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.

2.2. Test Results

The objectives outlined in S**ection 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:** Support@netiq.com
- **Web Site:** https://www.netiq.com/support/default.asp

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.

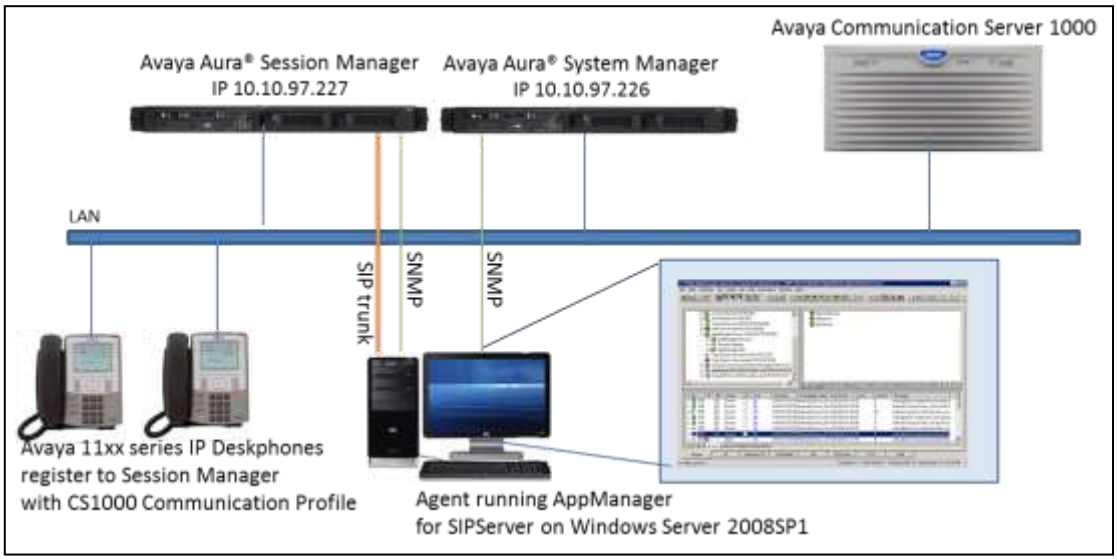


Figure 1: Test Solution Configuration

4. Equipment and Software Validated

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

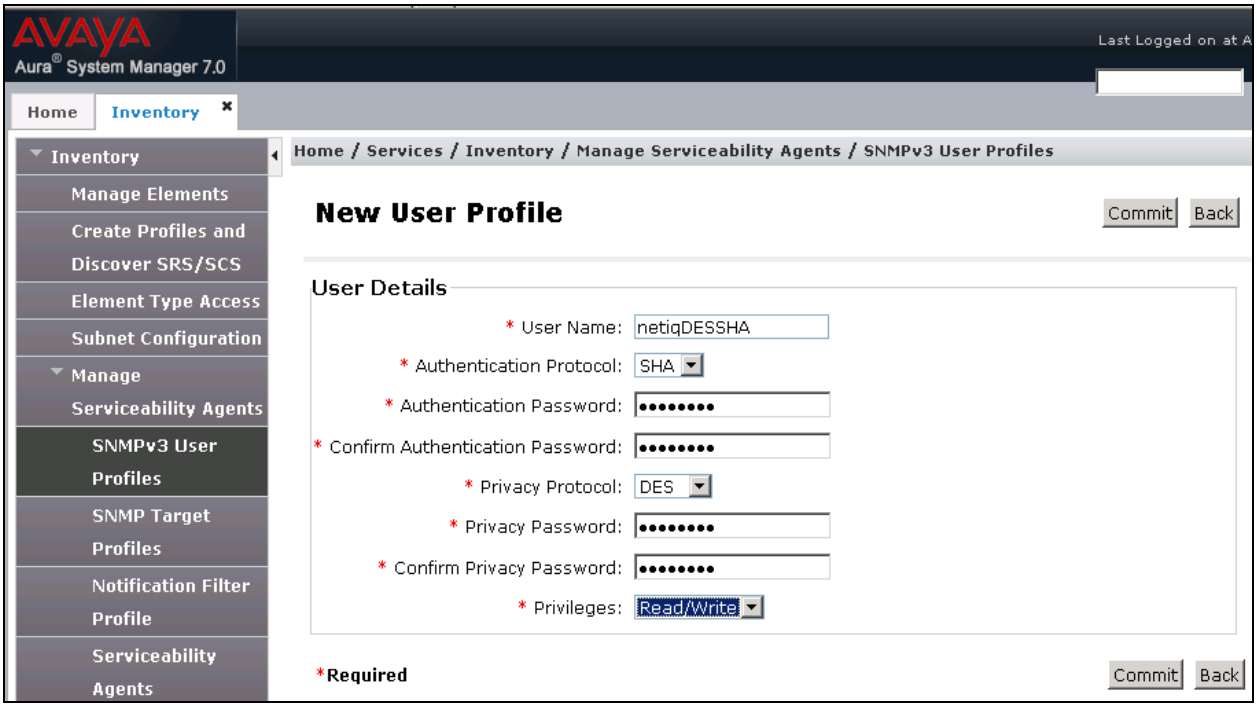
- Administer SNMPv3 User Profiles.
- Administer SNMPv3 Target Profiles.
- Assign SNMPv3 Target Profile to Avaya Aura® Session Manager and Avaya Aura® System Manager.
- Administer SIP trunk from AppManager to Avaya Aura® Session Manager.
- Create SIP user.
- Configure SIP phones to report quality of service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

5.1. Administer SNMPv3 User Profiles

In **Inventory** page, select **Manage Serviceability Agents → 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:** Enter any descriptive name such as netiqDESSHA.
- **Authentication Protocol:** Select SHA.
- **Authentication Password:** Enter any password, in this case default password was used, avaya123.
- **Confirm Authentication Password:** 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.

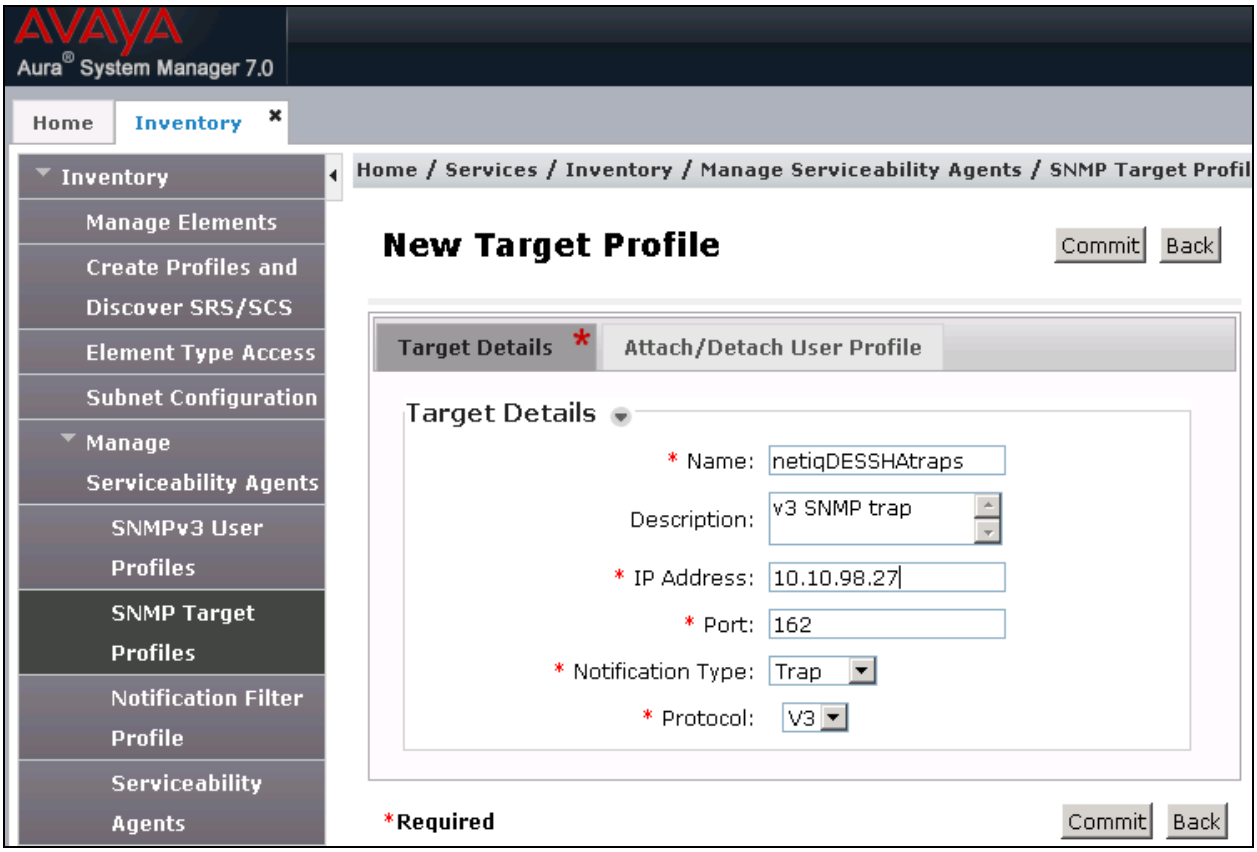
Click **Commit** to save changes.



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:

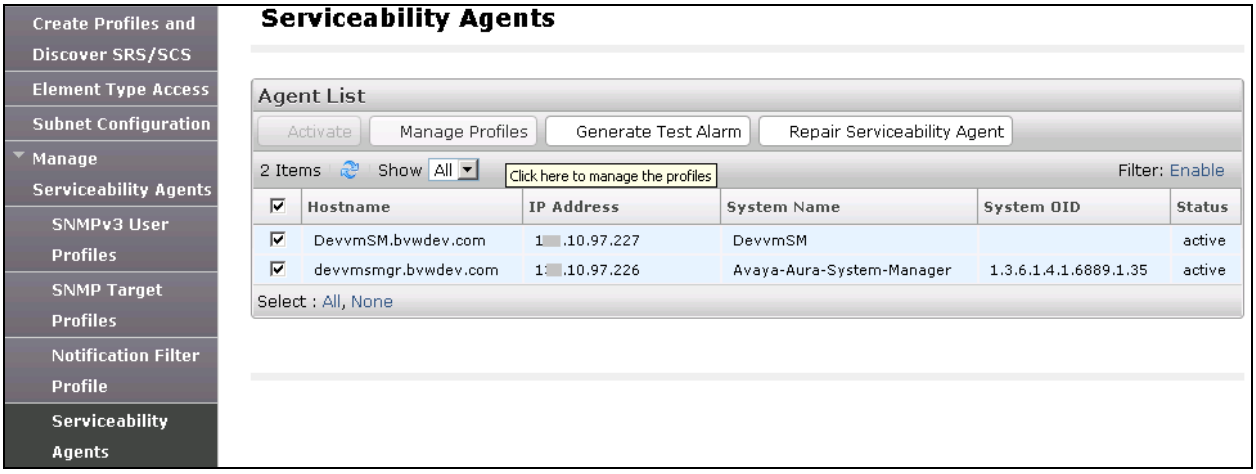
- **Name:** Enter any descriptive name, example: netiqDESSHAtraps.
- **Description:** Enter any description if needed.
- **IP Address:** Enter IP address of AppManager's PC, e.g., 10.10.98.27.
- **Port:** Use default value 162.
- **Notification Type:** Select Trap type.
- **Protocol:** Select V3.



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.

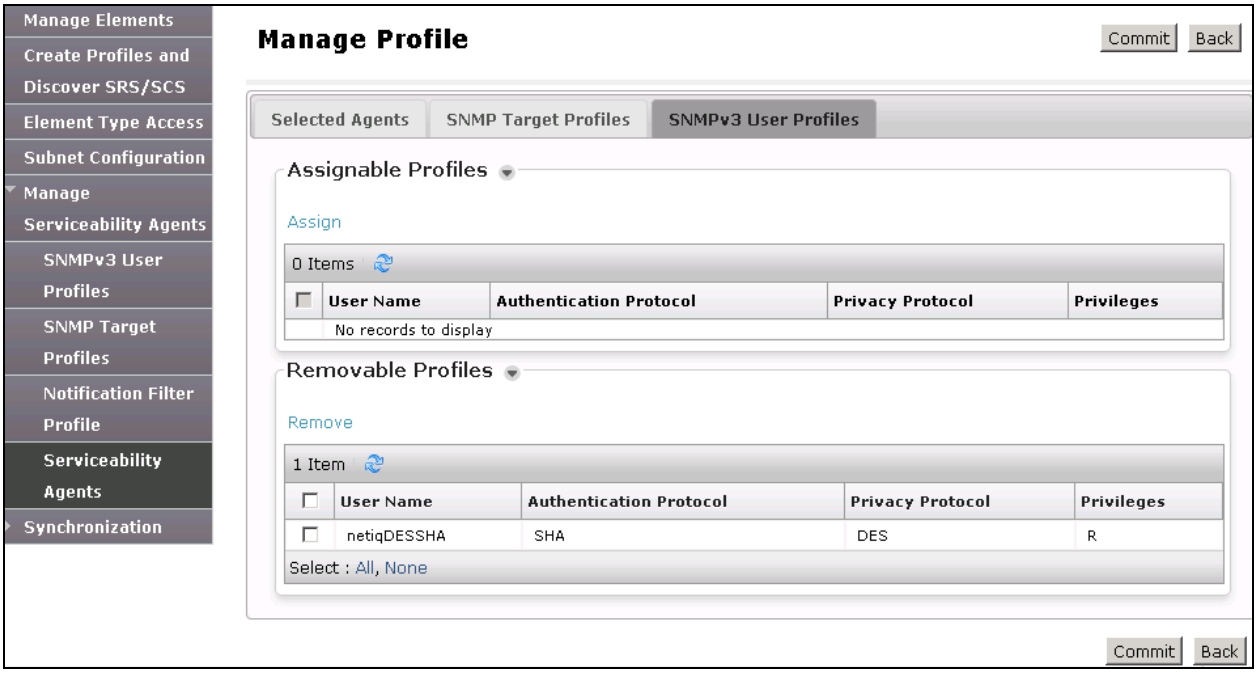


Click on **Manage Profiles** button verify selected Agents are listed in **Selected Agents** tab.

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:

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

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



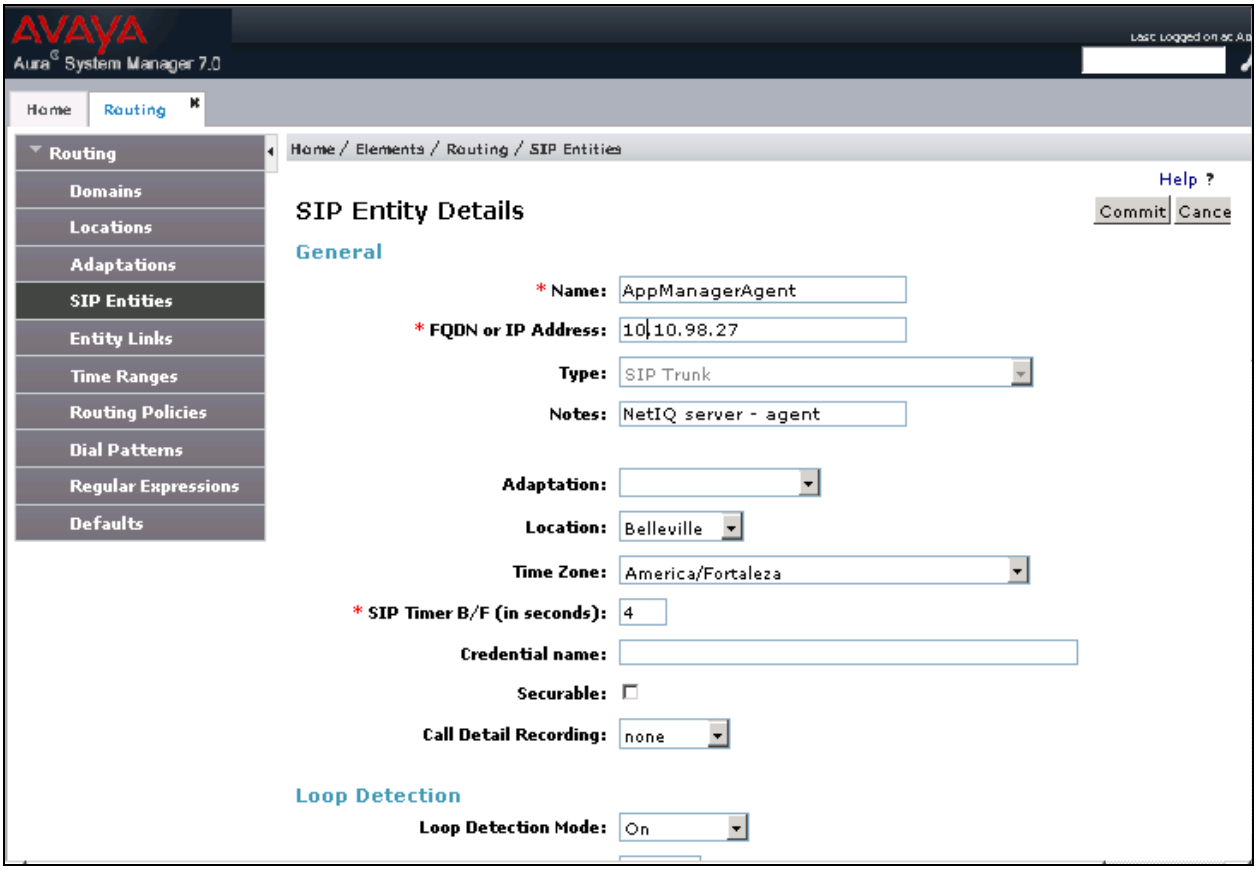
5.4. Administer SIP Trunk from AppManager to Avaya Aura® Session Manager

5.4.1. Administer SIP Entity

In **System Manager** home page, select **Element → Routing → 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.

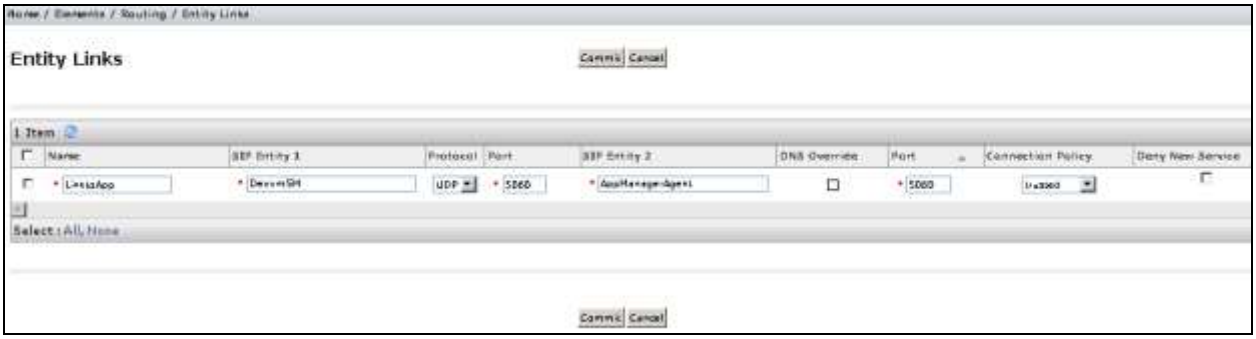


5.4.2. Administer Entity Links

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.

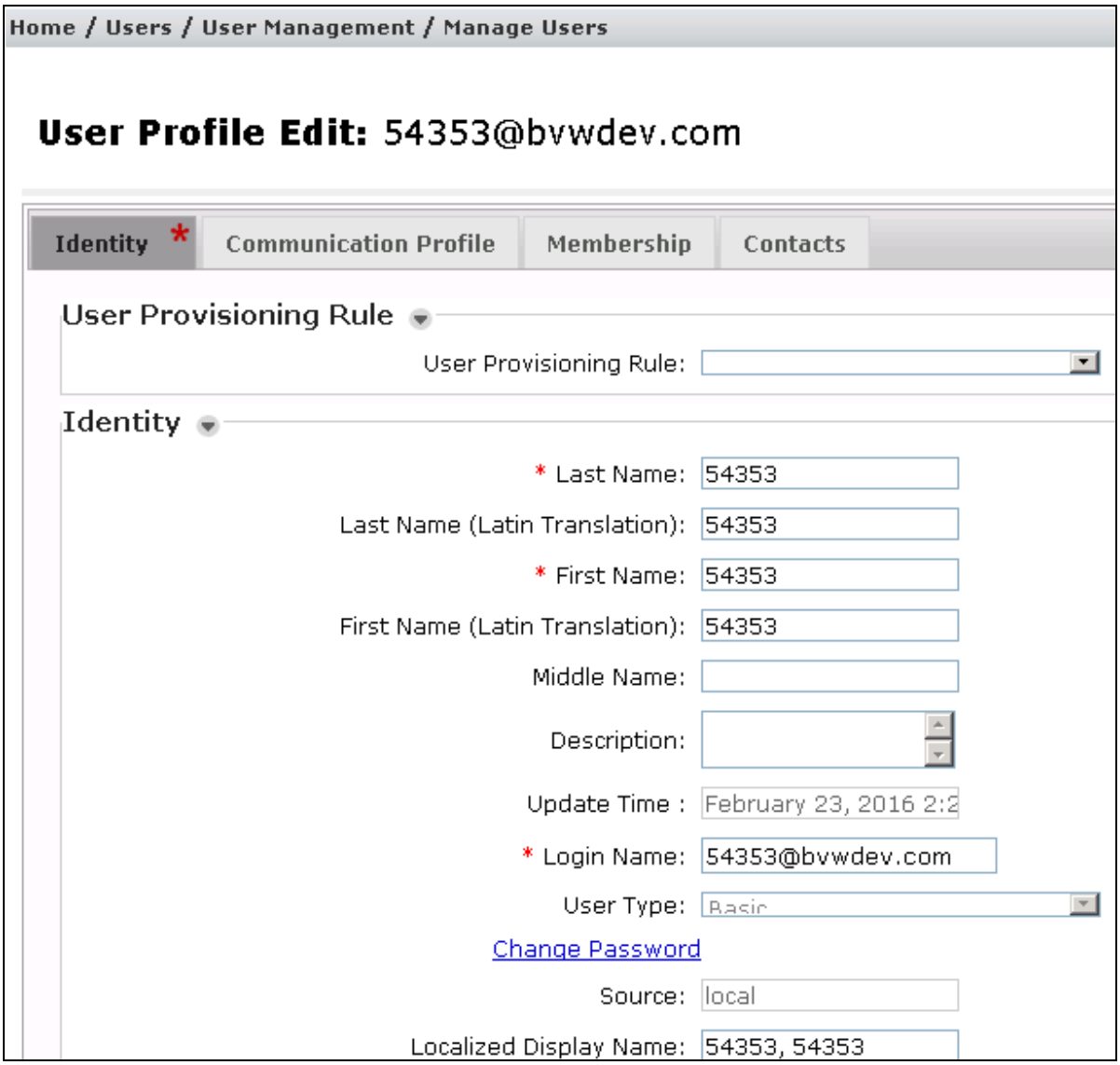


5.5. Create SIP user

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.

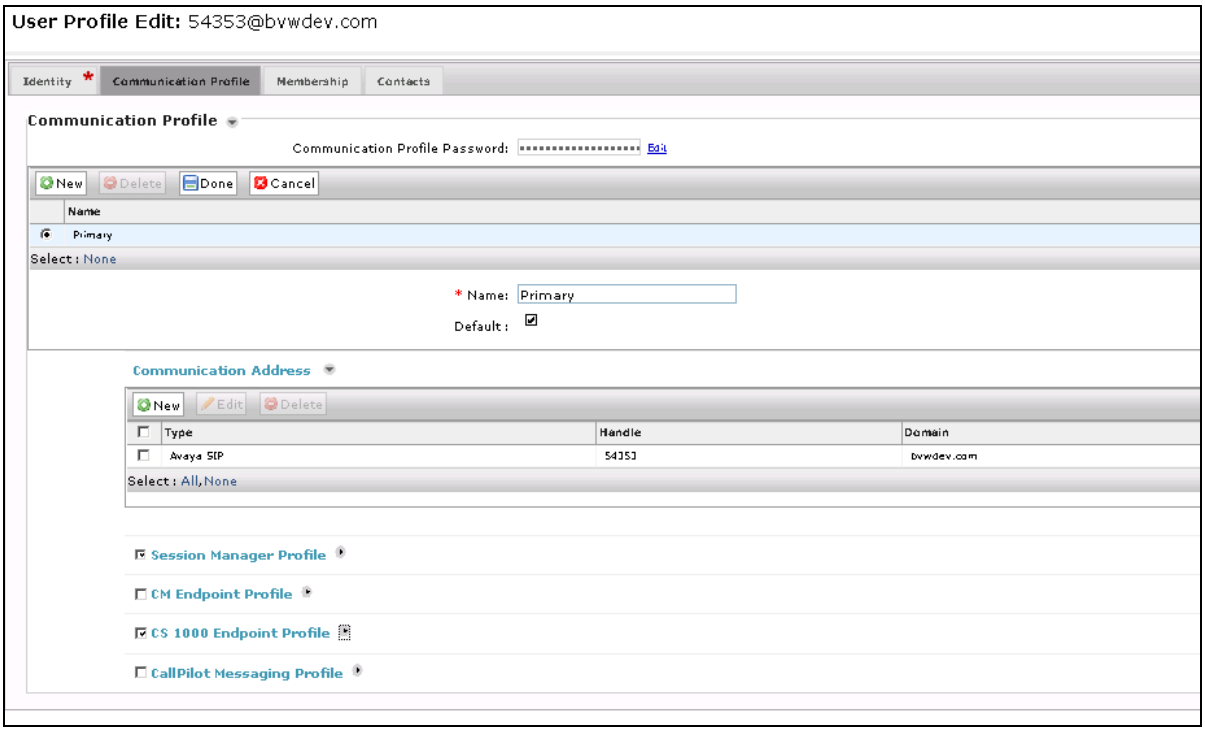
In **System Manager** home page, select **Users → User Management → Manage Users** and click on **New** button to add new user. Enter the following information for user in **Identity** tab:

- **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., 54353@bvwdev.com.

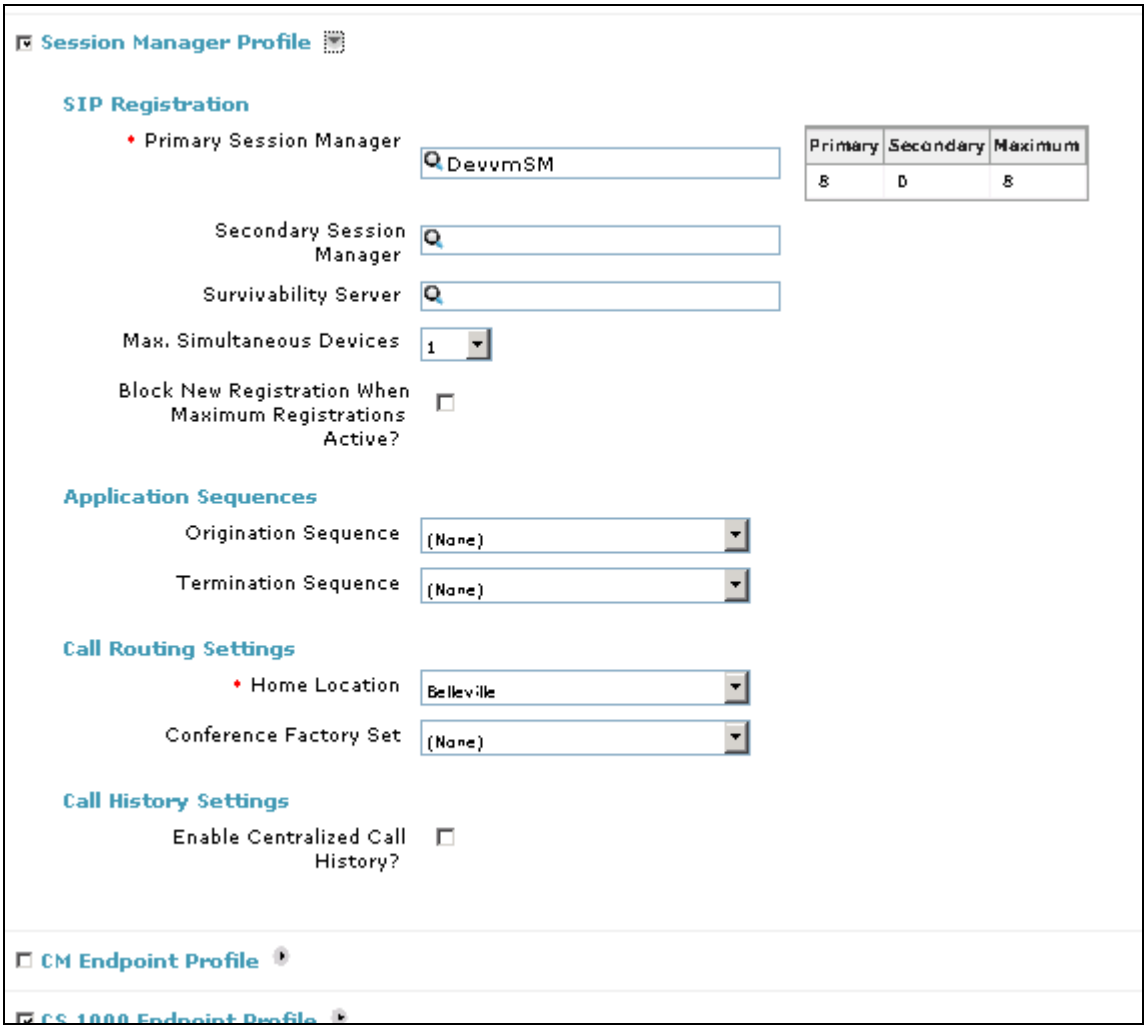


Configure **Communication Profile** tab – enter **Communication Profile Password**. And add new **Communication Address** as display below:

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



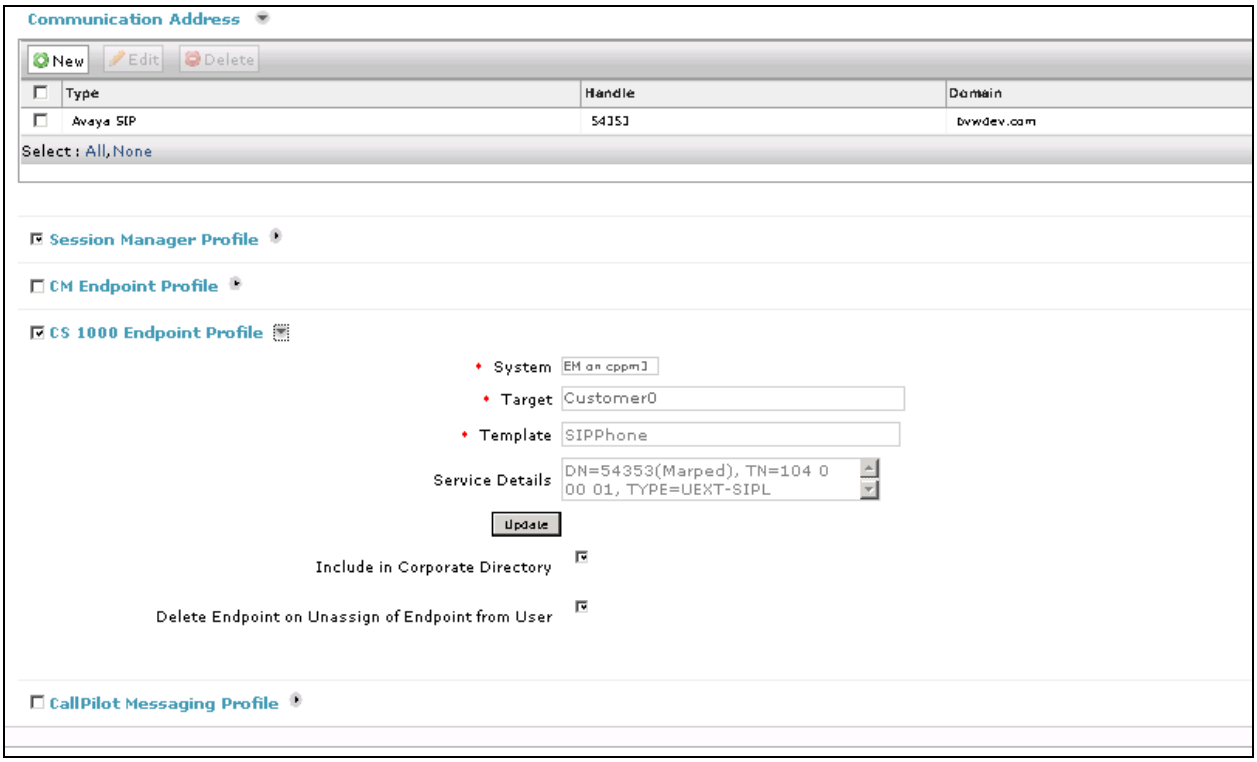
In **Session Manager Profile** – select Session Manager Information as shown below and click **Commit** to submit this new user. Then re-open this user again to configure **CS 1000 Endpoint Profile**.



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.



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_WARN 3276
JITTER_EXCE 32760
```

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 NetIQ 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:

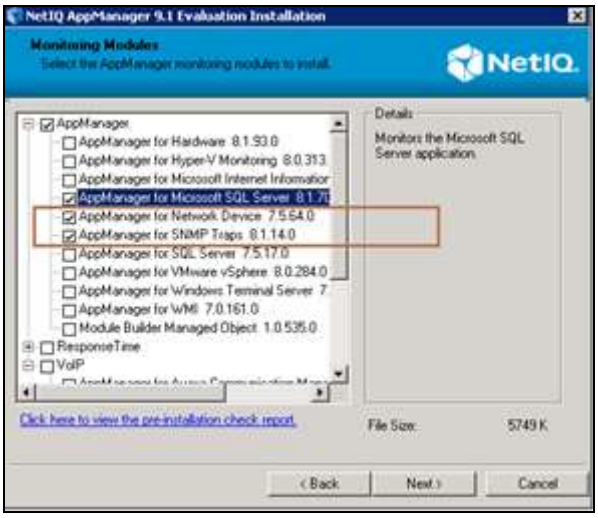
- AppManager Installation
- Activate the Netiq Trap Receiver Service
- Launch NetIQ Console
- Administer SNMPv3 trap Monitoring
- Administer SIP Call Quality Monitoring

6.1. AppManager Installation

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

- AppManager for NetworkDevice
- AppManager for SNMPTraps
- AppManager for SIPServer

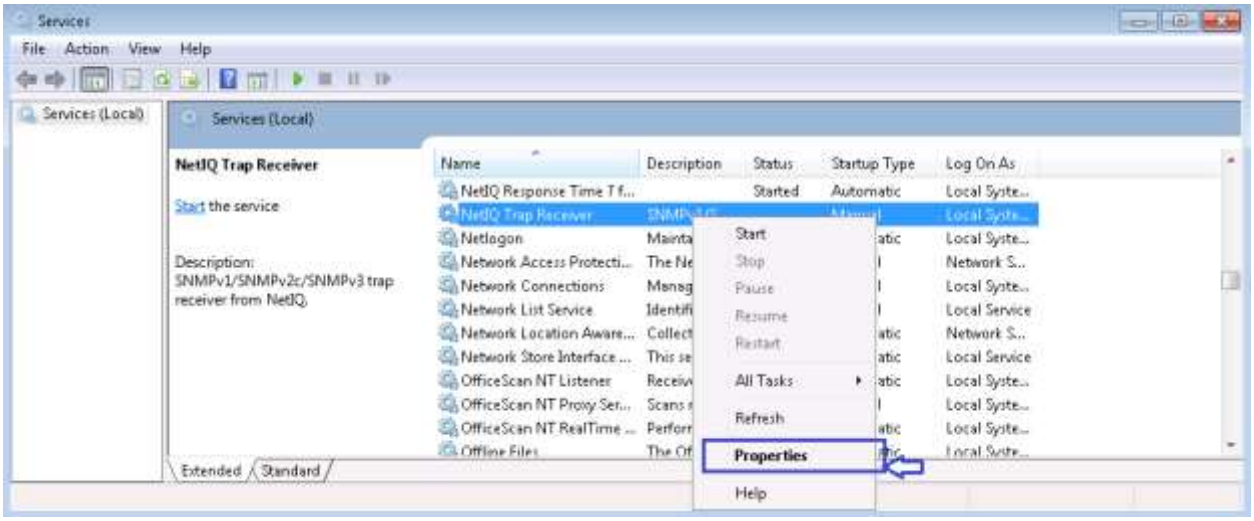
NetworkDevice and SNMPTraps modules are included in the AppManager 9.1 evaluation package available at https://www.netiq.com/products/appmanager/trial.html and may be selected during the installation of the AppManager 9.1 evaluation package.



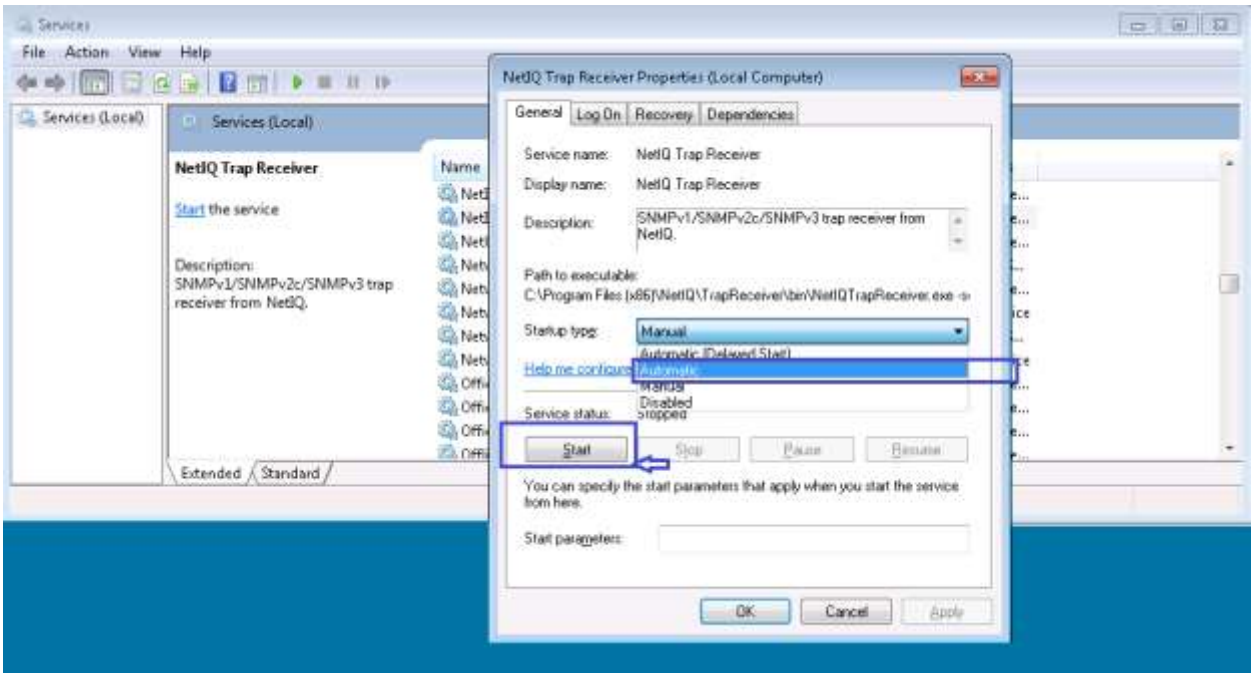
SIPServer is an Add-on module, installed as separately downloadable MSI.

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**.



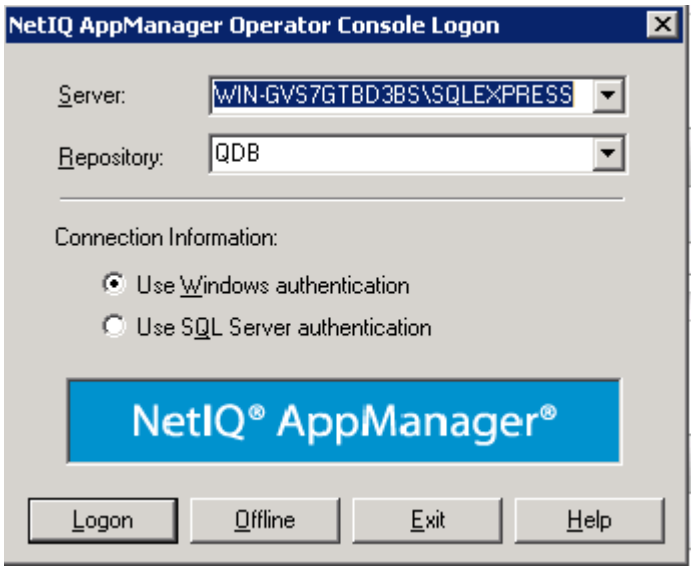
From the windows services menu as shown below and select "automatic" as the service start type. Click **OK** to save changes.



6.3. Launch NetIQ Console

In the NetIQ server navigate to **Start → All Programs → NetIQ → AppManager→ 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.

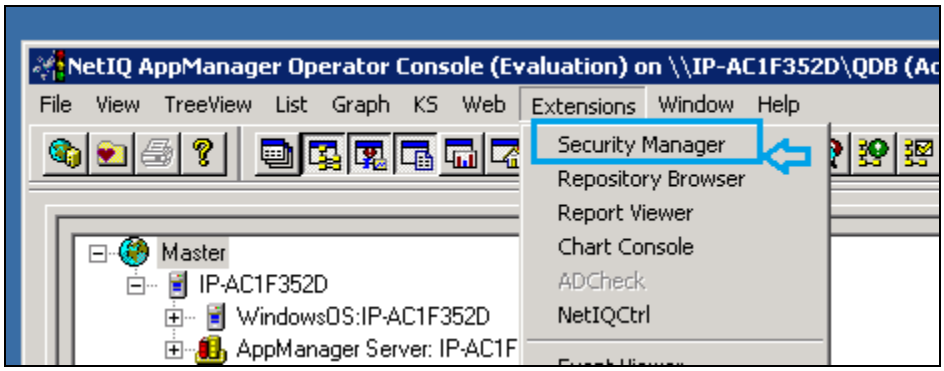


6.4. Administer SNMPv3 Trap Monitoring

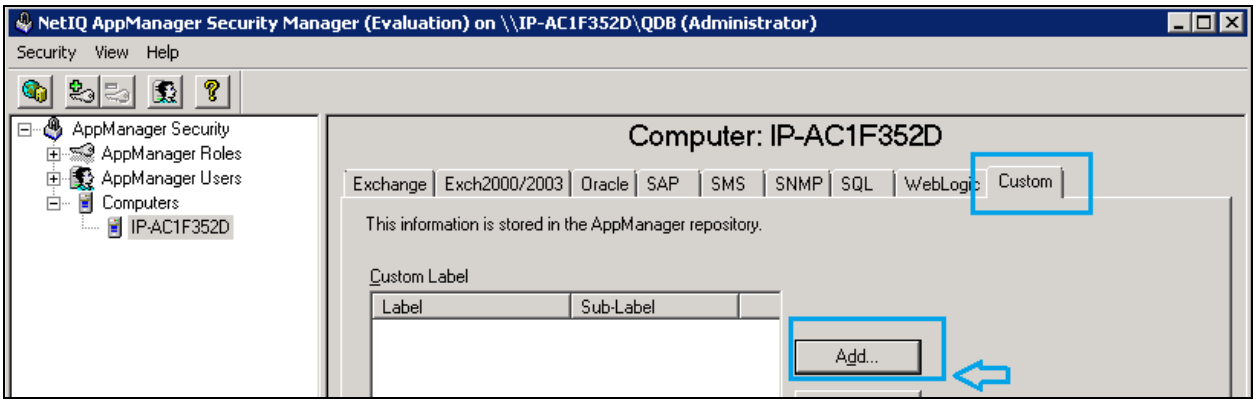
6.4.1. Configure Security Manager

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 → Security Manager** as shown in below.



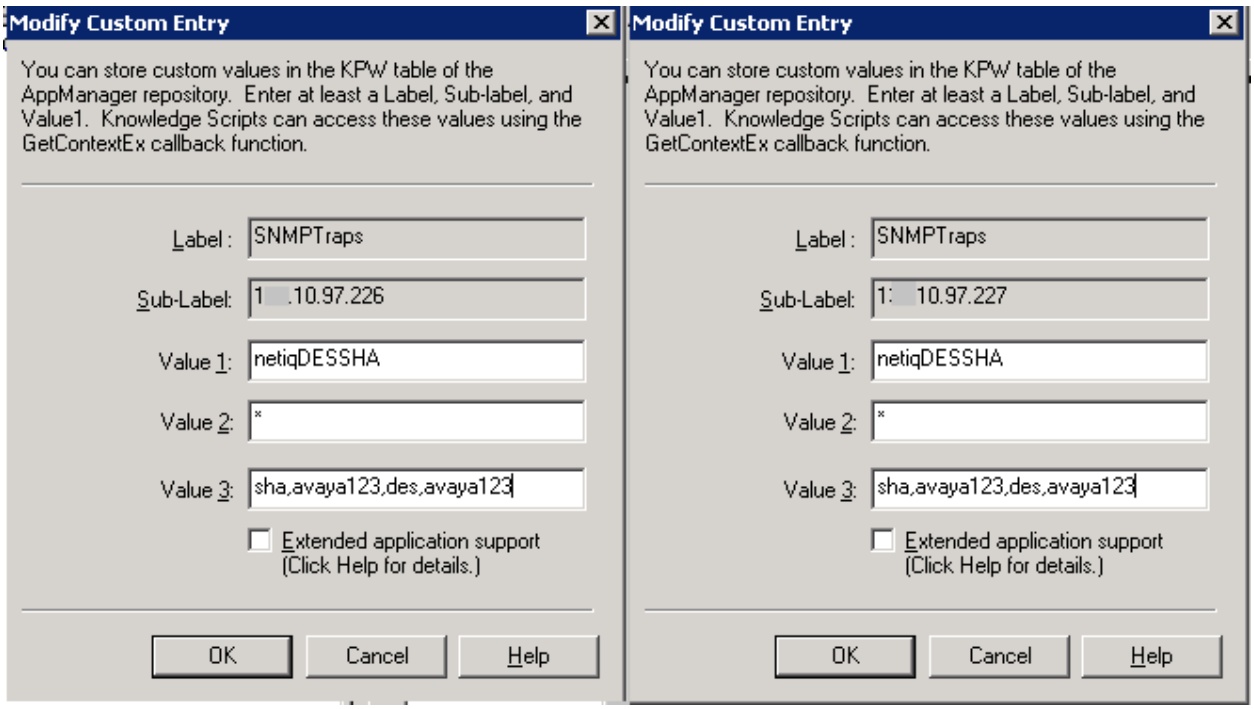
Add a custom profile:



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.

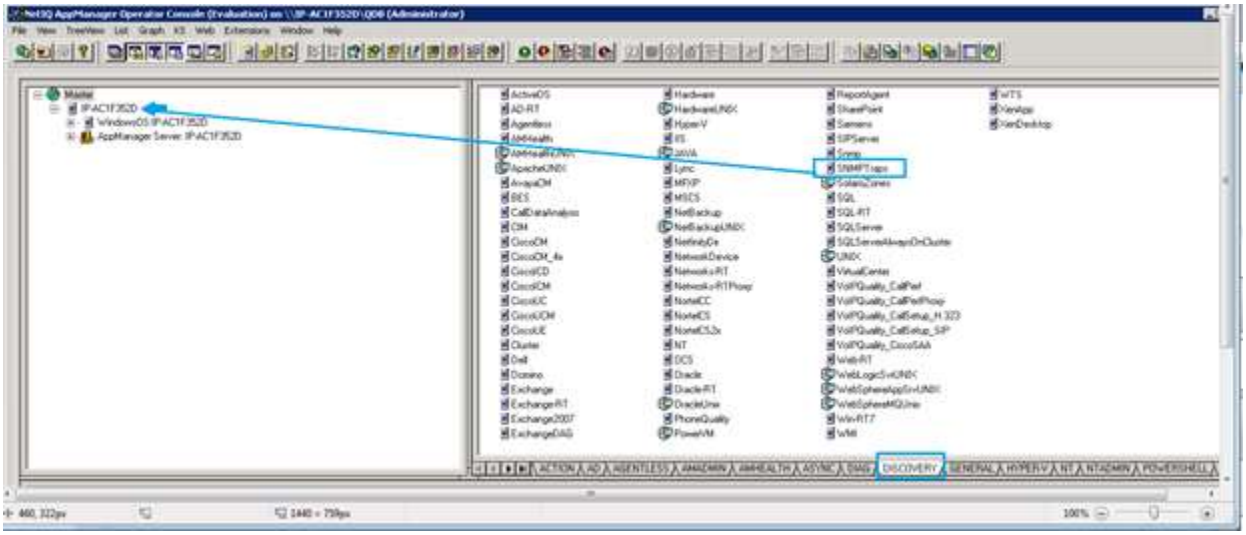
Create the same entry with Sub-Label set to the Session Manager IP address, e.g., 10.10.97.227 as displayed below:



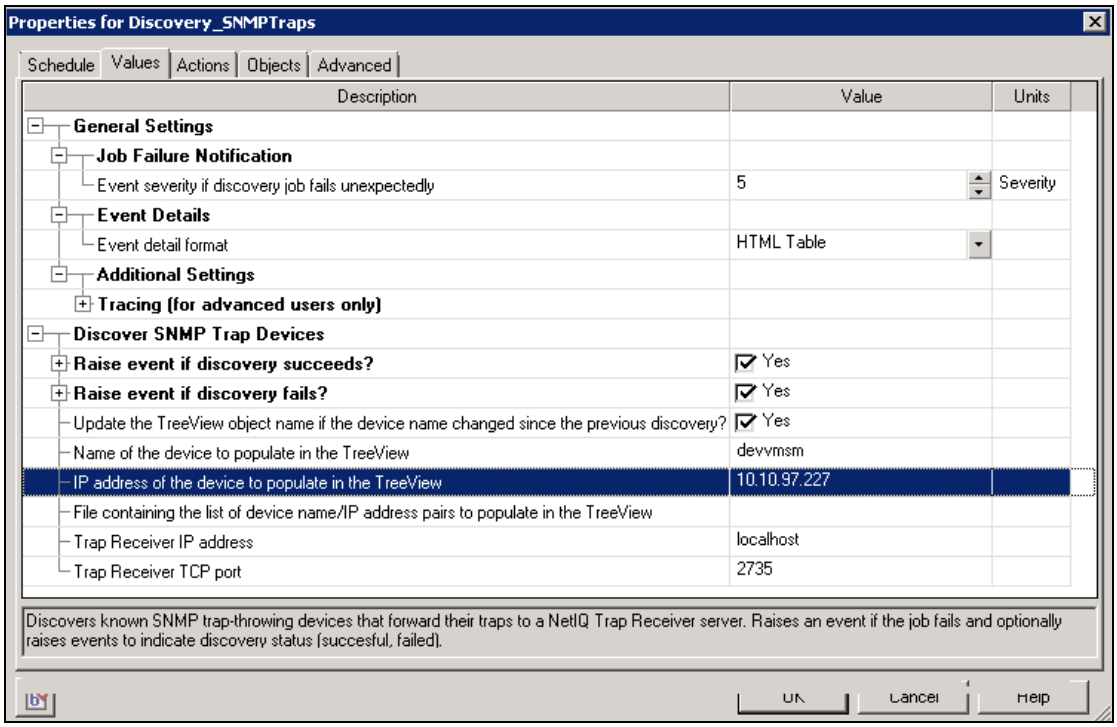
6.4.2. Discover the Device

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.

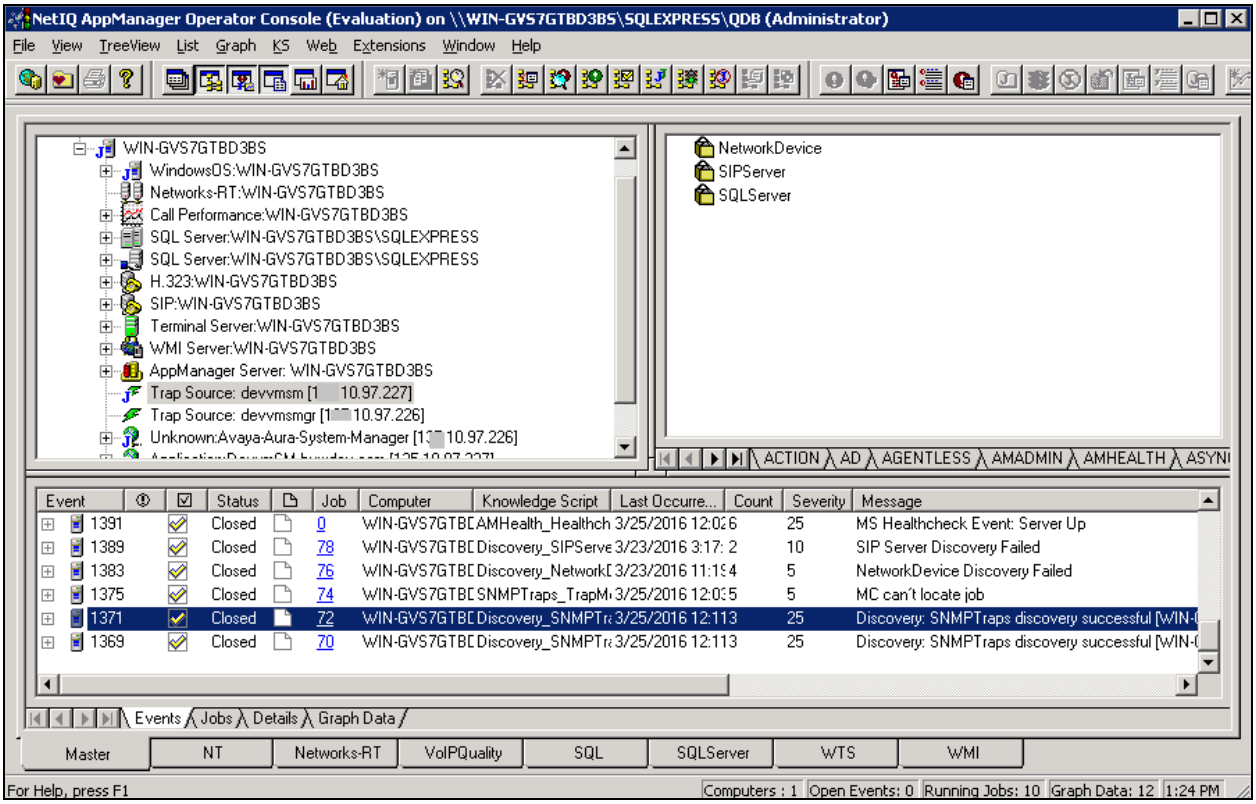
Navigate to the "**Discovery**" tab and drop the "SNMPTraps" Discovery KS (Knowledge Script) on the agent machine in the treeview to create the discovery job.



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

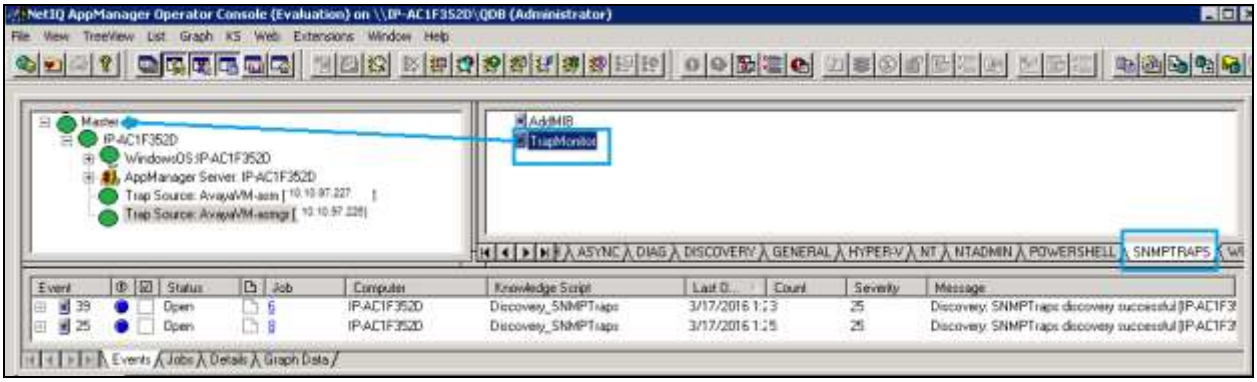


Confirm that Session Manager appears in the TreeView (which confirms the SNMPv3 credentials are valid and the NetIQ trap receiver service is available on the agent), in this case, it is Trap Source: devvmsm[10.10.97.226] and Trap Source: devsmgr[10.10.97.227]

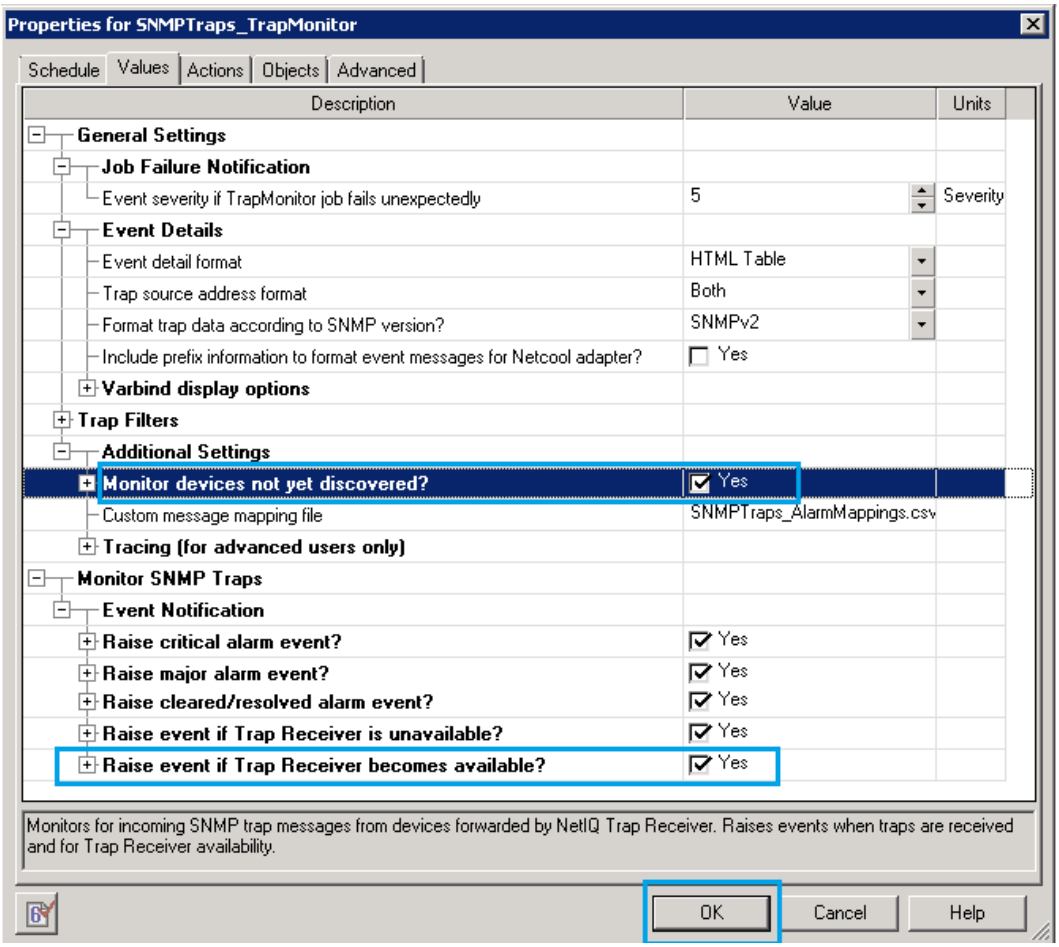


6.4.3. Start Trap Monitoring

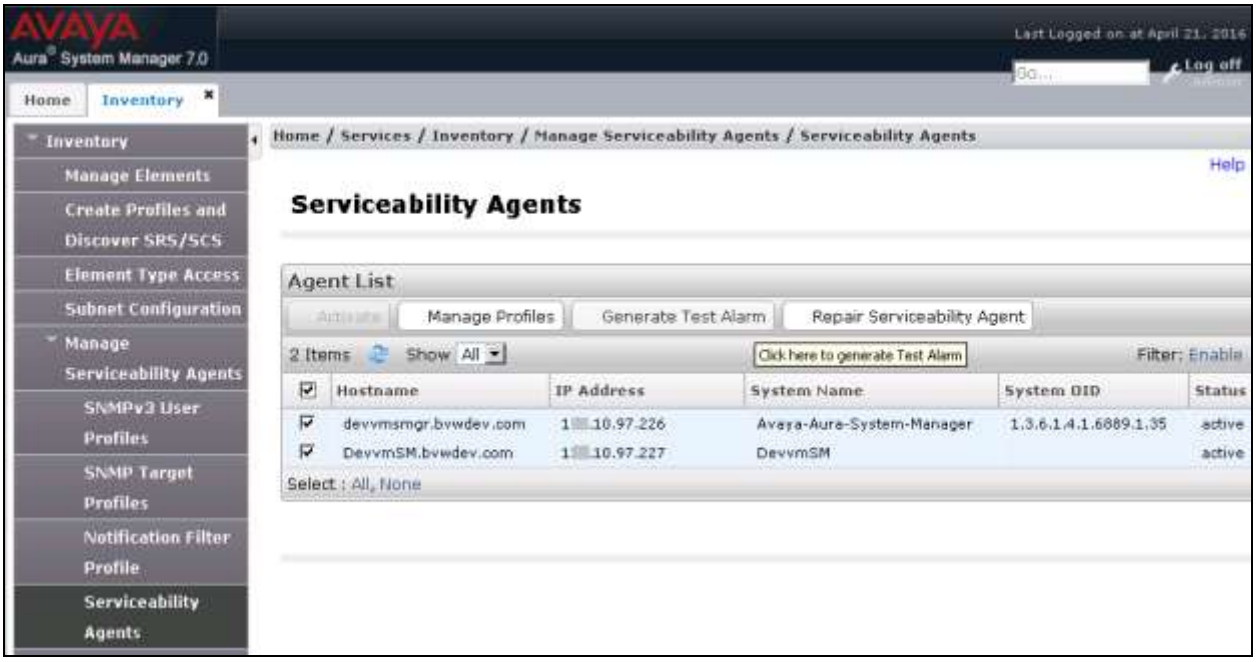
Next, run the SNMPTraps_TrapMonitor Knowledge Script on the agent computer and any SNMPv3 trap sources discovered in the treeview.



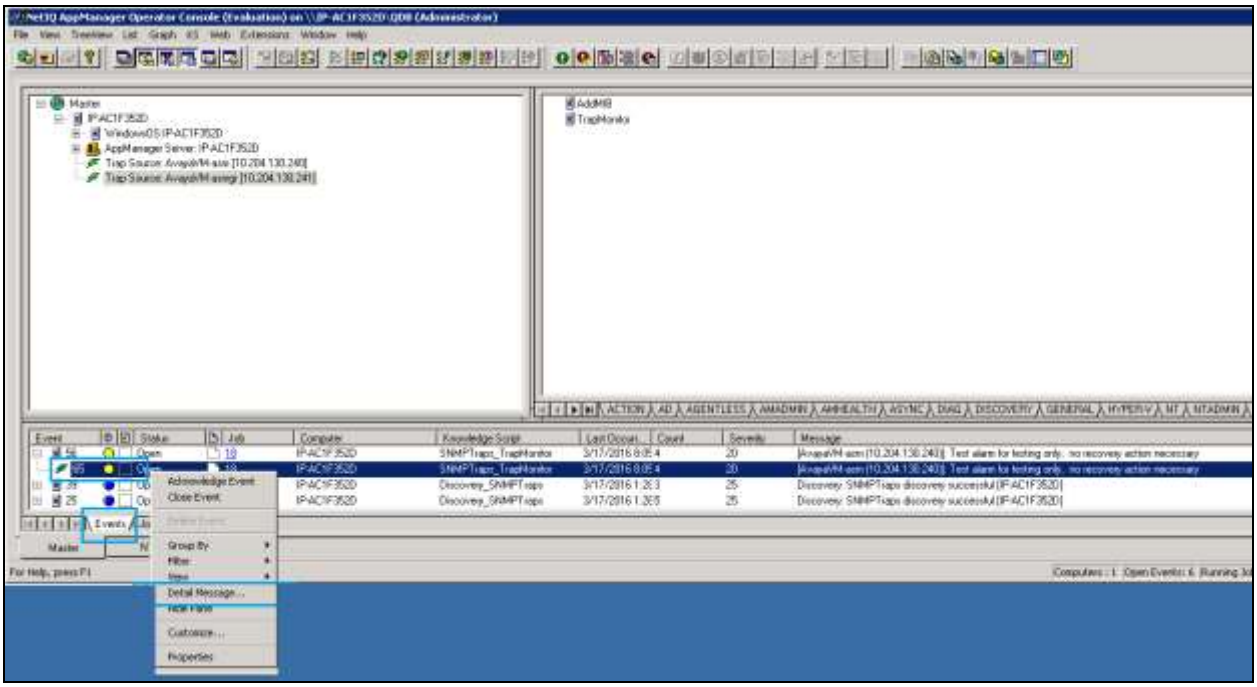
In the job detail make sure **Monitor devices not yet discovered?** and **Raise event if Trap Receiver become available**? options are checked.



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:

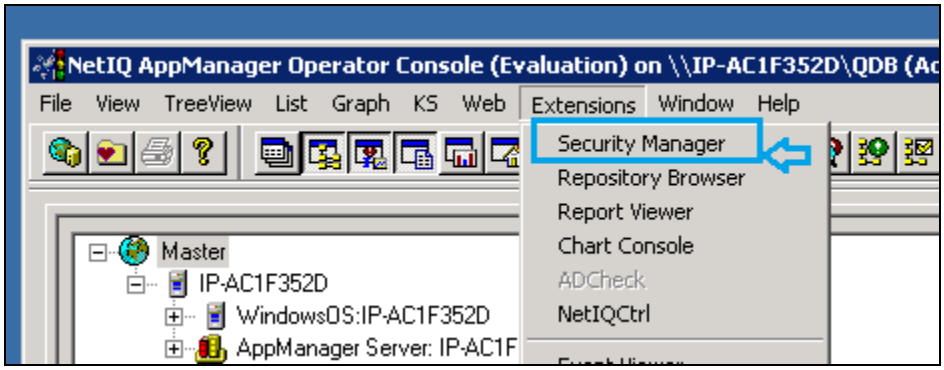


The test trap and any subsequent traps received will be reported in the AppManager console as events:

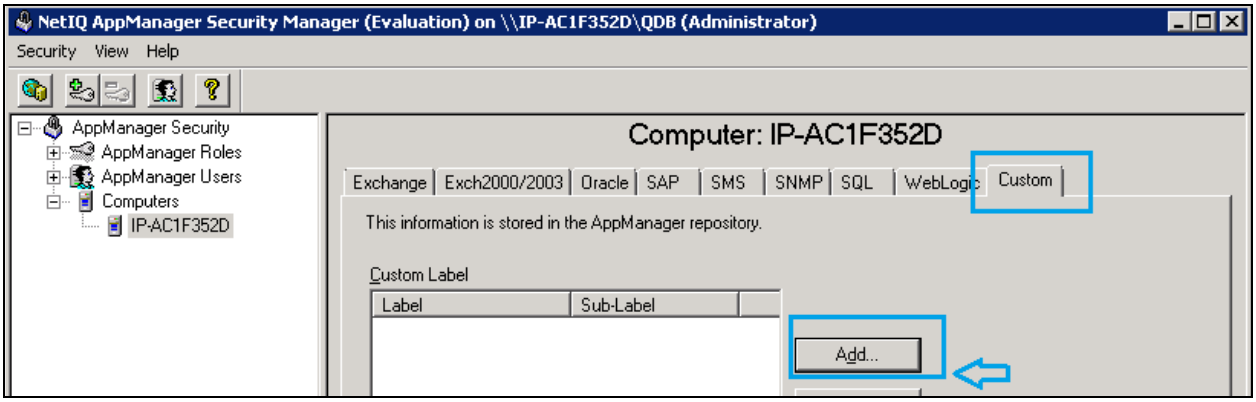


6.4.4. Administer Network Device

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:



Add a custom profile for Network Device:

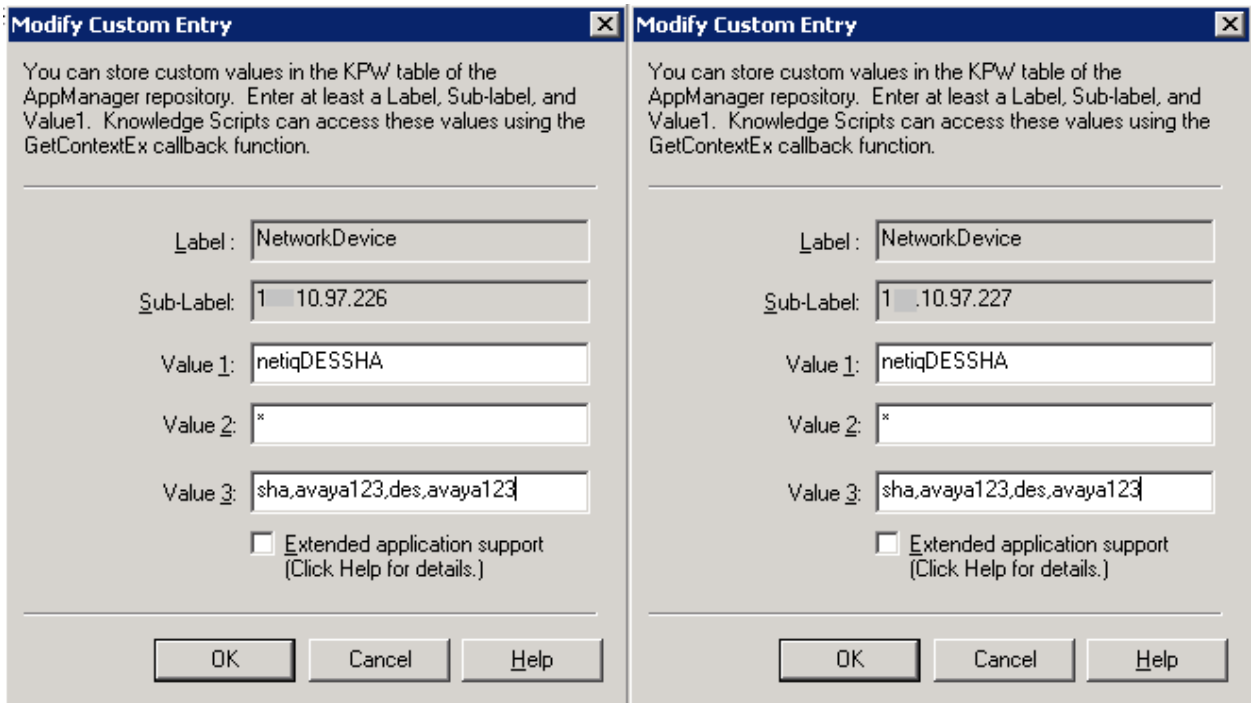


Enter the system manager SNMP profile into security manager. If all devices on your network will use the same SNMP configuration, enter "default" as the label2 string. If they are each different, enter the active IP address of the device as the label2 string:

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

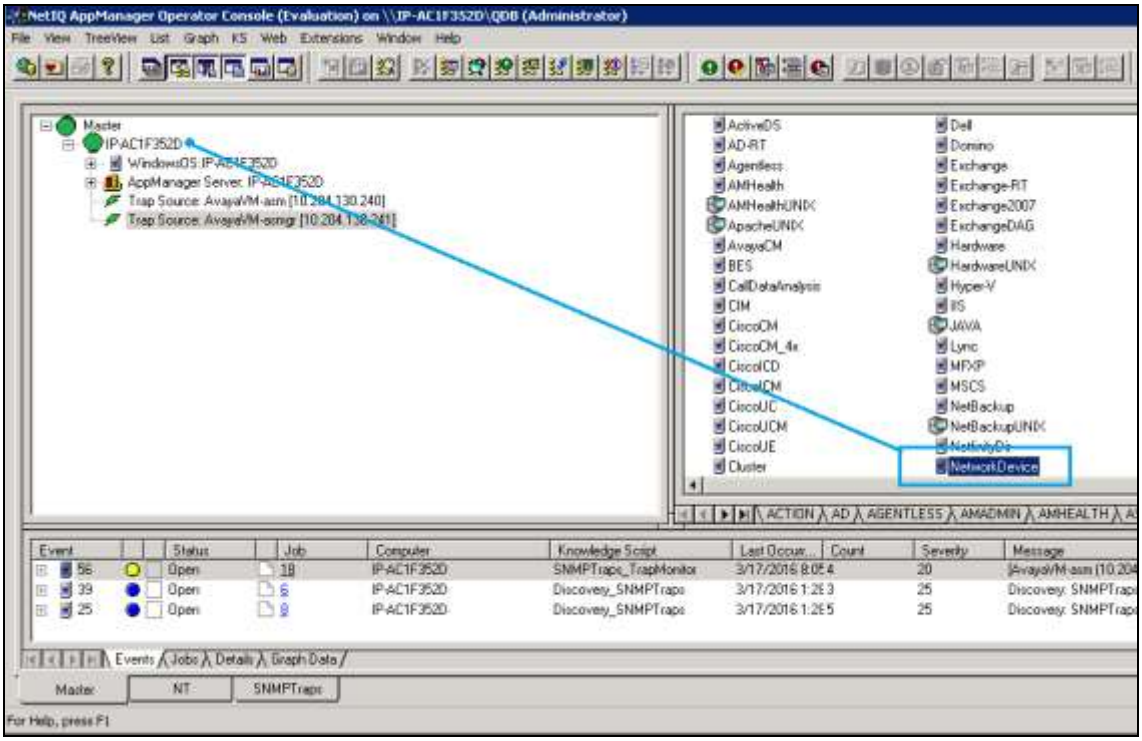
- **Label**: Enter any descriptive name, e.g., NetworkDevice.
- **Sub-Label**: Enter System manager's IP Address, e.g.,10.10.97.226.
- **Value 1**: Enter user name created in Section 5.3, e.g., netiqDESSHA..
- **Value 2**: Enter *.
- **Value 3**: Enter user created in Section 5.3 passwords, e.g., sha,avaya123,des,avaya123.

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

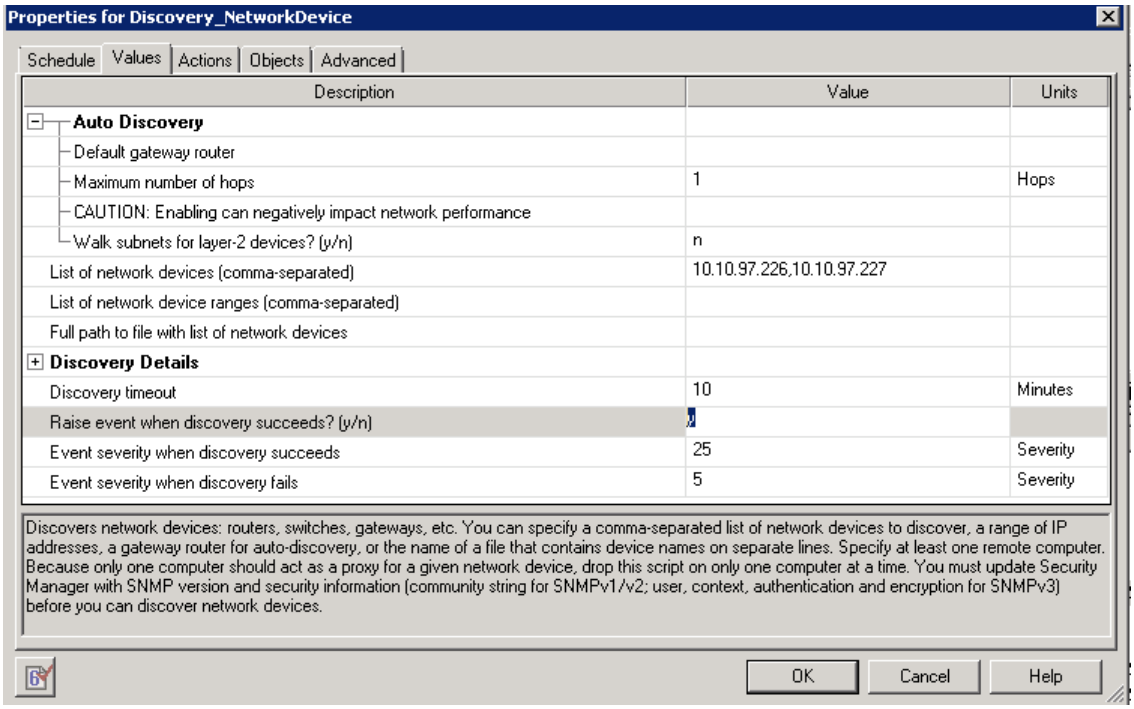


6.4.5. Discover the Device

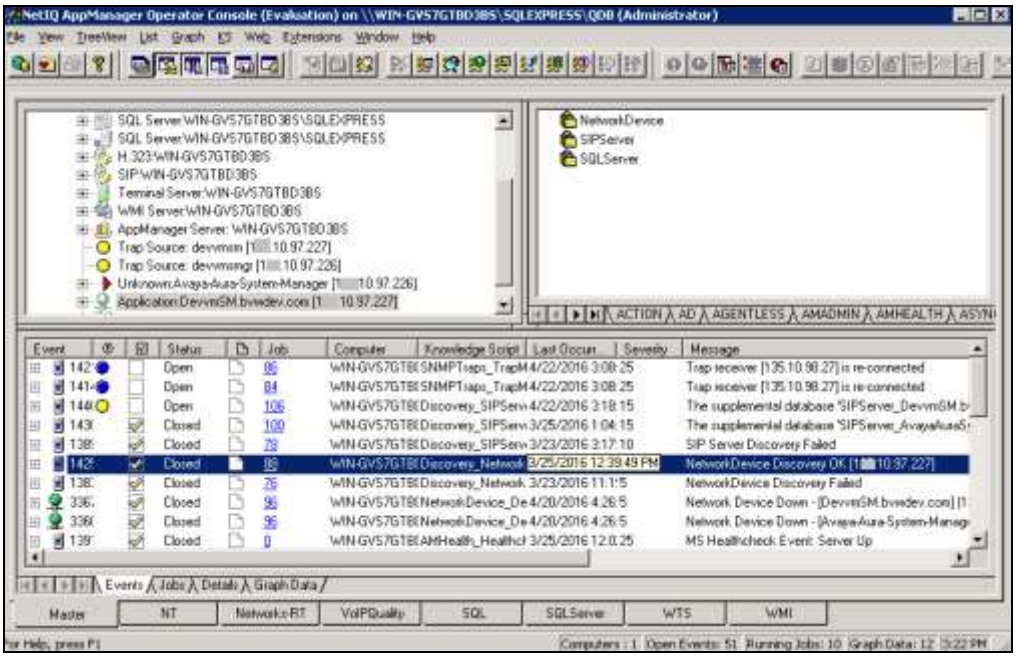
Navigate to the "Discovery" tab and drop the "NetworkDevice" Discovery KS on the agent machine in the treeview to create the discovery job for the devices.



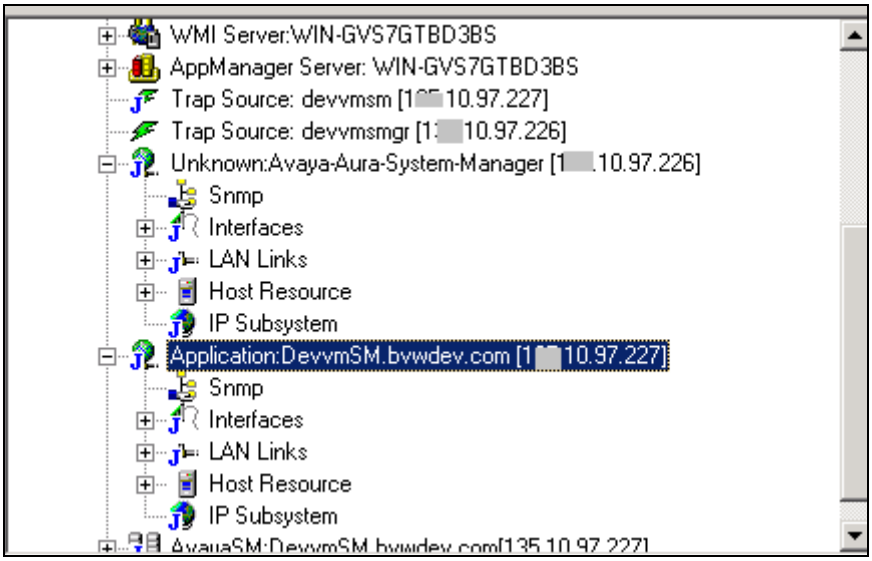
Enter the IP address of the Session Manager and System Manager in the job properties for **List of network devices (comma-separated),** in this case 10.10.97.227,10.10.97.226.



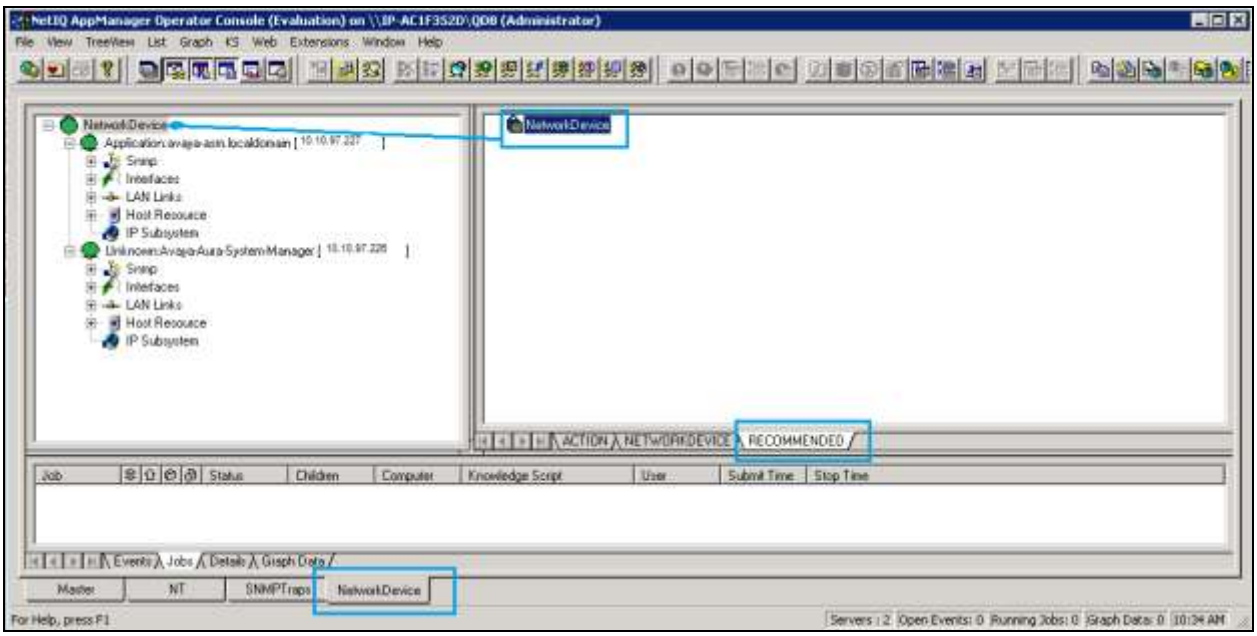
Discovery will create treeview objects for the session manager and system manager using SNMP Unknown: Avaya-Aura-System-Manager [10.10.97.226] and Application: DevvnSM.bvwdev.com[10.10.97.227] Discovery Network OK.



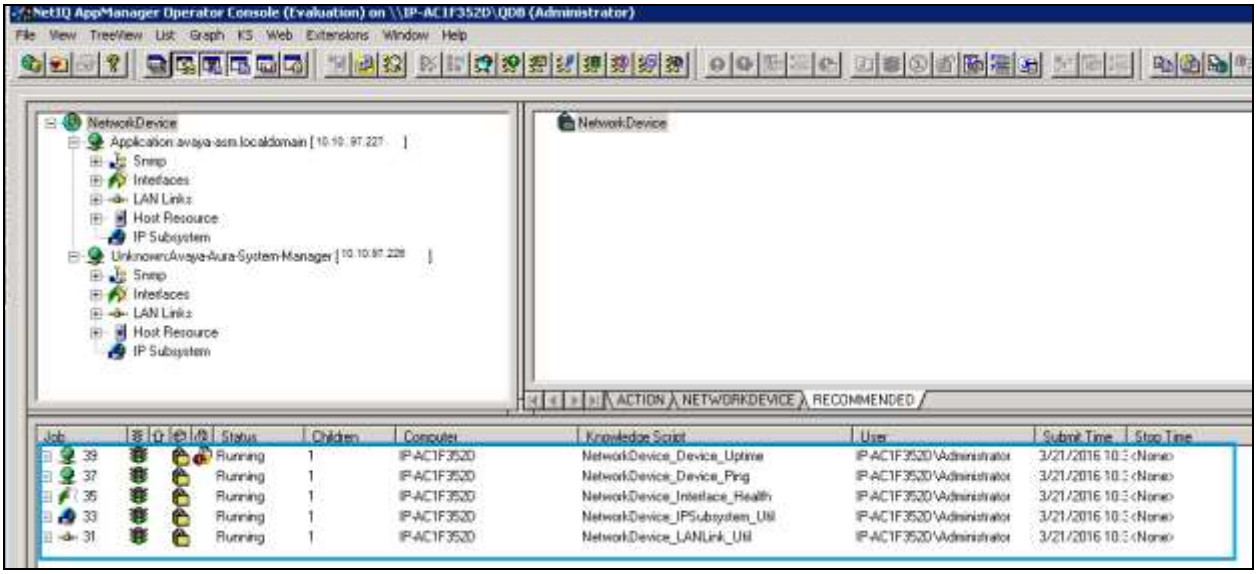
Click on the TreeView object to verify that platform details are available for both session and System Manager are listed such as Snmp, Interfaces, LAN links, Host Resource and IP Subsystem.



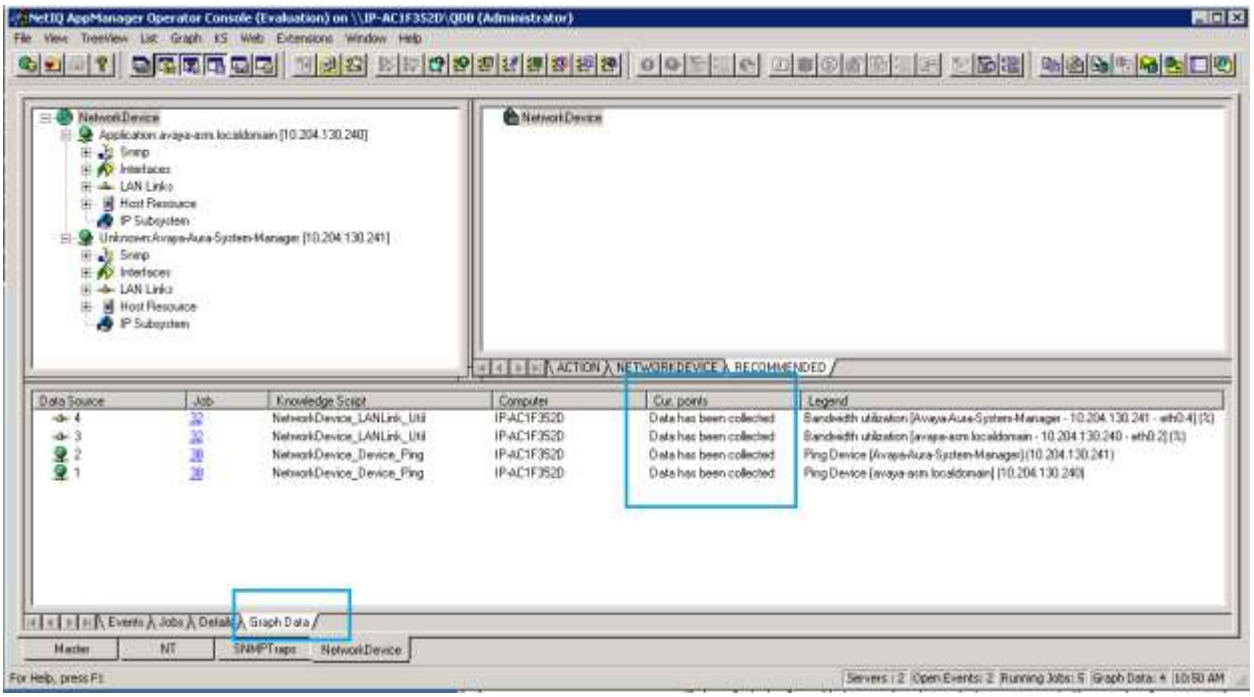
Start the **NetworkDevice** recommended knowledge script group for monitoring each device.



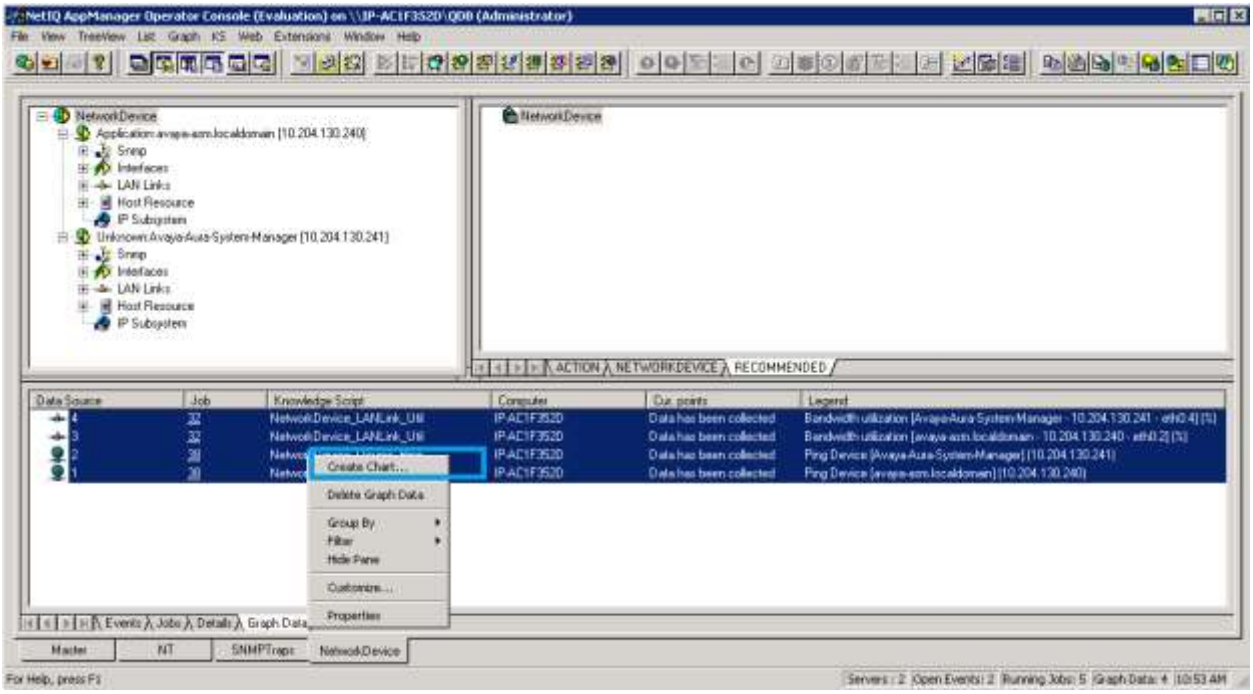
Confirm that the following device monitoring jobs have started: NetworkDevice_Device_Uptime, NetworkDevice_Device_Ping, NetworkDevice_Interfaces_Health, NetworkDevice_IPSubsystem_Ulti and NetworkDevice_LANLink_Ulti as shown in below screenshot.



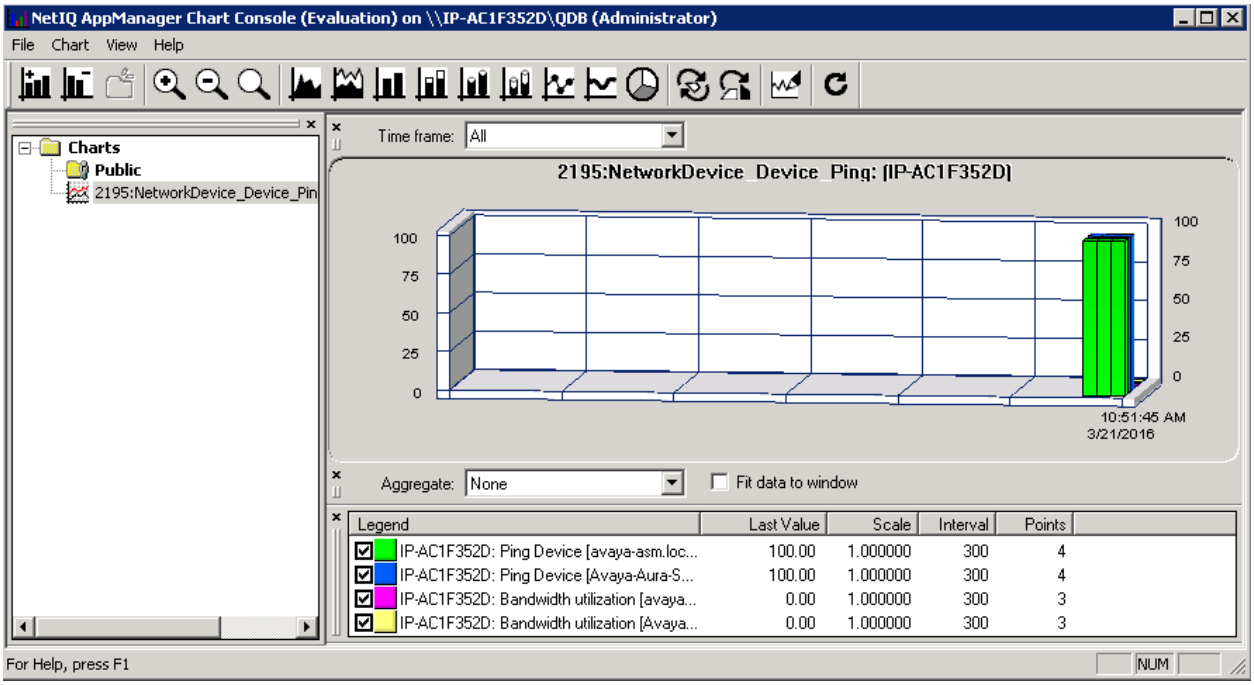
After a monitoring interval has been completed, data streams will be visible in the Graph Data pane as shown in below screenshot.



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



Below display the NetworkDevice_Device_Ping data in graphic chart.

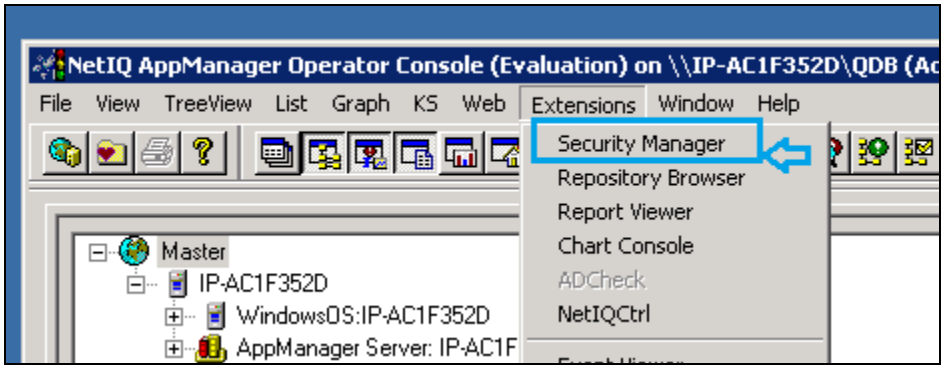


6.5. Administer SIP Call Quality Monitoring

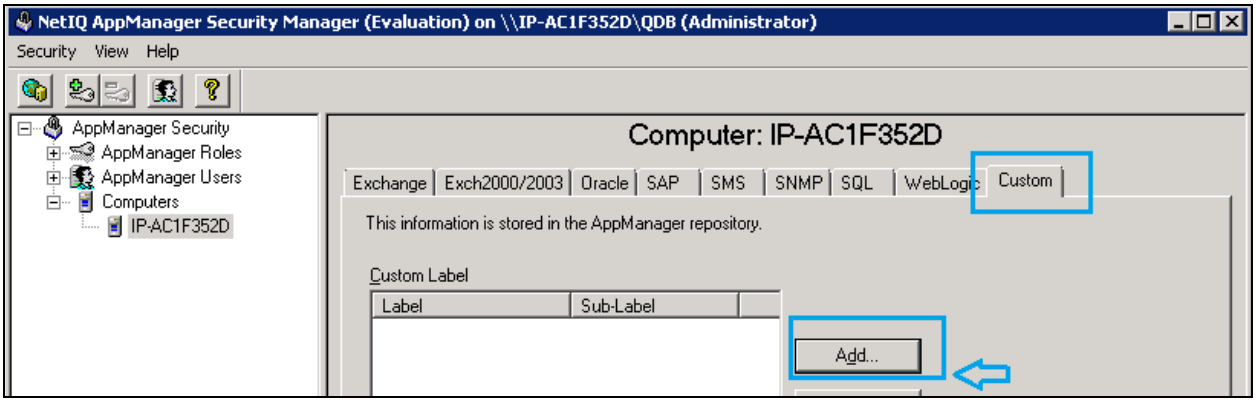
AppManager for SIPServer can discover the Session Manager using either SNMP or by manually configuring the device characteristics. To use SNMP, the SNMP v3 credentials previously created on session manager in **Section 5.1** will need to be entered into Security Manager for the SIPServer module.

6.5.1. Administer Security Manager for SIP Server

In AppManager console, select **Extensions → Security Manager**.

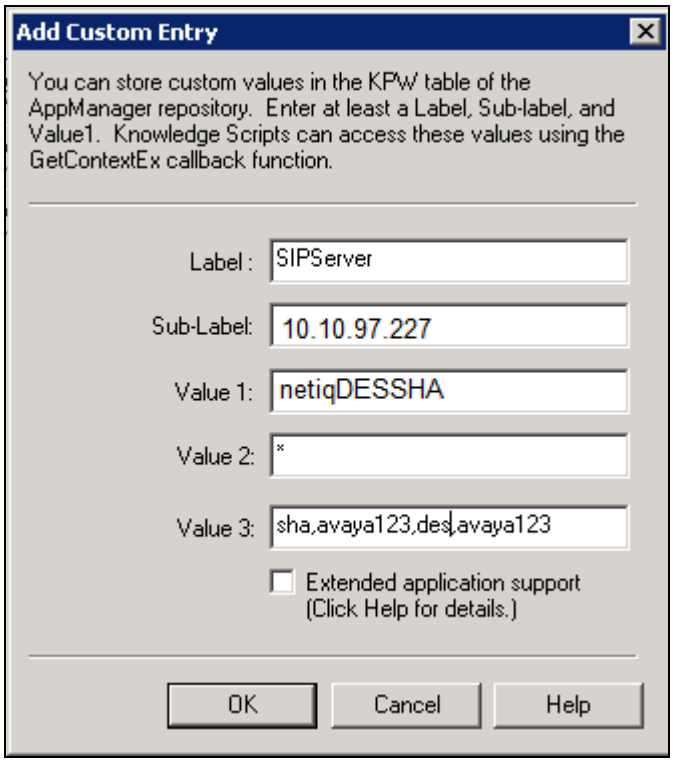


In **Custom** tab, click on **Add** button



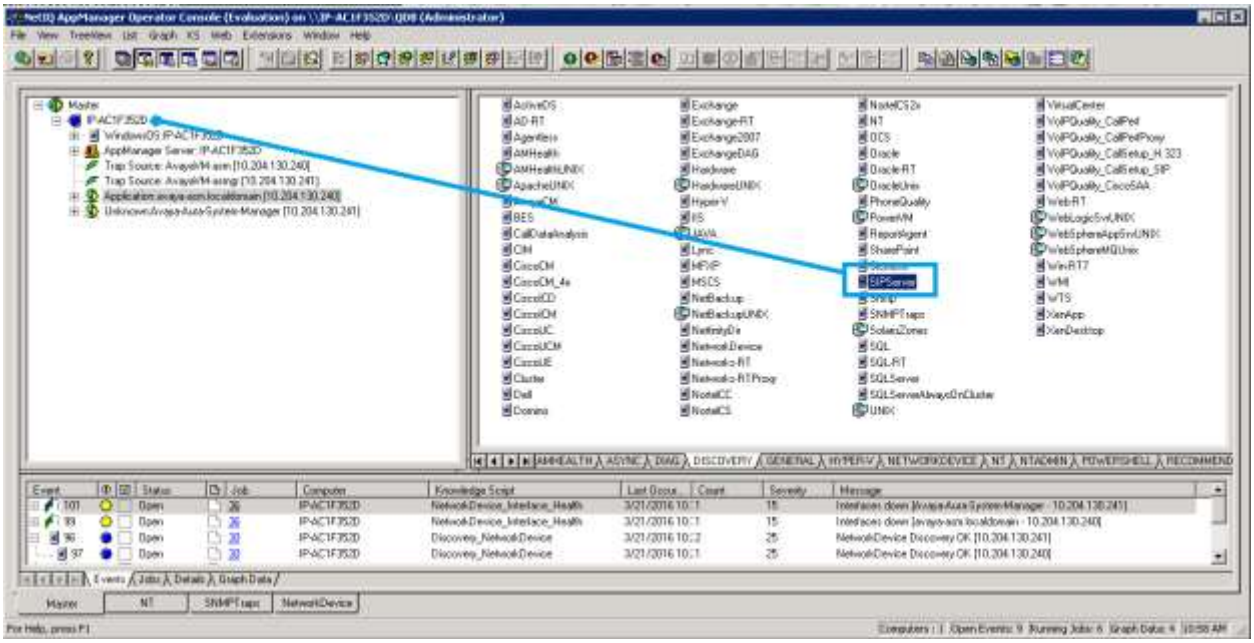
Enter the SNMPv3 User Profile created in **Section 5.1** as example display below used during compliance test for Security Manager:

- **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.



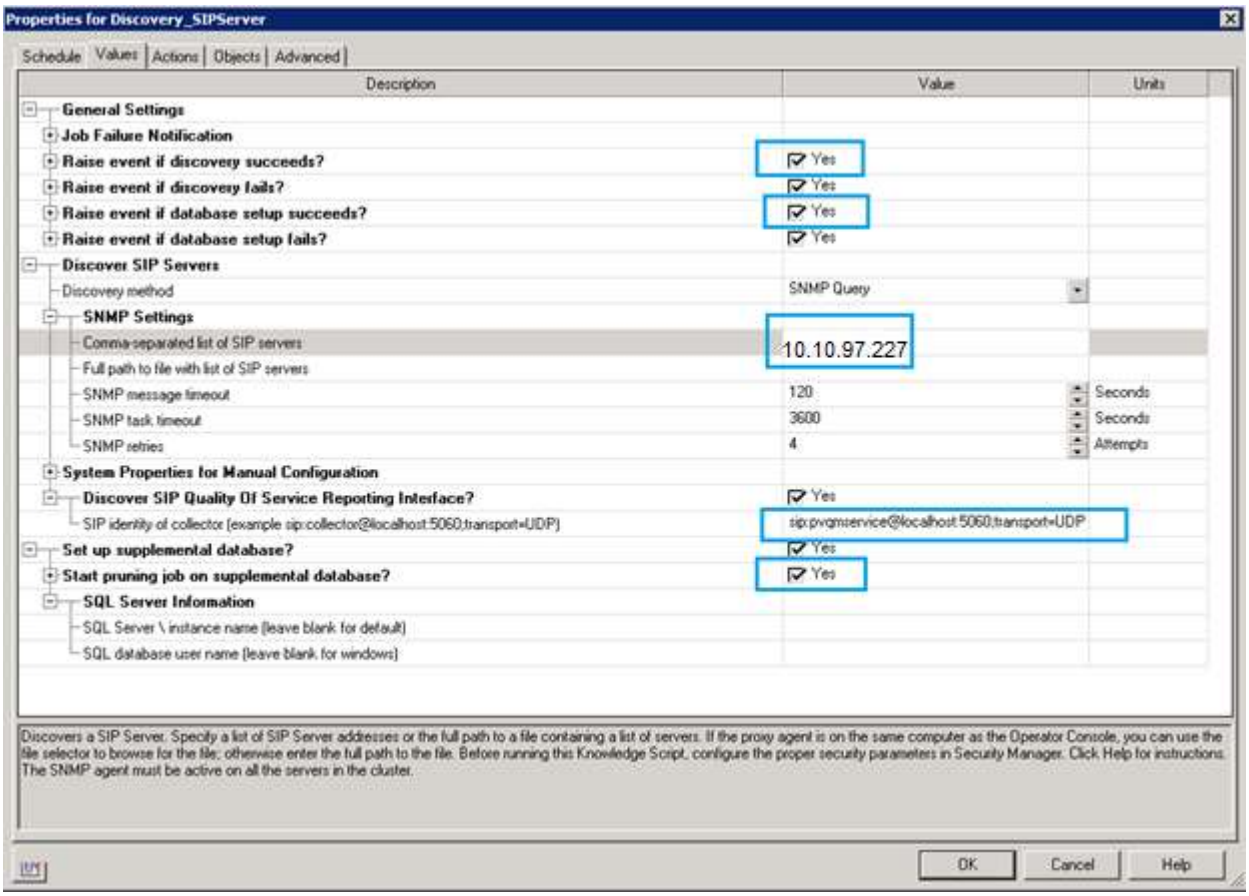
6.5.2. Discover Device

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.

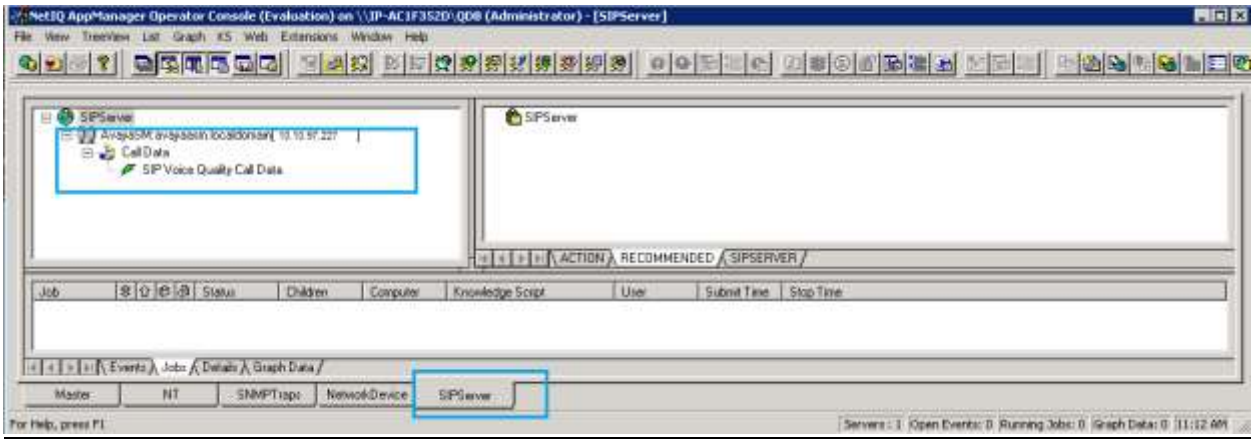


In the Discovery_SIPServer job properties, enter the folllowing IP as display below:

- **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**: SIP:pvqmservice@localhost:5060;transport=UDP.

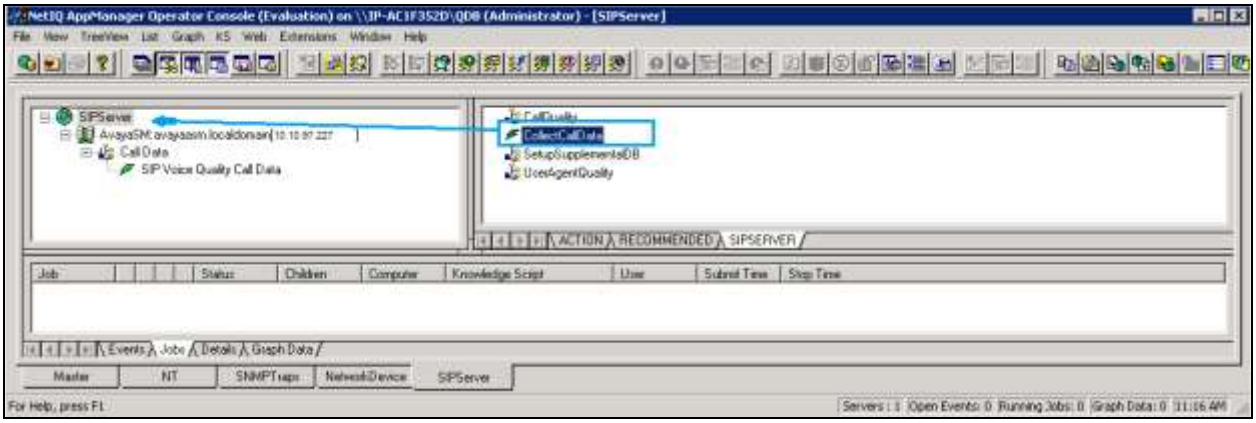


Confirm that a TreeView object for the session manager call data monitoring is created.

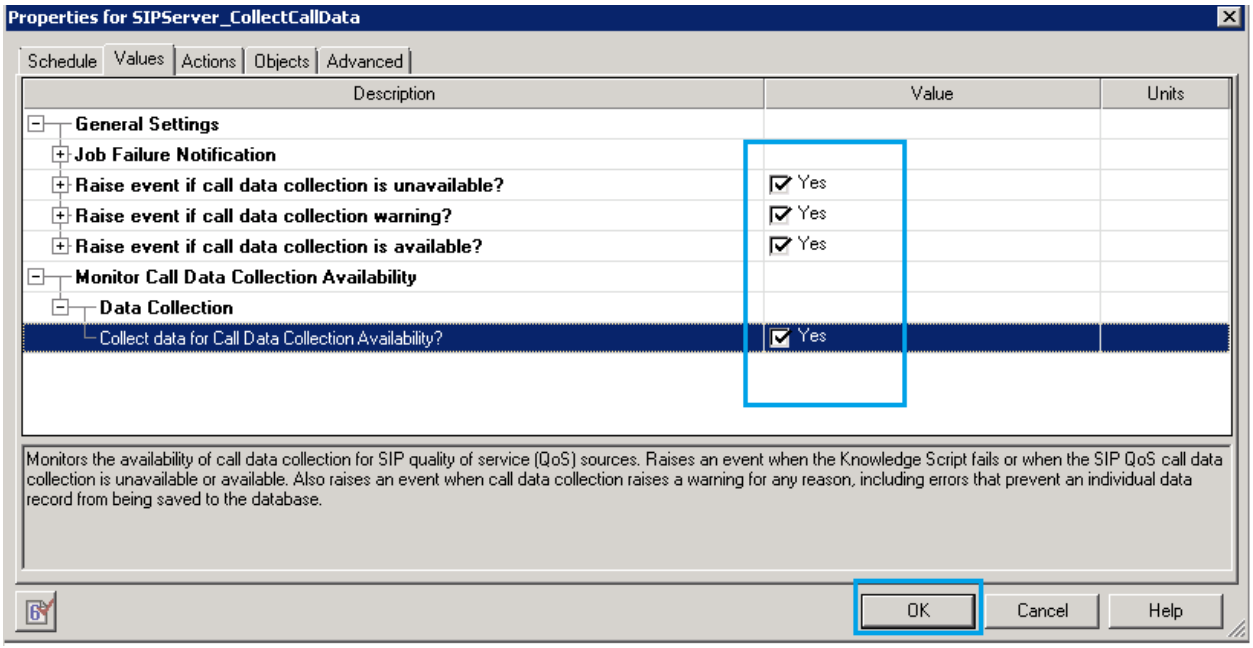


6.5.3. Collect Call Data

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



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

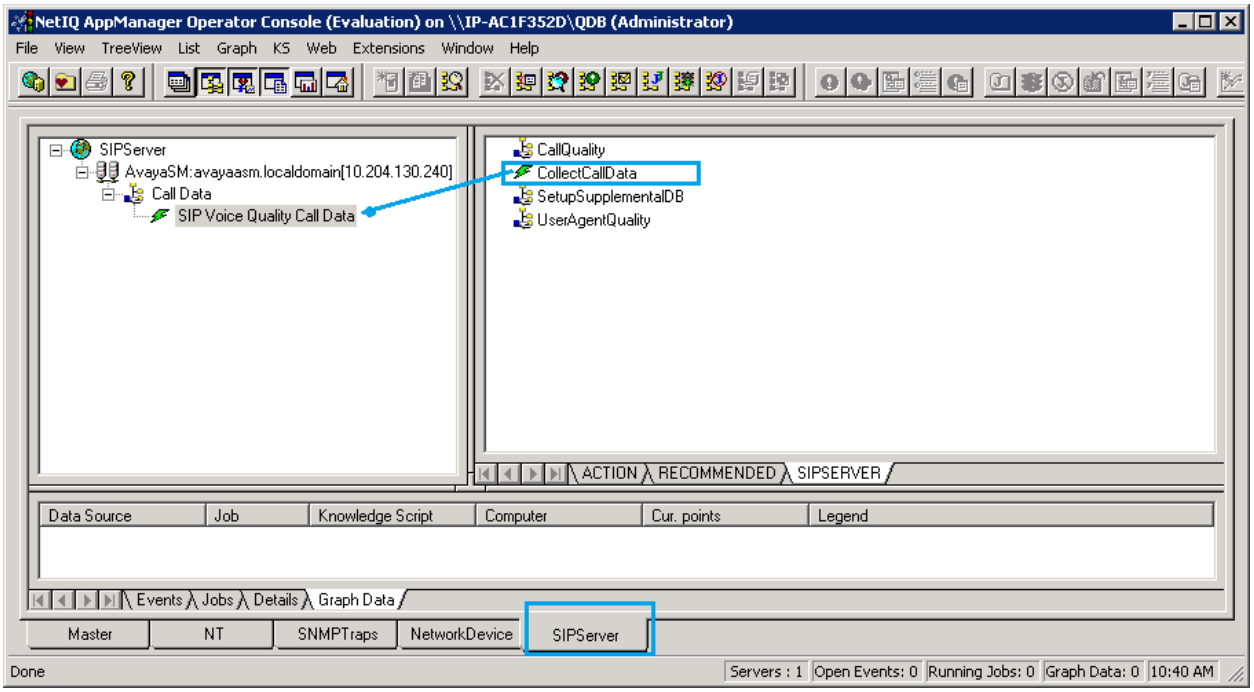


Confirm that the SIP trunk to AppManager now shows inservice by navigating to the **Session Manager → System Status → SIP Entity Monitoring** menu, selecting "run monitor" for the trunk just created in **Section 5.4**.

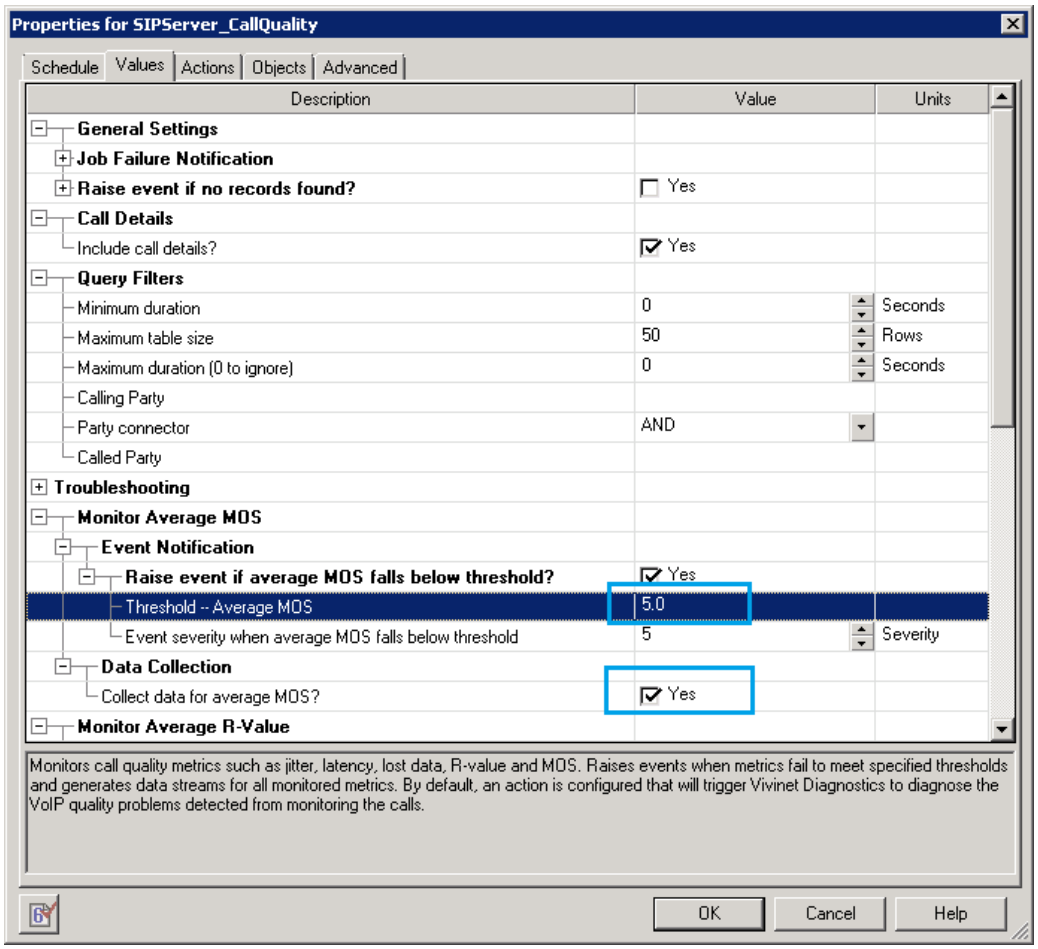
Verify this trunk will remain in-service (**Conn Status** is UP) as long as the CollectCallData job is running on the agent.

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.

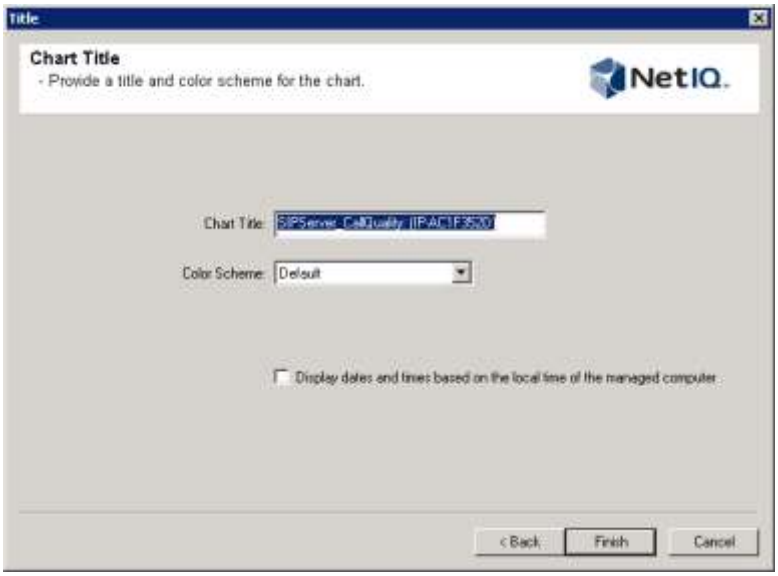


In **SIPServer_CallQuality**, select **Monitor Average MOS → Event Notification → Raise event if average MOS falls below threshold?** and set the MOS threshold for reporting very high (5.0) – this will ensure that all calls create events, allow confirming that data is collecting and reporting properly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

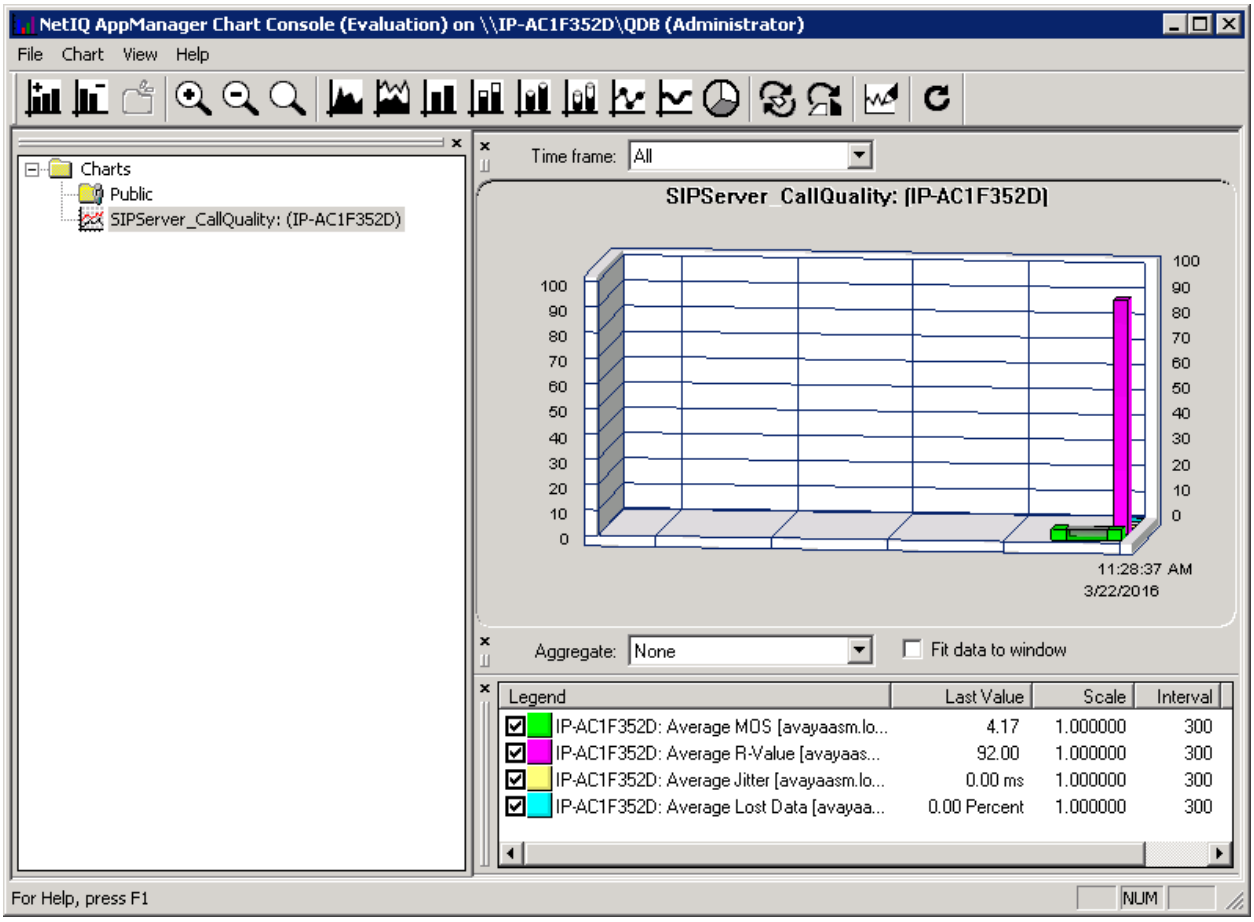


Make a call between two SIP phones.
Use the chart console to confirm that data has been collected for the calls made. The default reporting interval is 5 minutes, so you may need to wait up to 5 minutes to see results post to the chart:

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



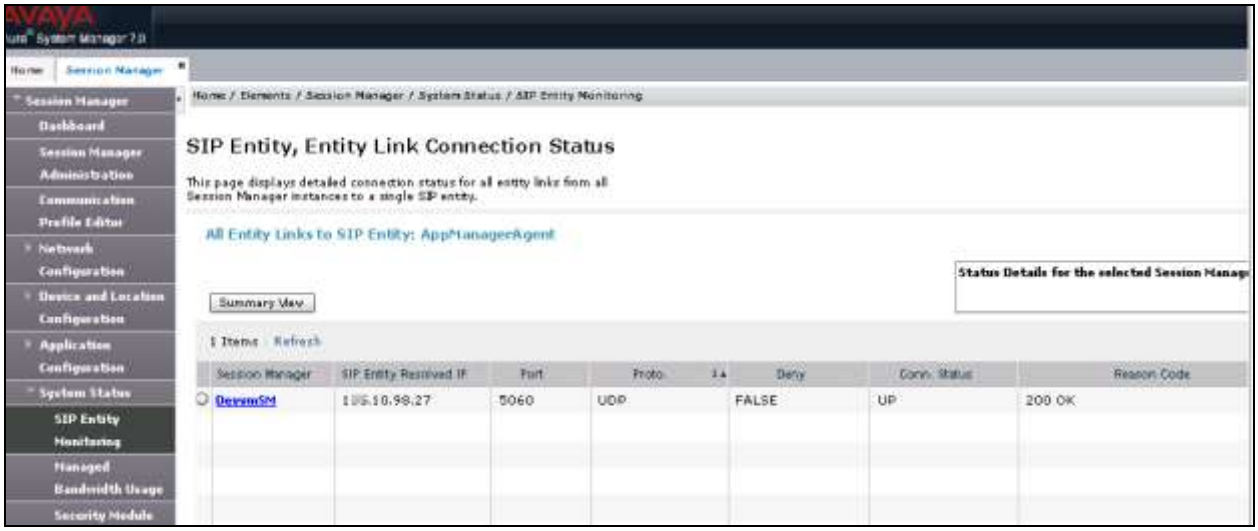
Graph data below display MOS, R-Value, jitter and Lost Data in the chart.



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:



- 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 http://support.avaya.com.

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: https://www.netiq.com/documentation/appmanager-modules/appmanagerforsipserver/data/b19cptxp.html
6. NetIQ Online help document for SNMP Traps Knowledge Scripts: https://www.netiq.com/documentation/appmanager-modules/appmanagerforsnmptraps/data/snmptraps_trapmonitor.html

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.