

Avaya Solution & Interoperability Test Lab

# Application Notes for NetIQ AppManager with Avaya Aura® Session Manager and Avaya Aura® System Manager – Issue 1.0

# Abstract

This document describes a solution comprised of an Avaya Aura® Session Manager, Avaya Aura® System Manager Release 7.0 and the NetIQ AppManager 9.1 in combination with Avaya 1100 Series IP Deskphones (SIP) on Avaya Communication Server 1000. AppManager is used to deliver systems management solution for the Session Manager, System Manager and 1100 Series SIP phones connected to the Session Manager. The monitoring described in this document is specific to the Session Manager (and associated System Manager) as well as to the SIP subscribers connected to Communication Server 1000 through the Session Manager. A NetIQ AppManager module (SNMP Traps) is used to monitor SNMP alarms for the Avaya Aura Session Manager and associated System Manager when the Session Manager is being used in place of the legacy Nortel NRS on Communication Server 1000.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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

This document describes a solution comprised of an Avaya Aura® Session Manager, Avaya Aura® System Manager Release 7.0 and the NetIQ AppManager 9.1 in combination with Avaya 1100 Series IP Deskphones (SIP) on Avaya Communication Server 1000.

AppManager is used to deliver systems management solution for Session Manager, System Manager and 1100 Series SIP Deskphones. The monitoring described in this document is specific to the Session Manager (and associated System Manager) as well as to the SIP subscribers connected to Communication Server 1000 through the Session Manager.

AppManager includes Knowledge Scripts create jobs that gather data for call quality and call activity metrics and stores the data in the SQL database. Each Knowledge Script can be customized to collect data for reporting and send proactive alerts for data in the supplemental database. The following Knowledge Scripts were run during the compliance testing:

- *Discovery\_SNMPtraps* script discover SNMP v3 source devices; in this case they are Session Manager and System Manager which require an additional handshake on engine ID.
- *SNMPTraps\_TrapMonitor* script monitor traps for SNMP v3 trap sources discovered from *Discovery\_SNMPtraps* script.
- *Discover\_NetworkDevice* script discovers the Session Manager and System Manager using SNMP to query the device characteristics such as SNMP, Interfaces, LAN Links, Host Resource and IP Subsystem.
- *Recommended* knowledge script group for monitoring each device discovered by *Discover\_NetworkDevice* script.
- Graph data: after a monitoring interval has been completed, data streams will be visible in the Graph Data pane for viewing in the chart.
- *Discovery\_SIPServer* script discover SIP Server and collect Session Manager call data monitoring.
- *SIPServer\_CollectCallData* script collect call data on Session Manager
- SIPServer\_CallQuality script reports call qualities such as MOS, R-Value, Jitter, latency and Packet Loss.

To perform the monitoring functions, AppManager uses the following interfaces into the Avaya IP Telephony environment.

- Simple Network Management Protocol (SNMP) AppManager uses SNMP to collect configuration and status information from Session Manager and System Manager.
- Session Initiation Protocol Event Package for Voice Quality Reporting (RFC6035 SIP) AppManager uses RFC6036 data from Avaya 1100 series IP Deskphones (SIP) to gather call quality metrics of a call. The call quality metrics include packet loss, latency, and jitter. From these metrics, the MOS (mean opinion score) and the R-Value are computed, which measure overall call quality.

# 2. General Test Approach and Test Results

The focus of this interoperability compliance testing was primarily to verify the basic functionalities of AppManager such as System Discovery SNMP v3, Reporting Events, Monitoring System Health, Device Inventory and Call Quality Reports. AppManager can work with Session Manager and System Manager System with no adverse impact on system or any other management interfaces.

The serviceability testing cases were performed by disconnecting and reconnecting the LAN cable to AppManager Server.

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

The general test approach was to integrate the AppManager into Avaya Communication Server 1000 system. The main objectives were to ensure that there is no adverse impact on the Communication Server 1000 system or any other management interfaces. The following features were executed during active calls:

- Discovery of Session Manager and System manager using SNMP v3.
- Retrieving inventories information from Session Manager and System Manager Device such as Interfaces, LAN Links, Host Resource and IP Subsystem.
- Monitor health of Session Manager and System Manager such as Uptime, Ping and Health.
- Viewing collected data using Graph Chart.
- Collecting call data on Session Manager.
- Collecting call qualities such as MOS, R-Value, Jitter, latency and Packet Loss.
- Viewing call quality using Graph Chart.

PM; Reviewed:
SPOC 6/14/2016

## 2.2. Test Results

The objectives outlined in Section 2.1 were verified and met. All tests were executed and passed.

# 2.3. Support

For technical support on AppManager, please contact NetIQ technical support team:

- **Telephone:** 1-713-418-5555
- Email: <u>Support@netiq.com</u>
- Web Site: <u>https://www.netiq.com/support/default.asp</u>

# 3. Reference Configuration

**Figure 1** illustrates the test configuration used during the compliance testing event between Avaya Communication Server 1000 Release 7.6 and AppManager 9.1.

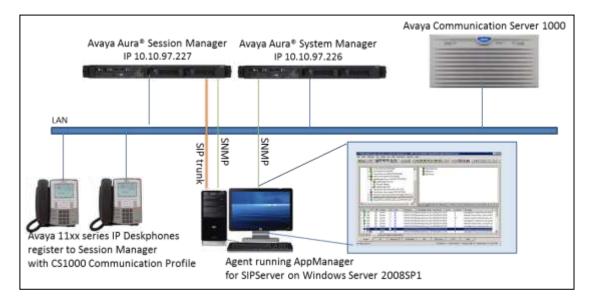


Figure 1: Test Solution Configuration

# 4. Equipment and Software Validated

Equipment/Software	Release/Version
Avaya Aura® Session Manager in Virtual	7.0 SP2
Environment	
Avaya Aura® System Manager in Virtual	7.0.0.2
Environment	
Avaya Communication Server 1000	7.6 SP7
Avaya 1100 Series IP Deskphones	4.4.23 (SIP)
NetIQ AppManager Server:	
Server hosting AppManager	Windows Server 2008 SP1
AppManager	SW Version 9.1 (Build 9.1.1.419)
AppManager for NetworkDevice	7.5.64
AppManager for SNMPTraps	8.1.14
AppManager for SIPServer	8.0.291

# 5. Configure Avaya Aura® Session Manager and Avaya Aura® System Manager

This section describes the steps to configure Session Manager and System Manger to work with AppManager.

Here is a summary of configuration on System Manager:

- Administer SNMPv3 User Profiles.
- Administer SNMPv3 Target Profiles.
- Assign SNMPv3 Target Profile to Avaya Aura® Session Manager and Avaya Aura® System Manager.
- Administer SIP trunk from AppManager to Avaya Aura® Session Manager.
- Create SIP user.
- Configure SIP phones to report quality of service to the AppManager.

## 5.1. Administer SNMPv3 User Profiles

In **Inventory** page, select **Manage Serviceability Agents**  $\rightarrow$  **SNMP3 User Profiles** and click on **New** button to add new user profile as used during compliance test, enter the following example used during compliance test:

•	User Name: Authentication Protocol:	Enter any descriptive name such as netiqDESSHA. Select SHA.
•	Authentication Password:	Enter any password, in this case default password was used, avaya123.
•	<b>Confirm Authentication Password</b>	Re-enter password.
•	Privacy Protocol:	Select DES.
•	Privacy Password:	Enter any password, in this case default password was used, avaya123.
•	Confirm Privacy Password:	Re-enter password.
•	Privileges:	Select Read/Write option.
Click	Commit to save changes.	

AVAYA			Last Logged on at A
Aura <sup>®</sup> System Manager 7.0			
Home Inventory ×			
Inventory	Home / Services / Inventory / Manag	e Serviceability Agents / SNMPv3 I	User Profiles
Manage Elements	New User Profile		Commit Back
Create Profiles and	New Oser Flome		Commic
Discover SRS/SCS	User Details		
Element Type Access			
Subnet Configuration	* User Name:		
▼ Manage	* Authentication Protocol:	SHA 💌	
Serviceability Agents	* Authentication Password:	•••••	
SNMPv3 User	* Confirm Authentication Password:	•••••	
Profiles	* Privacy Protocol:	DES 💌	
SNMP Target	* Privacy Password:	•••••	
Profiles	* Confirm Privacy Password:		
Notification Filter			
Profile	* Privileges:	Read/Write	
Serviceability	* De envire d		Constant Develo
Agents	*Required		Commit Back

# 5.2. Administer SNMPv3 Target Profiles

Configure Appmanager as target profile to receive traps. Navigate to **SNMP Target Profiles**, click on **New** button to add new target profile as profile display in below screenshot used during compliance test:

- Name: Enter any descriptive name, example: netiqDESSHAtraps.
- **Description:** Enter any description if needed.
- **IP Address:** Enter IP address of AppManager's PC, e.g., 10.10.98.27.
- **Port:** Use default value 162.
- Notification Type: Select Trap type.
- **Protocol:** Select V3.

AVAYA Aura <sup>®</sup> System Manager 7.0		
Home Inventory ×		
Tinventory	Home / Services / Inventory / Manage Serviceability Agents /	SNMP Target Profil
Manage Elements Create Profiles and	New Target Profile	Commit Back
Discover SRS/SCS	*	
Element Type Access	Target Details * Attach/Detach User Profile	
Subnet Configuration	Target Details 👳	
▼ Manage Serviceability Agents	* Name: netiqDESSHAtraps	
SNMPv3 User	Description: V3 SNMP trap	
Profiles	* IP Address: 10.10.98.27	
SNMP Target	* Port: 162	
Profiles	* Notification Type: Trap 💌	
Notification Filter Profile	* Protocol: V3 💌	
Serviceability		
Agents	*Required	Commit Back

To assign SNMPv3 user to SNMPv3 Target Profile, click on **Attach/Detach User Profile** tab, select user profile create in **Section 5.1** and click on Assign link to assign user to this new target profile. Click **Commit** to save changes.

## 5.3. Assign SNMPv3 Target Profile to Avaya Aura® Session Manager and Avaya Aura® System Manager

Navigate to **Serviceability Agents**, select Session Manager and System Manager in the Ag**ent** List as display in below screenshot.

reate Profiles and	Serviceability Age	ents			
scover SRS/SCS					
ement Type Access	Agent List				
bnet Configuration	Activate Manage Profil	es 🛛 Generate Test Ala	rm Repair Serviceability A	gent	
nage	2 Items 👌 Show All 💌 🛛	Click here to manage the profiles		Filter	: Enable
rviceability Agents	✓ Hostname	IP Address	System Name	System OID	Statu
SNMPv3 User	DevvmSM.bvwdev.com	1 .10.97.227	DevvmSM		activ
Profiles	devvmsmgr.bvwdev.com	1:.10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	activ
SNMP Target	Select : All, None				
Profiles					
Notification Filter					
Profile					
Serviceability					
Agents					

Click on Manage Profiles button verify selected Agents are listed in Selected Agents tab.

* Inventory	ome / Services / Inventory ,	/ Manage Service:	ability Agents / Serviceability Ag	ients				
Manage Elements	Manage Bastile			12000	mit Bac			
Create Profiles and Discover SRS/SCS	Manage Profile			Com	niti sec			
Element Type Access	Selected Agents SNMP	Target Profiles	SNMPv3 User Profiles					
Subnet Configuration	Selected Agents 💂							
<ul> <li>Manage</li> <li>Serviceability Agents</li> </ul>	2 Items 2 Filter: Enable							
SNMPv3 User	Hostname	IP Address	System Name	System OID	Status			
Profiles	DevvmSM.bvwdev.com	10.97.227	DevvmSM		active			
SNMP Torget	devymsmgr.bywdev.com	188.10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active			
Profiles								
Notification Filter				Com	mit Bad			
Profile				- Automation				
Serviceability								
Agents								

Click on **SNMP Target Profile** tab, select target profile create in **Section 5.2**, in this case, netiqDESSHAtraps and click on assign link as display below:

Inventory	tionic / ser	rices / the	entory / Manage Service	munt) rige	nee / service ability is	dener .				
Manage Elements	Mana	Manage Profile Commit Be								
Create Profiles and Discover SRS/SCS	Mana									
Element Type Access	Selecte	d Agents								
Subnet Configuration	Acci	gnable Pr	ofiles =							
<ul> <li>Manage</li> <li>Serviceability Agents</li> </ul>	Assig									
SNMPv3 User	2 Ibe	Click to Assign								
Profiles	Г	Name	Domair	Туре	IP Address	Port	SNMP Version			
SNMP Target		netigSNMPs	2 UDP		125.10.98.27	162	V2			
Profiles	2	netiqDESSH	Atraps UDP		13.10.98.27	162	V3			
Notification Filter	Select	t : All, None								
Profile		LL D	- Cl							
Serviceability	Rem	ovable Pi	ronies 🕴							
Agents	-									

Click on **SNMPv3 User Profiles** tab, select user created in **Section 5.1**, in this case netiqDESSHA as shown below.

- Inventory	Home / Servi	ces / Invent	ory / Manage Service	ability Agents / 9	Serviceability Agents					
Manage Elements	Manage	. Drafil				Commit Back				
Create Profiles and Discover SRS/SCS	Manage	Manage Profile Commit Ba								
Element Type Access	Selected									
Subnet Configuration	Assian	able Profi	les =							
* Monage Serviceability Agents	Assign									
SNMPv3 User	1 1t Cld.	to Assign								
Profiles	1 U	ser Name	Authentication	Protocol	Privacy Protocol	Privileges				
SNMP Target	n 14	etiqDESSHA	SHA		DES	R.				
Profiles	Select :	Ail, None								
Notification Filter Profile	Remo	vable Prof	iles 🔹							
Serviceability	Remove									
Agents	0 Items	2								

Click **Commit** button to save assigned user and target profiles as display below screenshot.

Manage Elements	Manage	Profile				Commit	Back	
Create Profiles and	Manage							
Discover SRS/SCS					_			
Element Type Access	Selected Age	ents SNM	IP Target Profiles	SNMPv3 User Profi	les			
Subnet Configuration	Assignat	le Profiles						
Manage								
Serviceability Agents	Assign							
SNMPv3 User	0 Items d	8						
Profiles	🔲 User M	User Name     Authentication Protocol     Privacy Protocol     Privileges						
SNMP Target	No re-	cords to displa	iy					
Profiles	Removal	ble Profile	s 💌				=	
Notification Filter								
Profile	Remove							
Serviceability	1 Item 🛛 🍣	à						
Agents	🗌 User	Name	Authentication	Protocol	Privacy Protocol	Privileges		
Synchronization	🗖 netic	DESSHA	SHA		DES	R		
	Select : All,	None						
						Commit	Deals	
						Commit	Back	

# 5.4. Administer SIP Trunk from AppManager to Avaya Aura® Session Manager

#### 5.4.1. Administer SIP Entity

In System Manager home page, select Element  $\rightarrow$  Routing  $\rightarrow$  SIP Entities and click on New button to create new entity for AppManager, enter the following value as shown in below screenshot which used during compliance test:

- Name: Enter any descriptive name, example: AppManagerAgent.
- FQDN or IP Address: Enter IP address of AppManager Agent, e.g., 10.10.98.27.
- **Type:** Select SIP trunk.

Leave default value for other fields. Click Commit to create new SIP Entity.

		Last Logged on at A
Aura <sup>©</sup> System Manager 7.0		
Hame Routing <sup>B</sup>		
Routing	Home / Elements / Routing / SIP Entitie	
Domains		Help ?
Locations	SIP Entity Details	Commit Cance
Adaptations	General	
SIP Entities	* Name:	AppManagerAgent
	* FQDN or IP Address:	10 10.98.27
Entity Links	-	
Time Ranges	Туре:	SIP Trunk
Routing Policies	Notes:	NetIQ server - agent
Dial Patterns		
Regular Expressions	Adaptation:	<b>•</b>
Defaults	Location:	Belleville 💌
	Time Zone:	America/Fortaleza
	* SIP Timer B/F (in seconds):	4
	Credential name:	
	Securable:	
	Call Detail Recording:	none
	Loop Detection	
	Loop Detection Mode:	On 🔽

#### 5.4.2. Administer Entity Links

In **Routing** page, select **Entity Links** and click on **New** button. Enter value for new Entity, below is an example of entity link used during compliance test.

- Name: Enter any descriptive name, e.g., LinkToAppManager.
- SIP Entity 1: Select Session Manager entity, e.g., DevvmSM.
- **SIP Entity 2:** Select AppManager entity created in **Section 5.4.1**.

Use default value for other fields. Click **Commit** to submit new entity link.

Norme / Electerits / Souting / E	Datity Links								
Entity Links				Commit Cancel					
1 Item 2	SEF Detay 3	Protocol	mica:	317 Entity 2	DNA Gverride	Port		Connection Policy	These sectors
Name     Select (All, Hone	* DerverSH		* SDED	*/desilierege-dgest		* 5060	i.	U-3360	Daty New Service
				Caninal Cenael					

## 5.5. Create SIP user

This step will describes steps to create SIP user for Avaya 1100 Series IP Deskphones register with Session Manager with Communication Server 1000 Communication Profile on System Manager. It is assumed Communication Server 1000, Session Manager and System Manager already installed, configured and operational.

In System Manager home page, select Users  $\rightarrow$  User Management  $\rightarrow$  Manage Users and click on New button to add new user. Enter the following information for user in Identity tab:

- Last Name: Enter any descriptive last name for user.
- First Name: Enter any descriptive first name for user.
- Login Name: Enter valid login name with domain name, e.g., <u>54353@bvwdev.com</u>.

lome / Users / User Management / Manage Users									
User Prof	User Profile Edit: 54353@bvwdev.com								
Identity *	Communication Profile	Membership	Contacts						
User Prov	isioning Rule 💩								
	User Pro	visioning Rule:		•					
Identity 🕤									
		* Last Name:	54353	]					
	Last Name (Lati	n Translation):	54353	]					
		* First Name:	54353	]					
	First Name (Lati	n Translation):	54353	]					
		Middle Name:		]					
		Description:	A V						
		Update Time :	February 23, 2016 2:2						
		* Login Name:	54353@bvwdev.com						
		User Type:	Basic	Y					
	<u>Ch</u>	ange Password		1					
		Source:							
	Localized	Display Name:	54353, 54353						

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. Configure **Communication Profile** tab – enter **Communication Profile Password**. And add new **Communication Address** as display below:

- **Type**: Use default value **Avaya SIP**.
- **Handle:** Enter user ID, in this case user extension: 54353.
- **Domain:** Enter valid domain, in this case bywdev.com.

User Pro	file Edit: 54353@	bvwdev.co	m			
Identity *	Communication Profile	Membership	Contacts			
Commun	ication Profile 💩					
		Communic	ation Profile P	assword: <u>Edi</u>		
😂 New	😂 Delete 📄 Done 💈	3 Cancel				
Name						
Prime						
Select : No	ne					
				* Name: Primary		
				Default : 🖉		
	Communication A	ddress 💌				
	🖉 New 🥒 Edit	🤤 Delete				
	🗖 Туре			Handle	Domain	
	🗖 Avaya SIP			54353	Dvwdev.com	
	Select : All, None					
	🖸 Session Manage	er Profile 🕚				
	🗖 CM Endpoint Pr	ofile 🔮				
	🖸 CS 1000 Endpoi	int Profile 📲				
	🗖 CallPilot Messa	ging Profile 🖲				

In Session Manager Profile – select Session Manager Information as shown below and click Commit to submit this new user. Then re-open this user again to configure CS 1000 Endpoint Profile.

<ul> <li>Primary Session Manager</li> </ul>		<b>R</b> _1, <b>1</b> , <b>1</b>	Essertions	Marian an
	Q DevvmSM	Primary 8	Secondary D	Maximum 8
Secondary Session	Q			
Manager Sumiushilitu Sexuer	0			
	Q			
Max. Simultaneous Devices	1 💌			
Block New Registration When Maximum Registrations Active?				
Application Sequences				
Origination Sequence	(Nane)			
Termination Sequence	(Nane)			
Call Routing Settings				
<ul> <li>Home Location</li> </ul>	Belleville 💌			
Conference Factory Set	(Nane)			
Call History Settings				
Enable Centralized Call History?				

Enter information of Communication Server 1000 (CS1000) as display below:

- System: Select available CS1000 system in dropdown list, e.g., EM on cppm3 used, with cppm3 is the name of CS1000 used during compliance test.
- Add New or Link Existing: Choose appropriated option, in this case: Add New.
- **Target**: Choose appropriated option, e.g., Customer 0.
- **Template**: Select template for SIP phone.
- **Prime DN**: Enter any available DN, e.g., 54353.
- **Terminal Number:** Enter available TN, e.g., 104 0 0 1.

Click **Commit** button to save changes.

Communication Address 💌		
🖉 New 🕜 Edit 😂 Delete		
Г Туре	Handle	Damain
Avaya SIP	54353	Dvwdev.com
Select : All, None		
🖻 Session Manager Profile 🔋		
🗖 CM Endpoint Profile 🔮		
CS 1000 Endpoint Profile		
<ul> <li>System</li> </ul>	EM an cppm]	
<ul> <li>Target</li> </ul>	Customer0	
Template	SIPPhone	
Service Details	DN=54353(Marped), TN=104 0 00 01, TYPE=UEXT-SIPL	<u>∧</u> ▼
Update	]	
Include in Corporate Directory	<b>•</b>	
Delete Endpoint on Unassign of Endpoint from User	T.	
CallPilot Messaging Profile 👂		

# 5.6. Configure SIP phones to report quality of service to the AppManager

Select two 1100 series phones for a test. Ensure that the address of the AppManager agent has been configured in the phones in the associated device configuration file as described at [1]. The agent IP being used below is 10.10.98.27.

```
VQMON_PUBLISH YES
VQMON_PUBLISH_IP 10.10.98.27 <- agent IP goes here, tested agent was 10.10.98.27
SESSION_RPT_EN YES
SESSION_RPT_INT 30
LISTENING_R_ENABLE YES
LISTENING_R_WARN 70
LISTENING_R_EXCE 60
PACKET_LOSS_ENABLE YES
PACKET_LOSS_WARN 256
PACKET_LOSS_EXCE 1280
DELAY_ENABLE YES
DELAY_WARN 150
DELAY_EXCE 175
JITTER_ENABLE YES
JITTER_ENABLE YES
JITTER_ENABLE YES
JITTER_ENABLE YES
JITTER_ENABLE YES
```

Check the phone display to make sure that

- The AppManager address has downloaded correctly from the configuration file.
- The timestamp displayed on the phone is correct.

# 6. Configure NetlQ AppManager

This section describes the steps to configure AppManager. This section assumes that AppManager has been installed. For more information about installing AppManager or about AppManager system requirements, refer to **Section 9**. The configurations explained are:

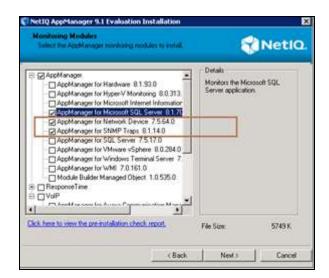
- AppManager Installation
- Activate the Netiq Trap Receiver Service
- Launch NetIQ Console
- Administer SNMPv3 trap Monitoring
- Administer SIP Call Quality Monitoring

## 6.1. AppManager Installation

In addition to the Core AppManager installation, the following product-specific AppManager modules should be installed:

- <u>AppManager for NetworkDevice</u>
- <u>AppManager for SNMPTraps</u>
- <u>AppManager for SIPServer</u>

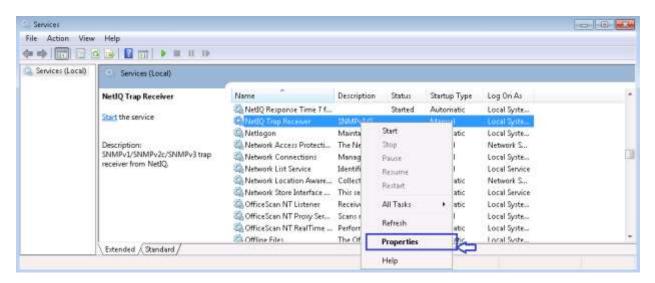
NetworkDevice and SNMPTraps modules are included in the AppManager 9.1 evaluation package available at <u>https://www.netiq.com/products/appmanager/trial.html</u> and may be selected during the installation of the AppManager 9.1 evaluation package.



SIPServer is an Add-on module, installed as separately downloadable MSI.

## 6.2. Activate the NetIQ Trap Receiver Service

When AppManager for SNMPTraps is initially installed, the NetIQ trap receiver is not activated. To activate the NetIQ trap receiver: Click Start on the agent computer, click in the Start Search box, and type services.msc to access the windows services menu. Right-click on NetIQ Trap Receiver service, select **Properties**.



From the windows services menu as shown below and select "automatic" as the service start type. Click **OK** to save changes.

**	2 🕞 🛛 📺 🕨 💷 💷	NetQ Trap Receiver Properties (Local Computer)	
Services (Local)	Shart the service Description: SNMPv1/SNMPv2c/SNMPv3 trap receiver from NetBQ.	General     Log On     Recovery     Dependencies       Met     Service name:     NetIQ     Trap Receiver       NetI     Display name:     NetIQ     Trap Receiver       NetI     Description:     SNMPv1/SNMPv2c/SNMPv3 trap receiver from NetIQ     E       NetI     Path to executable:     E     E       NetI     Path to executable:     E       Starkup typg:     Marcal     Ice       Neto     Starkup typg:     Marcal       Help me: conflore:     Automate:     Description:	
		Office         Displicit         R           Office         Statt         Stopped         R           Office         Statt         Stopped         R           You can specify the start parameters that apply when you start the service toon here.         Start parameters         R	

## 6.3. Launch NetlQ Console

In the NetIQ server navigate to Start  $\rightarrow$  All Programs  $\rightarrow$  NetIQ  $\rightarrow$  AppManager $\rightarrow$  Operator Console (not shown).

Select the required **Server** and **Repository** from the drop down menu and click on **Logon** as shown in below. During compliance testing **Use Windows authentication** was selected.

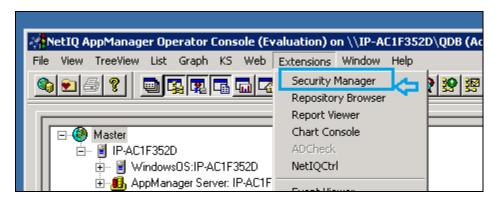
NetIQ AppManag	er Operator Console Logon	×
<u>S</u> erver: <u>R</u> epository:	WIN-GVS7GTBD3BS\SQLEXPRESS	
	ormation: /indows authentication <u>Q</u> L Server authentication	
Net	IQ® AppManager®	
Logon	<u>O</u> ffline <u>E</u> xit <u>H</u> elp	

## 6.4. Administer SNMPv3 Trap Monitoring

#### 6.4.1. Configure Security Manager

To enable AppManager to use SNMP to access Session Manager and System Manager devices, the SNMP community strings are required to be configured in the AppManager Security Manager.

From the AppManager Operator Console window navigate to **Extensions**  $\rightarrow$  **Security Manager** as shown in below.



Add a custom profile:

🐥 NetIQ AppManager Security Mana	ager (Evaluation) on \\IP-AC1F352D\QDB (Administrator)	
Security View Help		
🔹 😓 🕵 🤶		
	Computer: IP-AC1F352D	
⊕ ∰ AppManager Users ⊢… 🗑 Computers	Exchange Exch2000/2003 Oracle SAP SMS SNMP SQL WebLog Custom	
i⊟ iei Computers IP-AC1F352D	This information is stored in the AppManager repository.	
	<u>C</u> ustom Label	
	Label Sub-Label	
	A <u>dd</u>	

Enter the System Manager SNMPv3 User Profile created in **Section 5.1** as example display below used during compliance test for Security Manager:

- Label: Enter any descriptive name, e.g., SNMPTraps.
- Sub-Label: Enter System Manager's IP Address, e.g., 10.10.97.226
- Value 1: Enter user name created in Section 5.3.
- Value 2: Enter \*.
- Value 3: Enter user created in Section 5.3 passwords, e.g., sha,avaya123,des,avaya123.

Create the same entry with Sub-Label set to the Session Manager IP address, e.g., 10.10.97.227 as displayed below:

Modify Custom Entry 🛛 🗙	Modify Custom Entry
You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.	You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.
Label : SNMPTraps	Label : SNMPTraps
<u>S</u> ub-Label: 1.10.97.226	Sub-Label: 1: 10.97.227
Value <u>1</u> : netiqDESSHA	Value <u>1</u> : netiqDESSHA
Value <u>2</u> : *	Value <u>2</u> : *
Value <u>3</u> : sha,avaya123,des,avaya123	Value <u>3</u> : sha,avaya123,des,avaya123
<u>Extended application support</u> (Click Help for details.)	Extended application support (Click Help for details.)
OK Cancel <u>H</u> elp	OK Cancel <u>H</u> elp

#### 6.4.2. Discover the Device

To monitor SNMP trap source devices that require the use of SNMP version 3, run the Discovery\_SNMPTraps Knowledge Script on the agent computers which monitor those source devices.

Navigate to the "**Discovery**" tab and drop the "SNMPTraps" Discovery KS (Knowledge Script) on the agent machine in the treeview to create the discovery job.

MAN     MAN     MAN     MAN     MACHINE     MACHINE     MACHINE     MACHINE     MACHINE     MACHINE	SANNOS SANN SANN SANNOS Datesallulus SANNOS	Hindows     H	Reportper     Reportper     Reportper     Reportper     Reportper     Reportper     Some     Some     Some     SouthTran     SouthTran	∰urts ∰handan ∰handantg
---	--	---	--	-------------------------------

On the job creation panel, enter the name and IP address of the session manager

Properties for Discovery_SNMPTraps		×
Schedule Values Actions Objects Advanced		
Description	Value	Units
General Settings		
Job Failure Notification		
Event severity if discovery job fails unexpectedly	5 📫	Severity
Event Details		
Event detail format	HTML Table 🔹	
- Additional Settings		
+ Tracing (for advanced users only)		
+ Raise event if discovery succeeds?	🔽 Yes	
Raise event if discovery fails?	🔽 Yes	
- Update the TreeView object name if the device name changed since the previous discovery?	🔽 Yes	
-Name of the device to populate in the TreeView	devvmsm	
IP address of the device to populate in the TreeView	10.10.97.227	
-File containing the list of device name/IP address pairs to populate in the TreeView		
- Trap Receiver IP address	localhost	
Trap Receiver TCP port	2735	
Discovers known SNMP trap-throwing devices that forward their traps to a NetlQ Trap Receiver serv raises events to indicate discovery status (succesful, failed).	rer. Raises an event if the job fails and	optionally
<b>M</b>	UN Lancei	нер

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. Confirm that Session Manager appears in the TreeView (which confirms the SNMPv3 credentials are valid and the NetIQ trap receiver service is available on the agent), in this case, it is Trap Source: devvmsm[10.10.97.226] and Trap Source: devsmgr[10.10.97.227]

🚧 NetIQ AppManager Operator Consol	le (Evaluation) on \\WIN-GV	/S7GTBD3B5\SQI	EXPRESS\QDB (	Administrator)		
<u>File View TreeView List Graph K</u> S V	We <u>b</u> E <u>x</u> tensions <u>W</u> indow <u>H</u>	elp				
\$ • 5 ?   • <b>5</b>		œ   <del>29</del>   30   3⊠   3	J 38 30 10	isi olol	<b>⊾ ≋ </b> ∎  m	<b>S</b> AME E A
			2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2			
			1			1
⊡ 📑 WIN-GVS7GTBD3BS		<b>_</b>	Network	Device		
💮 🚽 Windows0S:WIN-GVS70	GTBD3BS		📗 \land SIPServi	er		
Networks-RT:WIN-GVS7			📗 🖰 SQLServ	ver		
🕀 🧱 Call Performance:WIN-G						
	GTBD3BS\SQLEXPRESS					
i gin and solution for the second se						
⊕      ⊕ H.323:WIN-GVS7GTBD3     ⊕      ⊕ SIP:WIN-GVS7GTBD3B3						
Terminal Server:WIN-GV						
WMI Server:WIN-GVS70						
🗄 🔂 AppManager Server: WII						
🕂 🌈 Trap Source: devvmsm [	[1 10.97.227]					
🖉 Trap Source: devvmsmg						
	iystem-Manager [10] 10.97.226]	<b>_</b>				
I to the function Decompleter					GENTLESS A AMA	ADMIN ) AMHEALTH ) ASYNI
Event 🔍 🗹 Status 🗅	Job Computer Knowl	edge Script   Last	Occurre Count	Severity Mes:	sage	
🕀 🗑 1391 🛛 🧭 Closed 🗋	0 WIN-GVS7GTBEAMHea	alth_Healthch 3/25	/2016 12:026	25 MS H	ealthcheck Event:	Server Up
	78 WIN-GVS7GTBEDiscov	ery_SIPServe 3/23.	/2016 3:17: 2	10 SIP S	erver Discovery Fai	iled
	76 WIN-GVS7GTBEDiscov	ery_Network[3/23.	/2016 11:194	5 Netw	orkDevice Discover	ry Failed
	74 WIN-GVS7GTBESNMP				an't locate job	
	<u>72</u> WIN-GVS7GTBEDiscov					discovery successful [WIN-0
🕀 🗑 1369 🛛 🧭 Closed 🗋	70 WIN-GVS7GTBEDiscov	ery_SNMPTra3/25/	/2016 12:113	25 Disco	ivery: SNMPTraps o	discovery successful [WIN-(
Events Jobs Details	\Graph Data /					
Master NT Ne	etworks-RT VolPQuality	SQL	SQLServer	WTS	WMI	]
For Help, press F1			Computers	: 1 Open Events	: 0 Running Jobs:	10 Graph Data: 12 1:24 PM //

### 6.4.3. Start Trap Monitoring

Next, run the SNMPTraps\_TrapMonitor Knowledge Script on the agent computer and any SNMPv3 trap sources discovered in the treeview.

Wew Troel	lew La	st. Graph	KS W	ebi Exte	nsions Window Help	20\Q08 (Administrator) (2) 왕 왕 년 왕 왕 타 타	<u> </u>		<u></u>	reas sea sea sea
	4C1F38 Winds AppM Trap S	52D anoger Serv Source: Ava Source: Ava	ver IP-Al waVM-ad	c1F3520 m [ 10.10	97.227 1		AG ) DISCOVERY	A GENERA	L / Нуреву/)	
Event	0 2	Status	B	Job	Computer	Knowledge Script	Lat 0.	Count	Severity	Message
<ul> <li>39</li> <li>25</li> </ul>	:8	Open Open	00		IP-AC1F3520 IP-AC1F3520	Discovery_SNMPTraps Discovery_SNMPTraps	3/17/2016 1 3/17/2016 1		25 25	Discovery, SNMPTraps discovery successful (PACIF3 Discovery, SNMPTraps discovery successful (PACIF3
ARTELEA	Events /	Jobs A Di	otals A	liaph Da	10/				100	

In the job detail make sure **Monitor devices not yet discovered?** and **Raise event if Trap Receiver become available**? options are checked.

Description	Value	Units
⊤ General Settings		
Job Failure Notification		
Event severity if TrapMonitor job fails unexpectedly	5	🔶 Severity
- Event Details		
– Event detail format	HTML Table	-
<ul> <li>Trap source address format</li> </ul>	Both	-
-Format trap data according to SNMP version?	SNMPv2	-
- Include prefix information to format event messages for Netcool adapter?	🗖 Yes	
+ Varbind display options		
+ Trap Filters		
Additional Settings		
Monitor devices not yet discovered?	Yes	
<ul> <li>Custom message mapping file</li> </ul>	SNMPTraps_AlarmMa	appings.csv
+ Tracing (for advanced users only)		
Monitor SNMP Traps		
Event Notification		
+ Raise critical alarm event?	🗹 Yes	
+ Raise major alarm event?	🗹 Yes	
+ Raise cleared/resolved alarm event?	Yes	
🕂 Raise event if Trap Receiver is unavailable?	🗹 Yes	
Haise event if Trap Receiver becomes available?	🗹 Yes	
		ien traps are receive

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. Finally, generate a test trap from the System Manager by select system to send trap, in this case they are Session Manager and System Manager, then click on **Generate Test Alarm** button as display in below screenshot:

lome Inventory *				Ga	
Inventory 4	Home / Services / Inventory / M	lanage Serviceability Ag	ents / Serviceability Agents		
Manage Elements					Hel
Create Profiles and Discover SR5/SCS	Serviceability Age	nts			
Element Type Access	Agent List				
Subnet Configuration	Automa Manage Profile	Generate Test Ala	rm Repair Serviceability A	gent	
Manage Serviceability Agents	2 Items 🤰 Show All 💌		Click here to generate Test Alarm	Filter	; Enable
SNMPv3 User	🗹 Hostname	IP Address	System Name	5ystem 010	Statu
Profiles	devvmsmgr.bvwdev.com	100.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
SNMP Target Profiles	Content : All, None	111110.97.227	DevvmSM		active
Notification Filter Profile					
Serviceability Agents					

The test trap and any subsequent traps received will be reported in the AppManager console as events:

AppMer Tingi So	D of5(PACTENED opp: Sever (PACTENED unit Anaphill and (DC2017) unit Anaphill and (DC2017)			€ hadrifi ∰ Traphtonko			
			. स्वास	•T##\Action\Ant\Ant	NTLESSXAM	рин Умаатці у міліс у ред у рержін у санант у ниди у н.	нтарма
Event (0 (0)		Corpute	Knowledge Scrut	Lan Occur. Court	Seven	Message	
0 94 000	Igan 110	IPACIE 3500	Knowledge Screet SNMPTraps_TrapHonton	Lan Occur. Court 3/17/2016 8:05 4	l Berenki 20	Message (Arage/Message/Hours(10.204.136.240)) Test elementar for feating anty, no recovery estimation records	e/
	Advandadge Event Op Okee Event		Knowledge Scrut	Lan Occur. Court	Seven	Message	e/
	Advandadge Event Op Okee Event	PAC#350 PAC#350 PAC#350	Knowledge Sorge SINMPTraps_TrapHoretor SINMPTraps_TrapHoretor Decovery_SINMPTraps	Las Occar, Court 3/17/2016 8:05 4 3/17/2016 8:05 4 3/17/2016 1:25 3	Serenti 20 20 20 20 25	Message     Message     Message     More 10,204,136,240 [] Test alive to feeting only, no recovery estim record     More VAL entrol 0.2044/36/2017 [not alive to feeting only, increased action occurs     Decrements 314497 [size alicence security] (PC-11753.01)     Decrements 31447 [size alicence security] (PC-11753.01)	e/
A Contraction of the second se	Annovember Street Annovember St	PAC#350 PAC#350 PAC#350	Knowledge Sorge SINMPTraps_TrapHoretor SINMPTraps_TrapHoretor Decovery_SINMPTraps	Las Occar, Court 3/17/2016 8:05 4 3/17/2016 8:05 4 3/17/2016 1:25 3	Serenti 20 20 20 20 25	Message Kooge/Million(10.204.136.240) Test alians to hoting only isomeorying action rescent Kooge/Million(10.204.136.240) and alians to hoting only, isomeorying action rescent Decrementy StelleTissign decorrely successful (FE421F3620) Decorrely StelleTisign decorrely successful (FE421F3620)	7
	Advantation Event Close Event N Group By + Hen + Ne +	PAC#350 PAC#350 PAC#350	Knowledge Sorge SINMPTraps_TrapHoretor SINMPTraps_TrapHoretor Decovery_SINMPTraps	Las Occar, Court 3/17/2016 8:05 4 3/17/2016 8:05 4 3/17/2016 1:25 3	Serenti 20 20 20 20	Message     Message     Message     More 10,204,136,240 [] Test alive to feeting only, no recovery estim record     More VAL entrol 0.2044/36/2017 [not alive to feeting only, increased action occurs     Decrements 314497 [size alicence security] (PC-11753.01)     Decrements 31447 [size alicence security] (PC-11753.01)	7
A Contraction of the second se	Annovember Street Annovember St	PAC97520 PAC97520 PAC97520	Knowledge Sorge SINMPTraps_TrapHoretor SINMPTraps_TrapHoretor Decovery_SINMPTraps	Las Occar, Court 3/17/2016 8:05 4 3/17/2016 8:05 4 3/17/2016 1:25 3	Serenti 20 20 20 20	Message Kooge/Million(10.204.136.240) Test alians to hoting only isomeorying action rescent Kooge/Million(10.204.136.240) and alians to hoting only, isomeorying action rescent Decrementy StelleTissign decorrely successful (FE421F3620) Decorrely StelleTisign decorrely successful (FE421F3620)	7
A Contraction of the second se	Annovelage Dreet Addressedge Dreet Close Dreet Group By Homosoft Detail Nessage.	PAC97520 PAC97520 PAC97520	Knowledge Sorge SINMPTraps_TrapHoretor SINMPTraps_TrapHoretor Decovery_SINMPTraps	Las Occar, Court 3/17/2016 8:05 4 3/17/2016 8:05 4 3/17/2016 1:25 3	Serenti 20 20 20 20	Message Kooge/Million(10.204.136.240) Test alians to hoting only isomeorying action rescent Kooge/Million(10.204.136.240) and alians to hoting only, isomeorying action rescent Decrementy StelleTissign decorrely successful (FE421F3620) Decorrely StelleTisign decorrely successful (FE421F3620)	7

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved.

#### 6.4.4. Administer Network Device

AppManager for NetworkDevice discovers the session and system manager using SNMP to query the device characteristics. To use SNMP, create the SNMP access credentials as follows: First, create an SNMP profile for the session manager. Note that this is different from the "Appmanager for SNMPTraps" profile created in **Section 6.4.1** because it is for snmp-get requests from the networkDevice module. Here we are entering SNMPv3 profile for session manager and system manager by select security manager:

👫 NetIQ AppManager Operator Console (Ev	aluation) on \\IP-AC1F352I	D\QDB (Ac
File View TreeView List Graph KS Web	Extensions Window Help	
\$ • <i>• • • • • • • • • </i>	Security Manager	) <u>:0</u> :2
	Repository Browser	
	Report Viewer	
🖃 🛞 Master	Chart Console	
🖻 🔋 IP-AC1F352D	ADCheck	
🗄 🖷 🗑 Windows0S:IP-AC1F352D	NetIQCtrl	
🗄 🔠 AppManager Server: IP-AC1F	Event Barren	

Add a custom profile for Network Device:

🍓 NetIQ AppManager Security Man	ager (Evaluation) on \\IP-AC1F352D\QDB (Administrator)	
Security View Help		
<b>*</b>		
E ∯ AppManager Security ⊕ ∰ AppManager Roles	Computer: IP-AC1F352D	
	Exchange Exch2000/2003 Oracle SAP SMS SNMP SQL WebLogic Custom	
i Computers IP-AC1F352D	This information is stored in the AppManager repository.	
	Label Sub-Label	
	Add	

Enter the system manager SNMP profile into security manager. If all devices on your network will use the same SNMP configuration, enter "default" as the label2 string. If they are each different, enter the active IP address of the device as the label2 string:

Enter the System Manager SNMPv3 User Profile created in Section 5.1 as example display below used during compliance test for Security Manager:

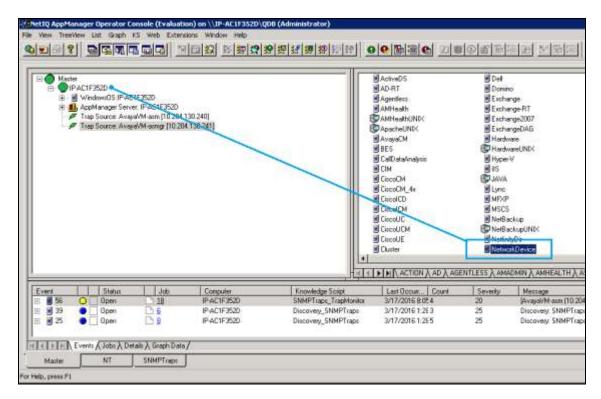
- **Label**: Enter any descriptive name, e.g., NetworkDevice.
- **Sub-Label**: Enter System manager's IP Address, e.g., 10.10.97.226.
- Value 1: Enter user name created in Section 5.3, e.g., netiqDESSHA..
- Value 2: Enter \*.
- Value 3: Enter user created in Section 5.3 passwords, e.g., sha,avaya123,des,avaya123.

Create the same entry with Sub-Label set to the Session Manager IP address, e.g., 10.10.97.227.

Modify Custom Entry 🛛 🗙	Modify Custom Entry
You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.	You can store custom values in the KPW table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.
Label : NetworkDevice	Label : NetworkDevice
<u>S</u> ub-Label: 1 10.97.226	Sub-Label: 1 .10.97.227
Value <u>1</u> : netiqDESSHA	Value <u>1</u> ; netiqDESSHA
Value <u>2</u> : ×	Value <u>2</u> : ×
Value <u>3</u> : sha,avaya123,des,avaya123	Value <u>3</u> : sha,avaya123,des,avaya123
Extended application support (Click Help for details.)	Extended application support (Click Help for details.)
OK Cancel <u>H</u> elp	OK Cancel <u>H</u> elp

### 6.4.5. Discover the Device

Navigate to the "Discovery" tab and drop the "NetworkDevice" Discovery KS on the agent machine in the treeview to create the discovery job for the devices.



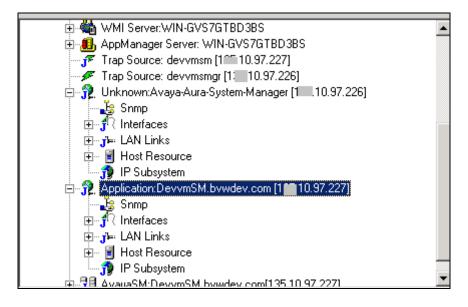
Enter the IP address of the Session Manager and System Manager in the job properties for List of network devices (comma-separated), in this case 10.10.97.227,10.10.97.226.

Description	Value	Units
Auto Discovery		
- Default gateway router		
- Maximum number of hops	1	Hops
- CAUTION: Enabling can negatively impact network performance		
└─ Walk subnets for layer-2 devices? (y/n)	n	
List of network devices (comma-separated)	10.10.97.226,10.10.97.227	
List of network device ranges (comma-separated)		
Full path to file with list of network devices		
Discovery Details		
Discovery timeout	10	Minutes
Raise event when discovery succeeds? (y/n)	2	
Event severity when discovery succeeds	25	Severity
Event severity when discovery fails	5	Severity
covers network devices: routers, switches, gateways, etc. You can specify a dresses, a gateway router for auto-discovery, or the name of a file that contains cause only one computer should act as a proxy for a given network device, dr inager with SNMP version and security information (community string for SNMP fore you can discover network devices.	device names on separate lines. Specify at lease op this script on only one computer at a time. You	st one remote compu u must update Secur

Discovery will create treeview objects for the session manager and system manager using SNMP Unknown: Avaya-Aura-System-Manager [10.10.97.226] and Application: DevvnSM.bvwdev.com[10.10.97.227] Discovery Network OK.

	SQL Server WIN- H 323 WIN-GVS7 SIP-WIN-GVS70 Teminal Server WIN- AppManager Sen Trap Source: dev Trap Source: dev	TBD3BS VIN-GVS76TBD3I -GVS7GTBD3BS ver: WIN-GVS76T vmmp [10] 10.97 vmmpg [10] 10.9	SQLEXPRESS 85 180.385 227)	_	E Netwo SPSe E SOLSe	e'vey			
	Application Devvi			+1	1 million	-			
* 9	Application Devvi	n/SM bywdev oon	10 97.2271	1	- Cognitional acceleration	benerative and a	in the second	ess X amadi	MIN入AMHEALTH入AS
Event 0	Application Deven	nSM bywdev con	(1 10.97.227]	*) Knowledge Script	Last Occur	Severity	Hessage	and the second	
i yent 0	Application Devin	n SM bivedevicion	Computer WIN-GVS7GTB	Transledge Script	M 4/22/2016 3:08	Severity 25	Message Trap leceiver	(135.10.98.27)	is re-connected
(vent 0 142 • 141 •	Application Devin	nSM bividev.com	Computer WIN GVS7GTB WIN GVS7GTB	Knowledge Scrip (SNMPTispi_Trep (SNMPTispi_Trep	Laik Occur M 4/22/2016 3:08 M 4/22/2016 3:08	Severity 25 25	Hessage Trap leceiver Trap leceiver	(135.10.98.27) (135.10.98.27)	is re-connected
Event 0 142 0 141-0 144 0	Application Dreven	nSM biviev con	Computer WIN GVS7GTB WIN GVS7GTB WIN GVS7GTB	Encontedge Script (SNMPTisps_Trap (SNMPTisps_Trap (Discovery_SIPSer	H Last Occur M 4/22/2016 3:08 M 4/22/2016 3:08 m 4/22/2016 3:18	<u>Severity</u> 125 125 115	Hessage Trap receiver Trap receiver The supplement	(1 25 10.98 27) (1 25 10.98 27) rital database '	is re-connected lis re-connected SIPServe_DevvmSM.br
Event 0 142 0 144 0	Application Dreven	nSM bividev.com	Computer WIN-GV57GTB WIN-GV57GTB WIN-GV57GTB WIN-GV57GTB WIN-GV57GTB	Knowledge Scrip (SNMPTispi_Trep (SNMPTispi_Trep	Lask Occur M4/22/2016 3:08 M4/22/2016 3:08 W4/22/2016 3:08 W4/22/2016 3:18 W3/25/2016 1:04	Severity 125 125 115 115	Hessage Trap teceiver Trap teceiver The supplement The supplement	(1 25 10.98 27) (1 25 10.98 27) rital database '	is re-connected lis re-connected SIPServe_DevvmSM b SIPServe_AvayaAuss5r
Event 0 142 141 141 144 144 144 144 144	Application Dreven	nSM bividev con	(† 10.97.227) Computer WINGVS7GTB WINGVS7GTB WINGVS7GTB WINGVS7GTB WINGVS7GTB	Enowledge Script (SNMPTieps_Trep (SNMPTieps_Trep (Discovery_SIPSer (Discovery_SIPSer	M 4/22/2016 3.08 M 4/22/2016 3.08 M 4/22/2016 3.08 w 4/22/2016 3.18 w 3/25/2016 1.04 w 3/23/2016 3.17	Severity 225 225 215 215 215 215	Message Trap teceiver Trap teceiver The suppleme The suppleme SIP Server Do	(135.10.98.27) (135.10.98.27) Intel database Intel database acovery Failed	is re-connected lis re-connected SIPServe_DevvmSM b SIPServe_AvayaAuss5r
	Application Dewn	nSM bividevi con	Consuler WIN GVS7GTB WIN GVS7GTB WIN GVS7GTB WIN GVS7GTB WIN GVS7GTB WIN GVS7GTB	Transledge Scrip (SNMPTispt_Trap (SNMPTispt_Trap (Discovery_SIPSer (Discovery_SIPSer (Discovery_SIPSer	Last Occur M 4/22/2016 3:08 M 4/22/2016 3:08 M 4/22/2016 3:18 M 3/25/2016 1:04 M 3/25/2016 1:04 M 3/23/2016 3:17	Severity 25 25 25 25 25 25 25 25 25 25 25 25 25	Message Trap receiver Trap receiver The supplement SIP Server Di Notice Difference	(135.10.98.27) (135.10.98.27) Intel database Intel database acovery Failed	jis re-connected Jis re-connected SIPServer_DevvmGM bi SIPServer_AvayahuseSr IS (140-110.97,227)
(vert 0) 142 0 141 0 144 0	Application Devin Devin Dpen Open Open Closed Closed Closed Closed	nSM bividevi con	(1 10.97.227) Computer WIN GVS7GTB WIN-GVS7GTB WIN-GVS7GTB WIN-GVS7GTB WIN-GVS7GTB WIN-GVS7GTB	Enoministan Script (SNMPTrept_Trep (SIMPTrapt_Trep (Discovery_SIPSer (Discovery_SIPSer (Discovery_SIPSer (Discovery_SIPSer (Discovery_Network)	Last Occur M 4/22/2016 3:08 M 4/22/2016 3:08 M 4/22/2016 3:08 M 4/22/2016 3:18 M 3/25/2016 1:04 M 3/25/2016 1:2 3 M 3/23/2016 1:1 1:	Severity 25 25 25 25 25 25 25 25 25 25 25	Message Trap leceiver Trap leceiver The supplement The supplement SIP Server Di NetworkDawn	(135.10.98.27) (135.10.98.27) Intal database intal database	jis re-connected Jis re-connected SIPServer_DevvmGM bi SIPServer_AvayahuseSr IS (140-110.97,227)
werk () 1 414 1 414 1 414 1 414 1 414 1 414 1 414 1 41 1	Application Devin     Den     Dpen     Dpen     Dpen     Dpen     Decod     Closed     Closed     Closed	nSM binideri con D S D S D S D 105 D 109 D 28 D 28 D 25	Computer WIN-GVS7GTB WIN-GVS7GTB WIN-GVS7GTB WIN-GVS7GTB WIN-GVS7GTB WIN-GVS7GTB WIN-GV57GTB WIN-GV57GTB	Trowledge Scrip (SNMPTsept_Trap (SNMPTsept_Trap (Discovery_SIPSer (Discovery_SIPSer (Discovery_SIPSer (Discovery_Network) (Discovery_Network)	Levil Occurr M 4/22/2016 3:08 M 4/22/2016 3:08 M 4/22/2016 3:18 M 3/25/2016 1:04 M 3/25/2016 1:04 M 3/23/2016 3:17 M 3/25/2016 1:2 3 M 3/23/2016 1:1 1: M 4/20/2016 4:26	Severity 225 225 215 215 215 215 210 217 210 217 217 217 217 217 217 217 217 217 217	Message Trap leceiver Trap leceiver The supplement SIP Server Dr NetworkDawn NetworkDawn Network Dev	(135.10.98.27) (135.10.98.27) Intel defabere intel defabere incovery Falod in Discovery Falod in Discovery Fi	jis re-connected jis re-connected SIPServer_DevvmSM b SIPServer_AvayafuseSr IS [1 as 10.87,227] alad

Click on the TreeView object to verify that platform details are available for both session and System Manager are listed such as Snmp, Interfaces, LAN links, Host Resource and IP Subsystem.



Srang     Interfaces     H      Host Resources     H      Host Resources     IP Subsyste	en a-Aura-System Manager   1 ace	# 437 ]	on D annos		
200 8000	5) Status Childre			COMMENDED	

Start the **NetworkDevice** recommended knowledge script group for monitoring each device.

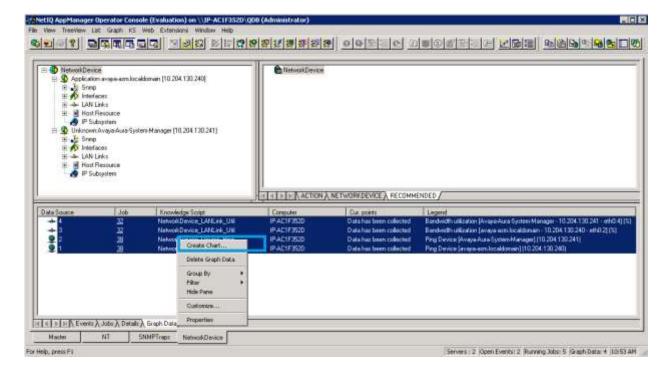
Confirm that the following device monitoring jobs have started: NetworkDevice\_Device\_Uptime, NetworkDevice\_Device\_Ping, NetworkDevice\_Interfaces\_Health, NetworkDevice\_IPSubsystem\_Ulti and NetworkDevice\_LANLink\_Ulti as shown in below screenshot.

	LAN Link     Host Res     Host Res     IP Subsy UnknowncAv     Snep     Interface     LAN Link     Host Res     IP Subsy	ource dem aya-Aura-System s s ource	Manager ( <sup>to 10</sup>	*		RECOMMENDED /	
				H			
Jab	18 0 10	A Status	Children	, H.	Knowledge Script	Use	Submit Time   Stop Time
Jab 39 39	8 6	Burning	I Ohiden	1,22	Knowledge Script NetworkDevice_Device_Uptime		Submit Time Stop Time 3/21/2016 10.5 (Name)
Jab 9 39 9 37	8 6	Burning Burning	Children 1	Conquier	Knowledge Script	Use	
	8 6	Burning Burning	I Children 1 1 1	P AC1F3520	Knowledge Script NetworkDevice_Device_Uptime	User IP ACTE3520 Widninistration	3/21/2016 10.5 (Naneo
37	8 6	Burning Burning	Chiden 1 1 1	PACIF3520 IPACIF3520 IPACIF3520	Knowledge Script NetworkDevice_Device_Uptime NetworkDevice_Device_Ping	PACIF3520 Administrator PACIF3520 Administrator PACIF3520 Administrator	3/21/2016 10.5 (Noneo 3/21/2016 10.5 (Noneo

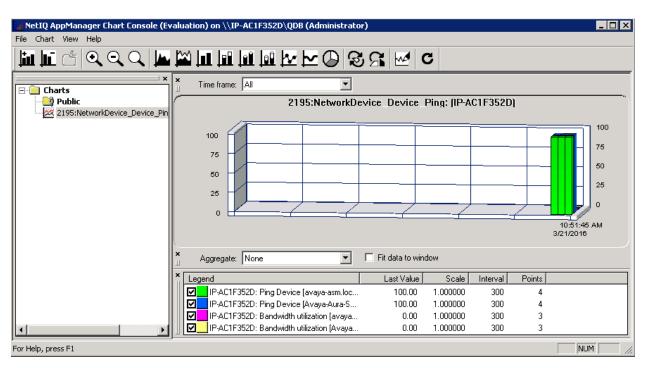
After a monitoring interval has been completed, data streams will be visible in the Graph Data pane as shown in below screenshot.

E 2 Sorro E 2 Sorro E 4 LAN L E 1 Heat F	n avaga-arm loca osc reko kootuace kyoten Avaga-Aura Syste cen wko lesource	kloniain (10.304.330.240) en-Maniager (10.204.130.241)	Anterest Device		
Data Source	Link	Knowledge Script	Computer	Cur, powls	Legerd
4 4 3 9 2 9 1	305 32 32 32 32 32	Networkperson_LANLink_Util NetworkDevice_LANLink_Util NetworkDevice_Device_Prog NetworkDevice_Device_Prog	PAC1F3520 IPAC1F3520 IPAC1F3520 IPAC1F3520 IPAC1F3520	Data has been collected Data has been collected Data has been collected Data has been collected	Laggerol Sandeidti uklandori (Avage-Ause-System-Manager - 10.204.130.241 - wh0.4[[2 Bandeidti uklandori (avage-aus localdonain - 10.204.130.240 - wh0.2](11) Ping Device (Avage-Ause-System-Manager)(10.204.130.241) Ping Device (avage-aus localdonain) (10.204.130.240)

This data may be displayed as a graph using "Create Chart" as display in below screenshot.



Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved.



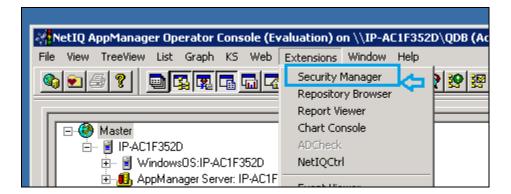
Below display the NetworkDevice\_Device\_Ping data in graphic chart.

## 6.5. Administer SIP Call Quality Monitoring

AppManager for SIPServer can discover the Session Manager using either SNMP or by manually configuring the device characteristics. To use SNMP, the SNMP v3 credentials previously created on session manager in **Section 5.1** will need to be entered into Security Manager for the SIPServer module.

#### 6.5.1. Administer Security Manager for SIP Server

In AppManager console, select **Extensions**  $\rightarrow$  **Security Manager**.



In Custom tab, click on Add button

🍓 NetIQ AppManager Security Man	ager (Evaluation) on \\IP-AC1F352D\QDB (Administrator)	_ 🗆 🗵
Security View Help		
<b>* *</b>		
⊡	Computer: IP-AC1F352D	
🗄 📆 AppManager Users 🖃 🗑 Computers	Exchange Exch2000/2003 Oracle SAP SMS SNMP SQL WebLogic Custom	
IP-AC1F352D	This information is stored in the AppManager repository.	
	Custom Label	
	Label Sub-Label	
	Add	

Enter the SNMPv3 User Profile created in **Section 5.1** as example display below used during compliance test for Security Manager:

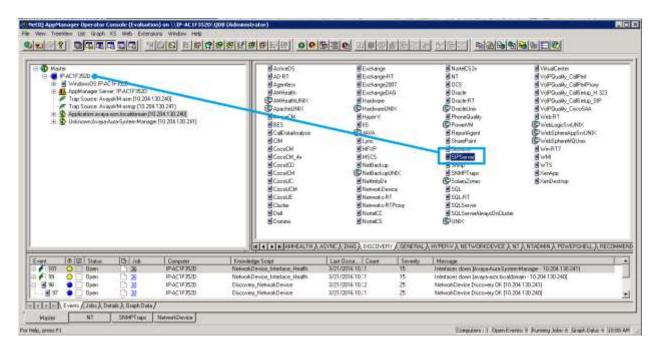
- Label: Enter any descriptive name, e.g., SIPServer.
- **Sub-Label**: Enter Session Manager's IP Address, e.g., 10.10.97.227.
- Value 1: Enter user name created in Section 5.3, e.g., netiqDESSHA.
- Value 2: Enter \*.
- Value 3: Enter user created in Section 5.3 passwords, e.g., sha,avaya123,des,avaya123.

Add Custom Entry	×
AppManager repository.	lues in the KPW table of the Enter at least a Label, Sub-label, and ots can access these values using the inction.
Label :	SIPServer
Sub-Label:	10.10.97.227
Value 1:	netiqDESSHA
Value 2:	×
Value 3:	sha,avaya123,deslavaya123
	Extended application support (Click Help for details.)
OK	Cancel Help

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved.

#### 6.5.2. Discover Device

Navigate to the "Discovery" tab and drop the "SIPServer" Discovery KS on the agent machine in the TreeView to create the discovery job for the devices.



In the Discovery\_SIPServer job properties, enter the following IP as display below:

• Comma-separated list of SIP Servers: Enter IP address of the session manager, e.g.,

10.10.97.227.

- Setup supplemental database? Check Yes option.
- SIP identity of the collector:

<u>SIP:pvqmservice@localhost:5060;transport=UDP</u>.

Description	Value	U
General Settings		
Job Failure Notification	1	
Baise event if discovery succeeds?	Ves Ves	
Baise event if discovery fails?	Ves Ves	
Plaise event if database setup succeeds?	🐼 Yes	
🗄 Raise event if database setup fails?	Ves Ves	
Discover SIP Servers		
- Discovery method	SNMP Query	
⇔ → SNMP Settings		
- Connie separated list of SIP servers	10.10.97.227	
- Full path to file with list of SIP servers	- Interest - Learning	
- SNMP message timeout	120	Second:
- SNMP task timeout	3600	Second: Second:
L SNMP retries	4	- Attempts
System Properties for Manual Configuration		
Discover SIP Quality Of Service Reporting Interface?	Yes	
SIP identity of collector (example sip:collector@localhost:5060;transport=UDP)	sip:pvgmtervice@localhost506	0,transport=UDP
	Yes	-
Start pruning job on supplemental database?	Yes	
SQL Server Information	1 m	
-SQL Server \ instance name (leave blank for default)		
SQL database user name (leave blank for windows)		

Confirm that a TreeView object for the session manager call data monitoring is created.

Ketti AppManager Operator Conside (cratication) on VUP-ACTF3520 (dol Re Very Tremen La Graph K5 Web Extensions Weday help Port 2 Part	(Administrator) - [SUServer] 新述講教授》
	INTERVIEW RECOMMENDED (SIPSERVER /
I SPSev Master NT SNMPTisp: Network/Device SPSev or Help, press P1	- John Sverker 1 Köpen Sverker D Running Jobs: 0 (Grigh Data: 0 111:12

PM; Reviewed: SPOC 6/14/2016 Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. 39 of 47 AppMgrCallQlty

#### 6.5.3. Collect Call Data

Start data collection by dragging the CollectCallData script to drop on the Session Manager TreeView instance.

Hale Line Action & RECOMMENDED & SIPSERVER /	

In the SIPServer\_CollectCallData job properties, verify all the following options are checked as display in below screenshot.

Properties for SIPServer_CollectCallData		×
Schedule Values Actions Objects Advanced		,
Description	Value	Units
General Settings		
Job Failure Notification		
+ Raise event if call data collection is unavailable?	🗹 Yes	
Raise event if call data collection warning?	🗹 Yes	
Raise event if call data collection is available?	🔽 Yes	
Monitor Call Data Collection Availability		
- Data Collection		
Collect data for Call Data Collection Availability?	Yes	
Monitors the availability of call data collection for SIP quality of service (QoS) sources. Raises an even collection is unavailable or available. Also raises an event when call data collection raises a warning for record from being saved to the database.		
	OK Cancel	Help

Confirm that the SIP trunk to AppManager now shows inservice by navigating to the **Session** Manager  $\rightarrow$  System Status  $\rightarrow$  SIP Entity Monitoring menu, selecting "run monitor" for the trunk just created in Section 5.4.

Verify this trunk will remain in-service (**Conn Status** is UP) as long as the CollectCallData job is running on the agent.

one / Linimon / Arthur i	tanoger / System St	and four chart	Monitoring				Help 7
IP Entity, Entity	Link Conne	ction Statı	IS				
s page displays detailed con sion Manager instances to a		entity links from a	all				
All Entity Links to SIP I	Entity: AppMana	gerAgent.					
				Status Details for the s	elected Session Mana	ger:	
Summary View							
Litzens Refresh							Filter: Enable
Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
DevvmSM	165.10.98.27	5060	UDP	FALSE	UP	200 OK	UP

## 6.5.4. Start Data Reporting Job

Start the Data Reporting job with parameters to even on all calls. Use the CollectCallQuality knowledge script to create a reporting job.

Image: Operator Console (Evaluation) on \/IP-AC1F352D\QDB (Administrator)         File View TreeView List Graph KS Web Extensions Window Help         Image: Participation of the state of the st
SIPServer Call Data SIP Voice Quality Call Data SIP Voice Quality Call Data CallQuality CollectCallData SubsetAgentQuality CollectCallData SubsetAgentQuality CollectCallData SubsetAgentQuality CollectCallData
Data Source         Job         Knowledge Script         Computer         Cur. points         Legend
Master         NT         SNMPTraps         NetworkDevice         SIPServer
Done Servers : 1 Open Events: 0 Running Jobs: 0 Graph Data: 0 10:40 AM

In SIPServer\_CallQuality, select Monitor Average MOS  $\rightarrow$  Event Notification  $\rightarrow$  Raise event if average MOS falls below threshold? and set the MOS threshold for reporting very high (5.0) – this will ensure that all calls create events, allow confirming that data is collecting and reporting properly for testing purpose as display below, leave all other fields at their default value.

Description	Value		Units	
General Settings				
+ Job Failure Notification				
+ Raise event if no records found?	🗖 Yes			
Call Details				
Include call details?	🗹 Yes			
Query Filters				
– Minimum duration	0	* *	Seconds	
– Maximum table size	50	-	Rows	
– Maximum duration (0 to ignore)	0	+	Seconds	
– Calling Party				
<ul> <li>Party connector</li> </ul>	AND	-		_
Called Party				
• Troubleshooting				
Monitor Average MOS				
Event Notification				
- Raise event if average MOS falls below threshold?	Ves			
- Threshold Average MOS	5.0			
$\square$ Event severity when average MOS falls below threshold	5	-	Severity	
Collect data for average MOS?	🗹 Yes			
Monitor Average R-Value				

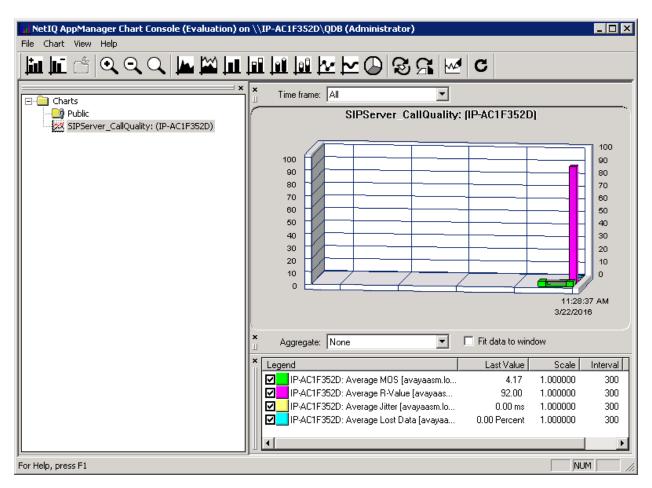
Make a call between two SIP phones.

Use the chart console to confirm that data has been collected for the calls made. The default reporting interval is 5 minutes, so you may need to wait up to 5 minutes to see results post to the chart:

View Treat/leve L	a Gash is w Galacia Galacia avayaam boakter	wit(10.204.130.240)	<u>Q</u> BBRR:	Control State		e decentra <b>le c</b> ete
Data Source	Job 12 50	Receivings Solpt SPS-ever Collocation SPS-ever_CollectCalDate	Computer IPAG19550 IPAG19550	Cur pants	Rected	Legend Average MOS (avegesime localdoment = 10, 11, 57, 257
IIIII NEwrote	A Jobs ), Details	Gisph Data /		Group By + Filter + Hole Pane		
Master	10-11 (10-11) (10-11)	MPTrape NetworkDevice	SIPServer	Customes, Properties		Servers ( 1, Open Events: + Running Jobsi 2, Graph Da

Enter any desciptive name, example below just just default name:

Chart Title - Provide a title and color scheme	for the chart.		NetIO
Chart Title	BPServe CADURY	IPACIESCO	
Color Scheme	Delault	E	
	🗂 Display dates and ti	nes based on the local	ime of the managed computer
		< Back	Finish Can



Graph data below display MOS, R-Value, jitter and Lost Data in the chart.

# 7. Verification Steps

The following tests were conducted to verify the solution between the Session Manager, System manager and SIP phones register to Session Manager with CS1000 Communication Profile and AppManager Application.

• Verify SIP trunk to AppManager is up and running:

AVAVA Via 59807 Managar 7.0									
Home Service Natager	•								
* Session Hanager	. 160	nec / Elements / Sex	sion Menager / System Sta	tus / AIP Critit	y Nanitaring				
flashboard									
Session Manager Administration	SIP Entity, Entity Link Connection Status This page displays detailed connection status for all entity links from all								
Communication Profile Editor	Sea	rion Manager Instan	ces to a single SIP entity.						
> Network Configuration	1	of Entity Links to	s SIP Entity: AppMan	agecAgent				Statu	Details for the selected Session Manage
<ul> <li>Denics and Location</li> <li>Configuration</li> </ul>		Summary Vev							
Application		I Items Refresh							
Configuration	1	Session Manager	SIP Entity Restrived IF	Part	Proto	2.4	Deny	Com Status	Reason Code
- System Status	0	DevenSM	105.10.98.27	5060	UDP		FALSE	UP	200 OK
SIP Entity Honitaring									
Hanaged Bandwidth Usage									
Security Medule									

- Verify AppManager can collect device information for Session Manager and System Manager, see **Section 6.4.4** and **6.4.5** for example screenshot detail of collected data.
- Make a phone call and verify AppManager reports Call Quality as mentioned in Section 6.5.3 and display collected data in the graph in Section 6.5.4.

# 8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 2**. The NetIQ AppManager 9.1 is considered compliant with Avaya Aura® Session Manager and Avaya Aura® System Manager and Avaya 1100 Series IP Deskphones (SIP phone registers to Session Manager with CS1000 Communication Profile).

# 9. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at <u>http://support.avaya.com</u>.

#### Avaya:

- 1. *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, Release 4.4, NN43170-600, Issue 06.06 Standards, December 2015.
- 2. Administering Avaya Aura® Session Manager, Release 7.0, Issue 1, August 2015.
- 3. Administering Avaya Aura® System Manager, Release 7.0, Issue 1, January 2016.

Product documentation for NetIQ AppManager may be found at https://www.netiq.com:

- 4. Administrator Guide NetIQ® AppManager®, April 2016. https://www.netiq.com/documentation/appmanager-9/pdfdoc/administratorguide/administratorguide.pdf
- 5. NetIQ Online help document for Device support for AppManager: <u>https://www.netiq.com/documentation/appmanager-</u> <u>modules/appmanagerforsipserver/data/b19cptxp.html</u>
- 6. NetIQ Online help document for SNMP Traps Knowledge Scripts: <u>https://www.netiq.com/documentation/appmanager-</u> modules/appmanagerforsnmptraps/data/snmptraps\_trapmonitor.html

#### ©2016 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and <sup>TM</sup> 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 <u>devconnect@avaya.com</u>.