



Avaya Solution & Interoperability Test Lab

Application Notes for ServicePilot ISM 8.3.1 with Avaya Aura® Communication Manager 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring ServicePilot ISM 8.3.1 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.

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 8.3.1 with Avaya Aura® Communication Manager 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 the Avaya Server. 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 Avaya IP Media Processor (MEDPRO) boards, media gateways, and IP 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 and its gateways.
- Call Detail Recording (CDR) Collection - ServicePilot ISM collects CDR information sent by Communication Manager.

2. General Test Approach and Test Results

The general test approach was to use ServicePilot ISM web interface to display the configurations of the Communication Manager systems and verify against what is displayed on the SAT interface. The SAT interface is accessed by using either telnet or Secure Shell (SSH) to the Avaya S8800 and S8300D Servers. Calls were placed between various Avaya endpoints and ServicePilot ISM web interface was used to display the RTCP and CDR information collected via the Call logs.

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.

2.1. Interoperability Compliance Testing

For feature testing, ServicePilot ISM web interface was used to view the configurations of Communication Manager such as port networks, cabinets, media gateways, ESS, LSP, trunk groups, route patterns, CLAN, MEDPRO and DS1 boards, IP network regions, stations, processor occupancy, alarm and error information. For the collection of RTCP and CDR information, the endpoints included Avaya H323, SIP, digital and analog telephones, and Avaya one-X® Communicator users. 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 ISM Server and Avaya Servers to simulate system unavailability. Interchanging of the Avaya S8800 Servers and failover to ESS and LSP were also performed during testing.

2.2. Test Results

All test cases passed successfully with the following observations:

The following CDR formats are supported:

- a. Expanded
- b. Enhanced Expanded
- c. Unformatted
- d. Enhanced Unformatted

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. It consists of a Communication Manager system running on a pair of Avaya S8800 Servers with one Avaya G650 Media Gateway, an Avaya G430 Media Gateway with Avaya S8300D Server as a Local Survivability Processor (LSP) and an Avaya G250-BRI Media Gateway. An Enterprise Survivable Server (ESS) running on VMware was also configured for failover testing. A second Communication Manager system runs on an Avaya S8300D Server with an Avaya G450 Media Gateway. Both systems have Avaya IP, digital and analog telephones, and Avaya one-X[®] Communicator users configured for making and receiving calls. IP Trunks connect the two systems together to allow calls between them. Avaya Aura[®] System Manager and Avaya Aura[®] Session Manager provided SIP support to the Avaya SIP telephones. ServicePilot ISM was installed on a server running Microsoft Windows Server 2008 R2 with Service Pack 1. The Avaya 4548GT-PWR Ethernet Routing Switch provides Ethernet connectivity to the servers, media gateways and IP telephones.

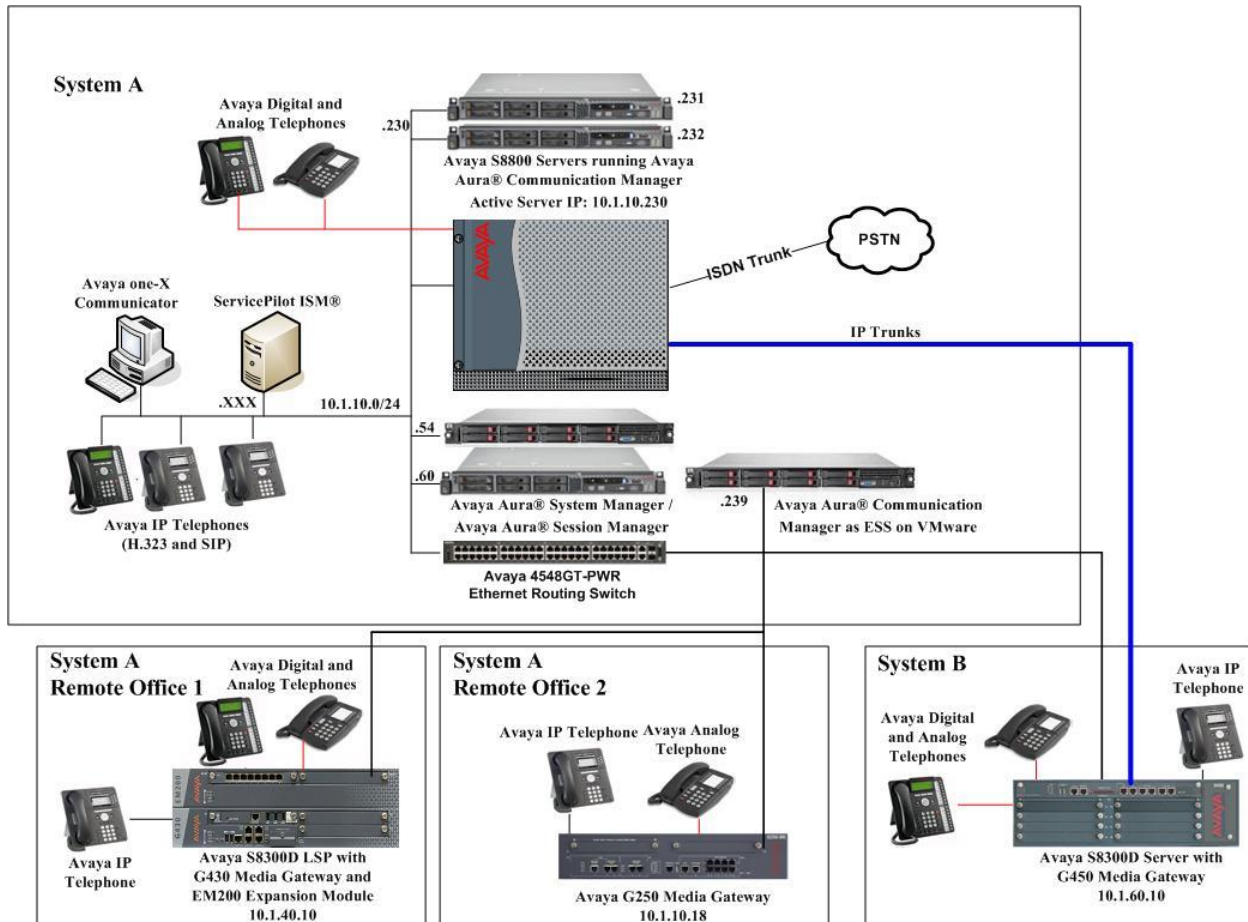


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Servers (System A)	6.3 SP 2.1
G650 Media Gateway - TN2312BP IP Server Interface - TN799DP C-LAN Interface (x 4) - TN2602AP IP Media Processor (x 2) - TN2302AP IP Media Processor (x 2) - TN2464BP DS1 Interface - TN2464CP DS1 Interface - TN793CP Analog Line - TN2214CP Digital Line	HW07, FW057 HW01, FW040 HW02 FW063 and HW02 FW063 HW20 FW121 and HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW011 HW08, FW015
G250 Media Gateway	30.27.1
Avaya Aura® Communication Manager running on Avaya S8300D Server (System B)	6.3 SP 2.1
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	34.5.1 HW01 FW008 HW07 FW014 HW10 FW098 HW03 FW014 HW11 FW052
Avaya Aura® Communication Manager running on Avaya S8300D Server (G430 Media Gateway - LSP)	6.3 SP 2.1
G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	34.5.1 HW07 FW014 HW12 FW098 HW31 FW098 HW05 FW022
Avaya Aura® Communication Manager running on VMware 5.0 (ESS)	6.3 SP 2.1
HP DL360 G7 running Avaya Aura® System Manager	6.3 SP4
Avaya S8800 Server running Avaya Aura® Session Manager	6.2 SP4

Equipment/Software	Release/Version
96xx Series IP Telephones - 9640G - 9620	3.2 (H323) or 2.6 SP10 (SIP)
96x1 Series IP Telephones - 9641G - 9611G	6.3 (H.323) or 6.2.2 (SIP)
1600 Series IP Telephones - 1616 - 1603SW	1.34 (H.323)
Digital Telephones - 1416 - 1408	SP1
Avaya Analog Phones	-
Desktop PC with Avaya one-X Communicator	6.1 SP8 (H.323)
Avaya 4548GT-PWR Ethernet Routing Switch	V5.6.1.052
ServicePilot ISM on Windows 2008 R2 SP1	8.3.1

5. Configure Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with ServicePilot ISM. This includes creating a login account and a SAT User Profile for ISM to access Communication Manager, enabling RTCP and CDR reporting and setting up SNMP. The steps are repeated for each Communication Manager system, ESS and LSP Servers. SNMP setup is also required for gateways.

5.1. Configure SAT User Profile

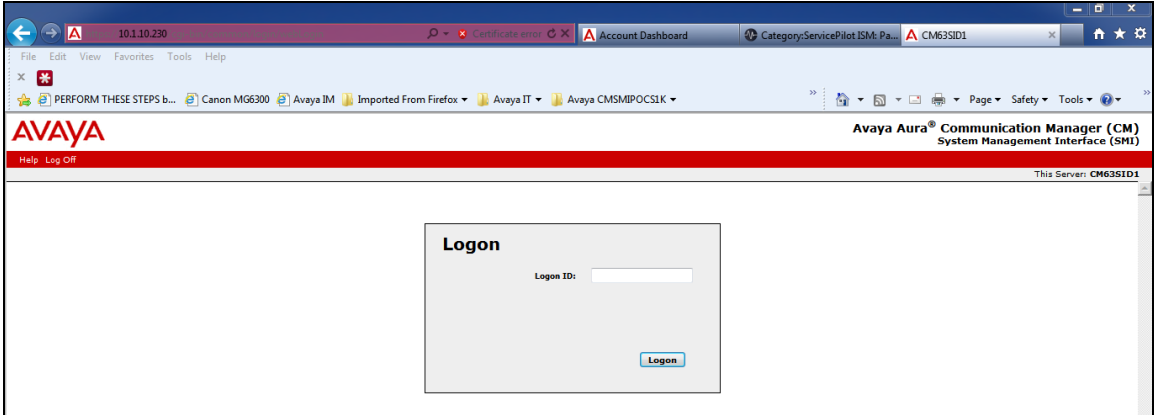
A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As ServicePilot ISM does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the ServicePilot ISM login account.

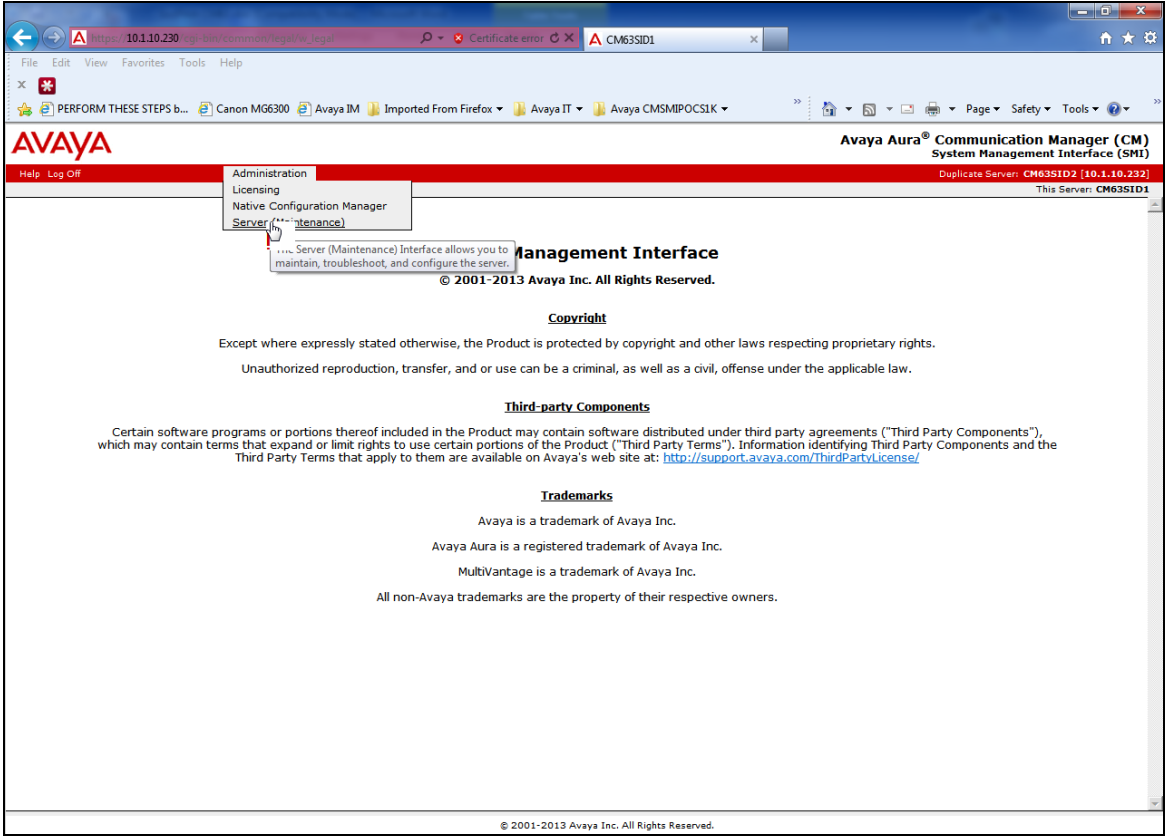
Step	Description																																																												
1.	Enter the add user-profile <i>n</i> command, where <i>n</i> is the next unused profile number. Enter a descriptive name for User Profile Name and enable all categories by setting the Enbl field to y . In this test configuration, the user profile 23 is created.																																																												
<div>add user-profile 23<div>Page1 of 41</div></div> <div>USER PROFILE 23</div> <div>User Profile Name: SPISM</div> <div>This Profile is Disabled? nShell Access? nFacility Test Call Notification? nAcknowledgement Required? nGrant Un-owned Permissions? nExtended Profile? n</div> <div><table><thead><tr><th>Name</th><th>Cat</th><th>Enbl</th><th>Name</th><th>Cat</th><th>Enbl</th></tr></thead><tbody><tr><td>Adjuncts</td><td>A</td><td>y</td><td>Routing and Dial Plan</td><td>J</td><td>y</td></tr><tr><td>Call Center</td><td>B</td><td>y</td><td>Security</td><td>K</td><td>y</td></tr><tr><td>Features</td><td>C</td><td>y</td><td>Servers</td><td>L</td><td>y</td></tr><tr><td>Hardware</td><td>D</td><td>y</td><td>Stations</td><td>M</td><td>y</td></tr><tr><td>Hospitality</td><td>E</td><td>y</td><td>System Parameters</td><td>N</td><td>y</td></tr><tr><td>IP</td><td>F</td><td>y</td><td>Translations</td><td>O</td><td>y</td></tr><tr><td>Maintenance</td><td>G</td><td>y</td><td>Trunking</td><td>P</td><td>y</td></tr><tr><td>Measurements and Performance</td><td>H</td><td>y</td><td>Usage</td><td>Q</td><td>y</td></tr><tr><td>Remote Access</td><td>I</td><td>y</td><td>User Access</td><td>R</td><td>y</td></tr></tbody></table></div>		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
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																																																								

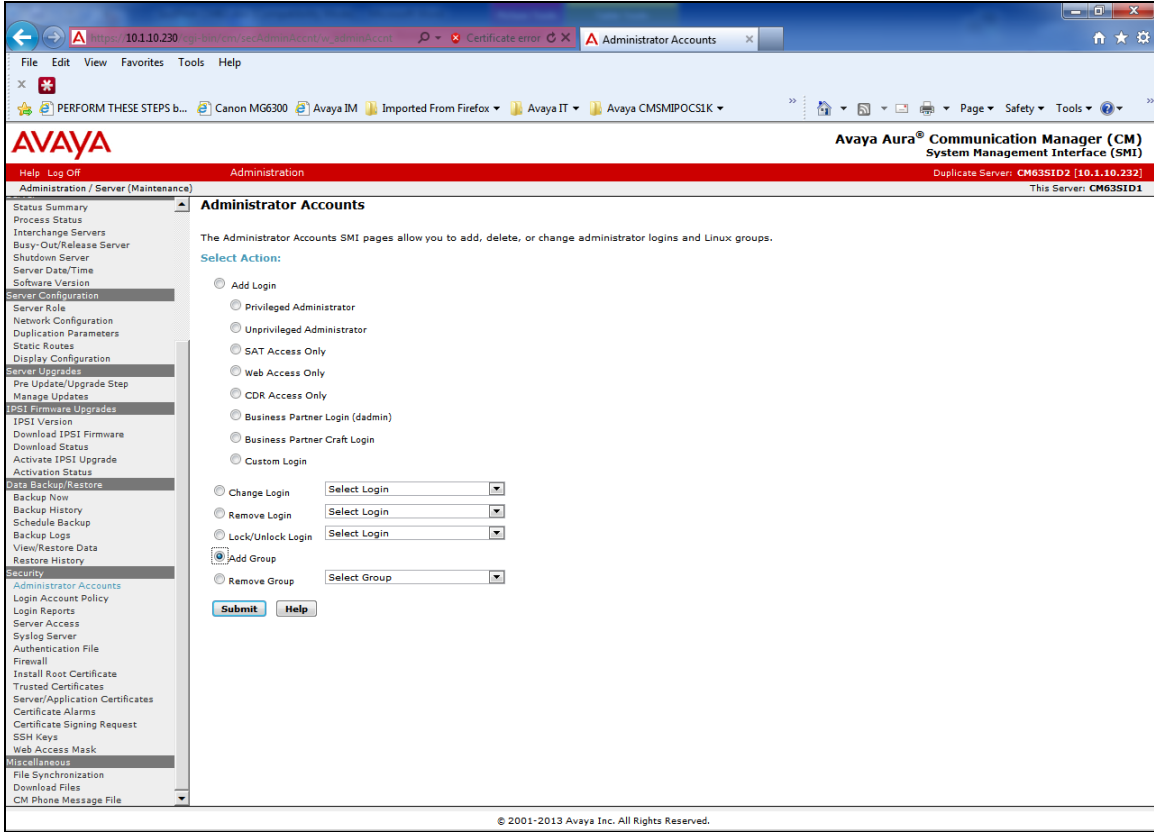
Step	Description																																													
2.	<p>On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to rm (read and maintenance). This can be accomplished by typing rm into the field Set All Permissions To. Submit the form to create the user profile.</p>																																													
	<div><div>add user-profile 23</div><div>Page 2 of 41</div></div> <div><div>USER PROFILE 23</div><div>Set Permissions For Category: To: Set All Permissions To: <div>rm</div></div><div>'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance</div><table><tr><th>Name</th><th>Cat</th><th>Perm</th></tr><tr><td>aar analysis</td><td>J</td><td><div>rm</div></td></tr><tr><td>aar digit-conversion</td><td>J</td><td><div>rm</div></td></tr><tr><td>aar route-chosen</td><td>J</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing 7103-buttons</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing enhanced</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing group</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing personal</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing system</td><td>C</td><td><div>rm</div></td></tr><tr><td>aca-parameters</td><td>P</td><td><div>rm</div></td></tr><tr><td>access-endpoints</td><td>P</td><td><div>rm</div></td></tr><tr><td>adjunct-names</td><td>A</td><td><div>rm</div></td></tr><tr><td>administered-connections</td><td>C</td><td><div>rm</div></td></tr><tr><td>aesvcs cti-link</td><td>A</td><td><div>rm</div></td></tr><tr><td>aesvcs interface</td><td>A</td><td><div>rm</div></td></tr></table></div>	Name	Cat	Perm	aar analysis	J	<div>rm</div>	aar digit-conversion	J	<div>rm</div>	aar route-chosen	J	<div>rm</div>	abbreviated-dialing 7103-buttons	C	<div>rm</div>	abbreviated-dialing enhanced	C	<div>rm</div>	abbreviated-dialing group	C	<div>rm</div>	abbreviated-dialing personal	C	<div>rm</div>	abbreviated-dialing system	C	<div>rm</div>	aca-parameters	P	<div>rm</div>	access-endpoints	P	<div>rm</div>	adjunct-names	A	<div>rm</div>	administered-connections	C	<div>rm</div>	aesvcs cti-link	A	<div>rm</div>	aesvcs interface	A	<div>rm</div>
Name	Cat	Perm																																												
aar analysis	J	<div>rm</div>																																												
aar digit-conversion	J	<div>rm</div>																																												
aar route-chosen	J	<div>rm</div>																																												
abbreviated-dialing 7103-buttons	C	<div>rm</div>																																												
abbreviated-dialing enhanced	C	<div>rm</div>																																												
abbreviated-dialing group	C	<div>rm</div>																																												
abbreviated-dialing personal	C	<div>rm</div>																																												
abbreviated-dialing system	C	<div>rm</div>																																												
aca-parameters	P	<div>rm</div>																																												
access-endpoints	P	<div>rm</div>																																												
adjunct-names	A	<div>rm</div>																																												
administered-connections	C	<div>rm</div>																																												
aesvcs cti-link	A	<div>rm</div>																																												
aesvcs interface	A	<div>rm</div>																																												

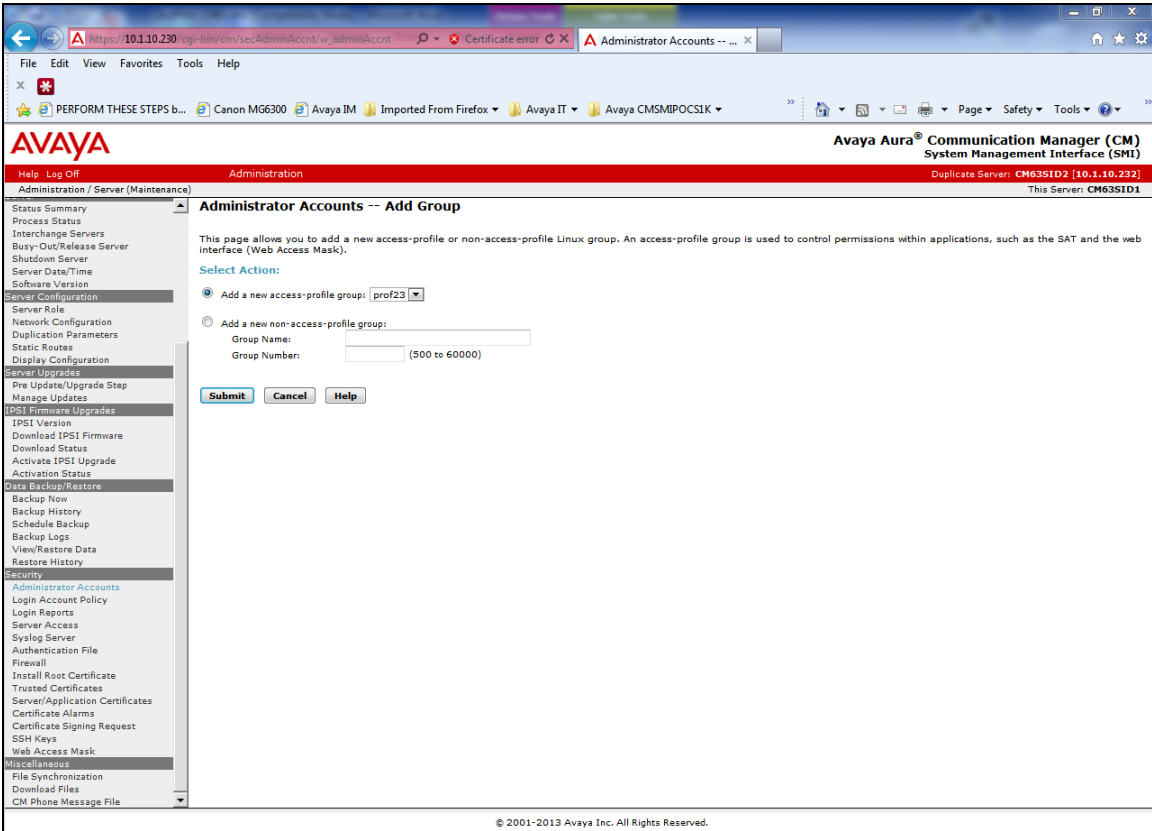
5.2. Configure Login Group

Create an Access-Profile Group on Communication Manager SMI to correspond to the SAT User Profile created in **Section 5.1**.

Step	Description
1.	<p>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.</p> 

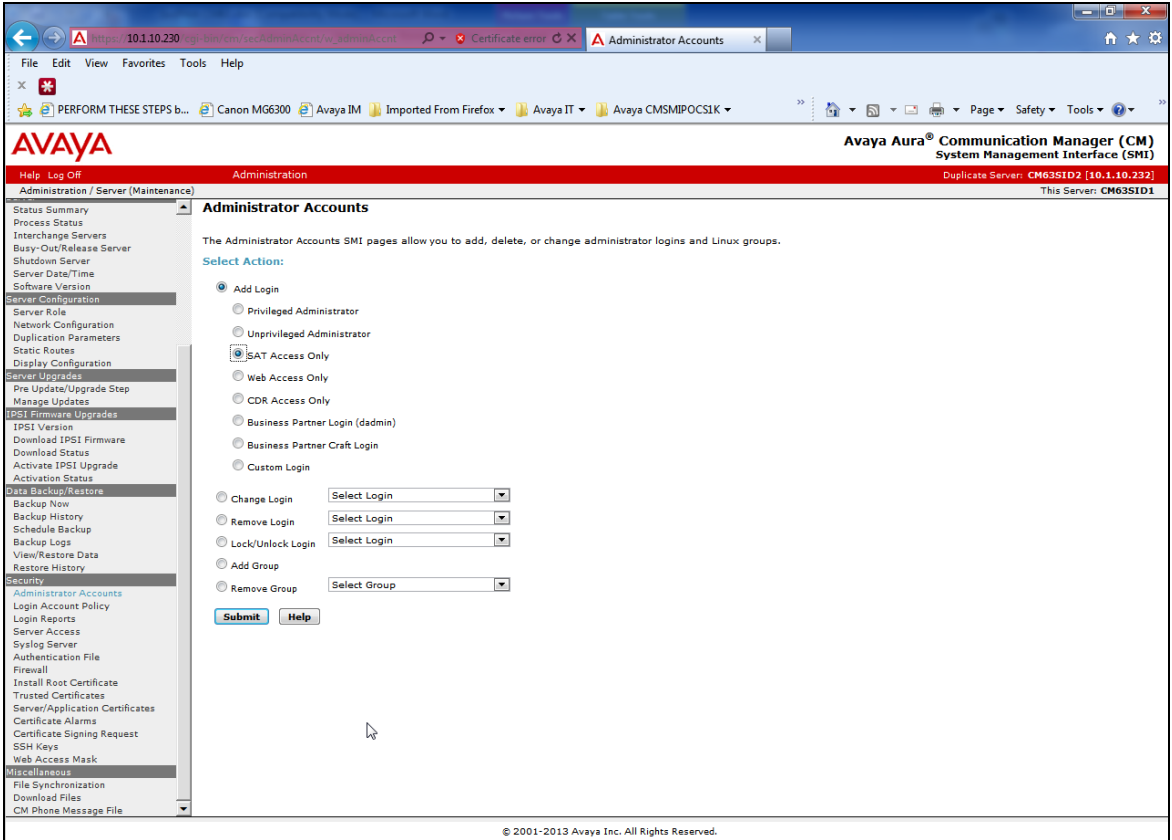
Step	Description
2.	<p>Click Administration → Server (Maintenance). This will open up the Server Administration Interface that will allow the user to complete the configuration process.</p>  <p>The screenshot shows a web browser window with the URL https://10.1.10.230/cgi-bin/common/legal/w_legal. The browser displays a 'Certificate error' and the page title is 'Avaya Aura® Communication Manager (CM) System Management Interface (SMI)'. The navigation menu includes 'Help', 'Log Off', 'Administration', 'Licensing', 'Native Configuration Manager', and 'Server (Maintenance)'. The 'Server (Maintenance)' option is highlighted, and a tooltip indicates: 'Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.' The main content area is titled 'Server Administration Interface' and contains the following text:</p> <p>© 2001-2013 Avaya Inc. All Rights Reserved.</p> <p>Copyright</p> <p>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.</p> <p>Third-party Components</p> <p>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/</p> <p>Trademarks</p> <p>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.</p> <p>© 2001-2013 Avaya Inc. All Rights Reserved.</p>

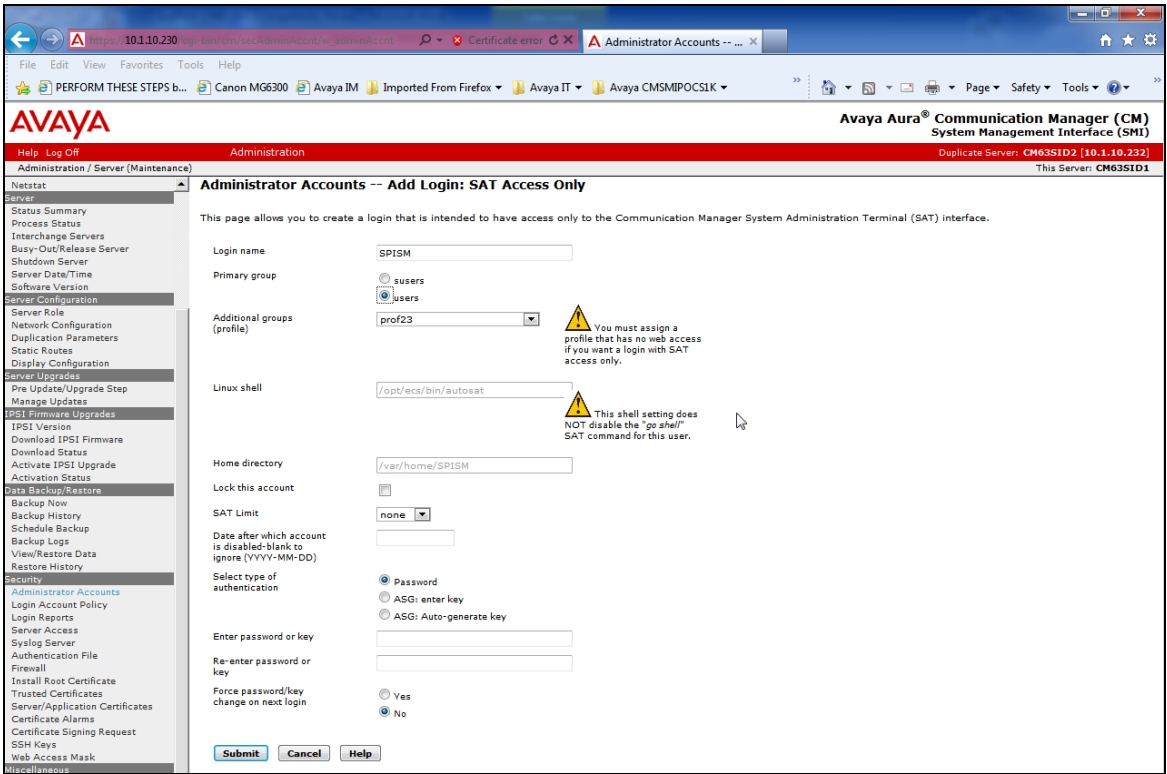
Step	Description
3.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Group and click Submit.</p> 

Step	Description
4.	<p>Select Add a new access-profile group and select prof23 from the drop-down box to correspond to the user-profile created in Section 5.1 Step 1. Click Submit. This completes the creation of the login group.</p> 

5.3. Configure Login

Create a login account for ServicePilot ISM to access the Communication Manager SAT.

Step	Description
1.	<p>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.</p> 

Step	Description
2.	<p>For the field Login name, enter the login. In this configuration, the login iptm is created. Configure the other parameters for the login as follows:</p> <ul style="list-style-type: none"> • Primary group: users [Limits the permissions of the login] • Additional groups (profile): prof23 [Select the login group created in Section 5.2.] • Select type of authentication: Password [Uses a password for authentication.] • Enter password or key / Re-enter password or key [Define the password.] <p>Click Submit to continue. This completes the configuration of the login.</p> 

5.4. 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.

Step	Description
1.	<p>Enter the change system-parameters ip-options command. In the RTCP MONITOR SERVER section, set Server IPV4 Address to the IP address of the ISM server. Set IPV4 Server Port to 5005 and RTCP Report Period (secs) to 5.</p> <pre> 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: 10.1.10.122 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 </pre>
2.	<p>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.</p> <p>Note: Only one RTCP MONITOR SERVER can be configured per IP network region.</p> <pre> 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 </pre>
3.	Repeat Step 2 for all IP network regions that are required to be monitored.

5.5. Configure CDR Monitoring

To allow ServicePilot ISM to monitor the CDR information, configure Communication Manager to send CDR information to the IP address of the ISM server.

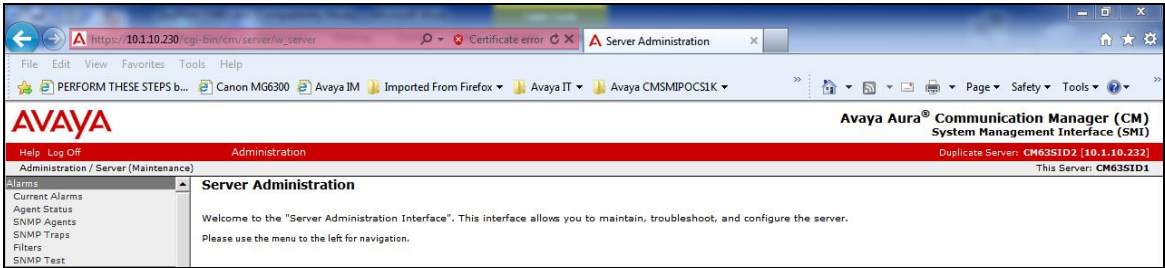
Step	Description
1.	<p>Enter the change ip-interface procr command to enable the processor-ethernet interface on the Avaya Server. Set Enable Interface to y. This interface will be used by Communication Manager to send out the CDR information.</p> <pre> change ip-interface procr Page 1 of 2 IP INTERFACES 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 </pre>
2.	<p>Enter 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 10.1.10.122. Note also the node name procr which is automatically added.</p> <pre> change node-names ip Page 1 of 2 IP NODE NAMES Name IP Address ESS 10.1.10.239 Gateway001 10.1.10.1 Gateway002 10.1.50.1 IPOffice 10.1.30.10 Invision 10.1.10.126 PC1 10.1.10.151 PC2 10.1.10.152 RDTT 10.1.10.153 SPISM 10.1.10.122 cms1 10.1.10.85 default 0.0.0.0 lsp-g430 10.1.40.10 n 10.3.10.253 procr 10.1.10.230 procr6 :: s8500-clan1 10.1.10.21 (16 of 24 administered node-names were displayed) Use 'list node-names' command to see all the administered node-names Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name </pre>


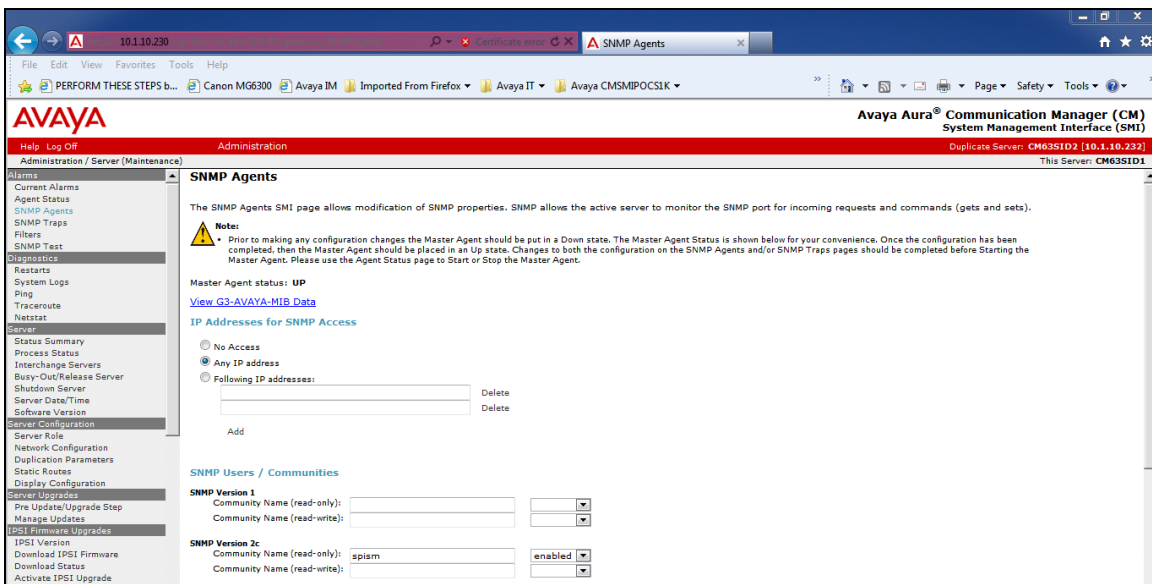
Step	Description																								
3.	<p>Enter the change ip-services command to define the CDR link. To define a primary CDR link, the following information should be provided:</p> <ul style="list-style-type: none">• Service Type: CDR1 [If needed, a secondary link can be defined by setting Service Type to CDR2.]• Local Node: procr [Communication Manager will use the processor-ethernet interface to send out the CDR]• Local Port: 0 [The Local Port is set to 0 because Communication Manager initiates the CDR link.]• Remote Node: SPISM [The Remote Node is set to the node name previously defined in Step 2]• Remote Port: 50000 [The Remote Port may be set to a value between 5000 and 64500 inclusive. 50000 is the default port number used by ServicePilot ISM. Note that ISM server uses the same port number for all Avaya Servers sending CDR information to it.]																								
<div>change ip-services<div>Page1 of 4</div></div> <table><tr><th colspan="6">IP SERVICES</th></tr><tr><th>Service Type</th><th>Enabled</th><th>Local Node</th><th>Local Port</th><th>Remote Node</th><th>Remote Port</th></tr><tr><td>AESVCS</td><td>y</td><td>procr</td><td>8765</td><td></td><td></td></tr><tr><td>CDR1</td><td></td><td>procr</td><td>0</td><td>SPISM</td><td>50000</td></tr></table>		IP SERVICES						Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	AESVCS	y	procr	8765			CDR1		procr	0	SPISM	50000
IP SERVICES																									
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																				
AESVCS	y	procr	8765																						
CDR1		procr	0	SPISM	50000																				
<p>On Page 3 of the form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the Reliable Protocol field to n.</p>																									
<div>change ip-services<div>Page3 of 4</div></div> <table><tr><th colspan="6">SESSION LAYER TIMERS</th></tr><tr><th>Service Type</th><th>Reliable Protocol</th><th>Packet Resp Timer</th><th>Session Connect Message Cntr</th><th>SPDU Cntr</th><th>Connectivity Timer</th></tr><tr><td>CDR1</td><td>n</td><td>30</td><td>3</td><td>3</td><td>60</td></tr></table>		SESSION LAYER TIMERS						Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	CDR1	n	30	3	3	60						
SESSION LAYER TIMERS																									
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer																				
CDR1	n	30	3	3	60																				

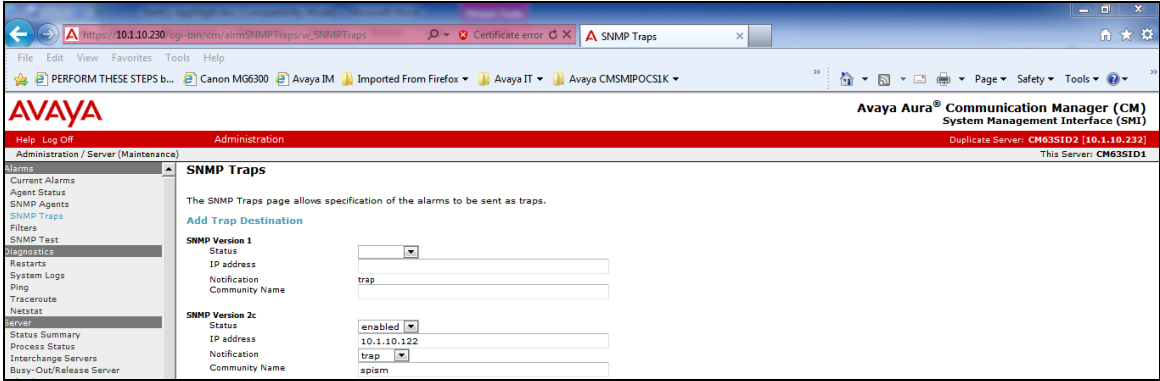
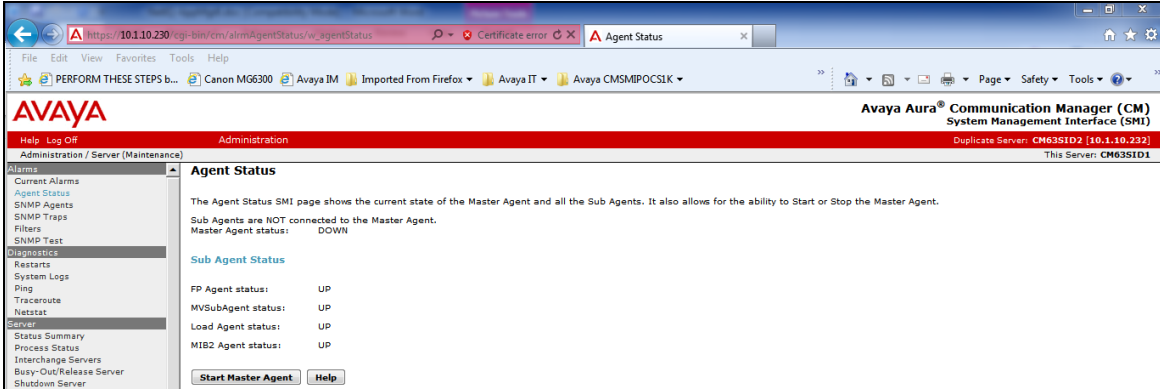
Step	Description
4.	<p>Enter the change system-parameters cdr command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test.</p> <ul style="list-style-type: none"> • CDR Date Format: month/day [day/month Date Format is also supported] • Primary Output Format: unformatted [Other Output Format include expanded, enhanced expanded, enhanced unformatted] • Primary Output Endpoint: CDR1 <p>The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See Reference [1] for a full explanation of each field. The test configuration used some of the more common fields described below.</p> <ul style="list-style-type: none"> • Intra-switch CDR: 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? n [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.] • Outg Trk Call Splitting? y [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.] • Inc Trk Call Splitting? y [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.] <pre> change system-parameters cdr 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 </pre>
5.	<p>If the Intra-switch CDR field is set to y on Page 1 of the SYSTEM-PARAMETERS CDR form, then enter 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 the CDR records.</p>

Step	Description
	<div>change intra-switch-cdr<div>Page1 of3</div></div> <div>INTRA-SWITCH CDR</div> <div>Assigned Members:11 of 5000 administered</div> <div>ExtensionExtensionExtensionExtension</div> <div><div>10001</div><div>10002</div><div>10003</div><div>10005</div><div>10016</div><div>10049</div><div>10050</div><div>10701</div><div>20001</div><div>481122</div><div>481123</div></div>
6.	<div>For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Enter the change trunk-group n command, where n is the trunk group number, to verify that the CDR Reports field is set to y. Repeat for all trunk groups to be reported.</div>
	<div>change trunk-group 1<div>Page1 of21</div></div> <div>TRUNK GROUP</div> <div>Group Number:1Group Type: isdnCDR Reports: y</div> <div>Group Name: PSTN - BRICOR: 95TN: 1TAC: #01</div> <div>Direction: two-wayOutgoing Display? nCarrier Medium: PRI/BRI</div> <div>Dial Access? yBusy Threshold: 255Night Service:</div> <div>Queue Length: 0</div> <div>Service Type: public-ntwrkAuth Code? nTestCall ITC: rest</div> <div>Far End Test Line No:</div> <div>TestCall BCC: 4</div>

5.6. Configure SNMP on Communication Manager

Step	Description
1.	<p>Access the Avaya Aura® Communication Manager System Management Web Interface as in Section 5.2 Steps 1 and 2. Navigate to Administration → Server Administration to display the following web page.</p> 

Step	Description
2.	<p>Click Alarms → Agent Status. Click Stop the Master Agent if the Master Agent status is <i>UP</i> to allow setup of SNMP Agent.</p> 
3.	<p>To allow ServicePilot ISM to use SNMP to collect configuration and status information from Communication Manager, navigate to Alarms → SNMP Agents in the left pane. Under IP Addresses for SNMP Access, select <i>Any IP address</i>. Under SNMP Users / Communities, configure the SNMP Version 2c section. Set the Community Name (read-only) field to <i>spism</i> and the drop-down box to the right to <i>enabled</i>. Click Submit at the bottom of the web page (not shown in the figure).</p> 

Step	Description
4.	<p>Navigate to Alarms → SNMP Traps web page below and configure ServicePilot as an SNMP trap receiver under the Add Trap Destination section. Next, configure the SNMP Version 2c parameters. Set the Status field to <i>enabled</i>, specify the IP address of ServicePilot ISM, set the Notification field to <i>trap</i>, and set the Community Name to spism. Click the Submit button.</p> 
5.	<p>Lastly, the SNMP agent must be started. Navigate to Alarms → Agent Status. . If the Master Agent status is <i>Down</i>, then click the Start Agent Status button. If the Master Agent status is <i>Up</i>, then the agent must be stopped and restarted.</p> 

5.7. 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 G250 and G450 Media Gateway.

- Administer community string
- Administer SNMP traps
- Show SNMP

5.7.1. Administer Community String

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) #
```

5.7.2. Administer SNMP Traps

Use the **snmp-server host** command shown below to enable SNMP traps to ServicePilot ISM, where *10.1.10.122* 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 10.1.10.122 traps v2c public  
Done!  
G430-003(super) #
```

5.7.3. 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-write            ***** read-only            *****

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

SNMP-Rec-Address      Model   Notification   Trap/Inform
UDP port              Level
User name
-----
10.1.10.230            v1      all             trap
162 - Dynamic Trap Manager
ReadCommN              noauth
10.1.10.122           v2c    all            trap
162                  noauth
```

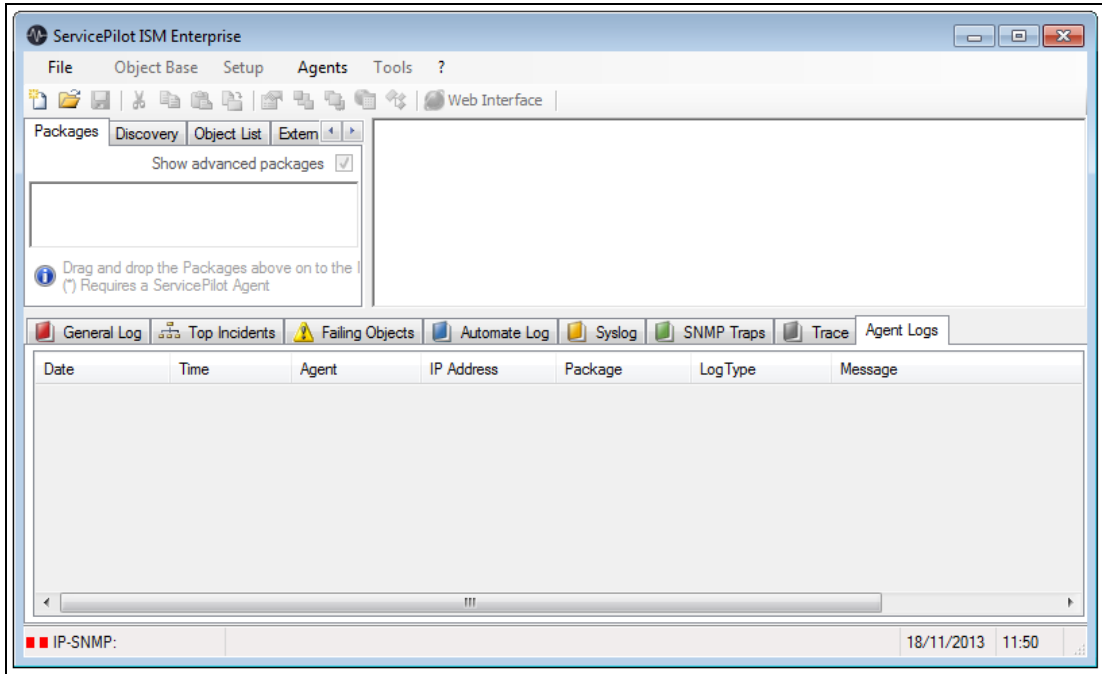
6. Configure ServicePilot ISM

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. The procedures cover the following operations:

- Launch ServicePilot ISM
- Run the New Configuration Wizard
- Add an Avaya Aura® Communication Manager
- Configure RTCP packets and CDRs
- Configure Call Quality thresholds
- Add an Avaya Media Gateway
- Configure the SNMP alarm server
- Create an Avaya dashboard

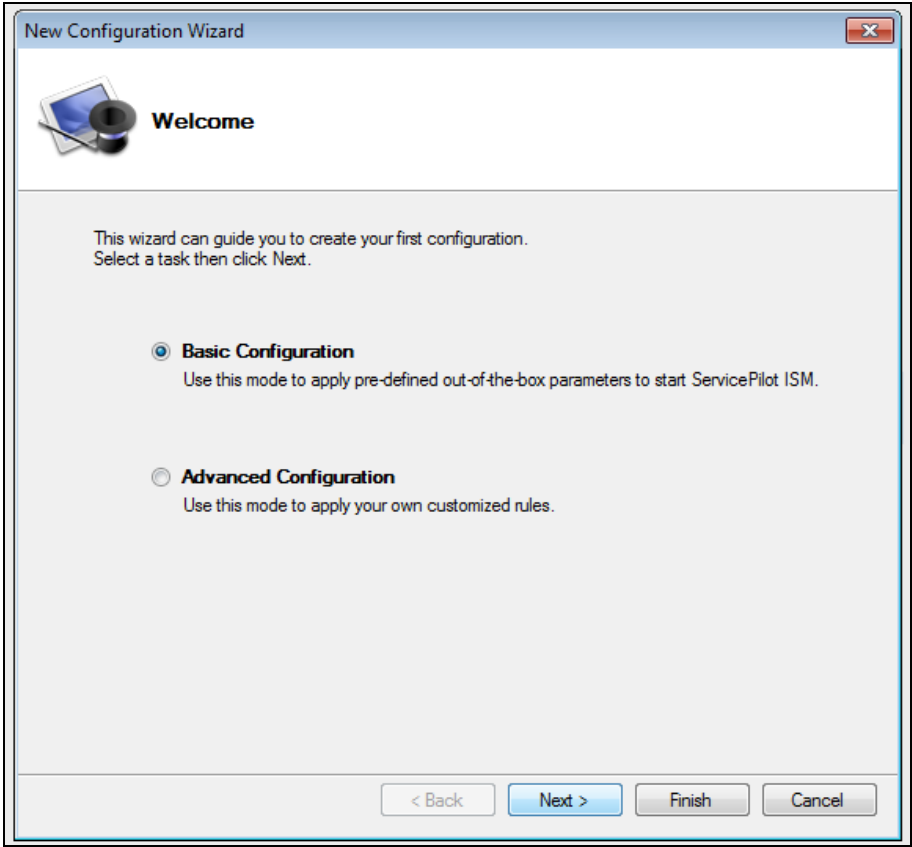
6.1. Launch ServicePilot ISM

ServicePilot ISM is initially configured using the **Administration Console**. Launch **ServicePilot ISM Administration Console** on the ServicePilot ISM server using the following procedure.

Step	Description
1.	<p>From the Windows Start menu, navigate to All Programs → ServicePilot → ServicePilot ISM Enterprise → ServicePilot ISM Enterprise.</p> <p>The main ServicePilot ISM Administration Console window appears as shown below.</p> 

6.2. Run the New Configuration Wizard

In order to interoperate with the Communication Manager, a new configuration needs to be created for ServicePilot ISM, following the steps below.

Step	Description
1.	<p>From the ServicePilot ISM Administration Console run the New Configuration Wizard by selecting File → New</p> <p>Select Basic Configuration then click Next.</p> 

2. From the drop-down list select **VoIP** and then select **Avaya** in the **VoIP** box. Optionally, enter a company name and choose a logo.

Then click **Next**.

New Configuration Wizard

Basic Configuration

Company Name:

Logo (optional): Maximum Size: 400*300 px

Select your environment:

VoIP

☒ Avaya ☐ Acme Packet ☐ ShoreTel

☐ Cisco ☐ Aastra

☐ Alcatel-Lucent ☐ Microsoft Lync

Avaya VoIP Portal will be imported after clicking on Next Button.

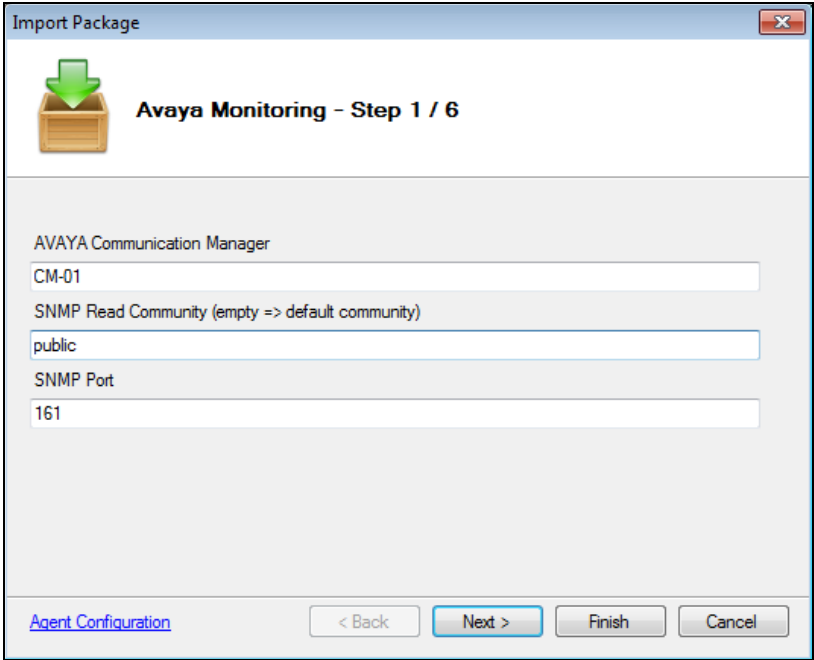
This will create the **Avaya VoIP Portal** on the main window.

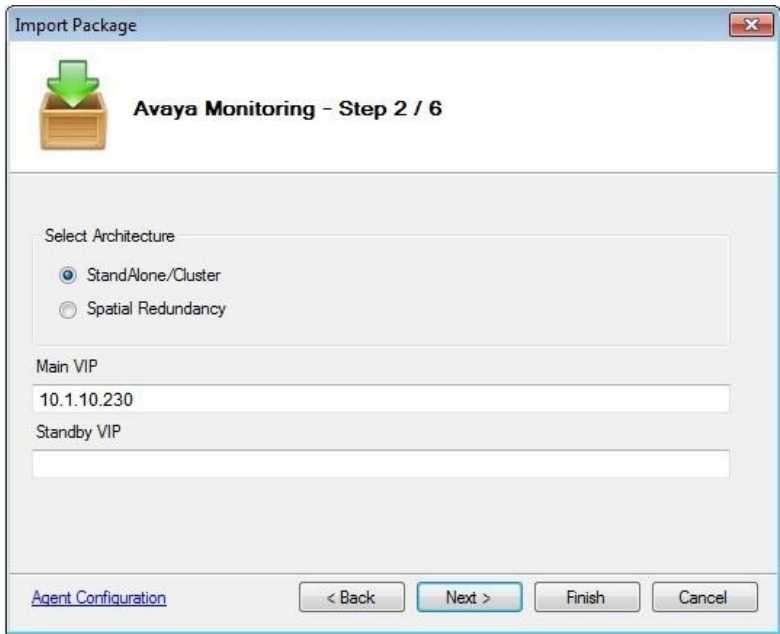
This completes the New Configuration Wizard and automatically launches the **Import Package** wizard for the Communication Manager (see next section)

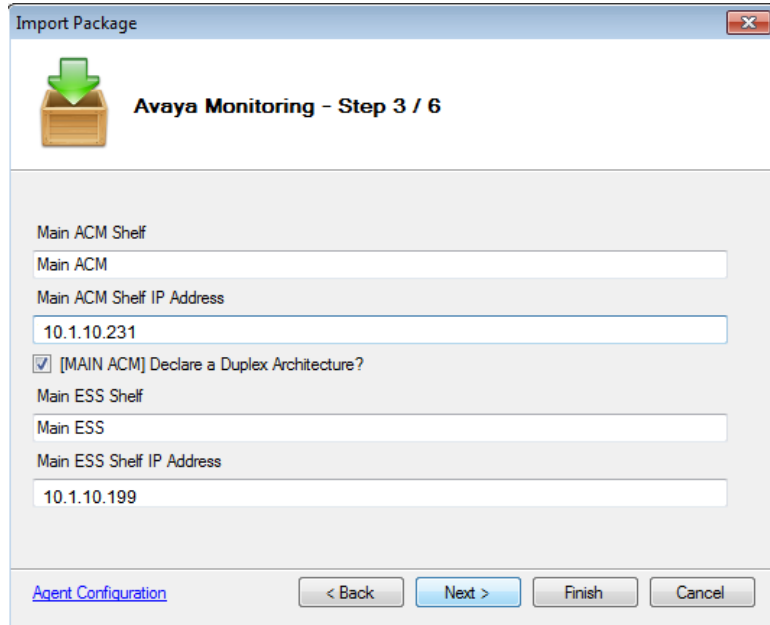
6.3. Add an Avaya Aura® Communication Manager

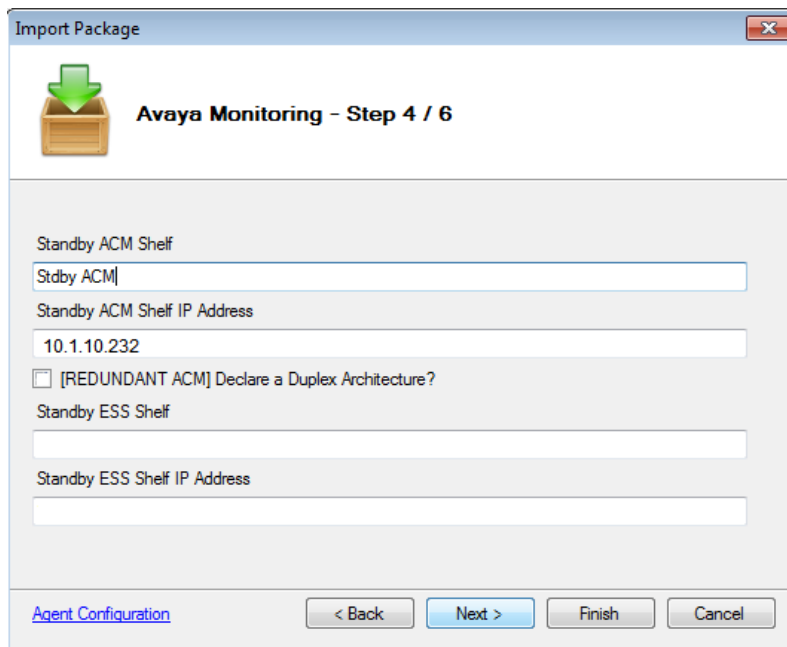
To add a Communication Manager to the newly created configuration, run the import wizard, (which will have been automatically launched by the previous procedure) following the steps below.

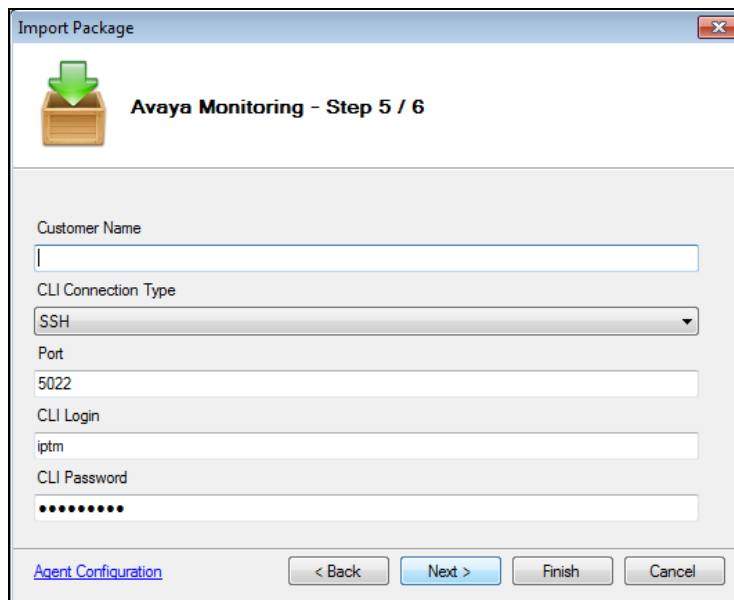
NOTE: If this procedure is not being run after the New Configuration Wizard, for example to deploy an additional Communication Manager into the monitoring environment, the **Import Package** can be started by doing a drag-and-drop of the **Avaya Monitoring** package, from the **Packages** tab onto the main window.

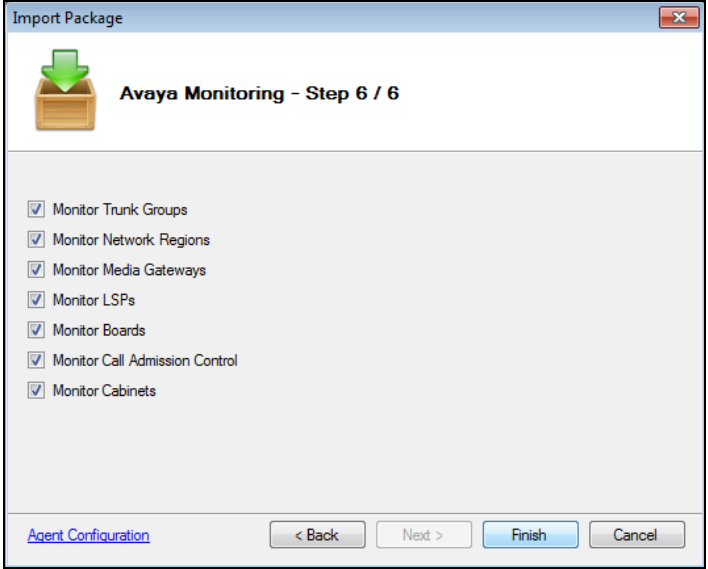
Step	Description
1.	<p>On the Import Package window, enter the following parameters for the Communication Manager:</p> <ul style="list-style-type: none"> - Name, e.g. CM-01 - SNMP read-only community, e.g. public - SNMP port, e.g. 161 <div data-bbox="451 485 1260 1140">  </div> <p>Click Next.</p>

Step	Description
2.	<p>Specify the right architecture by selecting one of the following 2 options:</p> <ul style="list-style-type: none"> - Standalone / Cluster - Spatial Redundancy <p>If Spatial Redundancy was selected, enter the following parameters:</p> <ul style="list-style-type: none"> - Virtual / shared IP address for the Main nodes - Virtual / shared IP address for the Standby nodes. <div data-bbox="467 590 1242 1220">  </div> <p>Click Next.</p>

Step	Description
3.	<p>Enter the following parameters for the Main Communication Manager shelf:</p> <ul style="list-style-type: none"> - Name - IP address <p>If a Main ESS is present, tick the [MAIN ACM] Declare a Duplex Architecture box and enter the following parameters for the Main ESS:</p> <ul style="list-style-type: none"> - Name - IP address <div data-bbox="467 592 1232 1213" data-label="Form">  <p>The screenshot shows a software configuration window titled 'Import Package' with a close button in the top right. Below the title bar is a green arrow icon pointing into a box, followed by the text 'Avaya Monitoring - Step 3 / 6'. The main area contains several input fields: 'Main ACM Shelf' with 'Main ACM' entered, 'Main ACM Shelf IP Address' with '10.1.10.231' entered, a checked checkbox labeled '[MAIN ACM] Declare a Duplex Architecture?', 'Main ESS Shelf' with 'Main ESS' entered, and 'Main ESS Shelf IP Address' with '10.1.10.199' entered. At the bottom left is a blue link 'Agent Configuration'. At the bottom right are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.</p> </div> <p>Click Next.</p>

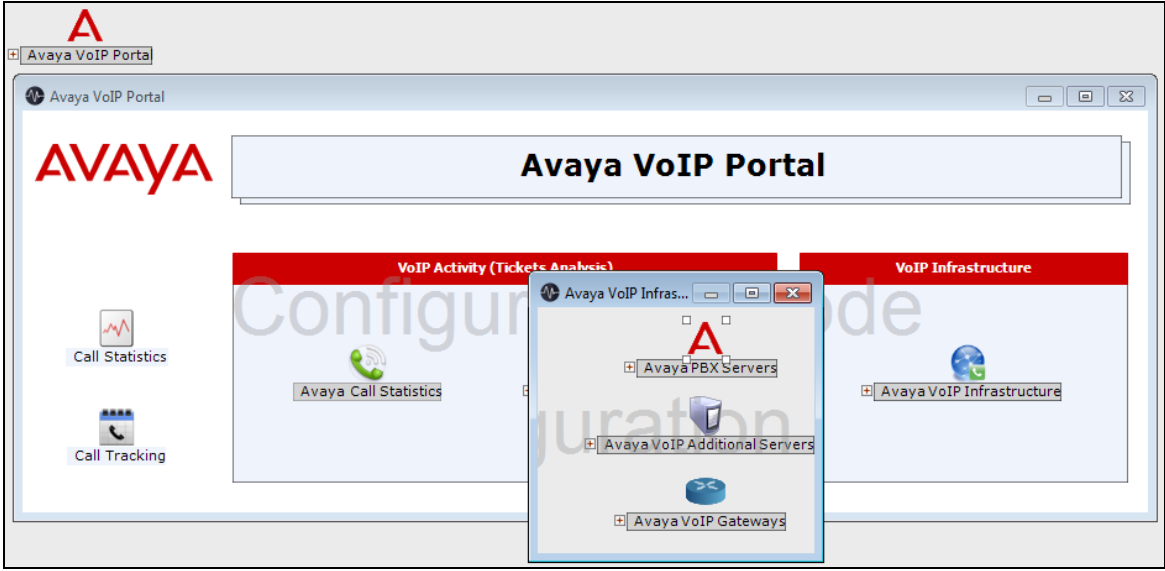
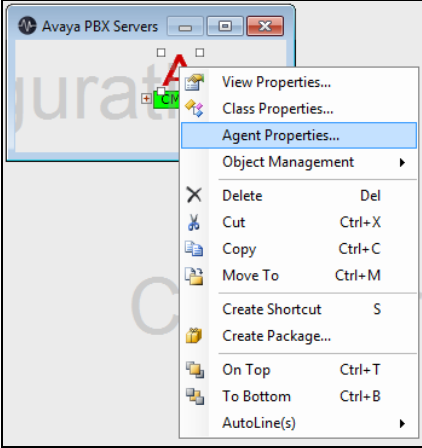
Step	Description
4.	<p>If the Standalone / Cluster option was selected on Step 2, skip this step.</p> <p>Otherwise, enter the following parameters for the Standby Communication Manager shelf:</p> <ul style="list-style-type: none"> - Name - IP address <p>If a Standby ESS is present, tick the [REDUNDANT ACM] Declare a Duplex Architecture box and enter the following parameters for the Standby ESS:</p> <ul style="list-style-type: none"> - Name - IP address <div data-bbox="457 697 1239 1339" data-label="Form">  </div> <p>Click Next.</p>

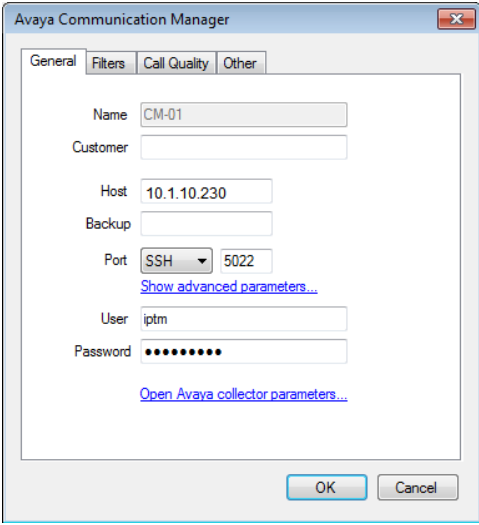
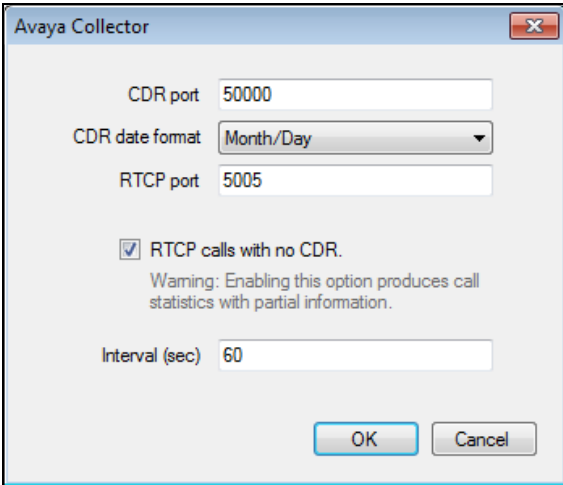
Step	Description
5.	<p>Leave the Customer Name field blank and enter the following parameters for the SAT connection between ServicePilot ISM and the Communication Manager:</p> <ul style="list-style-type: none"> - Connection type: from the drop-down list select either Telnet or SSH - Port: enter 5023 (if Telnet was selected) or 5022 (if SSH was selected) - Login: enter the same Login name as Step 2 in Section 5.3. - Password: enter the same password as Step 2 in Section 5.3. <div data-bbox="482 514 1211 1110" data-label="Form">  <p>The screenshot shows a software window titled 'Import Package' with a close button in the top right. Below the title bar is a header area with a green download icon and the text 'Avaya Monitoring - Step 5 / 6'. The main area contains several input fields: 'Customer Name' (empty), 'CLI Connection Type' (a dropdown menu showing 'SSH'), 'Port' (text box with '5022'), 'CLI Login' (text box with 'iptm'), and 'CLI Password' (password field with masked characters). At the bottom, there is a link 'Agent Configuration' and four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.</p> </div> <p>Click Next.</p>

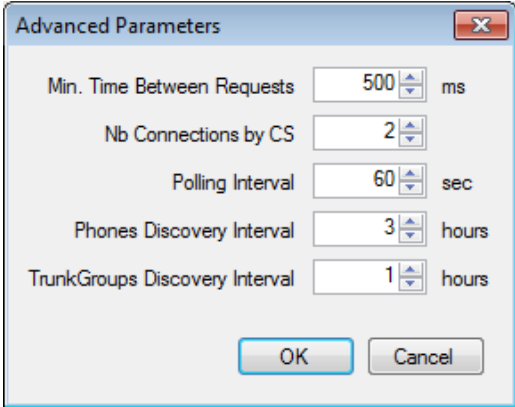
Step	Description
6.	<p>Tick or un-tick the following options, depending on the available Communication Manager's components to monitor:</p> <ul style="list-style-type: none"> - Trunk Groups - Network Regions - Media Gateways - LSPs - Boards - Call Admission Control (CAC policies) - Cabinets.  <p>Click Finish.</p>
7.	Click Close on the Package Information window that appears.
8.	<p>Click Close on the New Configuration Wizard window that appears.</p> <p>Skip this step if this procedure was started independently of the New Configuration Wizard.</p>

6.4. Configure RTCP Packets and CDRs

To provide call statistics and call quality details, ServicePilot ISM relies on the RTCP packets received from Avaya end points and on the CDRs received from the Communication Manager. Both features need to be configured in ServicePilot ISM following the procedure below.

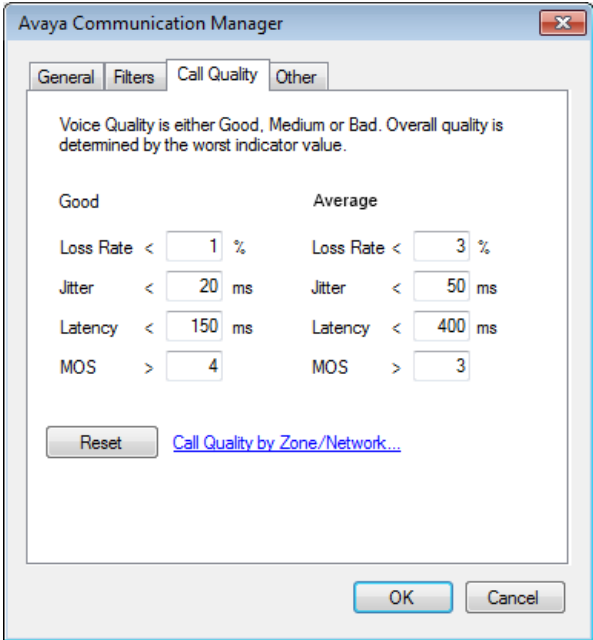
Step	Description
1.	<p>From the Administration Console, click on Avaya VoIP Portal → Avaya VoIP Infrastructure → Avaya PBX Servers.</p> 
2.	<p>Right-click on the newly imported Communication Manager (e.g. CM-01) and select Agent Properties.</p> 

Step	Description
3.	<p>Click on Open Avaya collector parameters.</p> 
4.	<p>On the Avaya Collector window that appears, enter the following:</p> <ul style="list-style-type: none"> - CDR port: enter the same value as Remote Port in Step 3, Section 5.5, e.g. 50000 - CDR date format: from the drop-down list select either Month/Day or Day/Month, so the selection matches the format in Step 4, Section 5.5 - RTCP port: enter the same port as Step 1, Section 5.4, e.g. 5005 - Tick the RTCP calls with no CDR box - Interval: specify how often ServicePilot ISM will process received RTCP packets and CDR records (default is 60 seconds)  <p>Click OK.</p>

Step	Description
5.	<p>NOTE: this step is optional.</p> <p>Click on Show advanced parameters.</p> <p>On the Advanced Parameters window that appears, you can adjust the following parameters for the SAT connection to the Communication Manager: (default values are shown in brackets)</p> <ul style="list-style-type: none"> - Minimum time between requests (500 ms) - Number of simultaneous connections for Communication Manager (2) - Polling interval (60 seconds) - Phones discovery interval (3 hours) - Trunk groups discovery interval (1 hour).  <p>Click OK.</p>
6.	Click OK to accept the changes.

6.5. Configure Call Quality Thresholds

The following procedure can be used to customize how ServicePilot ISM classifies calls as **Good**, **Average** or **Bad**.

Step	Description
1.	From the Administration Console , click on Avaya VoIP Portal → Avaya VoIP Infrastructure → Avaya PBX Servers , as in Step 1 in Section 6.4 .
2.	Right-click on the newly imported Communication Manager (e.g. CM-01) and select Agent Properties , as in Step 2 in Section 6.4 .
3.	Select the Call Quality tab.
4.	<p>To configure how ServicePilot ISM classifies call quality based on the four standard QoS (Quality of Service) metrics below, adjust the values for the Good and Average thresholds: (default values are shown in brackets)</p> <ul style="list-style-type: none"> - Packet Loss Rate (< 1%, < 3%) - Jitter (< 20ms, < 50ms) - Latency (< 150ms, < 400ms) - MOS (Mean Opinion Score, 1-5) (> 4, > 3) <p>NOTE (1): Calls falling outside the specified thresholds (above or below, depending on the metric) will automatically be classified as Bad.</p> <p>NOTE (2): Calls without sufficient call quality metrics will be classified as Other/Unknown.</p> 

Step	Description
5.	<p>NOTE: this step and Step 6 are optional. Click on Call Quality by Zone/Network.</p> <p>On the Call Quality by Zone/Network window that appears, tick the Activate Call Quality Statistics by Zone/Network box and select Call Quality by Zone.</p> <div data-bbox="506 445 1203 974" data-label="Image"> </div> <p>Then click on Edit Zones.</p>

Step	Description
6.	<p>On the Zones Setup window that appears,</p> <ul style="list-style-type: none"> - Use the Add button to add one or more zones - For each zone, use the buttons in the Includes/Excludes sections to define the zone in terms of any combination of any of the following elements: <ul style="list-style-type: none"> o Single IP address o Range of IP addresses o Network (IP address + subnet mask). <div data-bbox="467 594 1243 1281" data-label="Image"> <p>The screenshot shows the 'Zones Setup' window. On the left is a list of zones with a 'New Zone' entry. Below this are 'Collapse All' and 'Expand All' buttons, and an 'Organize Zones' section with up/down arrows and 'Add'/'Delete' buttons. On the right is the 'Zone Settings' panel for 'New Zone'. It has an 'Includes' section with a list containing 'All' and '+'/'-' buttons, and an 'Excludes' section with '+'/'-' buttons. An 'Add an include' dialog box is open, showing 'Type' as 'NETWORK', 'Ip' as '172.17.1.0', and 'Mask' as '255.255.255.0', with 'Add' and 'Cancel' buttons. At the bottom of the main window are 'Save Zones' and 'Cancel' buttons.</p> </div> <p>Click on Save Zones. Click Ok (not shown).</p>
7.	<p>Select the Other tab.</p> <p>Make sure the Call Quality Replay and Voice Stream Path boxes are both ticked.</p>
8.	<p>Click OK to accept the changes.</p>

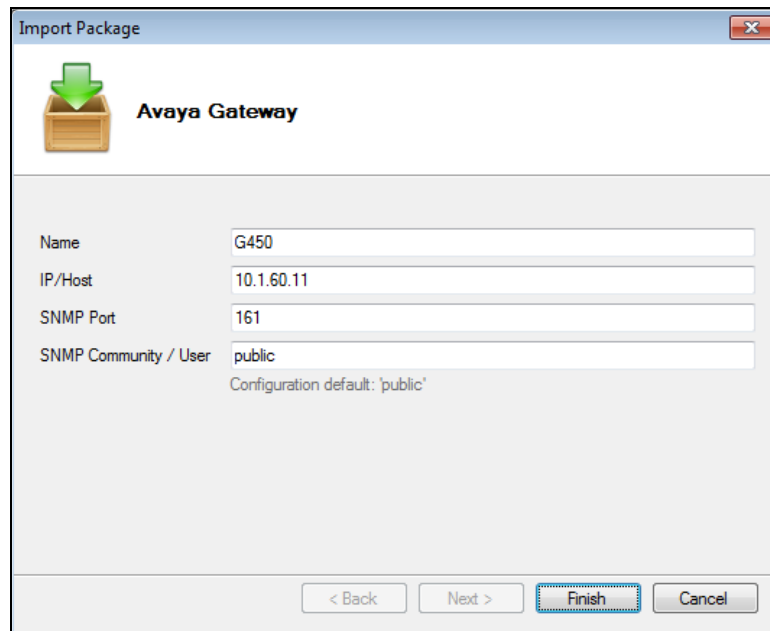
6.6. Add an Avaya Media Gateway

ServicePilot ISM automatically discovers Avaya Media Gateways by means of its SAT connection into the Communication Manager. However ServicePilot ISM can monitor Avaya Media Gateways directly by means of SNMP, and irrespective of the Communication Manager, as this provides a much richer set of metrics and statistics. Follow the procedure below to explicitly add an Avaya Media Gateway to the monitoring environment.


Step	Description
1.	<p>From the Administration Console, click on Avaya VoIP Portal → Avaya VoIP Infrastructure → Avaya VoIP Gateways, (see screenshot in Step 1 Section 6.4 as a reference).</p> <p>NOTE: This step is optional if there is no Avaya VoIP Portal on the main window.</p>
2.	<p>From the Packages tab, drag and drop the Avaya Gateway package into the Avaya VoIP Gateways window, as shown in the screenshot below.</p> <p>NOTE: The procedure works irrespective of where the Avaya Gateway package is actually dropped and irrespective of the Avaya VoIP Portal having been previously created.</p>

3, On the **Import Package** window that appears, enter the following parameters for the Avaya Media Gateway:

- **Name**
- **IP Address / Host**
- **SNMP port**
- **SNMP read-only community**



Import Package

 **Avaya Gateway**

Name: G450

IP/Host: 10.1.60.11

SNMP Port: 161

SNMP Community / User: public

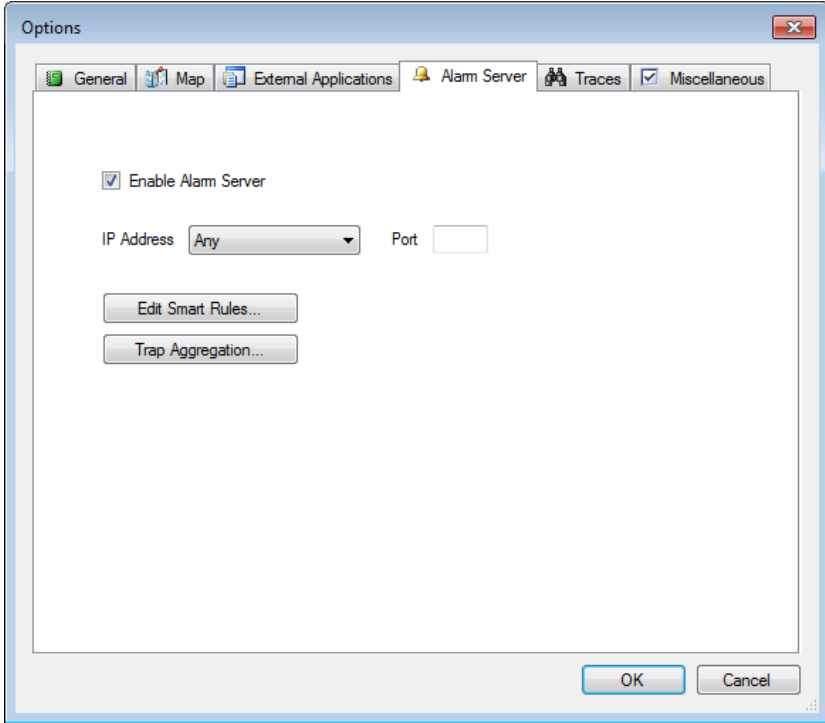
Configuration default: 'public'

< Back Next > **Finish** Cancel

4. Click **Finish** to complete the operation.

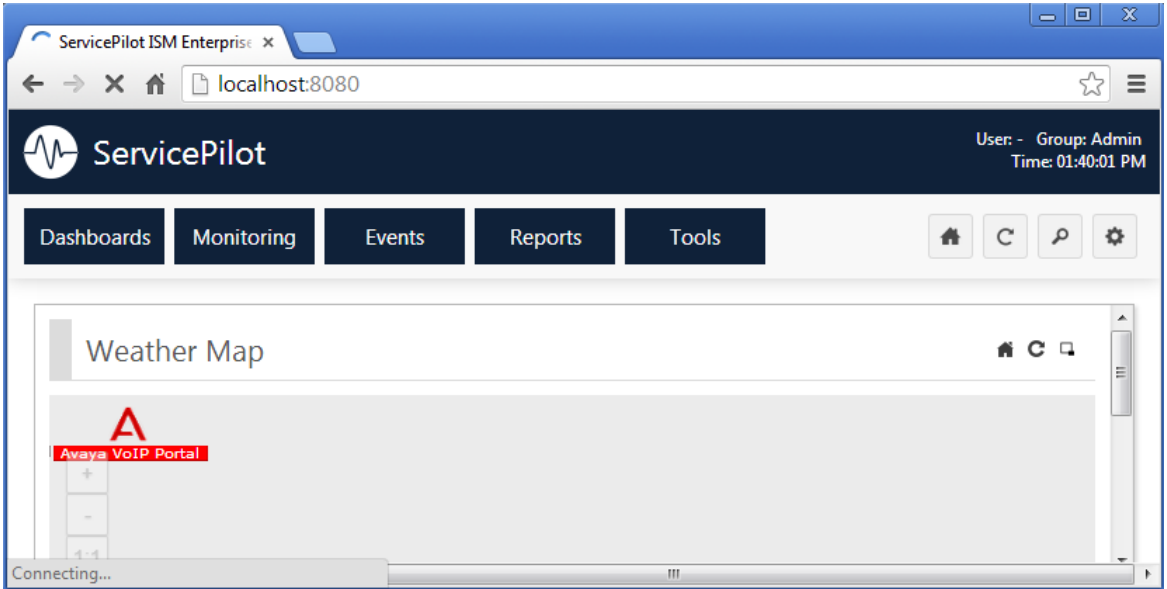
6.7. Configure the SNMP Alarm Server

To receive and display SNMP traps from the Communication Manager and the rest of the Avaya infrastructure, ServicePilot ISM's internal alarm server must be enabled and configured, using the procedure below.

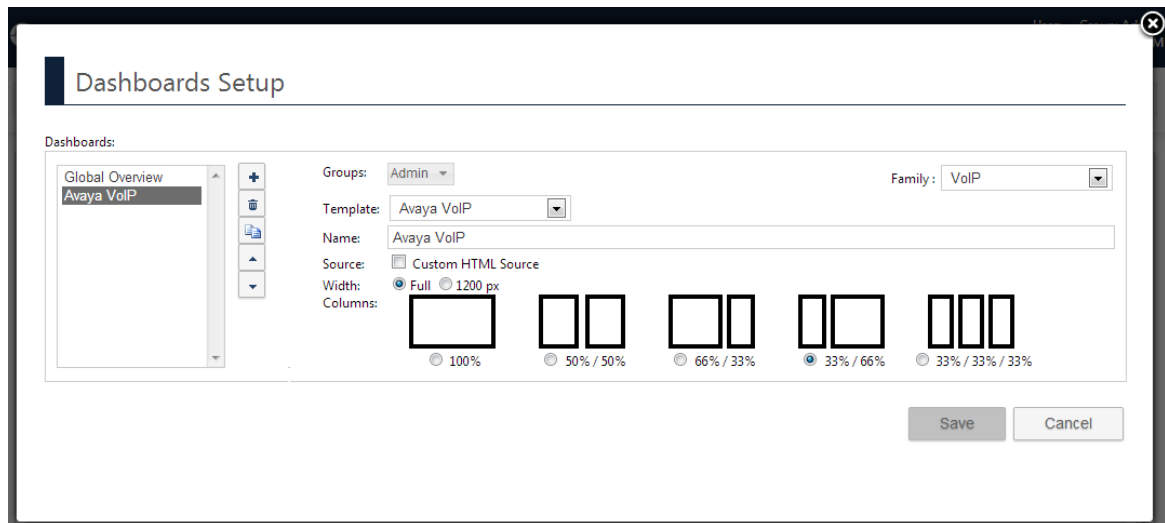
Step	Description
1.	<p>From the Administration Console select Setup → Options.</p> <p>On the Options window (not shown) that appears, select the Alarm Server tab.</p>
2.	<p>Tick the Enable Alarm Server box and make sure that Any is selected in the drop-down list next to IP Address.</p> 
3.	<p>Click OK to accept the changes.</p>

6.8. Create an Avaya Dashboard

To provide a unified view of all the data collected by ServicePilot ISM from the Communication Manager and the rest of the Avaya infrastructure (call quality statistics and performance measurements), a dedicated dashboard must be created, following the procedure below.

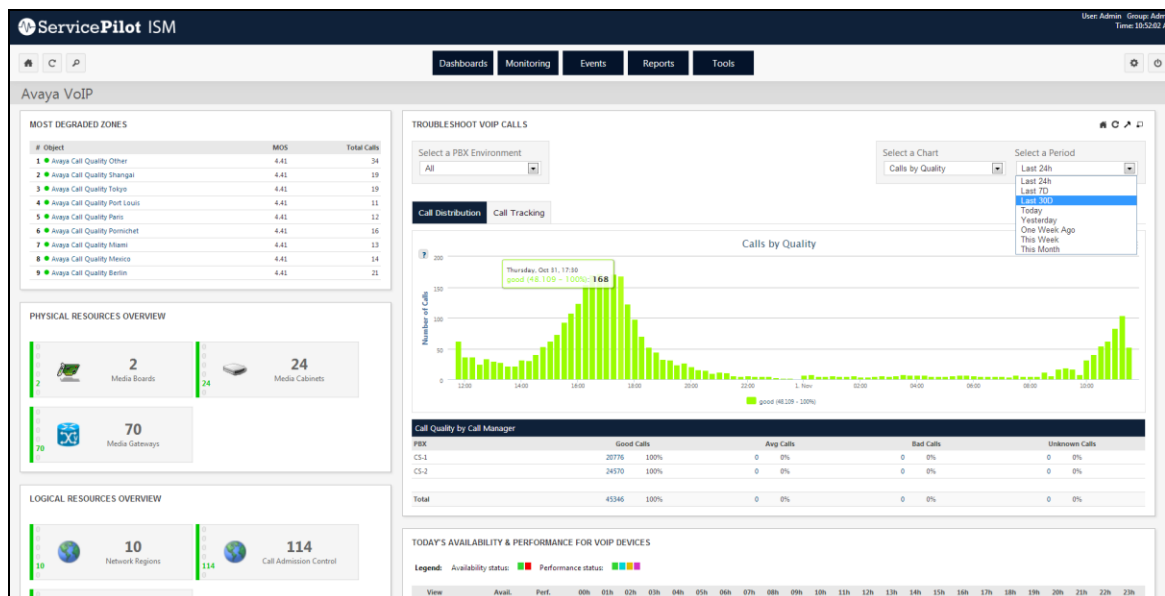
Step	Description
1.	<p>Open the ServicePilot ISM Web Interface by launching an Internet browser and navigating to the following URL:</p> <p>http://localhost:8080/</p> <p>Alternatively, the Internet browser can be launched from a machine other than the ServicePilot ISM server. In which case, navigate to the following URL:</p> <p><a href="http://<ServicePilot_ISM_IP_Address>:8080/">http://<ServicePilot_ISM_IP_Address>:8080/</p>  <p>Note: No authentication will be required at this point to access the ServicePilot ISM web interface with administrative privileges.</p>
2.	From the main menu bar, select Dashboard → Setup .

3. On the **Dashboards Setup** window that will appear,
 - Select the **Add (“+”)** button to create a new dashboard
 - Select **Avaya VoIP** from the **Template** drop-down list
 - Select the desired width, choosing between **Full** and **1200 pixels**.



Click **Save**.

4. The newly created dashboard is now accessible from the main menu bar, by selecting **Dashboard → Avaya VoIP**, as shown in the following example.



7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and ServicePilot ISM.

7.1. Verify Communication Manager

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

```
status logins
```

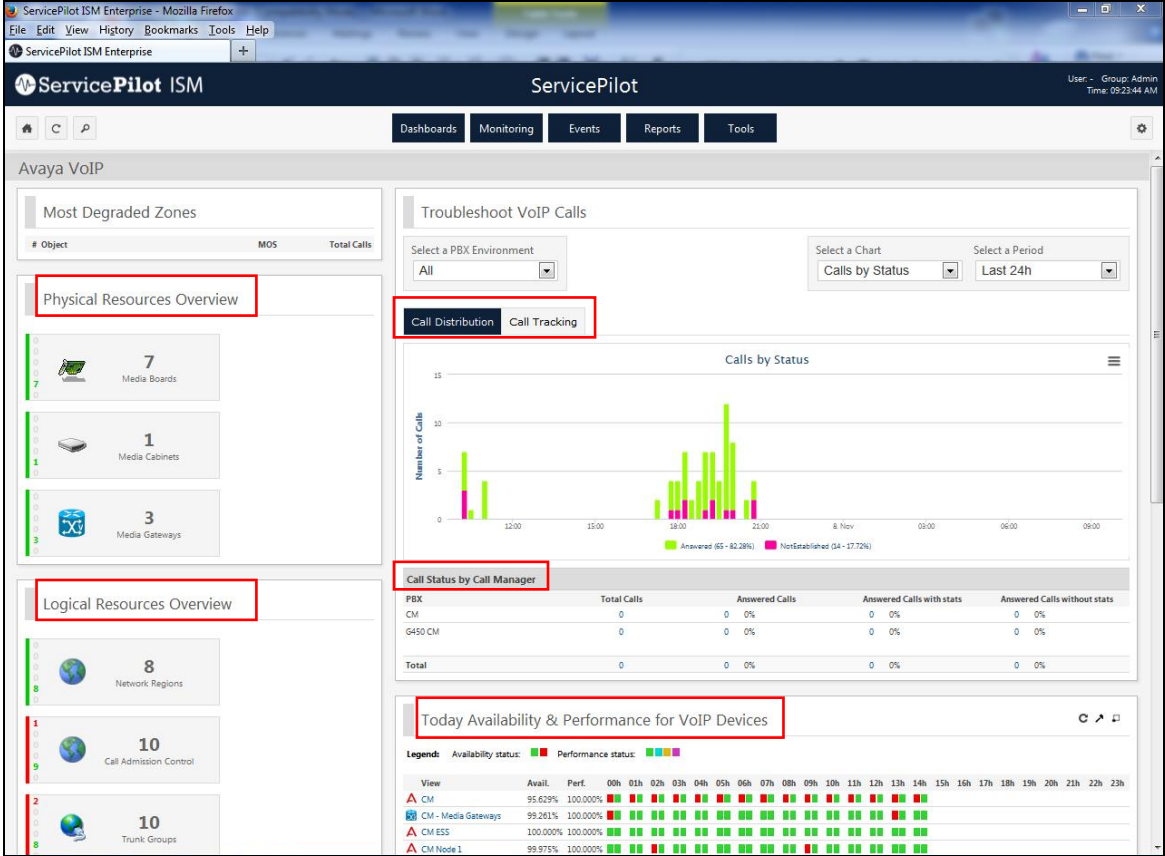
COMMUNICATION MANAGER LOGIN INFORMATION				
Login	Profile	User's Address	Active Command	Session
acpsnmp	17	127.0.0.1		1
*init	0	192.168.100.18	stat logins	3
SPISM	23	10.1.10.122		4
SPISM	23	10.1.10.122		5

Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.5** shows **up**.

```
status cdr-link
```

CDR LINK STATUS	
Primary	Secondary
Link State: up	CDR not administered
Date & Time: 2013/11/07 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	

7.2. Verify ServicePilot ISM

Step	Description
1.	<p>Logging into the web interface of ServicePilot ISM, click on Dashboards → VoIP → Avaya VoIP. The list of VoIP devices including Communication Manager Servers, Media Gateways configured is shown on the “Today Availability & Performance for VoIP Devices” pane on the lower right. An overview of Physical and Logical Resources is shown on the left. In order to troubleshoot VoIP calls, Call Distribution, Call Tracking and Call Status by Call Manager is also displayed on the screen.</p>  <p>The screenshot displays the ServicePilot ISM web interface for Avaya VoIP. The interface is divided into several sections:</p> <ul style="list-style-type: none"> Physical Resources Overview: A sidebar on the left showing a list of physical resources: 7 Media Boards, 1 Media Cabinet, and 3 Media Gateways. Logical Resources Overview: A sidebar on the left showing a list of logical resources: 8 Network Regions, 10 Call Admission Control, and 10 Trunk Groups. Troubleshoot VoIP Calls: A central panel with a bar chart titled 'Calls by Status' showing the number of calls over time. The chart includes a legend for 'Answered (65 - 82.28%)' and 'NotEstablished (34 - 17.72%)'. Below the chart is a table titled 'Call Status by Call Manager'. Call Status by Call Manager: A table showing call statistics for different PBX environments. Today Availability & Performance for VoIP Devices: A table at the bottom right showing the availability and performance of various VoIP devices. <p>Red boxes in the image highlight the following sections:</p> <ul style="list-style-type: none"> Physical Resources Overview Call Distribution Call Tracking Call Status by Call Manager Today Availability & Performance for VoIP Devices

2. Make a call between two Avaya IP telephones that belong to an IP Network Region that has been configured to send RTCP information to the ISM server. Hang up the call after say 1 minute. Verify that the call log in **Call Tracking** under **Troubleshoot VoIP Calls** section shows the quality of the call. By drilling into the **Call Details**, the graphical values of MOS, Jitter, Packet Loss and Latency are also plotted.

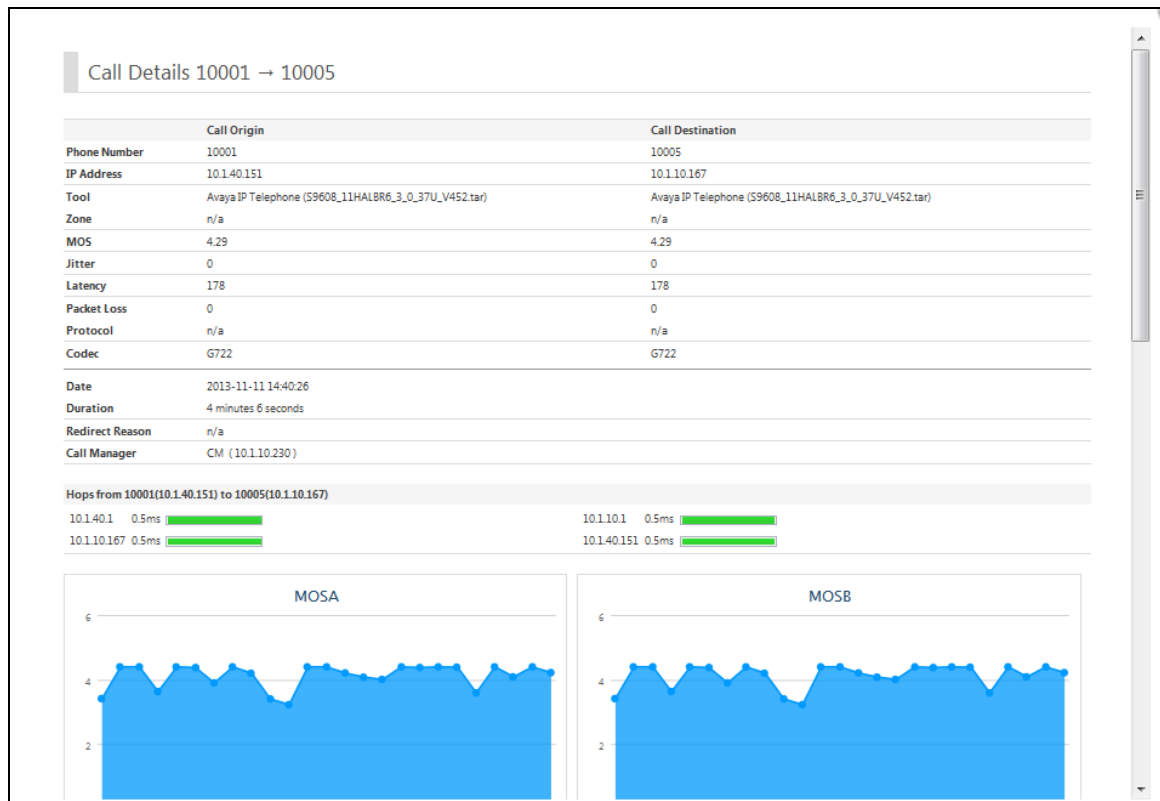
Call Log Call Log Stats

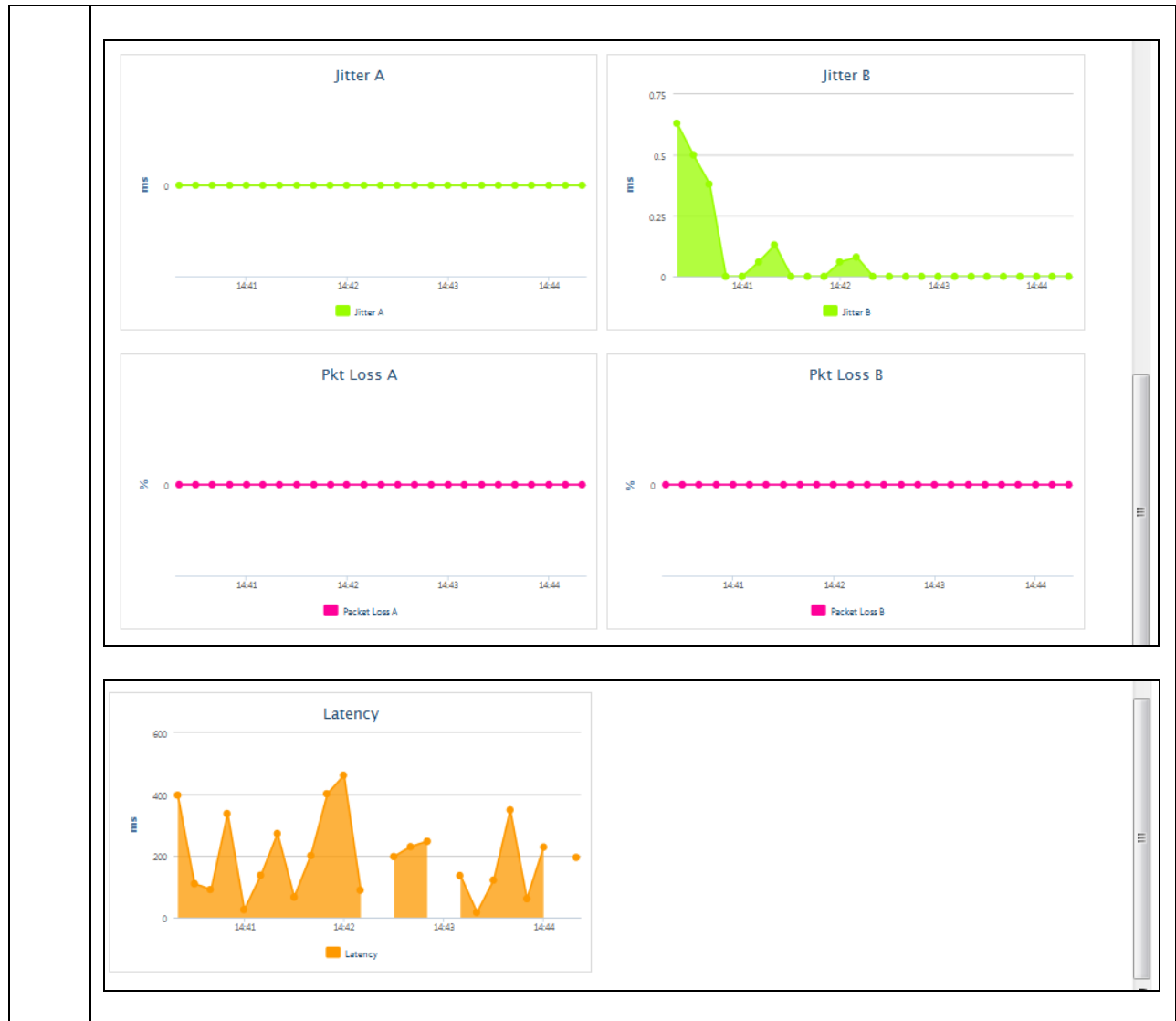
First Previous Next Last Rows on page 10

PBX Date Time	Call Manager	Calling Number	Called Number	Duration (s)	MOS	Packet Loss (%)	Jitter (ms)	Latency (ms)	Quality	Nb of Hops	Round Trip Time	Call Details
2013-11-11 14:40:26	CM	10001	10005	246	4.29 - 4.29	0.0 - 0.0	0 - 0	178 - 178	good	2 - 2	2 - 2	Call Details

First Previous Next Last Rows on page 10

Displaying result 1 - 1 of 1 calls





8. Conclusion

These Application Notes describe the steps required to configure ServicePilot ISM to interoperate with Avaya Aura® Communication Manager, including establishing a CDR link, sending RTCP data from the Avaya IP Telephones to ServicePilot ISM, enabling SNMP for collecting configuration data, and enabling ServicePilot ISM as an SNMP trap receiver. All test passed with observations in **Section 2.2**.

9. Additional References

The following Avaya documentation can be obtained on the <http://support.avaya.com>.

[1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, Issue 11.0, October 2013, Document Number 555-245-205.

[2] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 9.0, October 2013, Document Number 03-300509.

The following 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).

[3] ServicePilot® ISM QuickStart Guide, Release 8.3.1, November 2013

[4] ServicePilot UC datasheet for Avaya

[5] ServicePilot ISM Technical Overview for Avaya

[6] ServicePilot®ISM Administrator & User's Guide, Release 8.3.1, November 2013

©2014 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.