

11.6. Configure Session Manager PACKAGE

To configure the Session Manager PACKAGE scroll down in the built in configuration editor window, and right click on the **import** button relating to **PACKAGE : SM-1** (not shown). When the **import** window opens click on the **Basic Parameters** tab and enter the following:

• **Device Name**	Enter an informative name
• **IP Address**	Enter the IP address of the Session Manager
• **SNMP V3 User**	Enter **SNMPv3User** as configured in **Section 8.1**
• **SNMP V3 Authentication**	Enter **Authentication** password as configured in **Section 8.1**
• **SNMP V3 Privacy**	Enter the **Privacy** password as configured in **Section 8.1**
• **SNMP Port**	Enter **161**

Click on the **OK** button to save the configuration in the editor.

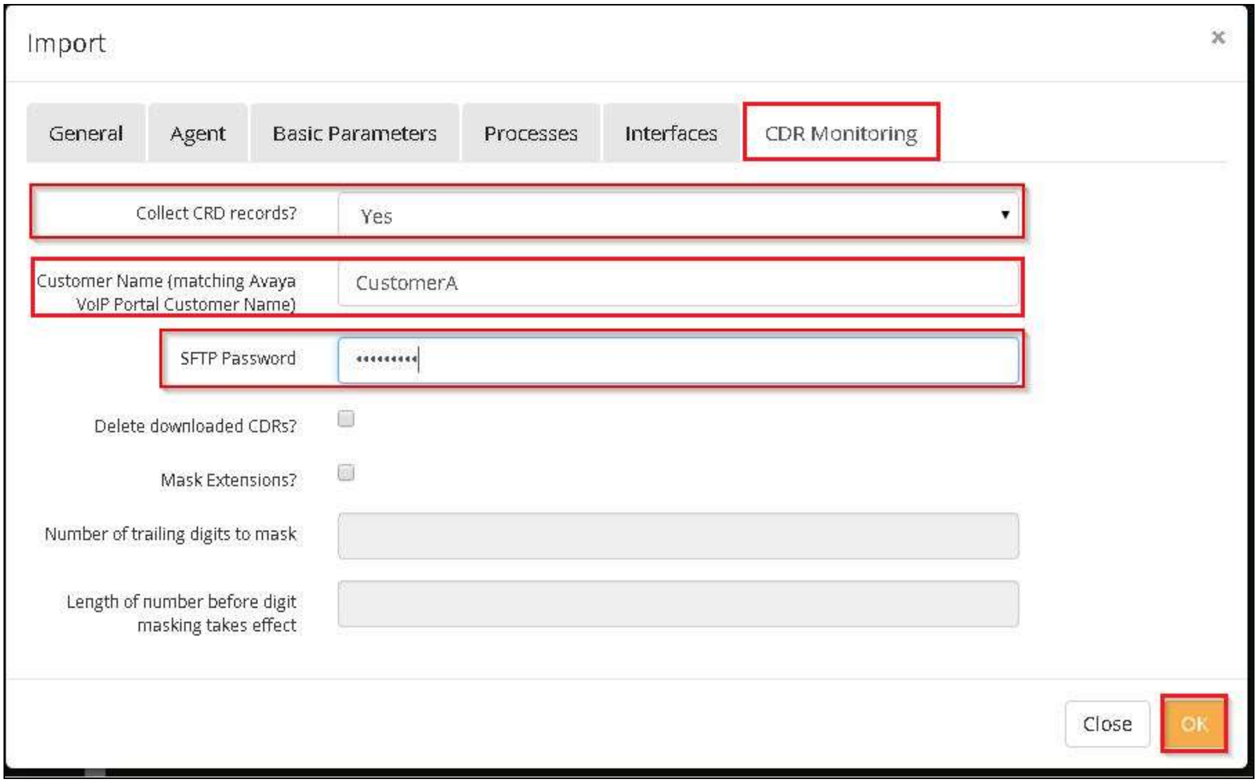


Device Name: SM-1
IP address: 10.10.16.213
SNMP V3 User: SNMPv3User
SNMP V3 Authentication: SNMPv3Auth
SNMP V3 Privacy: SNMPv3Priv
SNMP V3 Context:
SNMP Port: 161

In the **CDR monitoring** tab enter the following:

- **Customer Name** Enter an informative name
- **Collect CRD records** Select **Yes** from the drop down list
- **SFTP Password** Enter the password as configured in **Section 9.2**

Click on the **OK** button to save the configuration in the editor.



Import

Collect CRD records? Yes

Customer Name (matching Avaya VoIP Portal Customer Name) CustomerA

SFTP Password •••••••••

Delete downloaded CDRs? □

Mask Extensions? □

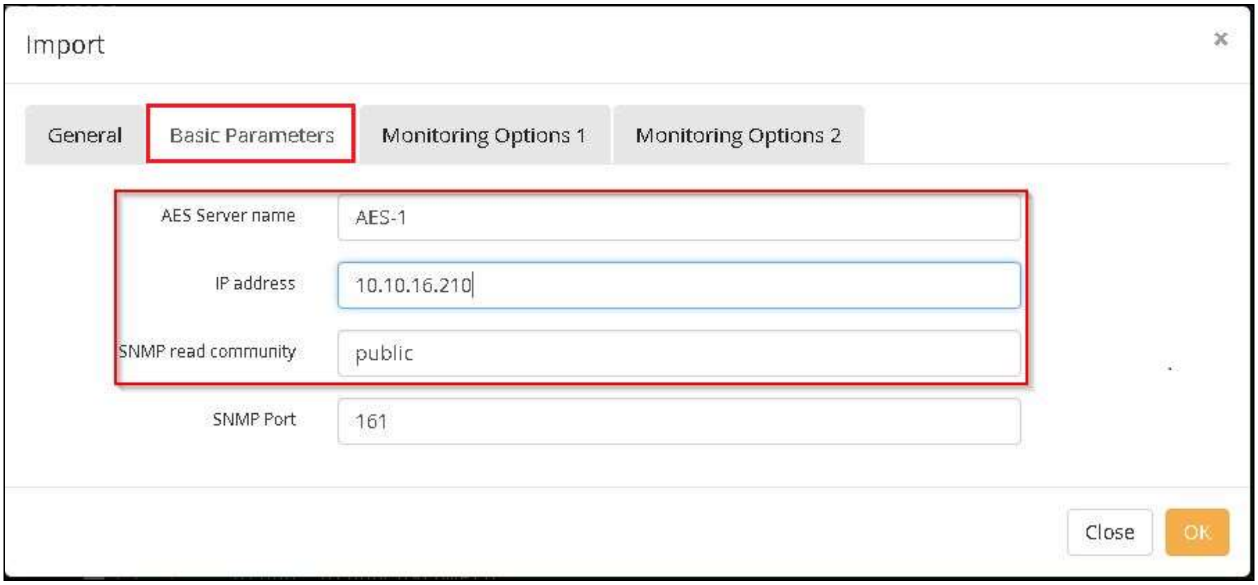
Number of trailing digits to mask

Length of number before digit masking takes effect

11.7. Configure Application Enablement Services PACKAGE

To configure the Application Enablement Services PACKAGE scroll down in the built in configuration editor window, and right click on the **import** button relating to **PACKAGE : AES-1** (not shown). When the **import** window opens click on the **Basic Parameters** tab and enter the following:

AES Server Name	Enter an informative name
IP Address	Enter the IP address of the AES
SNMP read community	Enter **public**



AES Server name: AES-1

IP address: 10.10.16.210

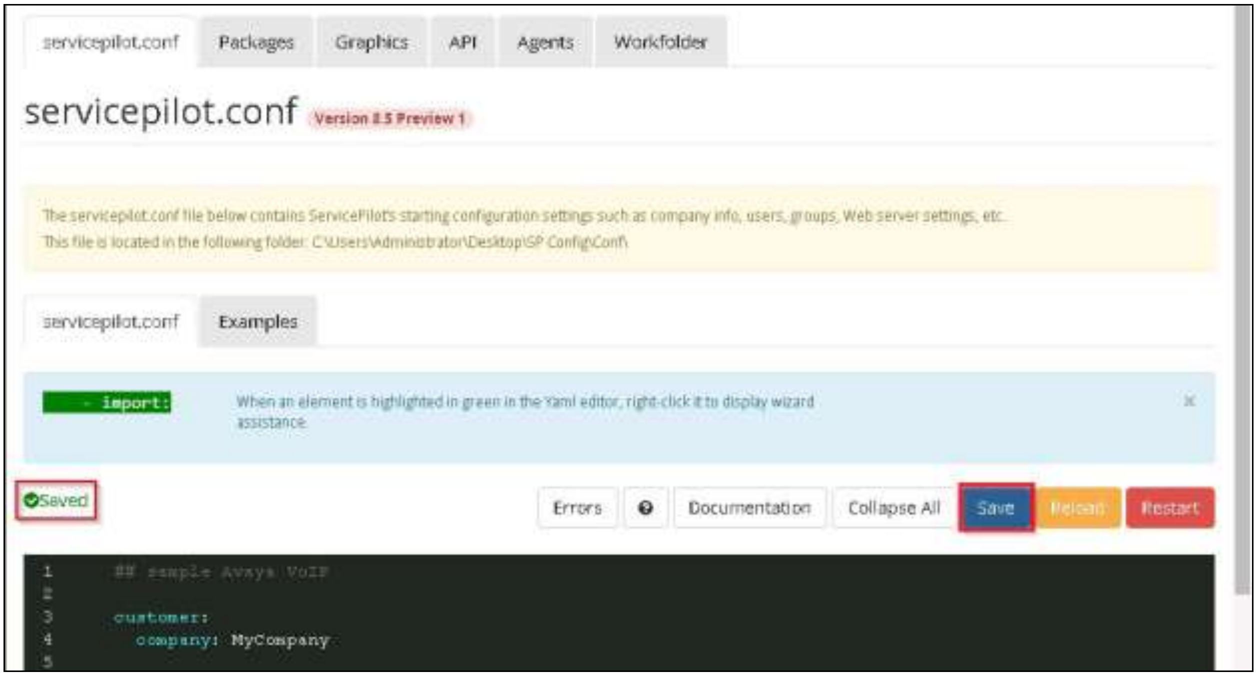
SNMP read community: public

SNMP Port: 161

In the **Monitoring Options 1** and **Monitoring Options 2** tabs tick all the available check boxes (not shown). Click on the **OK** button to save the configuration in the editor.

11.8. Save the servicepilot.conf configurations

After all the servicepilot.conf configurations are complete click on the **Save** button.



The servicepilot.conf file below contains ServicePilot's starting configuration settings such as company info, users, groups, Web server settings, etc.
This file is located in the following folder: C:\Users\Administrator\Desktop\SP Config\Conf\

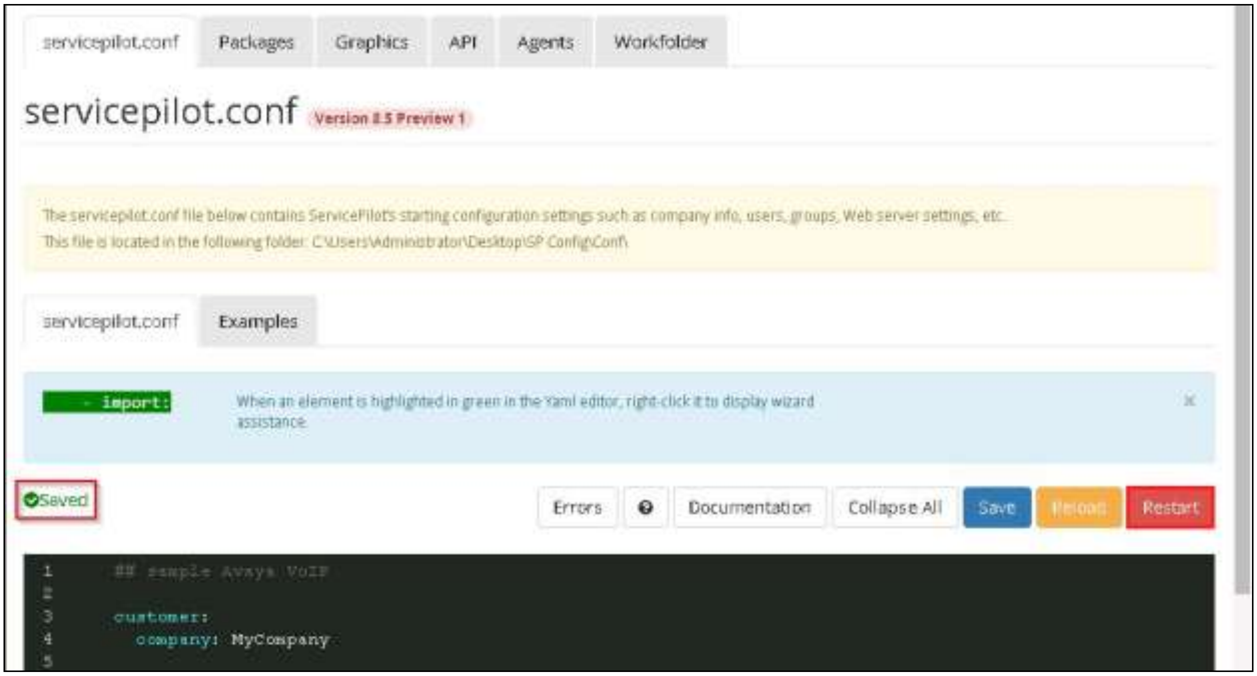
When an element is highlighted in green in the Yaml editor, right-click it to display wizard assistance.

```
## sample Avaya VoIP

customer:
  company: MyCompany
```

11.9. Restart ServicePilot ISM

Once the configurations are saved a restart of ServicePilot ISM is required. Click on the **Restart** button to initiate the restart.



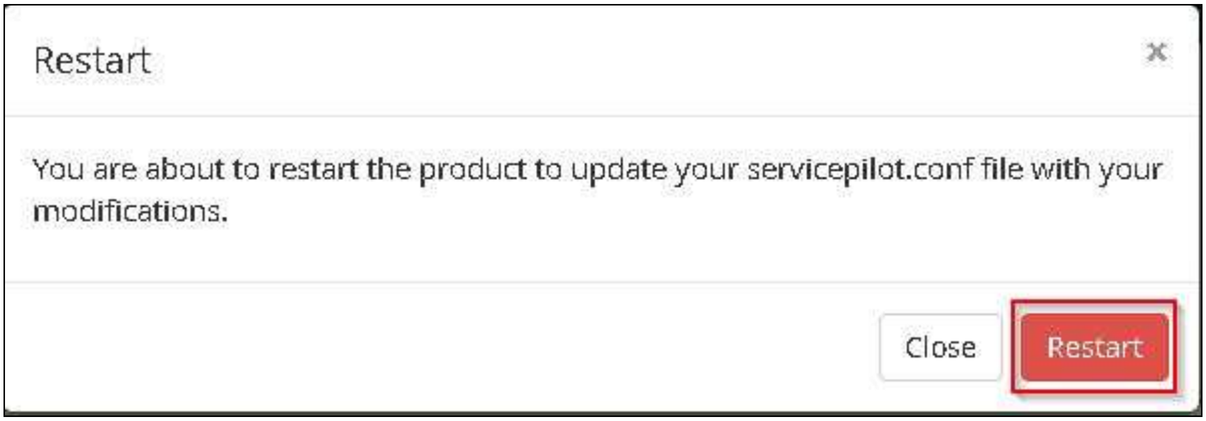
The servicepilot.conf file below contains ServicePilot's starting configuration settings such as company info, users, groups, Web server settings, etc.
This file is located in the following folder: C:\Users\Administrator\Desktop\SP Config\Conf\

When an element is highlighted in green in the Yaml editor, right-click it to display wizard assistance.

```
## sample Avaya VoIP

customer:
  company: MyCompany
```

Confirm the restart by clicking on the **Restart** button.



Restart

You are about to restart the product to update your servicepilot.conf file with your modifications.

12. Verification Steps

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

12.1. 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

 acpsnmp     17                                                          1
                     127.0.0.1
*init        0                         stat logins                       3
                     192.168.100.18
 SPISM       21                                                          4
                     10.10.16.223
 SPISM       21                                                          5
                     10.10.16.223
```

12.2. Verify the 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**.

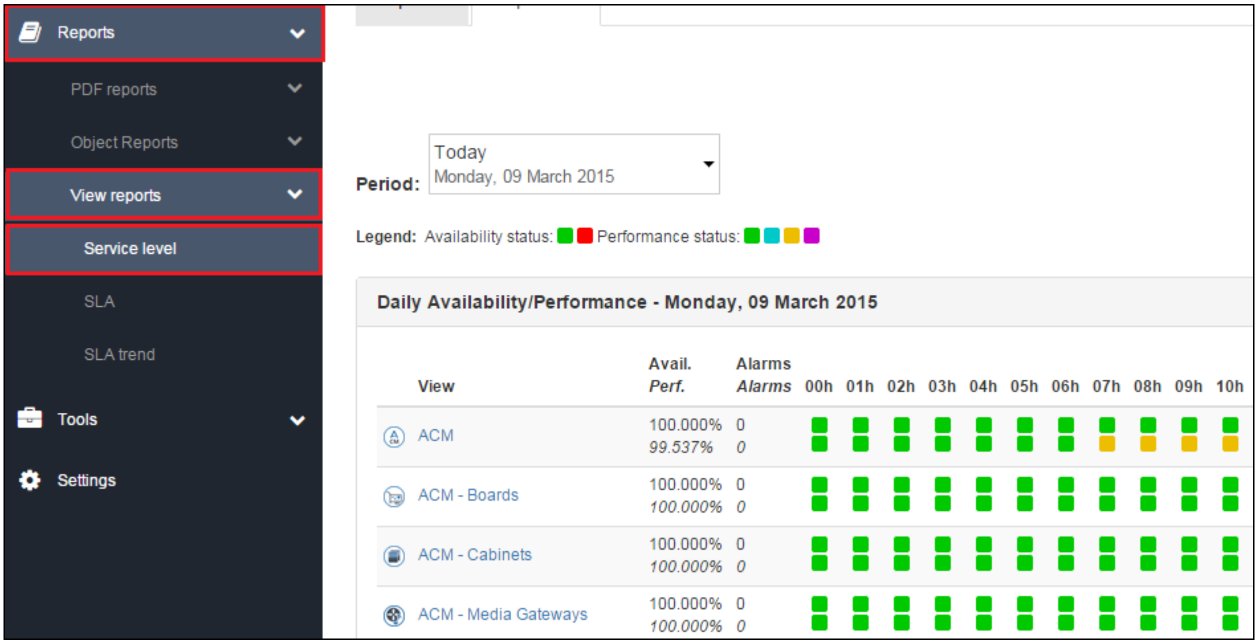
```
status cdr-link
                                CDR LINK STATUS
                   Primary                        Secondary

       Link State: up                             CDR not administered

      Date & Time: 2015/02/05 19:04:59            0000/00/00 00:00:00
  Forward Seq. No: 0                              0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                           0.00
      Reason Code: OK
```

12.3. Verify ServicePilot ISM

On the ServicePilot ISM 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 states show **red** then equipment is unreachable for monitoring purposes.



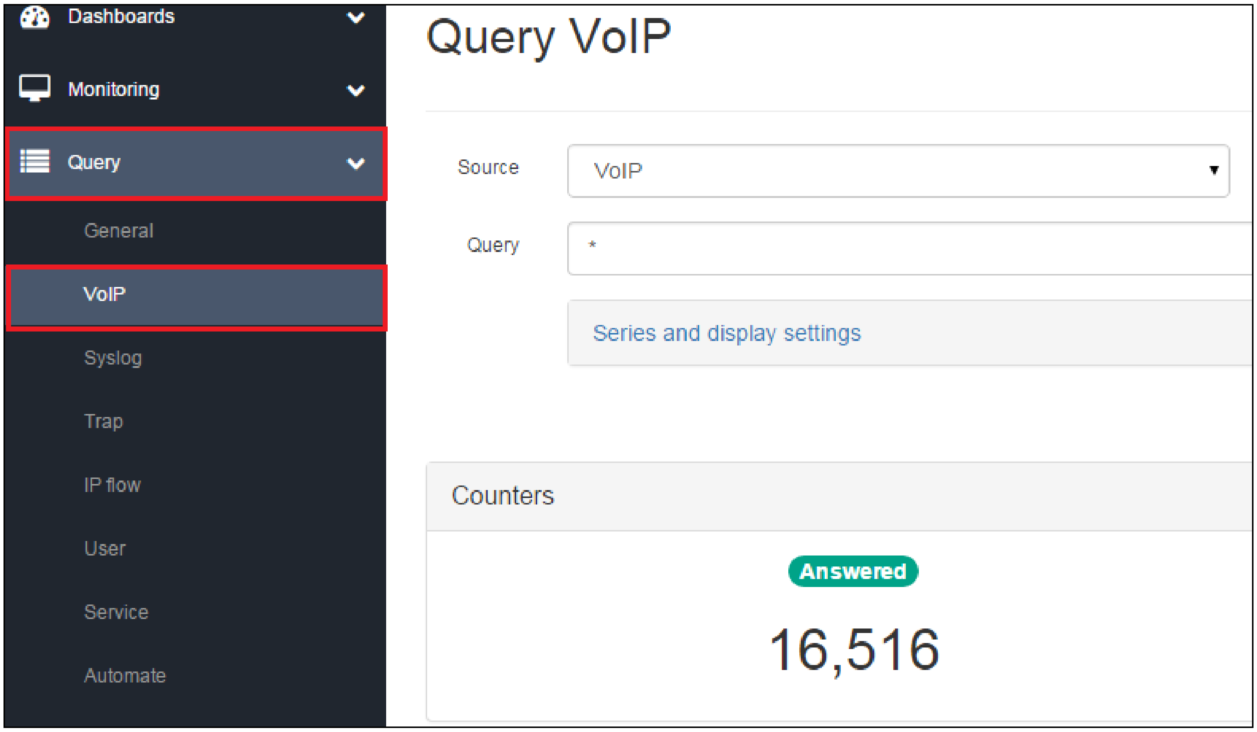
Period: Today
Monday, 09 March 2015

Legend: Availability status: 🟩🟥 Performance status: 🟩🟦🟨🟪

Daily Availability/Performance - Monday, 09 March 2015

View	Avail. *Perf.*	Alarms *Alarms*	00h	01h	02h	03h	04h	05h	06h	07h	08h	09h	10h
ACM	100.000% *99.537%*	0 *0*	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟨	🟩 🟨	🟩 🟨	🟩 🟨
ACM - Boards	100.000% *100.000%*	0 *0*	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩
ACM - Cabinets	100.000% *100.000%*	0 *0*	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩
ACM - Media Gateways	100.000% *100.000%*	0 *0*	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩

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.



Query VoIP

Source: VoIP

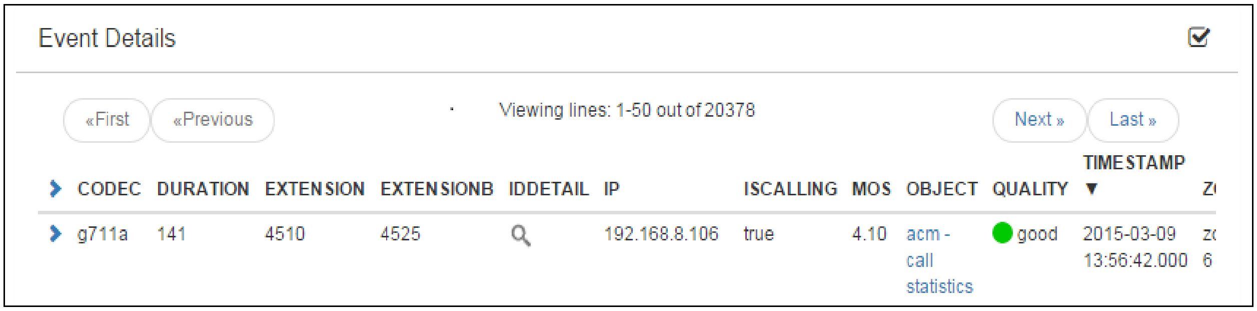
Query: *

Counters

Answered

16,516

Below is an example of a call detail with call quality detail link.



Event Details

Viewing lines: 1-50 out of 20378

	CODEC	DURATION	EXTENSION	EXTENSIONB	IDDETAIL	IP	ISCALLING	MOS	OBJECT	QUALITY	TIMESTAMP ▼	Z(
›	g711a	141	4510	4525	🔍	192.168.8.106	true	4.10	acm - call statistics	● good	2015-03-09 13:56:42.000	zc 6

13. Conclusion

These Application Notes describe the steps required to configure ServicePilot ISM to interoperate with Avaya Aura® Communication Manager, Avaya G430 Media Gateway, Avaya Aura® Session 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**.

14. 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 6.3, June 2014, Document Number 03-300509, Issue 10.

[2] Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.3, December 2014, Document Number 555-245-205, Issue 14.0.

[3] Administering Avaya Aura® Session Manager, Release 6.3, Issue 7 September 2014

[4] Administering Avaya Aura® System Manager, Release 6.3, Issue 5, October, 2014

[5] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.3 Document Number 02-300357 June 2014

[6] Administering Avaya G430 Branch Gateway R6.3, Issue 5 October 2013

ServicePilot ISM documentation can be obtained directly from the ServicePilot website http://www.servicepilot.com or contacting the ServicePilot Support Team (see Section 2.3 for contact details).

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.