



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the steps required for NetIQ AppManager to monitor Avaya Aura® Session Manager, Avaya Aura® System Manager, Avaya Aura® Communication Manager, Avaya 9600 Series and 1100 Series IP Deskphones using SNMP, CDR, RTCP, and PVQMon via SIP trunk interfaces.

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

These Application Notes describe the steps required for NetIQ AppManager to monitor Avaya Aura® Session Manager, Avaya Aura® System Manager, Avaya Aura® Communication Manager, Avaya 9600 Series and 1100 Series IP Deskphones using SNMP, CDR, RTCP, and PVQMon via SIP trunk interfaces.

AppManager uses SNMPv3 to discover Session Manager and System Manager as trap sources to collect and notify user about traps received from Session Manager and System Manager. Also via SNMPv3 AppManager discovers Session Manager and System manager characteristics such as LAN Links, Host Resource, Interface and IP Subsystem.

To discover and collect call quality for 1100 Series IP Deskphones, AppManager uses SNMPv3 to discover SIP server which 1100 registers to, in this case it is Session Manager. AppManager uses SIP trunk connection to Session Manager to get SIP Publish message to collect PVQMon call quality data of 1100 Series IP Deskphones.

To discover Communication Manager and 9600 Series IP Deskphones, AppManager uses SNMPv2 to discover and receive traps from Communication Manager and Communication Manager's configuration data such as Servers, Gateways, Trunk Groups, Hunt Groups and IP Stations. AppManager collects CDR call data from Communication Manager and RTCP call quality data from 9600 Series SIP and H323 IP Deskphones.

2. General Test Approach and Test Results

This section describes the testing performed to verify the interoperability of AppManager with Session Manager, System Manager, Communication Manager, 1100 and 9600 Series IP Deskphones. The testing covered feature and serviceability test cases. The feature testing covered the ability of AppManager monitoring Session Manager and System Manager with no adverse impact on system or any other management interfaces. AppManager ability to capture CDR call records, SNMP configuration data, and SNMP traps from Communication Manager. In addition, RTCP call quality metrics from H.323 and SIP calls were also captured.

The Communication Manager CDR data collected by AppManager database was compared to the CDR data received by an Avaya CDR Test tool. CDR data for various call scenarios were generated, including internal calls, inbound trunk calls, outbound trunk calls, transferred calls, and conference calls.

To verify the accuracy of the SNMP configuration data in AppManager, trunk groups, hunt groups and stations were added and removed from Communication Manager to verify that AppManager updated its inventory information accordingly.

To verify call quality metrics, the general approach was to place various types of calls to and from stations, and compare the quality data reported by AppManager with values from the Avaya 1100 and 9600 Series IP Deskphones.

Lastly, SNMP traps were generated on Communication Manager and the G450 Media Gateway to verify that AppManager displayed the SNMP traps properly.

The serviceability testing focused on the ability of the AppManager server to recover from adverse conditions such as loss of network connectivity and power loss.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality on AppManager:

- Retrieving inventory information via SNMP from Session Manager and System Manager such as Interfaces, LAN Links, Host Resource and IP Subsystem.
- Monitoring health of Session Manager and System Manager via SNMP such as Uptime, Ping and Health.
- Displaying collected inventory and health data such as use of Graph Chart.
- Collecting PVQMon data for 1100 Series IP Deskphones via Session Manager SIP trunks.
- Collecting RTCP data for 9600 Series IP Deskphones.
- Collecting PVQMon and RTCP call quality data such as MOS, R-Value, jitter, latency and packet loss.
- Displaying call quality data using Graph Chart.
- Collecting and storing Communication Manager CDR records in AppManager database.
- Displaying RTCP data in real-time.
- Capturing station inventory from Communication Manager via SNMP.
- Displaying SNMP traps from Communication Manager.
- Proper system recovery after loss of network connectivity and power loss.

Call quality metrics, SNMP traps, CDR records, and the phone inventory were accurately collected on AppManager. The data was verified by running the *CallQuery*, *CallQuality*, *PhoneQuality*, and *RetrieveConfigData* Knowledge Scripts. Sample reports are shown in **Section 9.3.4**.

2.2. Test Results

AppManager passed compliance testing with the observations noted below.

- The Reliable Session Protocol (RSP) for CDR collection is currently not supported by AppManager. CDR test cases were run with RSP disabled. AppManager requires that a custom CDR format be applied on Communication Manager. CDR test cases were run with a custom CDR format as described below and in reference [4].
Note: Since RSP is not currently supported by NetIQ, in case of AppManager application losing network connectivity, there will be loss of data until the application can regain the connectivity and communicate with Avaya Aura® Communication Manager. To eliminate the impact of this failure, a secondary CDR link on Communication Manager may be configured to output CDR records to another AppManager to collect CDR records in parallel with the primary link. Due to the above reason Avaya recommends using RSP over TCP/IP.
- Authorization code and Account code are collected by AppManager and stored in the AppManager supplemental database, but are not included in the AppManager Event messages generated from the database. CDR test cases for Authorization and Account codes were validated using the information in the AppManager application database rather than using event displays.
- In this solution CDR records are only collected, stored, and not used, nor can be polled by end customers.
- On the phone inventory report, there is one station that existed on Communication Manager but was not included in the inventory report produced (NetIQ issue ENG343709).
- An 1140 local phone was reported as a remote phone in the SIP PUBLISH event. This issue is fixed by Avaya team and will be available in next service package SP7 for 1100 Series IP Deskphone.

2.3. Support

For technical support on AppManager, contact NetIQ Support through the following:

Phone: (888) 323-6768 (Toll free)
Worldwide: www.netiq.com/support/contactinfo.asp
North and South America: 1-713-418-5555
Europe, Middle East, and Africa: +353 (0) 91-782 677

Web: <http://www.netiq.com/support>

Email: support@netiq.com

3. Reference Configuration

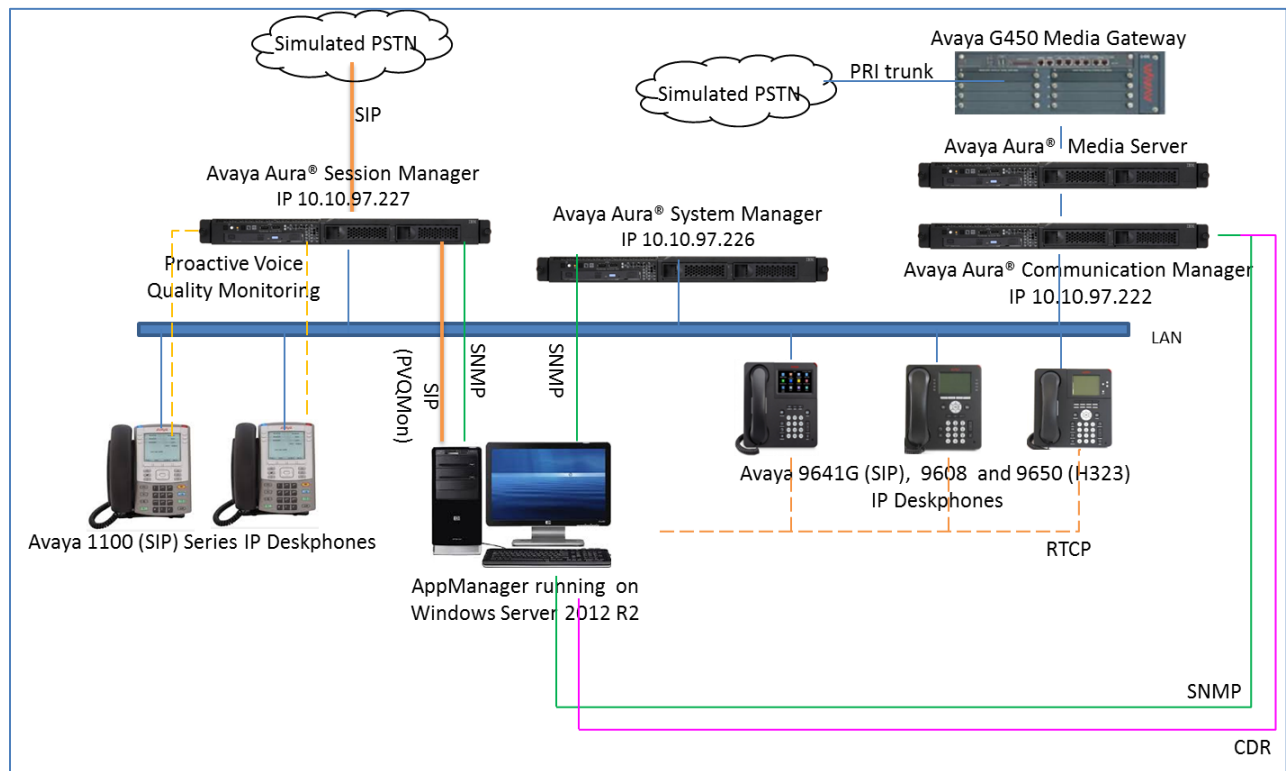


Figure 1 illustrates the configuration used for the compliance test. In the sample configuration, AppManager connected to Session Manager and System Manager and Communication Manager via SNMP. AppManager collected PVQMon call data from 1100 Series IP Deskphones via SIP trunks to Session Manager, CDR from Communication Manager and RTCP data from 9600 Series IP Deskphones. In this configuration AppManager was running on a Windows Servers 2012 R2 server.

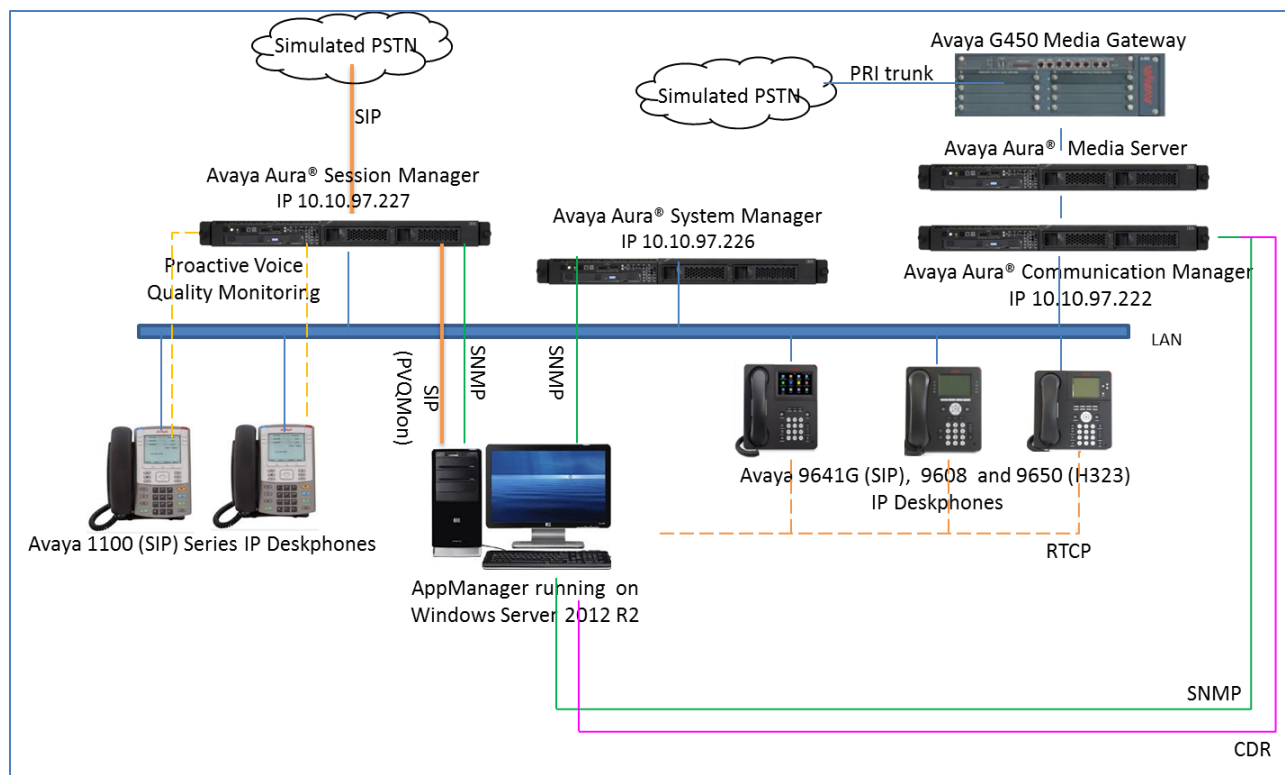


Figure 1: NetIQ AppManager with Avaya Aura® Communication Manager

4. Equipment and Software Validated

The following equipment and release/version were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Environment (VE)	7.0.1.1.1 SP1.1
Avaya G450 Media Gateway	7.0.1.2
Avaya Aura® Media Server in VE	7.7 SP2 (v.7.7.0.281)
Avaya Aura® Session Manager	7.0.1SP1
Avaya Aura® System Manager	7.0.1.1
Avaya 9621G IP Deskphone (SIP)	7.0.1.1.5
Avaya 9608 IP Deskphone (H323)	6.6229
Avaya 9650 IP Deskphone (SIP)	2.6.15
Avaya 1120E and 1140E IP Deskphones (SIP)	4.4.26
NetIQ AppManager running on Windows Server 2012R2 NetIQ AppManager Suite Module: <ul style="list-style-type: none">• AppManager Console• Repository Server• AvayaCM• NetworkDevice• SIPServer• SNMPTraps• SNMP Toolkit	9.1.1.419 9.1.1.419 9.1.1.419 7.6 7.5.64 8.0.291.0 8.1.24.0 7.5.41

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

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

Here is a summary of configuration on System Manager:

- Administer SNMPv3 user profiles
- Administer SNMPv3 target profiles
- Assign SNMPv3 target profiles
- Administer SIP trunk
- Create SIP user

5.1. Administer SNMPv3 User Profiles

Access the System Manager Web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials (not shown). On System Manager home page (not shown), select **Service** → **Inventory** to launch **Inventory** tab. In **Inventory** tab, select **Manage Serviceability Agents** → **SNMPv3 User Profiles** and click on **New** button (not shown) to add new user profile.

- **User Name:** Enter any descriptive name such as *netiqDESSHA*.
- **Authentication Protocol:** Select *SHA*.
- **Authentication Password:** Enter any password, for example, *avaya123*.
- **Confirm Authentication Password:** Re-enter password.
- **Privacy Protocol:** Select *DES*.
- **Privacy Password:** Enter any password, for example, *avaya123*.
- **Confirm Privacy Password:** Re-enter password.
- **Privileges:** Select *Read/Write* option.

Click **Commit** to save changes.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.0', and a 'Last Logged on at A' status indicator. Below the navigation bar, there are tabs for 'Home' and 'Inventory'. The 'Inventory' tab is active, and a sub-menu on the left shows 'Manage Elements', 'Create Profiles and Discover SRS/SCS', 'Element Type Access', 'Subnet Configuration', 'Manage', 'Serviceability Agents', 'SNMPv3 User Profiles', 'SNMP Target Profiles', 'Notification Filter Profile', and 'Serviceability Agents'. The 'SNMPv3 User Profiles' option is selected. The main content area shows the 'New User Profile' form. The form has a title 'New User Profile' and two 'Commit' and 'Back' buttons. The form is divided into a 'User Details' section. The fields in the 'User Details' section are: 'User Name' (text input, value: netiqDESSHA), 'Authentication Protocol' (dropdown menu, value: SHA), 'Authentication Password' (password input, value: masked with dots), 'Confirm Authentication Password' (password input, value: masked with dots), 'Privacy Protocol' (dropdown menu, value: DES), 'Privacy Password' (password input, value: masked with dots), 'Confirm Privacy Password' (password input, value: masked with dots), and 'Privileges' (dropdown menu, value: Read/Write). A red asterisk indicates required fields. At the bottom of the form, there is a red asterisk followed by the text '*Required' and two 'Commit' and 'Back' buttons.

5.2. Administer SNMPv3 Target Profiles

Configure AppManager as target profile to receive traps. Navigate to **Manage Serviceability Agents** → **SNMP Target Profiles**, click on **New** button (not shown) to add new target profile.

- **Name:** Enter any descriptive name, for example: *netiqDESSHAtrops*.
- **Description:** Enter any description if needed.
- **IP Address:** Enter IP address of AppManager server, e.g., *10.10.97.28*.
- **Port:** Use default value *162*.
- **Notification Type:** Select *Trap* type.
- **Protocol:** Select *V3*.

AVAYA
Aura® System Manager 7.0

Home Inventory

Inventory

- Manage Elements
- Create Profiles and Discover SRS/SCS
- Element Type Access
- Subnet Configuration
- Manage
 - Serviceability Agents
 - SNMPv3 User Profiles
 - SNMP Target Profiles**
 - Notification Filter Profile
 - Serviceability Agents

Home / Services / Inventory / Manage Serviceability Agents / SNMP Target Profile

New Target Profile

Commit Back

Target Details * Attach/Detach User Profile

Target Details

* Name: netiqDESSHAtrops

Description: v3 SNMP trap

* IP Address: 10.10.97.28

* Port: 162

* Notification Type: Trap

* Protocol: V3

*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 (not shown). Click **Commit** to save changes.

5.3. Assign SNMPv3 Target Profiles

Navigate to **Manage Serviceability Agents** → **Serviceability Agents**, select entries associated with Session Manager and System Manager in the **Agent List** as displayed in below screenshot.

Create Profiles and Discover SRS/SCS

Element Type Access

Subnet Configuration

▼ Manage

Serviceability Agents

SNMPv3 User Profiles

SNMP Target Profiles

Notification Filter Profile

Serviceability Agents

Serviceability Agents

Agent List

ActivateManage ProfilesGenerate Test AlarmRepair Serviceability Agent

2 Items Show All Click here to manage the profiles Filter: Enable

<input checked="" type="checkbox"/>	Hostname	IP Address	System Name	System OID	Status
<input checked="" type="checkbox"/>	DevvmSM.bvwdev.com	10.97.227	DevvmSM		active
<input checked="" type="checkbox"/>	devvmsmgr.bvwdev.com	10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active

Select : All, None

Click on **Manage Profiles** button (shown above) and verify selected entries are listed in **Selected Agents** tab.

HomeInventory

▼ Inventory

Manage Elements

Create Profiles and Discover SRS/SCS

Element Type Access

Subnet Configuration

▼ Manage

Serviceability Agents

SNMPv3 User Profiles

SNMP Target Profiles

Notification Filter Profile

Serviceability Agents

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

Manage Profile

CommitBack

Selected AgentsSNMP Target ProfilesSNMPv3 User Profiles

Selected Agents

2 Items Show All Filter: Enable

Hostname	IP Address	System Name	System OID	Status
DevvmSM.bvwdev.com	10.97.227	DevvmSM		active
devvmsmgr.bvwdev.com	10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active

CommitBack

Click on **SNMP Target Profile** tab, select target profile create in **Section 5.2**, in this case, *netiqDESSHAtraps* and click on **Assign** as displayed below.

Manage Profile Commit Back

Selected Agents **SNMP Target Profiles** SNMPv3 User Profiles

Assignable Profiles ▾

[Assign](#)

2 Items [Click to Assign](#)

<input type="checkbox"/>	Name	Domain Type	IP Address	Port	SNMP Version
<input type="checkbox"/>	netiqSNMPv2	UDP	10.10.97.28	162	V2
<input checked="" type="checkbox"/>	netiqDESSHAtraps	UDP	10.10.97.28	162	V3

Select : All, None

Removable Profiles ▾

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

Manage Profile Commit Back

Selected Agents SNMP Target Profiles **SNMPv3 User Profiles**

Assignable Profiles ▾

[Assign](#)

1 Item [Click to Assign](#)

<input checked="" type="checkbox"/>	User Name	Authentication Protocol	Privacy Protocol	Privileges
<input checked="" type="checkbox"/>	netiqDESSHA	SHA	DES	R

Select : All, None

Removable Profiles ▾

[Remove](#)

0 Items [Add](#)

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

Manage Elements

Create Profiles and Discover SRS/SCS

Element Type Access

Subnet Configuration

Manage

Serviceability Agents

SNMPv3 User Profiles

SNMP Target Profiles

Notification Filter Profile

Serviceability Agents

Synchronization

Manage Profile

CommitBack

Selected AgentsSNMP Target ProfilesSNMPv3 User Profiles

Assignable Profiles

Assign

0 Items

<input type="checkbox"/>	User Name	Authentication Protocol	Privacy Protocol	Privileges
No records to display				

Removable Profiles

Remove

1 Item

<input type="checkbox"/>	User Name	Authentication Protocol	Privacy Protocol	Privileges
<input type="checkbox"/>	netiqDESSHA	SHA	DES	R

Select : All, None

CommitBack

5.4. Administer SIP Trunk

This section describes steps to add SIP trunk from Session Manager to AppManager. This trunk is used in AppManager to collect call data from Session Manager for 1100 Series SIP deskphone.

5.4.1. Administer SIP Entity

In **System Manager** home page, select **Element** → **Routing** → **SIP Entities** (not shown) and click on **New** button (not shown) to create new SIP entity for AppManager, enter the following value as shown in below screenshot which used during compliance test:

- **Name:** Enter any descriptive name, for example: *AppManagerAgent*.
- **FQDN or IP Address:** Enter IP address of AppManager server, e.g., *10.10.97.28*.
- **Type:** Select *SIP Trunk*.
- **Location:** Select an existing location, for example: *Belleville*.
- **Call Detail Recording:** Select *none* in the dropdown list.

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

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo and the text 'Aura System Manager 7.0'. A breadcrumb trail shows 'Home / Elements / Routing / SIP Entities'. The left sidebar contains a menu with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. The form contains the following fields: 'Name' (required, value: AppManagerAgent), 'FQDN or IP Address' (required, value: 10.10.97.28), 'Type' (dropdown, value: SIP Trunk), 'Notes' (text area, value: NetIQ server - agent), 'Adaptation' (dropdown), 'Location' (dropdown, value: Belleville), 'Time Zone' (dropdown, value: America/Fortaleza), 'SIP Timer B/F (in seconds)' (required, value: 4), 'Credential name' (text area), 'Securable' (checkbox, unchecked), 'Call Detail Recording' (dropdown, value: none), and 'Loop Detection Mode' (dropdown, value: On). 'Commit' and 'Cancel' buttons are in the top right corner.

Field	Value
Name	AppManagerAgent
FQDN or IP Address	10.10.97.28
Type	SIP Trunk
Notes	NetIQ server - agent
Adaptation	
Location	Belleville
Time Zone	America/Fortaleza
SIP Timer B/F (in seconds)	4
Credential name	
Securable	<input type="checkbox"/>
Call Detail Recording	none
Loop Detection Mode	On

5.4.2. Administer Entity Links

In **Routing** tab, select **Entity Links** (not shown) 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., *LinkToApp*.
- **SIP Entity 1:** Select Session Manager entity, e.g., *DevvmSM*.
- **SIP Entity 2:** Select AppManager entity created in **Section 5.4.1**.
- **Protocol:** Select *UDP* protocol.
- **Port:** Once UDP protocol is selected the port will be updated to *5060*.

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

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel

1 Item

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	LinkToApp	DevvmSM	UDP	5060	AppManagerAgent	<input type="checkbox"/>	5060	Trusted	<input type="checkbox"/>

Select: All, None

Commit Cancel

6. Configure Avaya 1100 Series IP Deskphones

This section describes steps on how to configure 1100 Series IP Deskphones to send call quality data to AppManager. On the file server that services the 1100 Series IP Deskphones, open device configure file **SIPDeviceConfig.dat** and modify as shown below:

- **VQMON_PUBLISH:** Enter *YES*.
- **VQMON_PUBLISH_IP:** Enter AppManager IP address for example *10.10.98.28*.

Set the values for other fields as shown below and save the file. Reboot all 1100 Series IP Deskphones to pick up the updated device configuration.

```
VQMON_PUBLISH YES
VQMON_PUBLISH_IP 10.10.97.28  <- agent IP goes here, tested agent was 10.10.97.28

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
```

7. Configure Avaya Aura® Communication Manager

This section describes steps to configure Communication Manager to interoperate with AppManager. It assumes that the application and all required software components have been installed and properly licensed. This section is divided into three sub-sections describing the three interfaces used by AppManager to gather data:

- Configure SNMP
- Configure RTCP
- Configure CDR

The configuration of Communication Manager in **Section 7.1** was performed using the Web interface. The configuration described in **Sections 7.2** and **0** was performed using the System Access Terminal (SAT).

7.1. Configure SNMP

To access the Communication Manager web interface, enter the IP address of the Avaya Server into a web browser. Log in using appropriate credentials. Navigate to **Administration** → **Server (Maintenance)** (not shown) to display the following web page.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar is red with the Avaya logo on the left and the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the navigation bar, there is a red bar with "Help Log Off" and "Administration". The main content area is titled "Server Administration" and contains a welcome message: "Welcome to the 'Server Administration Interface'. This interface allows you to maintain, troubleshoot, and configure the server. Please use the menu to the left for navigation." The left sidebar menu includes "Alarms", "Current Alarms", "SNMP", "Agent Status", "Access", "Incoming Traps", "FP Traps", "FP Trap Test", and "FP Filters". The "SNMP" section is expanded, showing "Agent Status", "Access", "Incoming Traps", "FP Traps", "FP Trap Test", and "FP Filters". The "Access" link is highlighted in blue.

To allow AppManager to use SNMP to collect configuration and status information from Communication Manager, navigate to **SNMP** → **Access**, and click on **Add/Change** button to add new or change existing access.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) with the "Access" page selected. The top navigation bar is red with the Avaya logo on the left and the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the navigation bar, there is a red bar with "Help Log Off" and "Administration". The main content area is titled "Access" and contains the following information: "The Access SMI page is used to configure SNMP access to CM.", "Master Agent status: UP", and a link "View AVAYA-AURA-CM-MIB Data". Below this, there is a section titled "Current Settings" with a table of settings. The table has columns for "IP address", "Access", "SNMP Version", "Community / User Name", "V3 Security Model", "Authentication Password", "Authentication Protocol", "Privacy Password", and "Privacy Protocol". The first row of data shows "10.10.98.28", "read-write", "2c", "public", and empty cells for the remaining columns. At the bottom of the table, there are three buttons: "Add/Change", "Delete", and "Help". The left sidebar menu includes "Alarms", "Current Alarms", "SNMP", "Agent Status", "Access", "Incoming Traps", "FP Traps", "FP Trap Test", "FP Filters", "Diagnostics", "Restarts", "System Logs", "Ping", "Traceroute", "Netstat", "Server", and "Status Summary". The "Access" link is highlighted in blue.

Below is detail of access created for AppManager, configure the **SNMP Version 2c** section. Set the **Access** field to *read-write*, enter *public* for **Community Name** as displayed in below screenshot. Click **Submit** at the bottom of the screen.

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

Help Log Off Administration

Administration / Server (Maintenance) This Server: DevvmCM

Alarms

- Current Alarms
- SNMP**
 - Agent Status
 - Access
 - Incoming Traps
 - FP Traps
 - FP Trap Test
 - FP Filters
- Diagnostics
 - Restarts
 - System Logs
 - Ping
 - Traceroute
 - Netstat
- Server
 - Status Summary
 - Process Status
 - Shutdown Server
 - Server Date/Time
 - Software Version
- Server Configuration
 - Server Role
 - Network Configuration
 - Static Routes
 - Display Configuration
 - Time Zone Configuration

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

SNMP Version 2c

IP address: 10.10.98.28

Access: read-write

Community Name: public

Add SNMP Users / Communities

SNMP Version 1

IP address:

Access:

Community Name:

SNMP Version 3

Access:

User Name:

Authentication Protocol:

Authentication Password: Minimum 8 characters. (for authentication and privacy)

Privacy Protocol:

Privacy Password: Minimum 8 characters. (for privacy)

Submit Cancel Help

To configure AppManager as an SNMP trap receiver, navigate to **SNMP → FP Traps** in the left pane. In the **FP Traps** screen, click the **Add/Change** button shown below.

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

Help Log Off Administration

Administration / Server (Maintenance) This Server: DevvmCM

Alarms

- Current Alarms
- SNMP**
 - Agent Status
 - Access
 - Incoming Traps
 - FP Traps**
 - FP Trap Test
 - FP Filters
- Diagnostics
 - Restarts
 - System Logs
 - Ping
 - Traceroute
 - Netstat
- Server
 - Status Summary
 - Process Status
 - Shutdown Server
 - Server Date/Time
 - Software Version
- Server Configuration
 - Server Role
 - Network Configuration
 - Static Routes
 - Display Configuration
 - Time Zone Configuration

FP Traps

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

Note:

- The FP Traps SMI page is for the administration of CM Fault Performance Traps only. It is not for INADS. INADS traps are configured using the "almenable" and the "almsnmpconf" CLI command. Additionally, Fault Performance Traps should not be sent to SAL IP Addresses.

Master Agent status: **UP**

[View AVAYA-AURA-CM-ALARM-MIB Data](#)

Current Settings

IP address	Port	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Authentication Protocol	Privacy Password	Privacy Protocol	Engine ID
<input checked="" type="checkbox"/>	10.10.98.28	162 trap	2c	public						

Add/Change Delete Help

Under the **SNMP Version 2c** section, specify the **IP address** of AppManager, for example **10.10.97.28**, set the **Notification** field to **trap**, and set the **Community Name** to **public**. Click the **Submit** button.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for the server DevvmCM. The left sidebar contains a navigation menu with categories: Alarms, SNMP, Diagnostics, Server, and Server Upgrades. The main content area is titled "FP Traps" and includes a description: "The FP Traps page allows specification of the alarms to be sent as traps." Below this, there are three sections for configuring traps: "SNMP Version 2c", "Add Trap Destination", and "SNMP Version 3". The "SNMP Version 2c" section has fields for IP address (10.10.98.28), Notification (trap), and Community Name (public). The "Add Trap Destination" section has fields for IP address, Port (162), Notification (trap), and Community Name. The "SNMP Version 3" section has fields for IP address, Port (162), Notification, User Name, Authentication Protocol, Authentication Password (with a note "Minimum 8 characters. (for authentication and privacy)"), Privacy Protocol, Privacy Password (with a note "Minimum 8 characters. (for privacy)"), and Engine ID. At the bottom of the main content area are buttons for "Submit", "Cancel", and "Help".

Lastly, the SNMP agent must be started. Navigate to **SNMP → Agent Status**. If the **Master Agent status** is **DOWN**, then click the **Start Master Agent** button. If the **Master Agent status** is **UP**, then the agent must be stopped and restarted.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for the server DevvmCM. The left sidebar contains a navigation menu with categories: Alarms, SNMP, Diagnostics, Server, and Server Upgrades. The main content area is titled "Agent Status" and includes a description: "The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent." Below this, there are two sections: "Sub Agent Status" and "Agent Status". The "Sub Agent Status" section shows the status of the Master Agent (UP) and all Sub Agents (FP Agent status: UP, CMSubAgent status: UP, Load Agent status: UP). The "Agent Status" section shows the status of the Master Agent (UP). At the bottom of the main content area are buttons for "Stop Master Agent" and "Help".

7.2. Configure RTCP

This section describes the RTCP configuration. It is performed using the Communication Manager SAT interface.

Use the **change system-parameters ip-options** command to set the **RTCP MONITOR SERVER** parameters. These values will be sent from Communication Manager to each 9600 Series H.323 IP Deskphone so that the phones will know where to send RTCP data.

- **Server IPV4 Address:** Enter IP address of the AppManager server.
- **IPV4 Server Port:** Enter number between 1-65535, for example 5005.
- **RTCP Report Period(secs):** Enter number between 5-30, for example 5.

```
change system-parameters ip-options                               Page 1 of 3
                        IP-OPTIONS SYSTEM PARAMETERS

IP MEDIA PACKET PERFORMANCE THRESHOLDS
  Roundtrip Propagation Delay (ms)      High: 800      Low: 400
      Packet Loss (%)                   High: 40       Low: 15
      Ping Test Interval (sec): 20
  Number of Pings Per Measurement Interval: 10
      Enable Voice/Network Stats? n

RTCP MONITOR SERVER
  Server IPV4 Address: 10.10.97.28      RTCP Report Period(secs): 5
      IPV4 Server Port: 5005
  Server IPV6 Address:
      IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
  Link Failure? y

H.323 IP ENDPOINT
H.248 MEDIA GATEWAY      Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5      Primary Search Time (sec): 75
      Periodic Registration Timer (min): 20
      Short/Prefixed Registration Allowed? N
```

Use the **change ip-network-region** command to enable RTCP reporting for 9600 Series H.323 IP Deskphones. In the compliance test, the 9600 Series H.323 IP Deskphones belonged to IP network region 1. Set the **RTCP Reporting Enabled** field to y.

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

RTCP Reporting Enabled? y

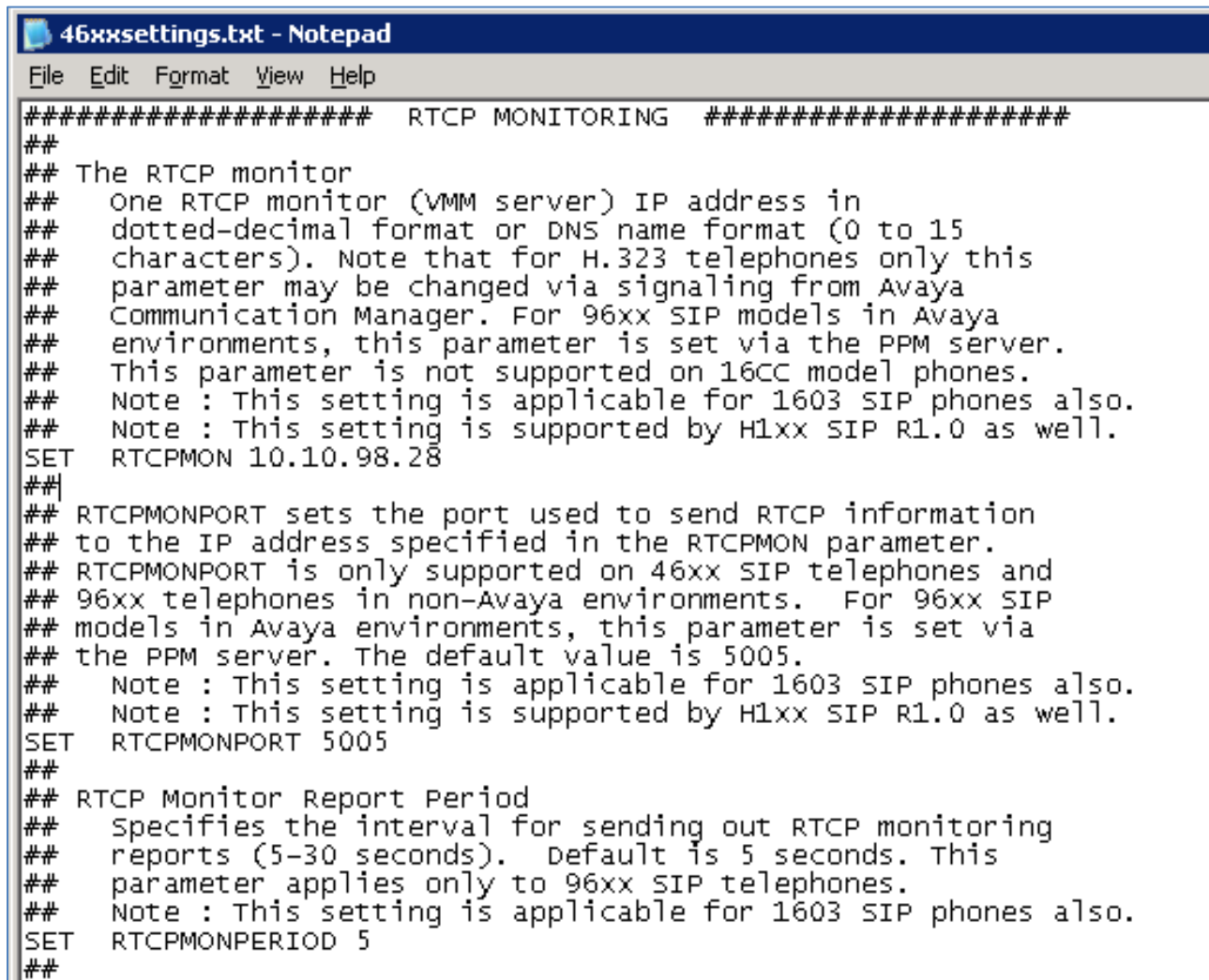
RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? y
```

7.3. Configure RTCP on 9600 SIP Deskphone

This section describe steps need to configure 9600 Series SIP IP Deskphone to send RTCP data to AppManager. On the file server, locate to the **46xxsettings.txt** settings file. Open the settings file in a text editor. Set the required parameters as displayed below:

- **RTCPMON**: Enter IP or DNS address of AppManager for RTCP monitor for example *10.10.98.28*.
- **RTCPMONPORT**: Enter RTCP monitor port number for example *5005*.
- **RTCPMONPERIOD**: Use default value, for example 5 seconds.

Save the settings file. Reboot 9600 SIP IP Deskphones to update the new setting file.



```
##### RTCP MONITORING #####
##
## The RTCP monitor
## One RTCP monitor (VMM server) IP address in
## dotted-decimal format or DNS name format (0 to 15
## characters). Note that for H.323 telephones only this
## parameter may be changed via signaling from Avaya
## Communication Manager. For 96xx SIP models in Avaya
## environments, this parameter is set via the PPM server.
## This parameter is not supported on 16CC model phones.
## Note : This setting is applicable for 1603 SIP phones also.
## Note : This setting is supported by H1xx SIP R1.0 as well.
SET RTCPMON 10.10.98.28
##
## RTCPMONPORT sets the port used to send RTCP information
## to the IP address specified in the RTCPMON parameter.
## RTCPMONPORT is only supported on 46xx SIP telephones and
## 96xx telephones in non-Avaya environments. For 96xx SIP
## models in Avaya environments, this parameter is set via
## the PPM server. The default value is 5005.
## Note : This setting is applicable for 1603 SIP phones also.
## Note : This setting is supported by H1xx SIP R1.0 as well.
SET RTCPMONPORT 5005
##
## RTCP Monitor Report Period
## Specifies the interval for sending out RTCP monitoring
## reports (5-30 seconds). Default is 5 seconds. This
## parameter applies only to 96xx SIP telephones.
## Note : This setting is applicable for 1603 SIP phones also.
SET RTCPMONPERIOD 5
##
```

7.4. Configure CDR

This section describes the CDR configuration. It is performed using Communication Manager SAT interface. Use the **change node-names ip** command to associate the IP address of AppManager to a node name. In the compliance test, the node name *NetIQ* was assigned to IP address *10.10.97.28*. Also, highlighted in the example below is the node name *procr*, which represents the IP address of Communication Manager's Processor C-LAN as the source of CDR data.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
DevvmAES	10.10.97.224	
AVAYARDTT	10.10.98.71	
GW-G450	10.10.97.223	
NetIQ	10.10.97.28	
default	0.0.0.0	
procr	10.10.97.222	

Use the **change ip-services** command to define the CDR link between Communication Manager and AppManager.

- **Service Type:** Enter *CDR1* for the primary CDR link.
- **Local Node:** Enter the node name that will terminate the CDR link on Communication Manager. In the compliance test, the **Local Node** was *procr*.
- **Remote Node:** Enter AppManager's node name, for example *NetIQ*.
- **Remote Port:** Enter number between 5000 and 64500, for example *9000*.

change ip-services					Page	1 of	4
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	procr	8765				
CDR1		procr	0	NetIQ	9000		
CDR2		procr	0	AVAYARDTT	9001		

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

change ip-services					Page 3 of 4
SESSION LAYER TIMERS					
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer
CDR1	n	30	3	3	60
CDR2	y	30	3	3	60

Use the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The settings for the compliance test are described below.

- **CDR Date Format:** Set this to *month/day*.
- **Primary Output Format:** Set this to *customized*.
- **Primary Output Endpoint:** Set this to *CDR1*.
- **Intra-switch CDR:** Set to *y*, this allows call records for internal calls involving specific stations.
- **Record Outgoing Calls Only:** Set to *n*, this allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.
- **Outg Trk Call Splitting:** Set to *y*, this allows a separate call record for any portion of an outgoing call that is transferred or conferenced.
- **Suppress CDR for Ineffective Call Attempts:** Set to *n*, this prevents calls that are blocked from appearing in the CDR record.
- **Inc Trk Call Splitting:** Set to *y*, this allows a separate call record for any portion of an incoming call that is transferred or conferenced.

Default values may be used for all other fields.

```
change system-parameters cdr                                     Page 1 of 2
                                CDR SYSTEM PARAMETERS

Node Number (Local PBX ID):                                     CDR Date Format: month/day
    Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format: unformatted Secondary Output Endpoint: CDR2
        Use ISDN Layouts? n                Enable CDR Storage on Disk? n
        Use Enhanced Formats? n            Condition Code 'T' For Redirected Calls? n
        Use Legacy CDR Formats? n          Remove # From Called Number? n
Modified Circuit ID Display? n                                Intra-switch CDR? y
                                Record Outgoing Calls Only? n    Outg Trk Call Splitting? y
    Suppress CDR for Ineffective Call Attempts? n    Outg Attd Call Record? y
        Disconnect Information in Place of FRL? n    Interworking Feat-flag? n
    Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                                Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n    Record Agent ID on Outgoing? y
    Inc Trk Call Splitting? y                Inc Attd Call Record? y
    Record Non-Call-Assoc TSC? n            Call Record Handling Option: warning
        Record Call-Assoc TSC? n    Digits to Record for Outgoing Calls: dialed
        Privacy - Digits to Hide: 0    CDR Account Code Length: 3
Remove '+' from SIP Numbers? y
```


On **Page 2**, the customized CDR format used by AppManager is defined. Each field in the CDR record is entered in the **Data Item** column, followed by the expected length of the field in the **Length** column. This is the format that Communication Manager will use when sending CDR records to AppManager.

change system-parameters cdr			Page 2 of 2		
CDR SYSTEM PARAMETERS					
Data Item - Length		Data Item - Length		Data Item - Length	
1: acct-code	- 15	17:	-	33:	-
2: attd-console	- 2	18:	-	34:	-
3: auth-code	- 13	19:	-	35:	-
4: clg-num/in-tac	- 15	20:	-	36:	-
5: code-dial	- 4	21:	-	37:	-
6: code-used	- 4	22:	-	38:	-
7: cond-code	- 1	23:	-	39:	-
8: date	- 6	24:	-	40:	-
9: dialed-num	- 23	25:	-	41:	-
10: in-crt-id	- 3	26:	-	42:	-
11: in-trk-code	- 4	27:	-	43:	-
12: out-crt-id	- 3	28:	-	44:	-
13: sec-dur	- 5	29:	-	45:	-
14: time	- 4	30:	-	46:	-
15: return	- 1	31:	-	47:	-
16: line-feed	- 1	32:	-	48:	-
Record length = 104					

If the **Intra-switch CDR** field is enabled as seen earlier, use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the **Extension** field, enter a specific extension whose usage will be tracked with a CDR record. Add an entry for each additional extension of interest. For example below is list of extensions that were monitored.

change intra-switch-cdr				Page 1 of 3	
INTRA-SWITCH CDR					
		Assigned Members: 10 of 1000 administered			
Extension	Extension	Extension	Extension	Extension	
56101					
56102					
56103					
56105					
56201					
56202					
56204					
56205					
56301					
56302					
Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add new members and 'change intra-switch-cdr <ext>' to change/remove other members					

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. To do this, use the **change trunk-group *n*** command, where *n* is the trunk group number, and verify that the **CDR Reports** field is set to y. This applies to all trunk group types.

The example below shows the ISDN-PRI trunk to the PSTN.

```
change trunk-group 5                                     Page 1 of 22
                                     TRUNK GROUP
Group Number: 5                Group Type: isdn          CDR Reports: y
  Group Name: To-IPO via T1      COR: 1                TN: 1          TAC: #005
  Direction: two-way            Outgoing Display? n      Carrier Medium: PRI/BRI
  Dial Access? y                Busy Threshold: 255      Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n            TestCall ITC: rest
                               Far End Test Line No:
TestCall BCC: 4
```

The example below shows the SIP trunk between Communication Manager and Session Manager.

```
change trunk-group 1                                     Page 1 of 22
                                     TRUNK GROUP
Group Number: 1                Group Type: sip          CDR Reports: y
  Group Name: Private trunk      COR: 1                TN: 1          TAC: #001
  Direction: two-way            Outgoing Display? y
  Dial Access? n                Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n
                               Member Assignment Method: auto
                               Signaling Group: 1
                               Number of Members: 15
```

8. Configure NetIQ AppManager

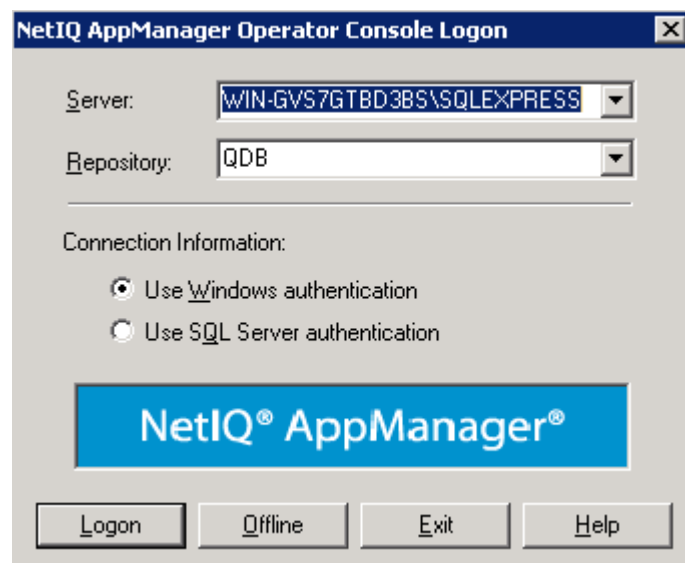
This section describes the configuration of AppManager. It assumes that the application and all required software components have been installed and properly licensed. The procedures fall into the following areas:

- Launch NetIQ Console
- Administer SNMPv3 trap monitoring
- Administer SIP call quality monitoring
- Configure SNMP, CDR, and RTCP parameters
- Discover Communication Manager
- Retrieve configuration data
- Add IP Deskphones

8.1. 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.

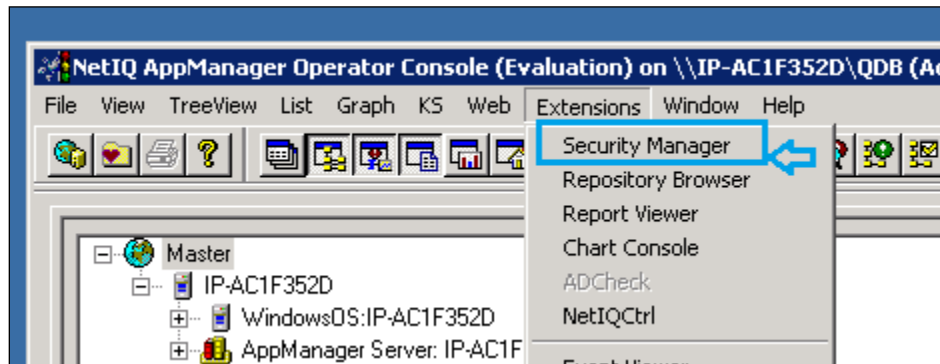


8.2. Administer SNMPv3 Trap Monitoring

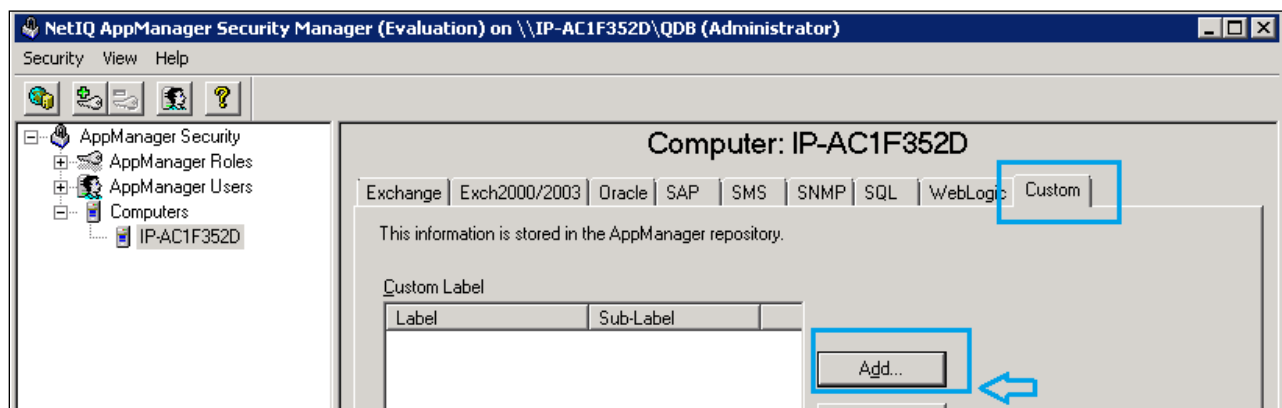
This section describes steps to enable AppManager to use SNMP with Session Manager and System Manager, the SNMP community strings are required to be configured in the AppManager Security Manager as configured in **Section 5**.

8.2.1. Configure Security Manager

From the **NetIQ AppManager Operator Console** window navigate to **Extensions → Security Manager** as shown in below.



Add a custom profile for Session Manager and Session Manager by clicking on **Add** button as displayed below:



Enter the System Manager SNMPv3 user profile created in **Section 5.1** as shown below:

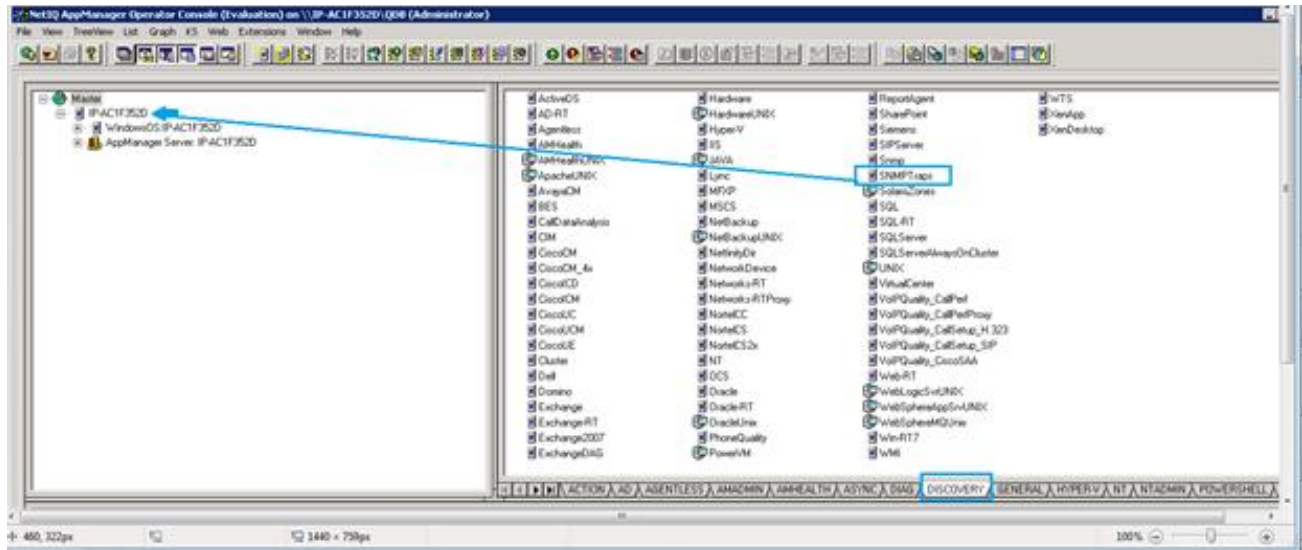
- **Label:** Enter any descriptive name, e.g., *SNMPTraps*.
- **Sub-Label:** Enter System Manager's IP address, e.g., *10.10.97.226*.
- **Value 1:** Enter user name created in **Section 5.1**.
- **Value 2:** Enter *.
- **Value 3:** Enter the authentication protocol, authentication password, privacy protocol, and privacy password from **Section 5.1**, e.g., *sha,avaya123,des,avaya123*.

Create a similar entry with Session Manager IP address, e.g., *10.10.97.227* as displayed below:

The image displays two side-by-side "Modify Custom Entry" dialog boxes. Both dialogs contain the same text: "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." Below this text are five input fields: "Label:" (containing "SNMPTraps"), "Sub-Label:" (containing "10.10.97.226" on the left and "10.10.97.227" on the right), "Value 1:" (containing "netiqDESSHA"), "Value 2:" (containing "*"), and "Value 3:" (containing "sha,avaya123,des,avaya123"). At the bottom of each dialog is an unchecked checkbox labeled "Extended application support (Click Help for details.)" and three buttons: "OK", "Cancel", and "Help".

8.2.2. Discover the Device

To monitor SNMP trap source devices that require the use of SNMP version 3, run the Discover_SNMPTTraps Knowledge Script, navigate to the **DISCOVERY** tab in the bottom right pane and drag and drop the **SNMPTTraps** Discovery Knowledge Script (KS will be used as abbreviation) on the AppManager server in the TreeView to create the discovery job.



The **Discovery_SNMPTTraps** properties window is displayed. Modify job properties as shown below:

- **Name of the device to populated in the TreeView:** enter the DNS name of Session Manager for example: *devvmsm*.
- **IP address of the device to populate in the TreeView:** IP address of the Session Manager for example *10.10.97.227*.

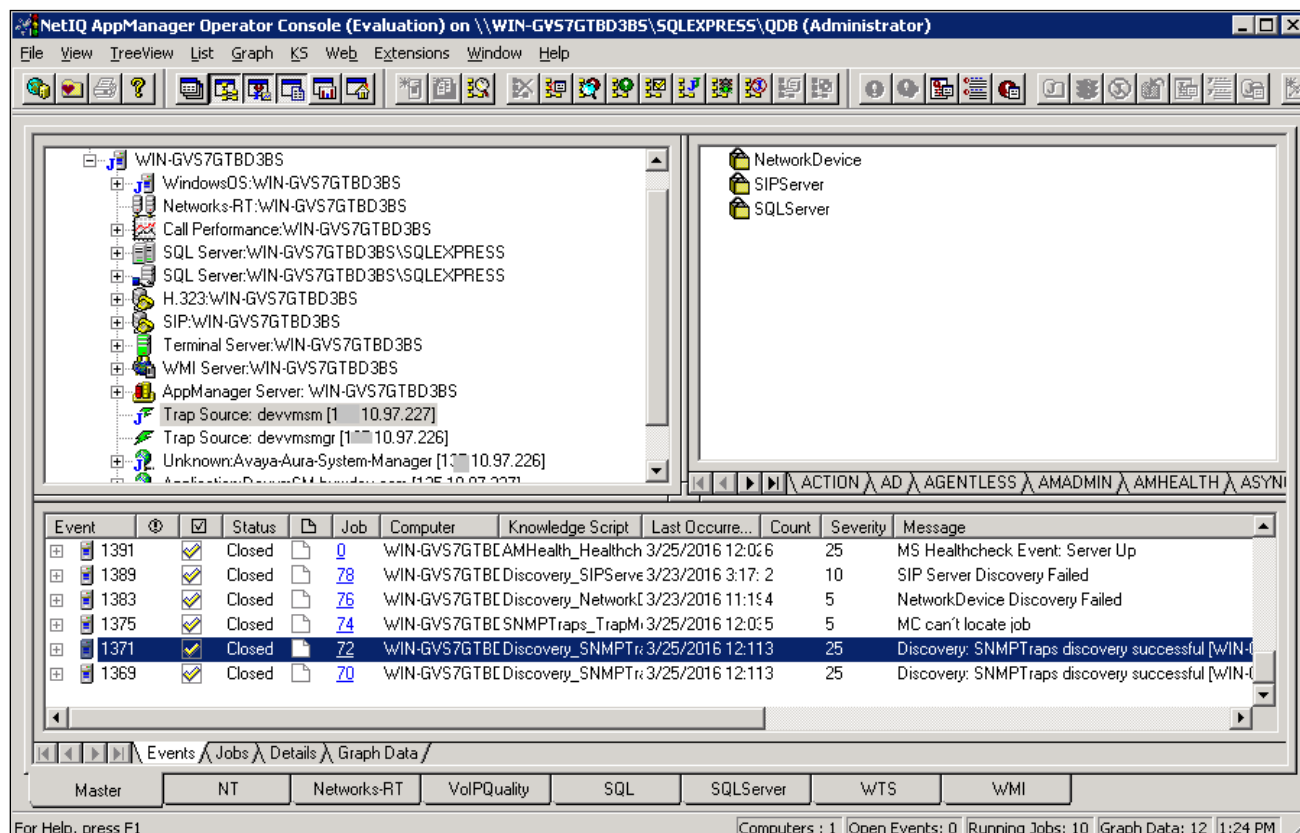
Description	Value	Units
General Settings		
Job Failure Notification		
Event severity if discovery job fails unexpectedly	5	Severity
Event Details		
Event detail format	HTML Table	
Additional Settings		
+ Tracing (for advanced users only)		
Discover SNMP Trap Devices		
+ Raise event if discovery succeeds?	<input checked="" type="checkbox"/> Yes	
+ Raise event if discovery fails?	<input checked="" type="checkbox"/> Yes	
Update the TreeView object name if the device name changed since the previous discovery?	<input checked="" type="checkbox"/> 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 NetIQ Trap Receiver server. Raises an event if the job fails and optionally raises events to indicate discovery status (successful, failed).

OK Cancel Help

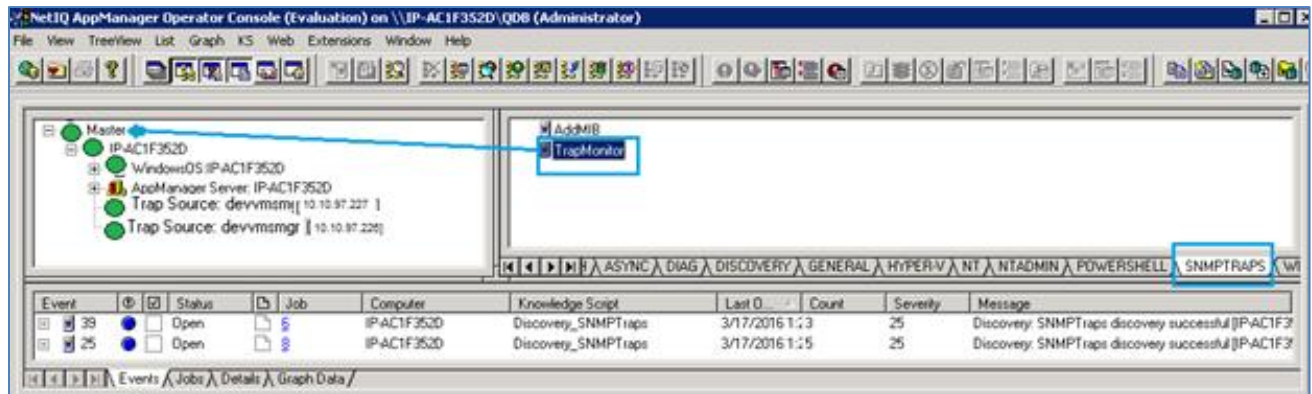
Repeat same steps for System Manager with name *devvmsmgr* and IP address *10.10.97.226*.

Confirm that Session Manager and System Manager appear in the TreeView (which confirms the SNMPv3 credentials are valid and the NetIQ trap receiver service is available), in this case, it is *Trap Source: devvmsm[10.10.97.227]* and *Trap Source: devvmsmgr[10.10.97.226]*.



8.2.3. Start Trap Monitoring

Next, run the SNMPTraps_TrapMonitor Knowledge Script on Session Manager and System Manager, discovered in the TreeView, to start monitor traps from those sources by select **TrapMonitor** and drag it to TreeView as displayed below:



The **Properties for SNMPTraps_TrapMonitor** window is displayed, make sure **Monitor devices not yet discovered** and **Raise event if Trap Receiver become available** options are checked.

Properties for SNMPTraps_TrapMonitor

Schedule | Values | Actions | Objects | Advanced

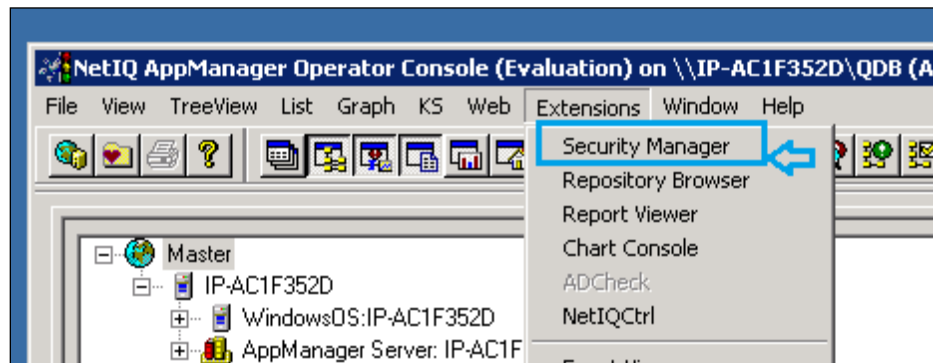
Description	Value	Units
General Settings		
Job Failure Notification		
Event severity if TrapMonitor job fails unexpectedly	5	Severity
Event Details		
Event detail format	HTML Table	
Trap source address format	Both	
Format trap data according to SNMP version?	SNMPv2	
Include prefix information to format event messages for Netcool adapter?	<input type="checkbox"/> Yes	
Varbind display options		
Trap Filters		
Additional Settings		
Monitor devices not yet discovered?	<input checked="" type="checkbox"/> Yes	
Custom message mapping file	SNMPTraps_AlarmMappings.csv	
Tracing (for advanced users only)		
Monitor SNMP Traps		
Event Notification		
Raise critical alarm event?	<input checked="" type="checkbox"/> Yes	
Raise major alarm event?	<input checked="" type="checkbox"/> Yes	
Raise cleared/resolved alarm event?	<input checked="" type="checkbox"/> Yes	
Raise event if Trap Receiver is unavailable?	<input checked="" type="checkbox"/> Yes	
Raise event if Trap Receiver becomes available?	<input checked="" type="checkbox"/> Yes	

Monitors for incoming SNMP trap messages from devices forwarded by NetIQ Trap Receiver. Raises events when traps are received and for Trap Receiver availability.

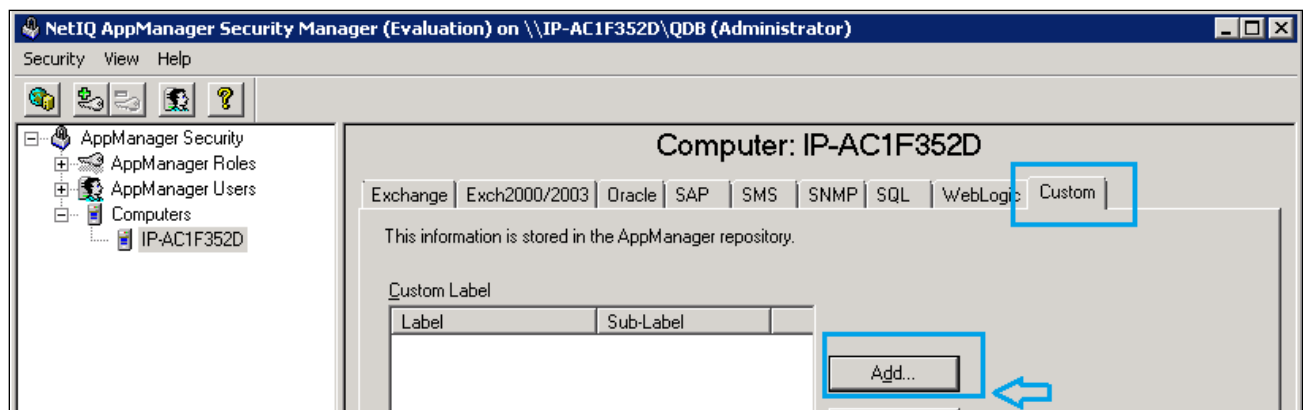
OK Cancel Help

8.2.4. Administer Network Device

NetworkDevice discovers Session Manager and System Manager using SNMP to query the device characteristics. To use SNMP queries, create the SNMP access credentials as follows: Create an SNMP profile for Session Manager. Note that this is different from the SNMPTraps profile created in **Section 8.2.1** because this is for snmp-get requests from the NetworkDevice module. Here enter SNMPv3 profile for Session Manager by selecting **Extensions → Security Manager**:



Add a custom profile for Network Device:



Enter the Session Manager SNMP profile into Security Manager. If all devices on the network will use the same SNMP configuration, enter *default* for **Sub-Label** in the second entry. If the SNMP configuration is different, enter the active IP address of the device for **Sub-Label** in the second entry.

Enter the Session Manager SNMPv3 user profile created in **Section 5.1** as shown below 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 5.1**, e.g., *netiqDESSHA*.
- **Value 2:** Enter ***.
- **Value 3:** Enter the authentication protocol, authentication password, privacy protocol, and privacy password from **Section 5.1**, e.g., *sha,avaya123,des,avaya123*.

Create a similar entry with Session Manager IP address, e.g., *10.10.97.227*.

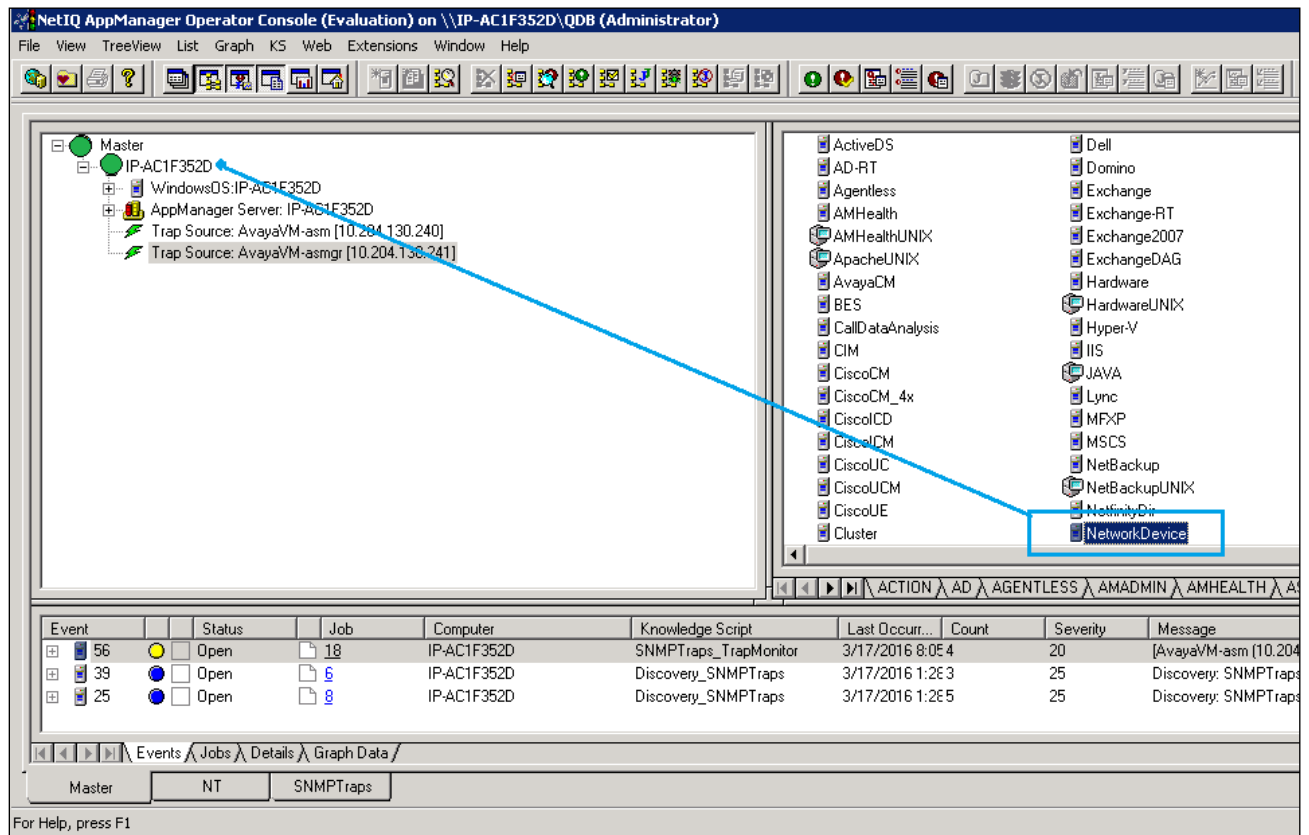
The image displays two identical 'Modify Custom Entry' dialog boxes side-by-side. Each dialog box contains the following fields and values:

- Label:** NetworkDevice
- Sub-Label:** 10.10.97.226 (left) / 10.10.97.227 (right)
- Value 1:** netiqDESSHA
- Value 2:** *
- Value 3:** sha,avaya123,des,avaya123

Below the fields is a checkbox labeled 'Extended application support (Click Help for details.)' which is unchecked. At the bottom of each dialog are three buttons: 'OK', 'Cancel', and 'Help'.

8.2.5. Discover the Devices

This section describes steps to let AppManager discover Session Manager and System Manager. On the right window of screenshot below, navigate to the **DISCOVERY** tab, select **NetworkDevice** script, drag and drop it on to AppManager server in the TreeView on the left panel to create the discovery job for Session Manager and System Manager devices.



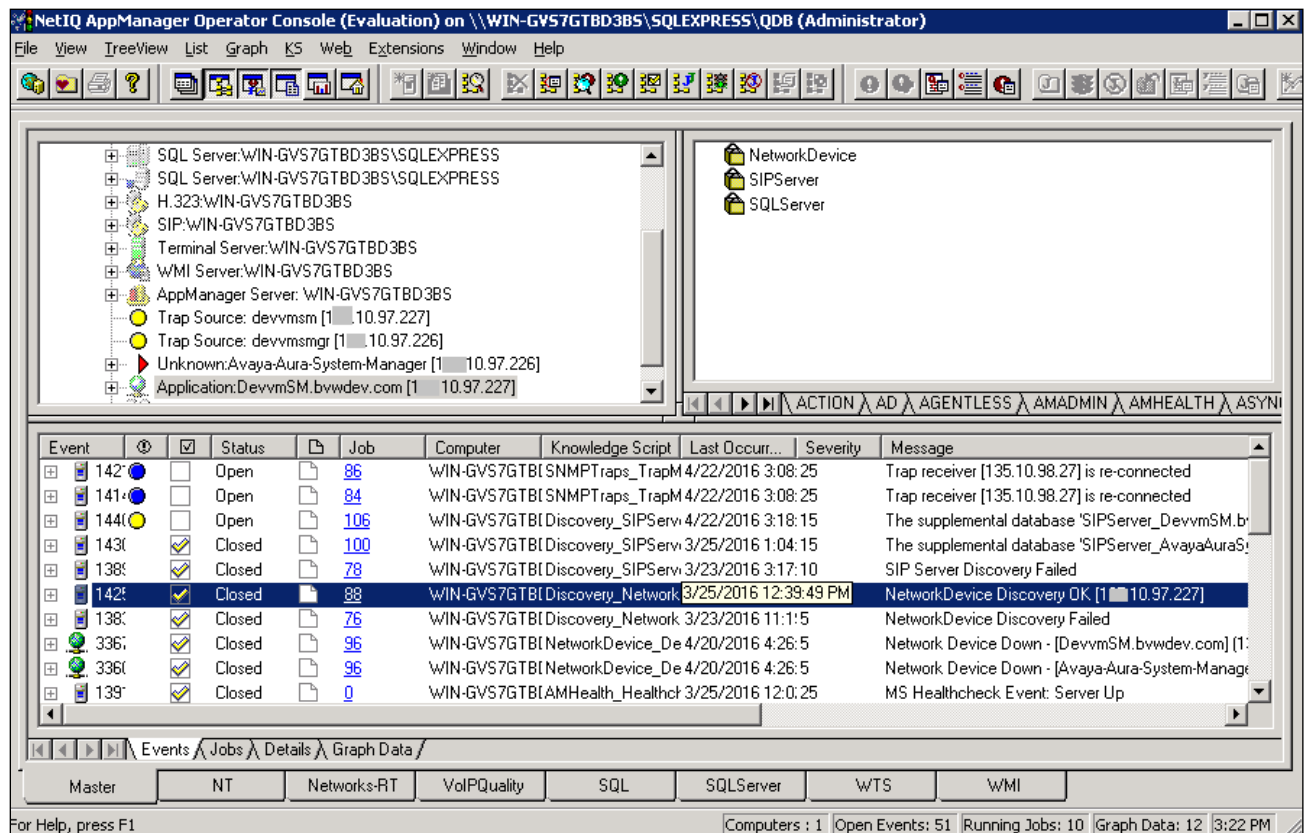
The **Properties for Discovery_NetworkDevice** window is displayed. Enter the IP address of the System Manager and Session Manager in **List of network devices (comma-separated)**, in this case *10.10.97.226,10.10.97.227*. Click **OK**.

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)	<input checked="" type="checkbox"/>	
Event severity when discovery succeeds	25	Severity
Event severity when discovery fails	5	Severity

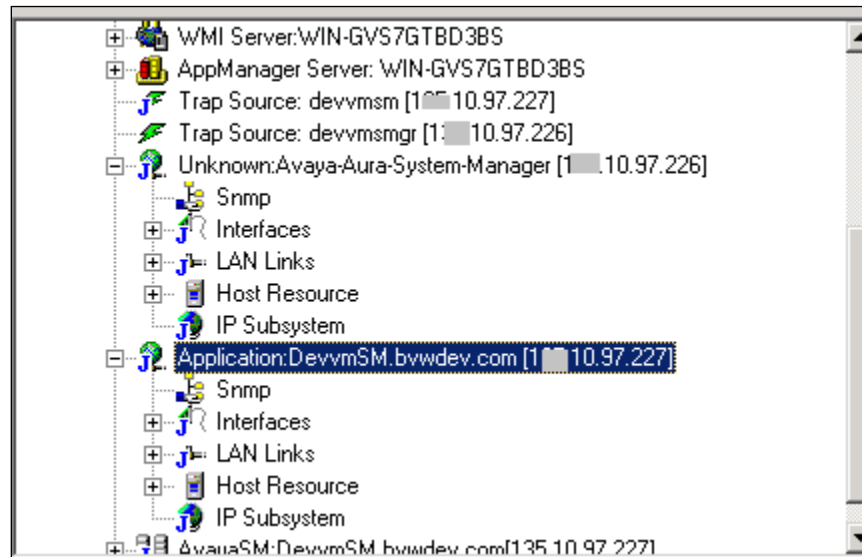
Discovers network devices: routers, switches, gateways, etc. You can specify a comma-separated list of network devices to discover, a range of IP addresses, a gateway router for auto-discovery, or the name of a file that contains device names on separate lines. Specify at least one remote computer. Because only one computer should act as a proxy for a given network device, drop this script on only one computer at a time. You must update Security Manager with SNMP version and security information (community string for SNMPv1/v2; user, context, authentication and encryption for SNMPv3) before you can discover network devices.

OK Cancel Help

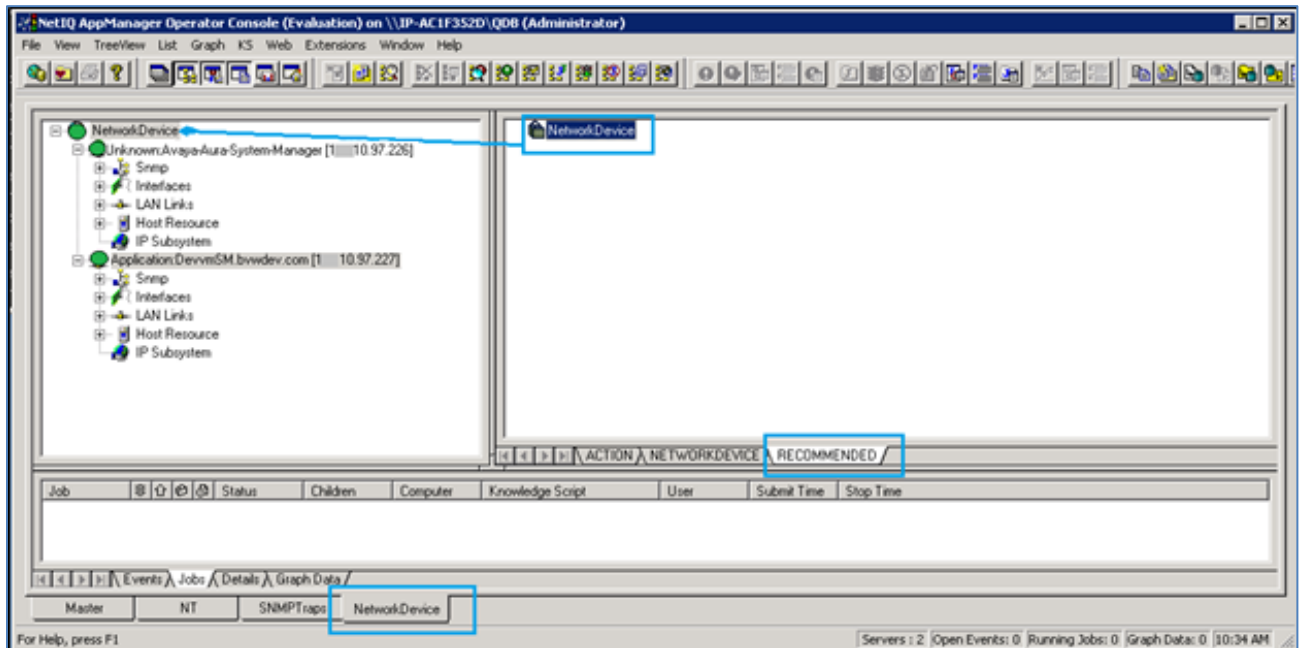
Discovery will create TreeView objects for System Manager and Session Manager as display in below screenshot: **Unknown:Avaya-Aura-System-Manager [10.10.97.226]** and **Application: DevvmSM.bvwdev.com[10.10.97.227]** and returned successful message for discovery job with **NetworkDevice Discovery OK**.



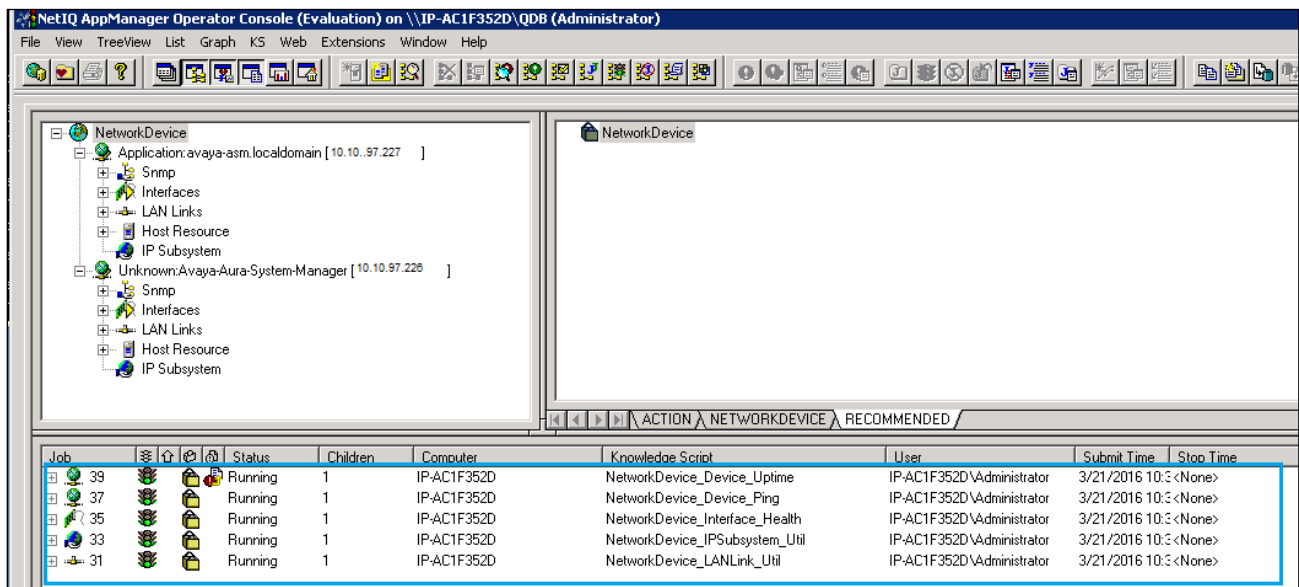
Click on the TreeView object to verify that device details are available for both Session Manager and System Manager as listed below such as **Snmp**, **Interfaces**, **LAN links**, **Host Resource** and **IP Subsystem**.



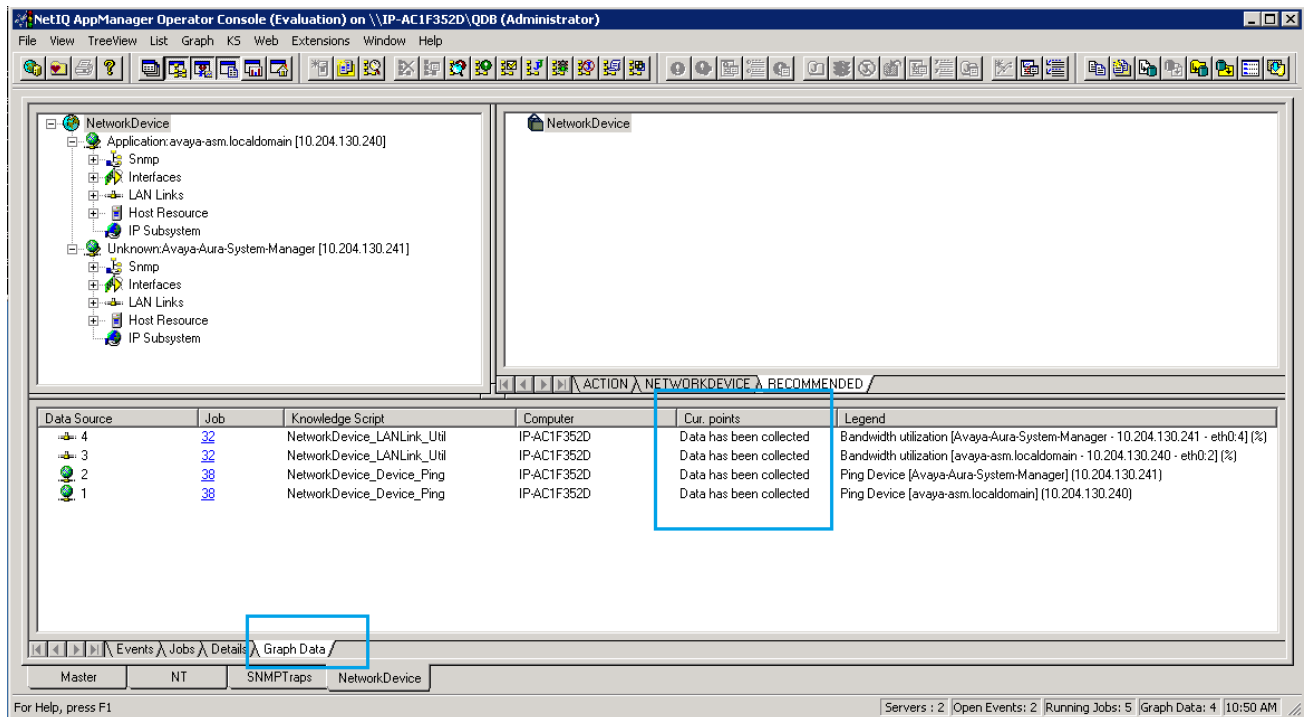
On the right panel, browse to **RECOMMENDED** tab, select **NetworkDevice** script, drag and drop it on NetworkDevice in the left panel to start monitoring each device for example Session Manager and System Manager as shown in below screenshot.



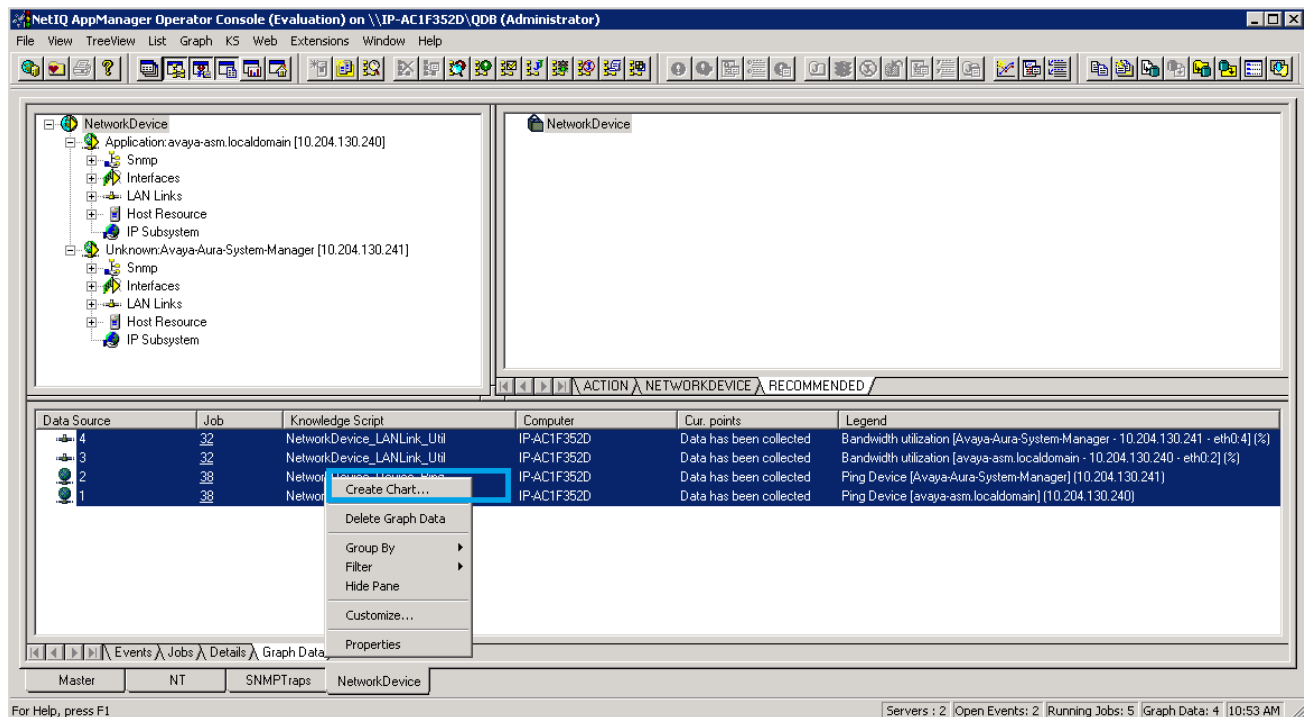
Confirm that the following device monitoring jobs have started: **NetworkDevice_Device_Uptime**, **NetworkDevice_Device_Ping**, **NetworkDevice_Interfaces_Health**, **NetworkDevice_IPSubsystem_Util** and **NetworkDevice_LANLink_Util** as shown below.



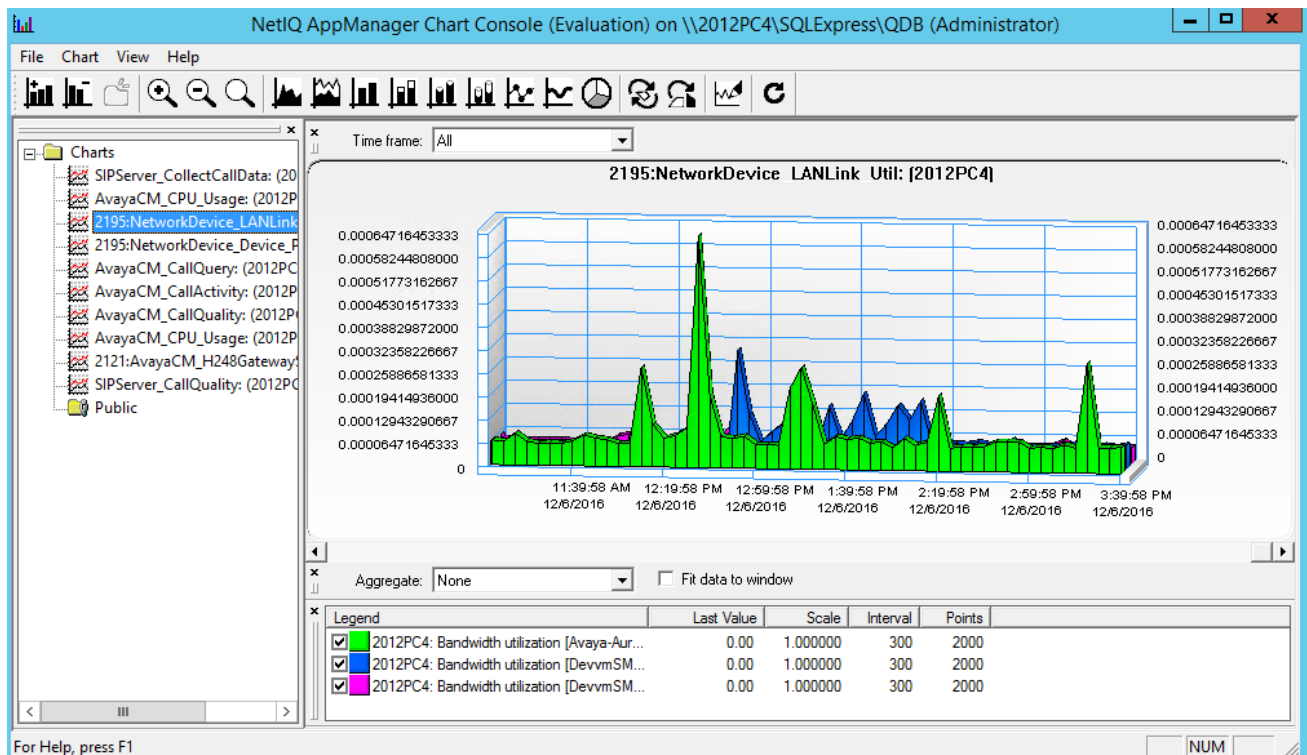
After a monitoring interval has been completed, data streams will be visible in the **Graph Data** pane as shown in below screenshot.



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



Following the instruction in popup window (not shown) to enter graph name, etc. Below is the **NetworkDevice_LANLink** data in graphic chart created during compliance test.

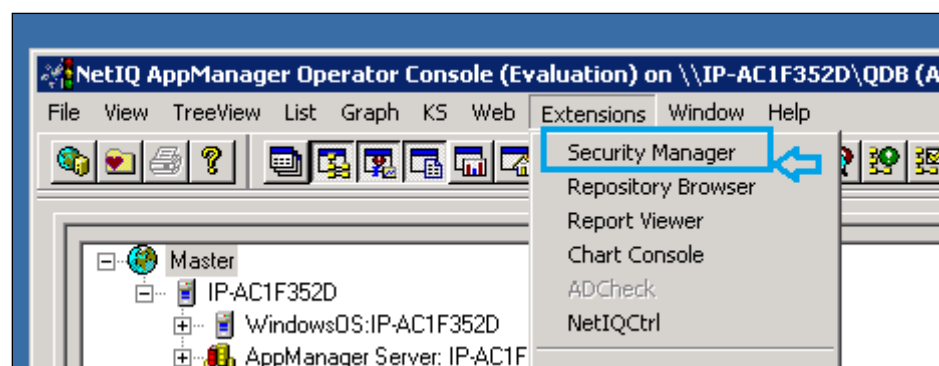


8.3. Administer SIP Call Quality Monitoring for 1100 Series IP Deskphones

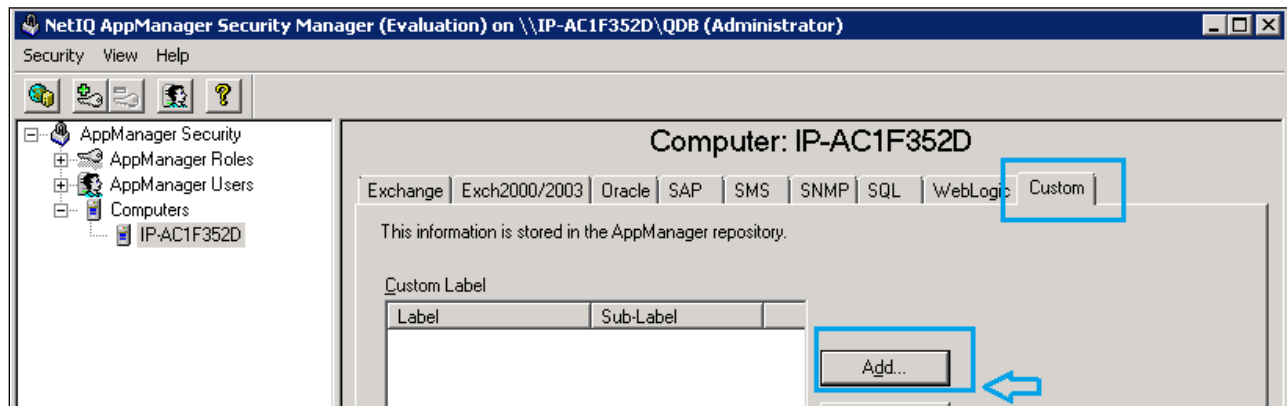
This section describes steps to configure AppManager to connect to Session Manager to collect call data for 1100 Series IP Deskphones. AppManager uses SNMPv3 to discover Session Manager using the user profile credentials previously created on Session Manager in **Section 5.1**, 1100 Series IP Deskphone send PVQMon data to Session Manager, AppManager connects to Session Manager via SIP trunk to collect voice quality of 1100 Series SIP IP Deskphones.

8.3.1. Administer Security Manager for SIP Server

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



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



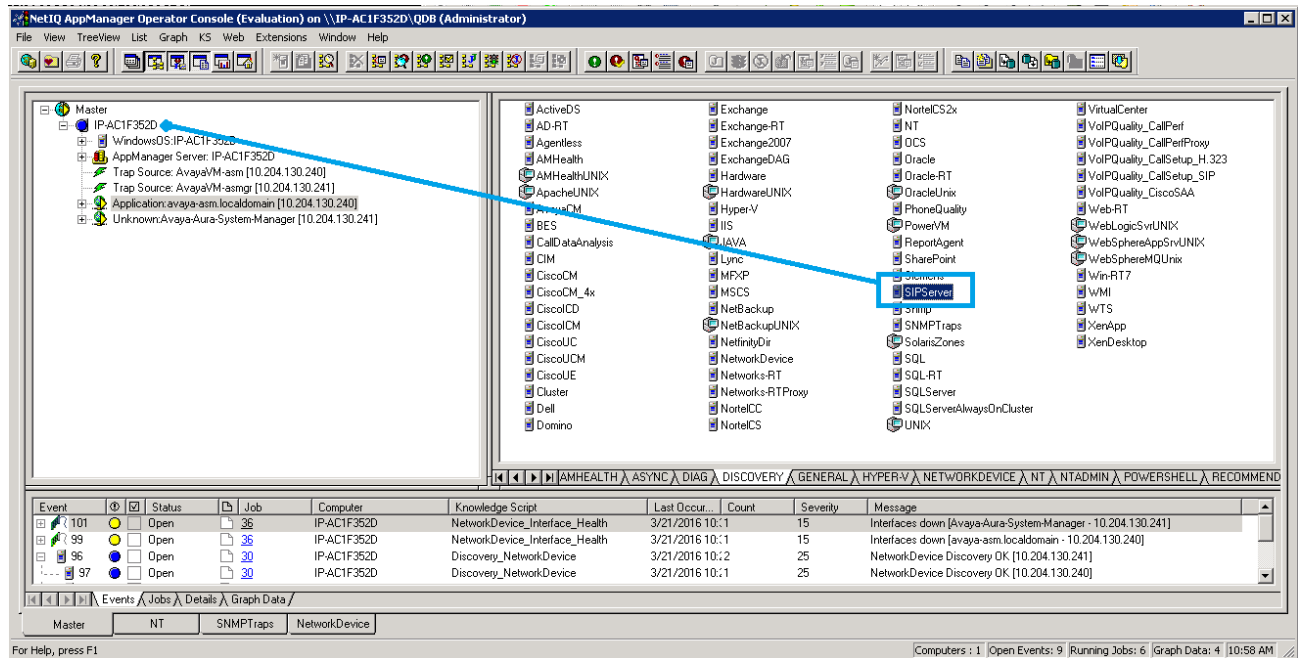
Enter the user profile information created in **Section 5.1** as shown below:

- **Label:** Enter any descriptive name, for example *SIPServer*.
- **Sub-Label:** Enter Session Manager IP address, for example, *10.10.97.227*.
- **Value 1:** Enter SNMP user name created in **Section 5.1**, e.g., *netiqDESSHA*.
- **Value 2:** Enter *.
- **Value 3:** Enter the authentication protocol, authentication password, privacy protocol, and privacy password from **Section 5.1**, for example: *sha,avaya123,des,avaya123*.

The 'Add Custom Entry' dialog box is shown. It has a title bar with a close button. The main text area contains instructions: '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.' Below this are five input fields: 'Label' with 'SIPServer', 'Sub-Label' with '10.10.97.227', 'Value 1' with 'netiqDESSHA', 'Value 2' with '*', and 'Value 3' with 'sha,avaya123,des,avaya123'. There is a checkbox labeled 'Extended application support (Click Help for details.)' which is currently unchecked. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

8.3.2. Discover Device

Navigate to the **DISCOVERY** tab in the bottom right pane, drag and drop **SIPServer** script on AppManager server in the left panel to enable discovery of Session Manager.



The **Properties for Discovery_SIPServer** window is displayed, enter the following as displayed below:

- **Raise event if discovery succeeds:** Check *Yes*.
- **Raise event if database setup succeeds:** Check *Yes*.
- **Comma-separated list of SIP servers:** Enter IP address of Session Manager, e.g., *10.10.97.227*.
- **Setup supplemental database:** Check *Yes*.
- **SIP identity of collector:** [sip:pvqmservice@localhost:5060;transport=UDP](#) with port and transport as created in **Section 5.4**.

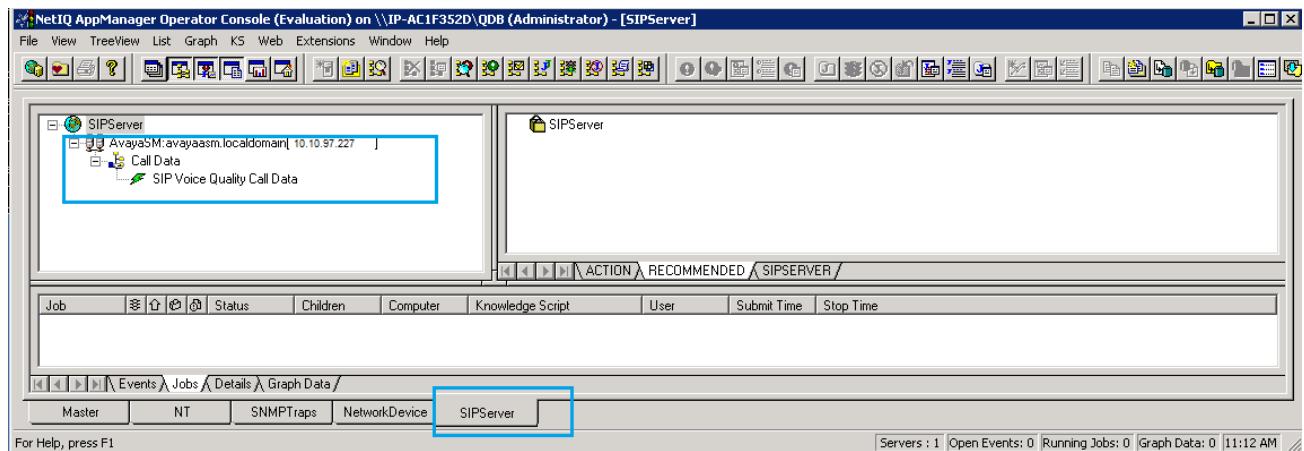
Click **OK** to submit this job.

Description	Value	Units
General Settings		
Job Failure Notification		
Raise event if discovery succeeds?	<input checked="" type="checkbox"/> Yes	
Raise event if discovery fails?	<input checked="" type="checkbox"/> Yes	
Raise event if database setup succeeds?	<input checked="" type="checkbox"/> Yes	
Raise event if database setup fails?	<input checked="" type="checkbox"/> Yes	
Discover SIP Servers		
Discovery method	SNMP Query	
SNMP Settings		
Comma-separated list of SIP servers	10.10.97.227	
Full path to file with list of SIP servers		
SNMP message timeout	120	Seconds
SNMP task timeout	3600	Seconds
SNMP retries	4	Attempts
System Properties for Manual Configuration		
Discover SIP Quality Of Service Reporting Interface?	<input checked="" type="checkbox"/> Yes	
SIP identity of collector (example sip:collector@localhost:5060;transport=UDP)	sip:pvqmservice@localhost:5060;transport=UDP	
Set up supplemental database?		
Start pruning job on supplemental database?	<input checked="" type="checkbox"/> Yes	
SQL Server Information		
SQL Server \ instance name (leave blank for default)		
SQL database user name (leave blank for windows)		

Discovers a SIP Server. Specify a list of SIP Server addresses or the full path to a file containing a list of servers. If the proxy agent is on the same computer as the Operator Console, you can use the file selector to browse for the file; otherwise enter the full path to the file. Before running this Knowledge Script, configure the proper security parameters in Security Manager. Click Help for instructions. The SNMP agent must be active on all the servers in the cluster.

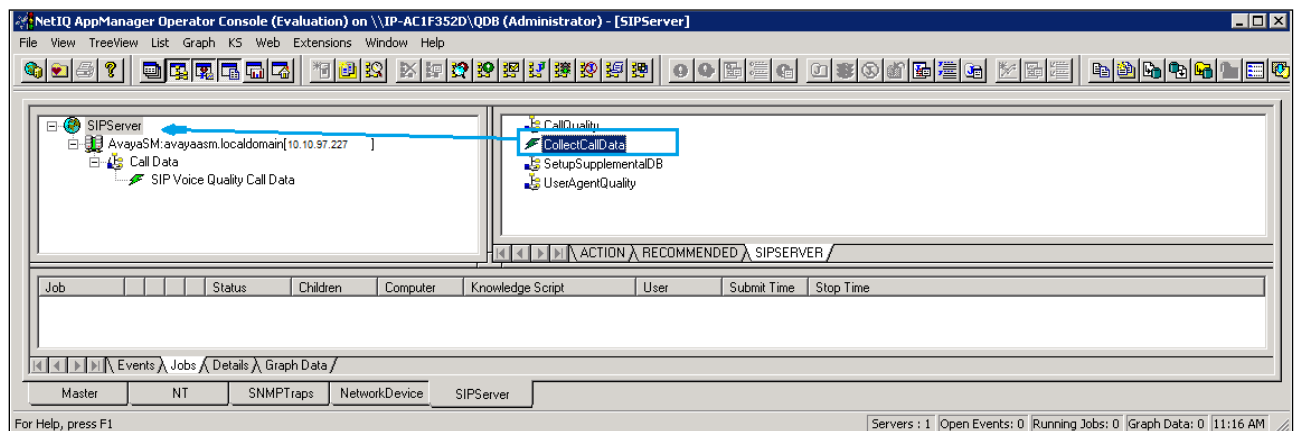
OK Cancel Help

Once the discovery job is completed, confirm that an object for Session Manager PVQMon call data monitoring is created as shown below in the **SIPServer** tab.

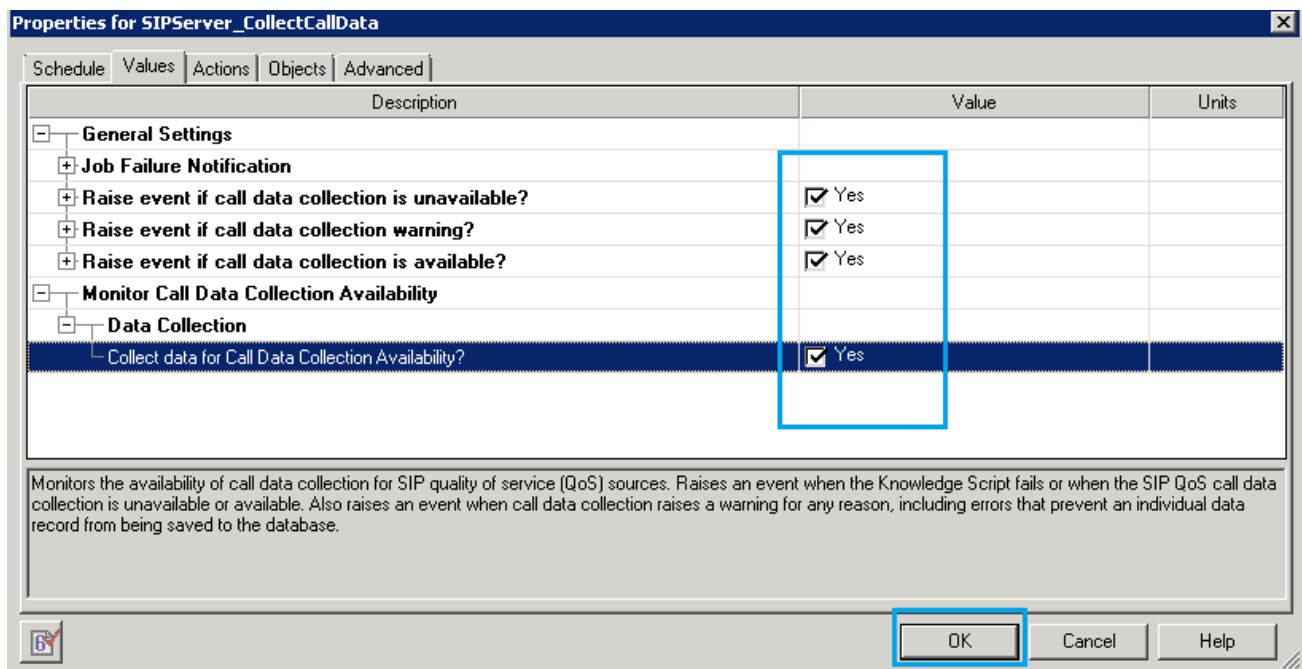


8.3.3. Collect Call Data

In **SIPServer** tab, start data collection by drag and drop the **CollectCallData** script on the Session Manager TreeView instance.

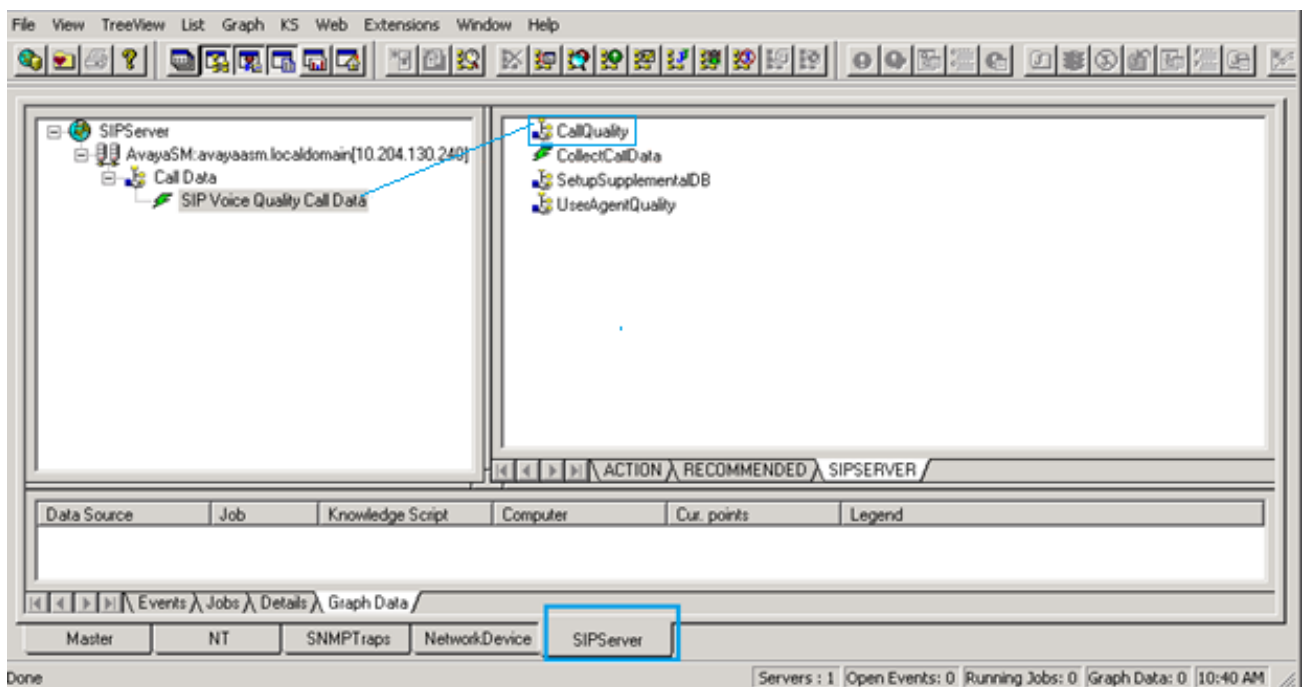


The **Properties for SIPServer_CollectCallData** window is displayed, verify all following options are checked as displayed in below screenshot.



8.3.4. Start Data Reporting Job

Use the **CallQuality** knowledge script to create a reporting job by select, drag and drop **CallQuality** script to the TreeView in the left panel.



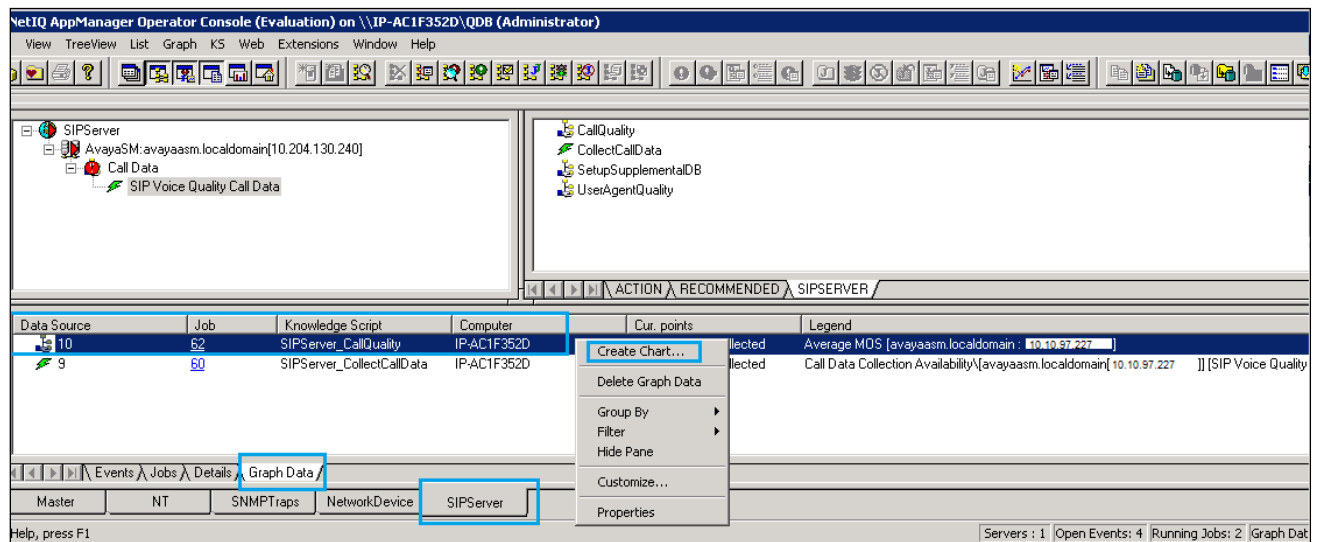
The **Properties for SIPServer_CallQuality** window is displayed, select **Monitor Average MOS** → **Event Notification** → **Raise event if average MOS falls below threshold** and set **Threshold – Average MOS** to a high value, this will ensure that all calls create events, for confirmation that data is collecting and reporting properly for testing purpose, leave all other fields at their default value as shown below.

Description	Value	Units
General Settings		
Job Failure Notification		
Raise event if no records found?	<input type="checkbox"/> Yes	
Call Details		
Include call details?	<input checked="" type="checkbox"/> Yes	
Query Filters		
Minimum duration	0	Seconds
Maximum table size	50	Rows
Maximum duration (0 to ignore)	0	Seconds
Calling Party		
Party connector	AND	
Called Party		
Troubleshooting		
Monitor Average MOS		
Event Notification		
Raise event if average MOS falls below threshold?	<input checked="" type="checkbox"/> Yes	
Threshold -- Average MOS	5.0	
Event severity when average MOS falls below threshold	5	Severity
Data Collection		
Collect data for average MOS?	<input checked="" type="checkbox"/> Yes	
Monitor Average R-Value		

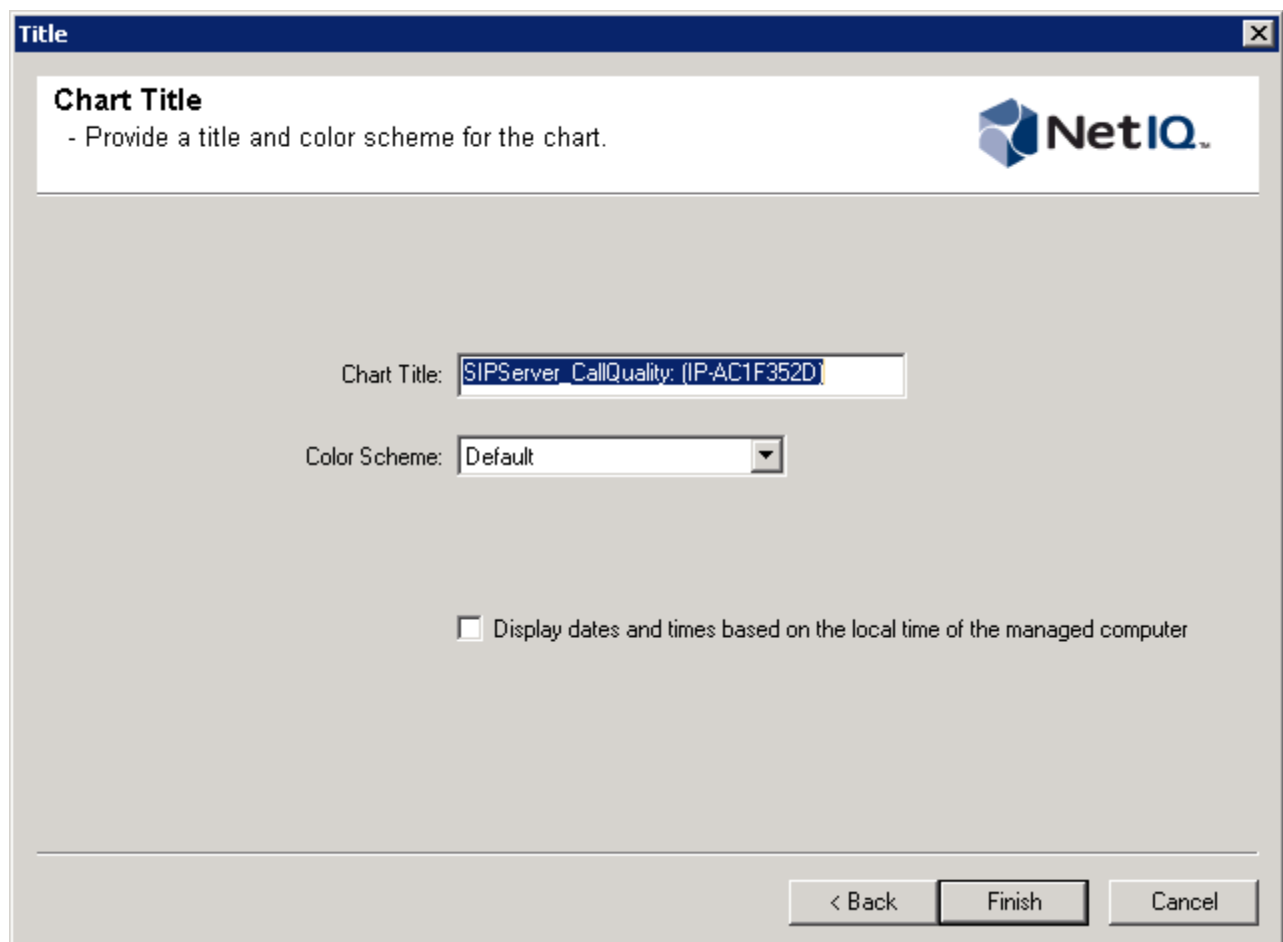
Monitors call quality metrics such as jitter, latency, lost data, R-value and MOS. Raises events when metrics fail to meet specified thresholds and generates data streams for all monitored metrics. By default, an action is configured that will trigger Vivinet Diagnostics to diagnose the VoIP quality problems detected from monitoring the calls.

OK Cancel Help

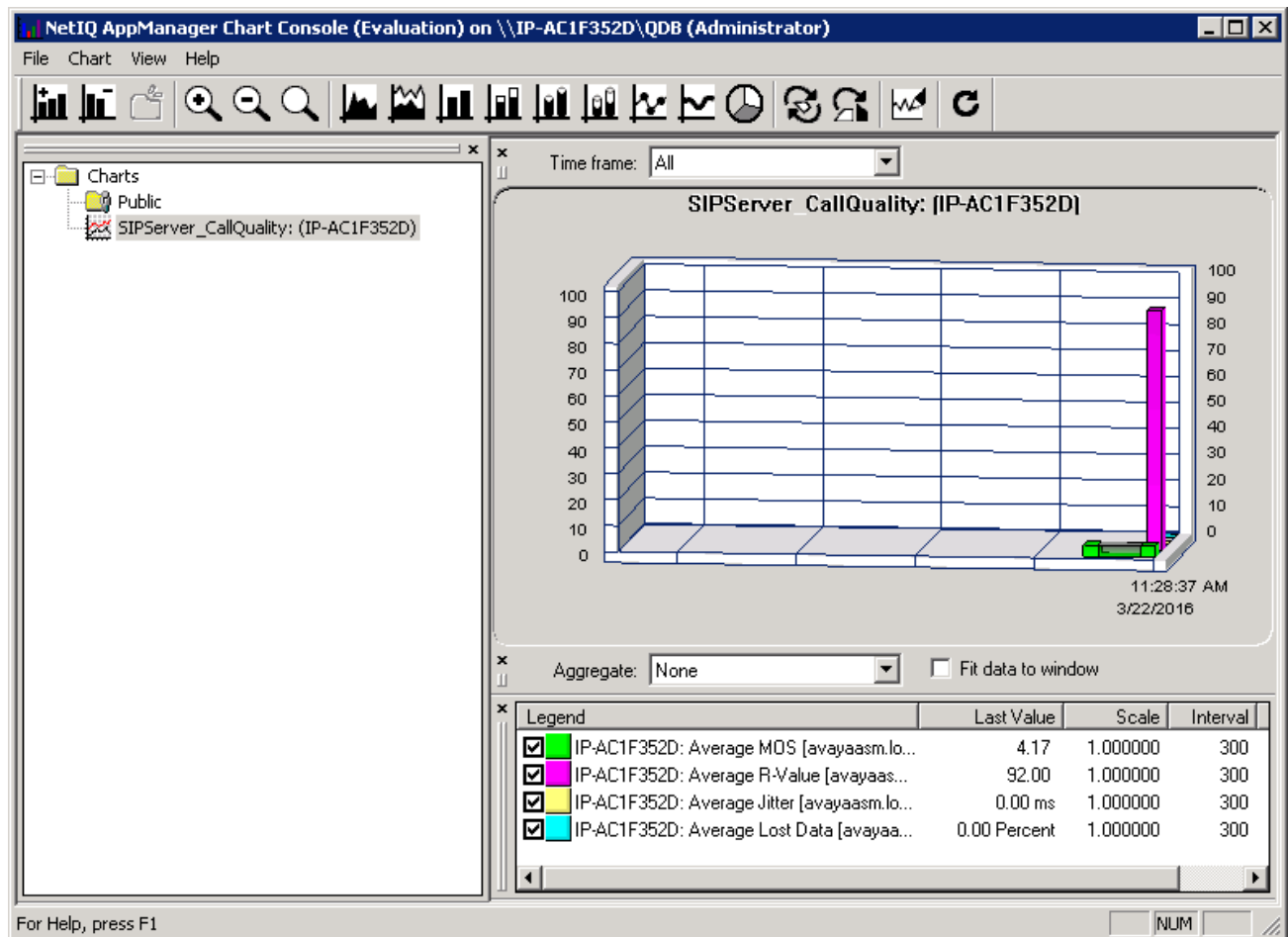
Make a call between two 1100 Series IP Deskphones. Use the chart console to confirm that data has been collected for the calls made as displayed in the following screenshots below. To create chart, right click on **SIPServer_CallQuality**.



On the job detail window, enter any descriptive name, example below is using default names:



Graph data below displays **MOS**, **R-Value**, **Jitter** and **Lost Data** in the chart. The default reporting interval is 5 minutes, so one may need to wait up to 5 minutes to see results posted to the chart.

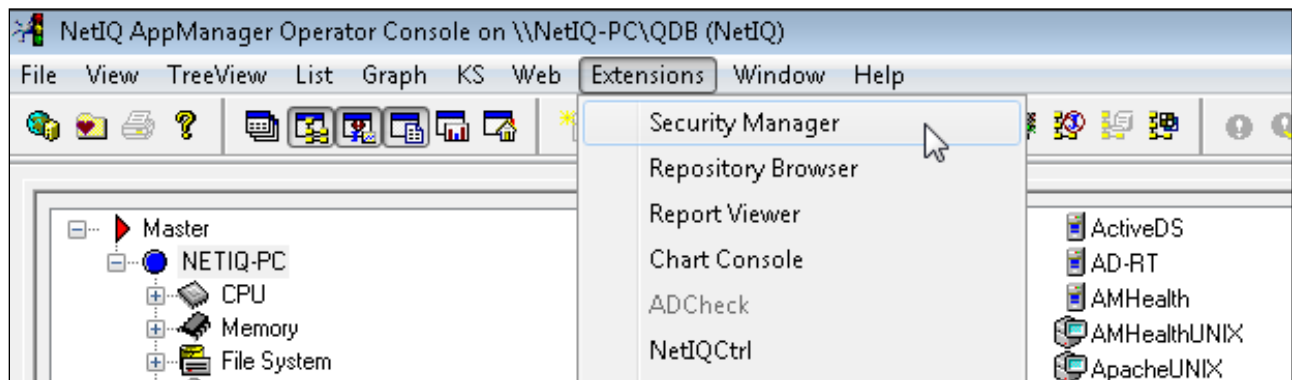


8.4. Configure AppManager to connect to Avaya Aura® Communication Manager

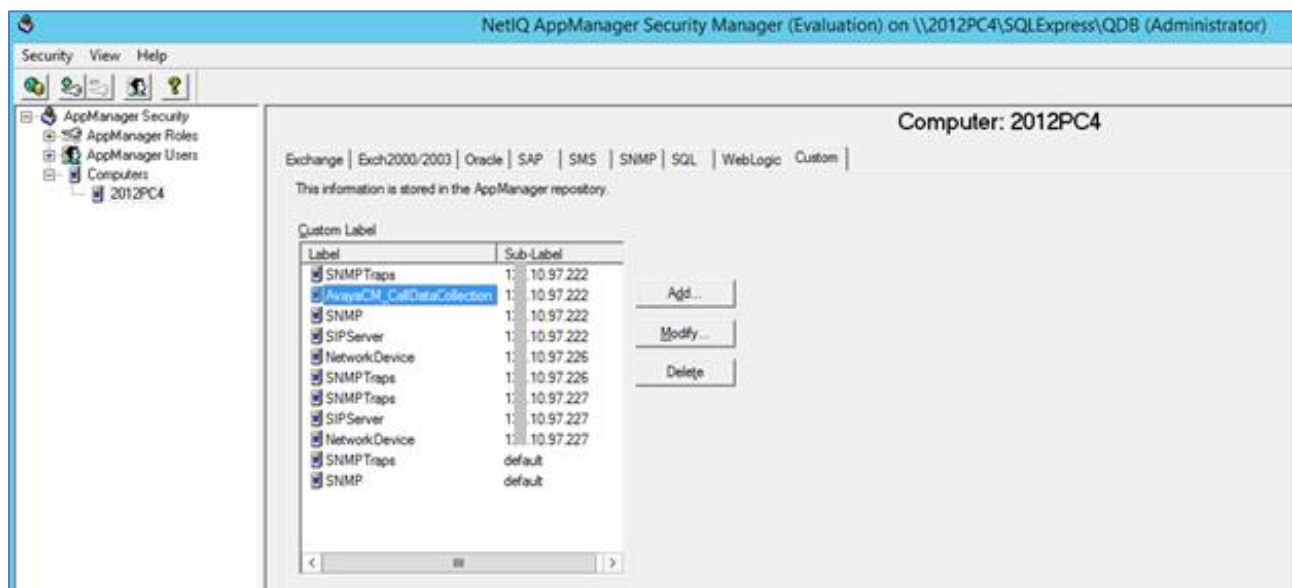
This section will describe steps to configure AppManager to connect to Communication Manager via SNMPv2 and collect CDR and RTCP data for 9600 Series IP Deskphones.

8.4.1. Administer custom Security profile for Communication Manager

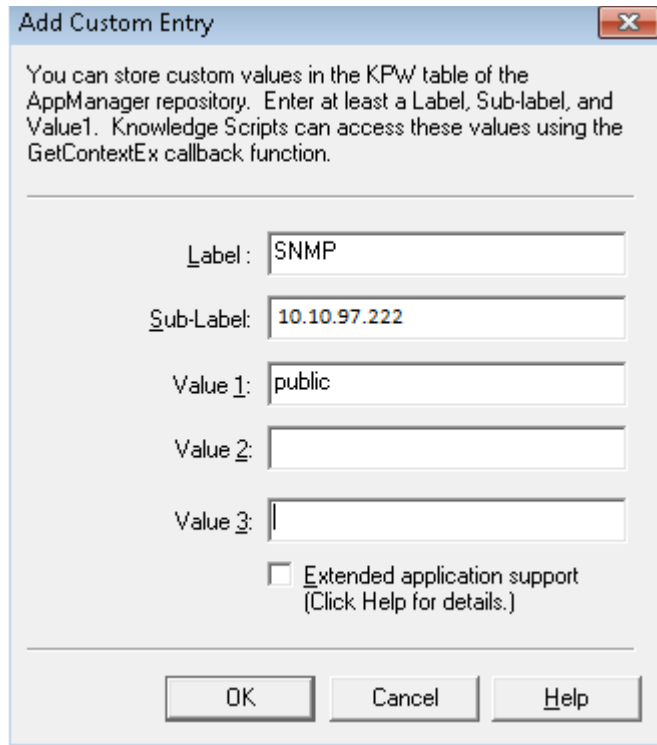
From the **NetIQ AppManager Operator Console** window, navigate to **Extensions → Security Manager** from the menu across the top of the window as shown below.



Click the **Custom** tab. The example below shows custom entries to communicate with Communication Manager (10.10.97.222) via SNMPv2. The **AvayaCM_CallDataCollection** entry covers CDR and RTCP. These entries were originally created by clicking the **Add** button and will be covered next.



Click on the **Add** button in the Security Manager window shown in the screen above to configure the SNMP connection parameters. The dialog box as shown below is displayed. Enter *SNMP* for the **Label** field. Enter the IP address of Communication Manager in the **Sub-Label** field. Enter the SNMP community string (read-write) configured in **Section 7.1** in the **Value 1** field. Click **OK**.



The image shows a Windows-style dialog box titled "Add Custom Entry". It contains a text area with instructions: "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." Below this are five input fields: "Label:" with the text "SNMP", "Sub-Label:" with the IP address "10.10.97.222", "Value 1:" with the text "public", "Value 2:" which is empty, and "Value 3:" which is empty. There is a checkbox labeled "Extended application support (Click Help for details.)" which is currently unchecked. At the bottom are three buttons: "OK", "Cancel", and "Help".

Similarly click on the **Add** button in the Security Manager window to configure the SNMP trap connection parameters (not shown). Enter *SNMPTrap* for the **Label** field. Enter the IP address of Communication Manager in the **Sub-Label** field. Enter the SNMP community string (read-write) configured in **Section 7.1** in the **Value 1** field. Click **OK**.

Click the **Add** button in the Security Manager window again to configure the CDR and RTCP connection parameters as displayed below:

- **Label:** Enter *AvayaCM_CallDataCollection*.
- **Sub-Label:** Enter the IP address of Communication Manager in the field, example *10.10.97.222*.
- **Value 1:** Enter the port number used for CDR data, for example *9000*. This must match the value configured on Communication Manager in **Section 7.4**.
- **Value 2:** Enter port number used for RTCP data, for example *5005* as configured on Communication Manager **Section 7.2** for H323 and **Section 7.3** for SIP phones.
- **Value 3:** Enter the RTCP report period in second, for example *5*. This value must match the value configured on Communication Manager in **Section 7.2** and **Section 7.3**.

Click **OK**.

Add 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.

Label:

Sub-Label:

Value 1:

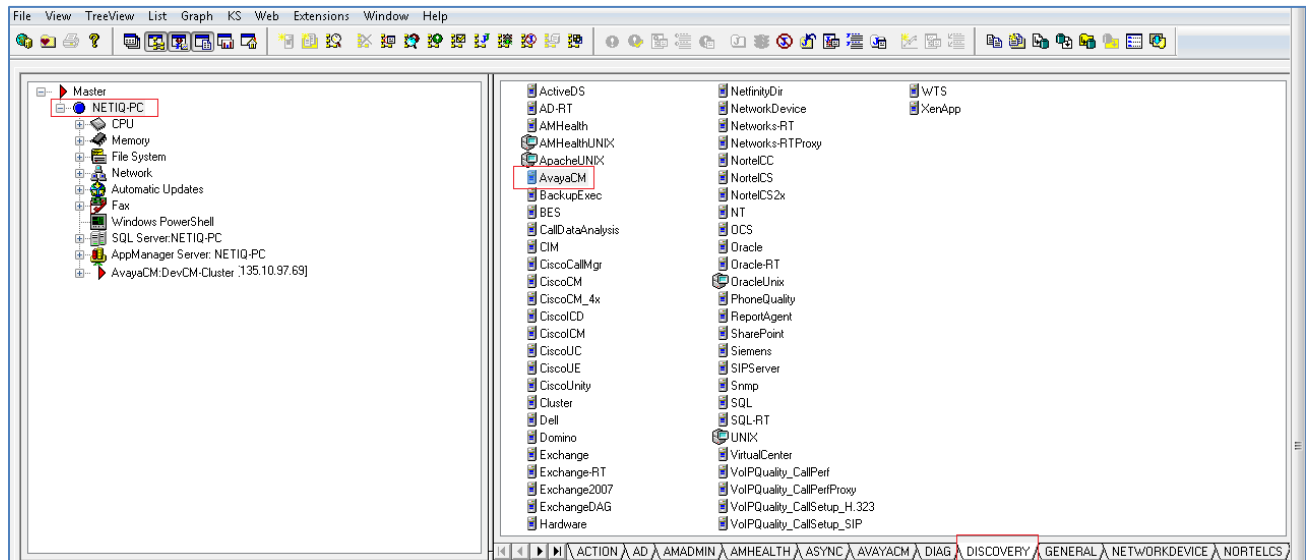
Value 2:

Value 3:

☐ Extended application support
(Click Help for details.)

8.4.2. Discover Avaya Aura® Communication Manager

Once the connection parameters have been defined as shown in **Section 8.4.1**, then the components of Communication Manager can be discovered using SNMP. To do this, select the **DISCOVERY** tab. Drag the **AvayaCM** script to the TreeView as displayed below.



The following pop-up window will appear. Enter the IP address of Communication Manager in the field labeled **Comma-separated list of active Communication Manager** . Enable **Discover Trap Receiver**. Optionally, the **Raise event if discovery succeeds** option may be enabled. Click **OK**.

This action will continue to fill out the TreeView with all the Communication Manager components in the main Operator Console window, except for the individual IP Deskphones.

Properties for Discovery_AvayaCM

Schedule Values Actions Objects Advanced

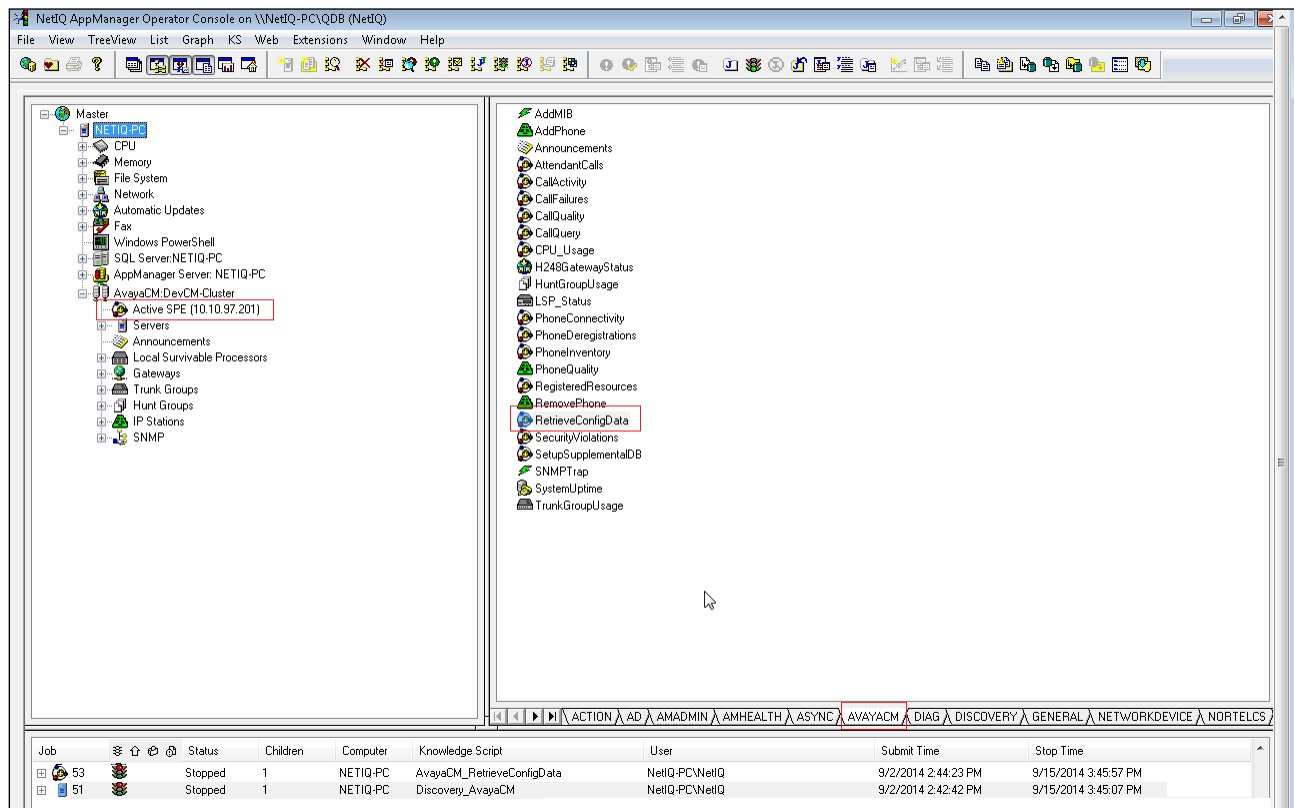
Description	Value	Units
General Settings		
+ Job Failure Notification		
+ Set up supplemental database?	<input checked="" type="checkbox"/> Yes	
- SNMP		
Global SNMP Message timeout	120	Seconds
Global SNMP Task timeout	3600	Seconds
Global SNMP retries	4	Attempts
- Enable use of SNMP GETBulk operations during discovery?	<input checked="" type="checkbox"/> Yes	
Number of rows to request for each GETBulk operation	10	Number
Interval to pause between GETBulk operations	100	Msec
+ Raise event if discovery succeeds?	<input checked="" type="checkbox"/> Yes	
+ Raise event if discovery fails?	<input checked="" type="checkbox"/> Yes	
- Discover Avaya Communication Manager servers		
Discovery timeout for all servers	30	Minutes
Maximum number of concurrent discoveries	10	Discoveries
Comma-separated list of active Communication Manager servers	10.10.97.222	
Comma-separated list of Communication Manager IP address pairs in a single NAT c		
Full path to file with list of active Communication Manager servers		
Add Avaya index to discovered names?	<input checked="" type="checkbox"/> Yes	
Resolve server names locally on agent?	<input type="checkbox"/> Yes	
Discover using manual configuration?	<input type="checkbox"/> Yes	
+ Discover Trap Receiver?	<input type="checkbox"/> Yes	

Discovers an Avaya Communication Manager cluster. Specify a list of active Communication Managers or the full path to a file containing a list of servers. If the proxy agent is on the same computer as the Operator Console, you can use the file selector to browse for the file, otherwise enter the full path to the file. Before running this Knowledge Script, configure the proper security parameters in Security Manager. Click Help for instructions. The SNMP agent must be active on all the servers in the cluster.

6 OK Cancel Help

8.4.3. Retrieve Configuration Data

Even though the TreeView is now populated with the Communication Manager components, additional detailed information must be retrieved using SNMP and stored in the supplemental database. To do this, select the **AVAYACM** tab and drag the **RetrieveConfigData** script to the **Active SPE** in the left pane.



The following pop-up window appears. Retain the default values. Optionally, the **Raise event if configuration retrieval succeeds** option may be enabled. Click **OK**.

Properties for AvayaCM_RetrieveConfigData

Schedule Values Actions Objects Advanced

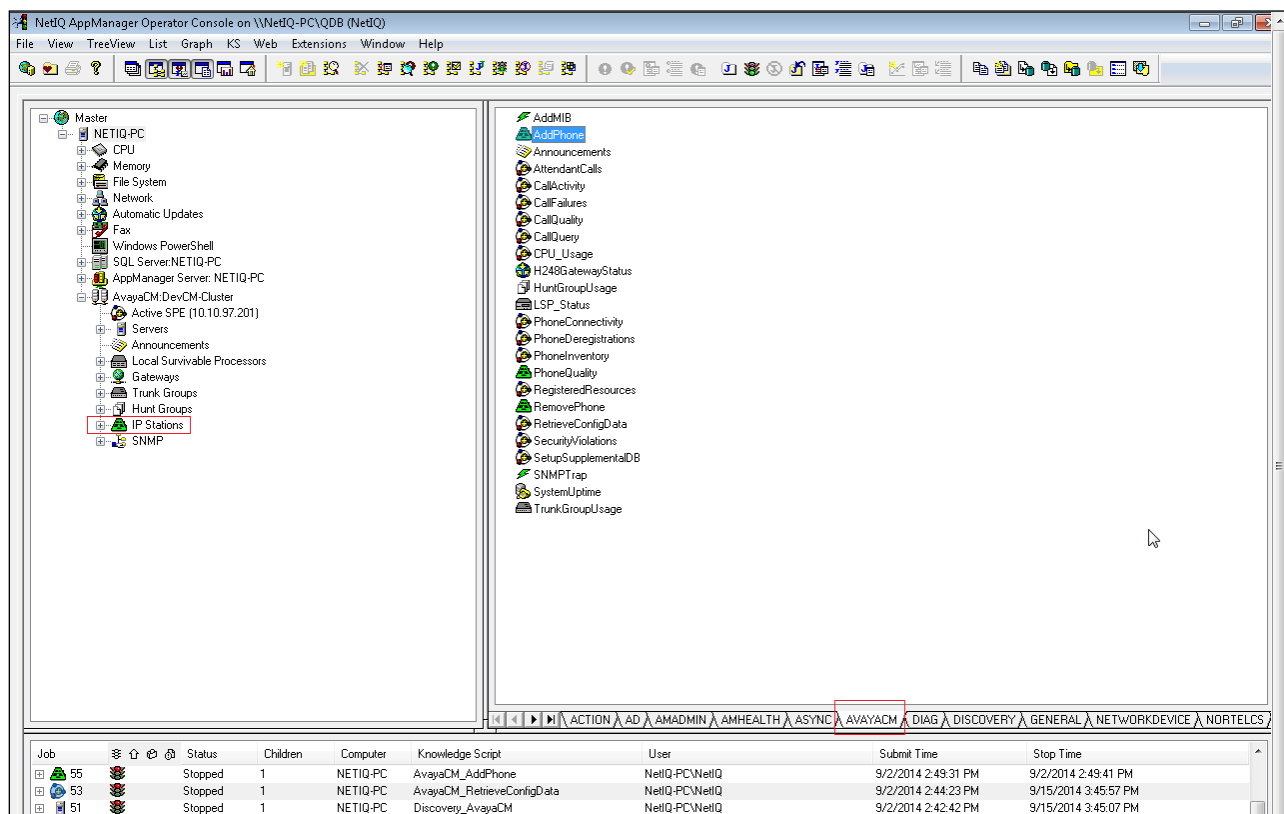
Description	Value	Units
General Settings		
Job Failure Notification		
Enable use of SNMP GETBulk operations?	<input checked="" type="checkbox"/> Yes	
Number of rows to request for each GETBulk operation	10	Number
Interval to pause between GETBulk operations	100	Msec
Raise event if configuration retrieval succeeds?	<input checked="" type="checkbox"/> Yes	

Retrieves Communication Manager configuration data about stations and gateways and stores it in the Avaya CM supplemental database for use by the PhoneQuality, CallQuality, CallFailures, PhoneConnectivity, and PhoneDeregistrations scripts. Before running this script, run the SetupSupplementalDB script to create the supplemental database for the cluster.

OK Cancel Help

8.4.4. Add Avaya 9600 Series IP Deskphones

Lastly, in order to run a script (specifically the *PhoneQuality* script) for an individual 9600 Series IP station on Communication Manager, that station extension must be entered in the TreeView. To add station extension to the TreeView, select the **AVAYACM** tab and drag the **AddPhone** script to **IP Stations** in the left pane. The pop-up window as seen in the next screen will appear.




Enter the relevant station extensions in the **List of phone extensions** field as shown below. Optionally, the **Raise event if all phones are added successfully** option may be enabled. Click **OK**. This action will fill out the TreeView with the individual extensions shown in the TreeView as seen in the next screen. Sample AppManager phone quality reports are shown in **Section 9.3.4**.

Properties for AvayaCM_AddPhone X

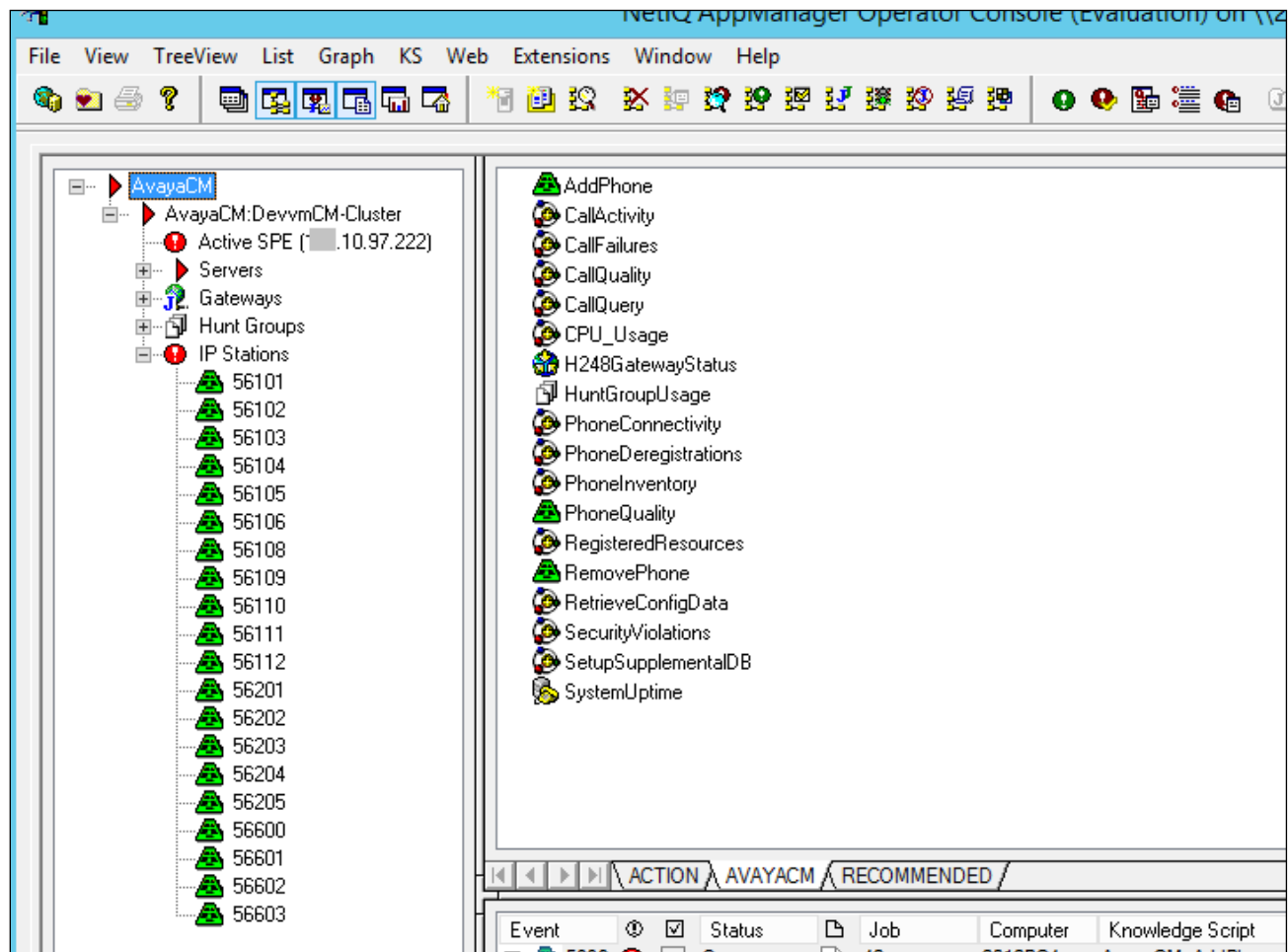
Schedule Values Actions Objects Advanced

Description	Value	Units
General Settings		
+ Job Failure Notification		
Retrieve SNMP configuration data for these phones?	<input checked="" type="checkbox"/> Yes	
- Configuration Settings		
List of phone extensions	56100-56199,56200-56299,56300-56399,56600-56699	
Full path to file with list of phone extensions		
- Event Notification		
+ Raise event if all phones are added successfully?	<input checked="" type="checkbox"/> Yes	
+ Raise event if configuration retrieval succeeds?	<input checked="" type="checkbox"/> Yes	

Adds Avaya IP phones as objects for monitoring with the PhoneQuality Knowledge Script. Raises events if phones are added successfully or cannot be added.

 OK Cancel Help

After adding the IP station extensions using the procedure above, the extensions are then displayed under **IP Stations** in the TreeView as shown below. During the compliance testing these were the same extensions that were monitored as mentioned in **Section 7**.



9. Verification Steps

This section provides the tests that can be performed to verify the configuration of Communication Manager, Session Manager, System Manager, 1100 Series IP Deskphone, 9600 Series IP Deskphone, and AppManager.

9.1. Verify SNMPv3 Connections with Avaya Aura® Session Manager and Avaya Aura® System Manager

The following tests were conducted to verify the AppManager ability to discover and receive traps from Session Manager and System Manager. From the **Serviceability Agents** screen shown in **Section 5.3**, generate a test trap by selecting system entries to send trap, in this case they are Session Manager and System Manager, then click on **Generate Test Alarm** as shown below.

AVAYA
Aura® System Manager 7.0

Last Logged on at April 21, 2016

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

Serviceability Agents

Agent List

Activate Manage Profiles Generate Test Alarm Repair Serviceability Agent

2 Items Show All Click here to generate Test Alarm Filter: Enable

	Hostname	IP Address	System Name	System OID	Status
<input checked="" type="checkbox"/>	devvsmgr.bvwdev.com	10.97.226	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
<input checked="" type="checkbox"/>	DevvmSM.bvwdev.com	10.97.227	DevvmSM		active

Select : All, None

The test trap and any subsequent traps received will be reported in the AppManager console as events in the bottom pane below.

NetIQ AppManager Operator Console (Evaluation) on \\2012PC4\\SQLExpress\\QDB (Administrator)

File View TreeView List Graph KS Web Extensions Window Help

SNMPTraps

- Trap Source: DevSM [10.97.227]
- Trap Source: DevSMGR [10.97.226]

Diagnose DiagnoseNortelIPT DiagnoseVolPQQuality DominoCommand DosCommand DumpTran ExtendedSNMPTrap IISContinueSite IISPauseSite IISRestartServer IISRestartSite MapMail Messenger NotesMail NTEventLog RunPowerShell RunSql SendReportToPrinter SMTPMail SMTPMailRpt SnmptTrap StartServices StopServices Traceroute TracerouteNetworks-RT UpdateEventStatus UxCommand WriteMsgToFile

Event	Status	Job	Computer	Knowledge Script	Last Occurrence	Count	Severity	Message
1735	Open		2012PC4	SNMPTraps_TrapMonitor	12/6/2016 12:33:58 PM	395	15	[DevSM (10.97.227)]: Trap AV-AURA-SESSION-MANAGER-THIRDPARTY-MIB:av
1537	Open		2012PC4	SNMPTraps_TrapMonitor	12/6/2016 10:49:20 AM	108	10	[DevSMGR (10.97.226)]: Remote backups are not taken for specified number of day

Master NT SQL VoIPQuality SQLServer WMI WTS AMHealth AvayaCM SNMPTraps NetworkDevice SIPServer

9.2. Verify SIP Trunk Connection with Session Manager and PVQMon from 1100 Series IP Deskphones

This section will describe step to verify that AppManager is successfully connected to Session Manager and able to collect 1100 Series IP Deskphone PVQMon call quality data via SIP Publish message from Session Manager.

Confirm that the SIP trunk to AppManager by navigating to the **Session Manager → System Status → SIP Entity Monitoring** screen. Verify this trunk is in-service (**Conn Status** is *UP*) whenever the CollectCallData job created in **Section 8.3.3** is running on the AppManager server.

AVAYA
Aura® System Manager 7.0

Configurations

Go...

Home Session Manager

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Help ?

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: **AppManagerAgent**

Status Details for the selected Session Manager:

Summary View

1 Items Refresh Filter: Enable

Session Manager Nan	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> DevvmSM	10.10.98.28	5060	UDP	TRUE	UP	200 OK	DENY

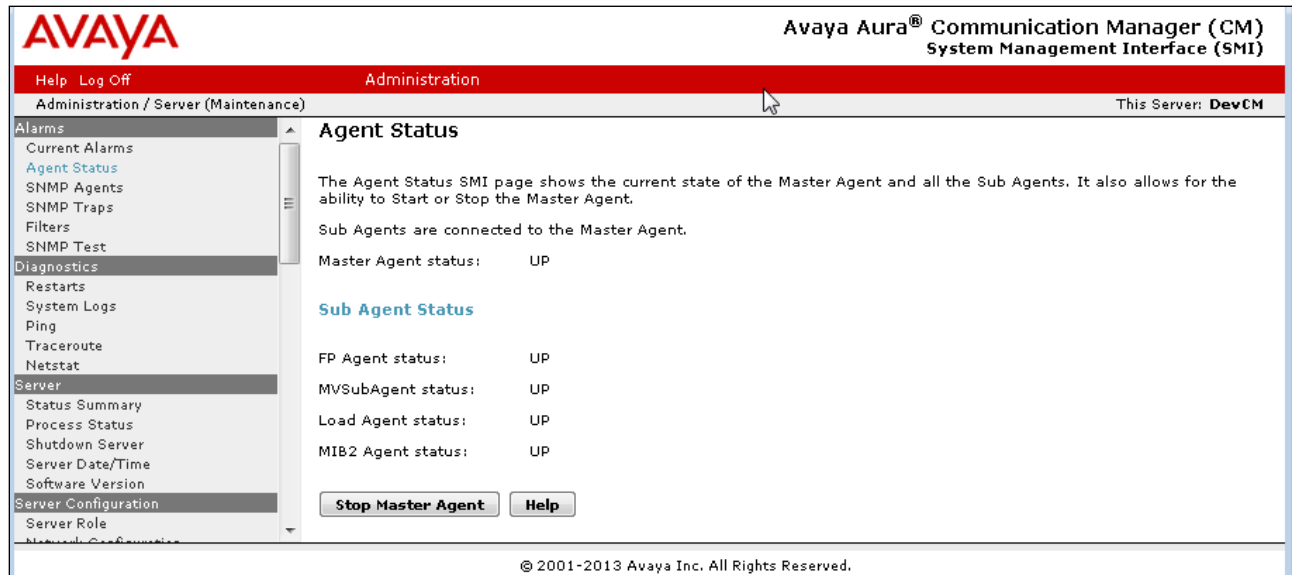
Verify AppManager can collect device information for Session Manager and System Manager, see **Section 8.2.5** for sample screenshot of collected data.

Make a phone call and verify AppManager reports call quality shown in the graph in **Section 8.3.4**.

9.3. Verify Connections with Avaya Aura® Communication Manager

9.3.1. Verify SNMPv2 Connection on Communication Manager

This section describes step to verify the SNMPv2 connection with Communication Manager. From the Communication Manager web interface, click on **Agent Status** on the left pane to verify that the **Master Agent Status** is up as shown in the screen below.



9.3.2. Verify SNMPv2 Connection on AppManager

The following steps may be used to verify the configuration of AppManager. This section covers running various Knowledge Scripts to verify that data can be collected on AppManager. Note that running a script causes a job to be created in AppManager.

To capture SNMP traps, drag *SNMPTrap* script into the **SNMP** item in the TreeView (not shown). SNMP traps will be displayed in the **Events** tab of AppManager. To view a detailed message of the SNMP trap, right-mouse click on the SNMP trap and then select **Detailed Message** from the pop-up menu (not shown). Below is a sample SNMP detailed message.

Event Properties: 1345

Event Message Comments

Trap G3-AVAYA-TRAP::alarmResolved received on 9/7 3:28:05 PM

From	Device Uptime	Trap OID
10.10.97.201	0:01:04.15	G3-AVAYA-TRAP::alarmResolved [1.3.6.1.4.1.6889.1.8.1.0.12]

Trap details

Name	Value
CM Hostname	DevCM
Maintenance Object	SVC_MON
Generation Time	N/A
Resolution Time	09/07/2016 @ 15:27:37
New/Modified alarm	New
Derived G3 Alarm Port	service crond was successfully restarted.

Varbinds

OID	Type	Value
G3-AVAYA-MIB::g3clientExternalName [1.3.6.1.4.1.6889.2.8.2.1.1.4]	STRING	DevCM
G3-AVAYA-MIB::g3alarmsProductID [1.3.6.1.4.1.6889.2.8.1.4.6.1.18]	STRING	1000000000
G3-AVAYA-MIB::g3alarmsAlarmNumber [1.3.6.1.4.1.6889.2.8.1.4.6.1.17]	STRING	FPA:00000:0000000000:0907152737::N
G3-AVAYA-MIB::g3alarmsPort [1.3.6.1.4.1.6889.2.8.1.4.6.1.1]	STRING	A:\service crond was successfully restarted.\
G3-AVAYA-MIB::g3alarmsMaintName [1.3.6.1.4.1.6889.2.8.1.4.6.1.3]	STRING	SVC_MON
G3-AVAYA-MIB::g3alarmsOnBrd [1.3.6.1.4.1.6889.2.8.1.4.6.1.4]	STRING	3
G3-AVAYA-MIB::g3alarmsAlarmType [1.3.6.1.4.1.6889.2.8.1.4.6.1.6]		
G3-AVAYA-MIB::g3alarmsIPAddress [1.3.6.1.4.1.6889.2.8.1.4.6.1.26]	STRING	10.10.97.201
G3-AVAYA-MIB::g3alarmsCategory [1.3.6.1.4.1.6889.2.8.1.4.6.1.27]		

To retrieve an inventory of all stations on Communication Manager, drag the *PhoneInventory* script to the **Active SPE** item in the TreeView (not shown). This script generates a data file with the retrieved phone inventory as shown below.

```
=====
Active SPE,Select By,Criteria,Status Filter,Start Time
-----,-----,-----,-----
DevvmCM,Extension,,Any,2016-11-11 15:15:50
=====
|
Extension,StationType,Name,Building,Floor,Room,Status,Status Time
-----,-----,-----,-----,-----,-----,-----
"56101","9608","StationNameOneOOne","Unknown","Unknown","Unknown","Re
gistered","2016-11-11 15:15:50"
"56102","9641","OneOTwo","Unknown","AA1-
F1","1","Registered","2016-11-11 15:15:50"
"56103","9611","OneOThree","Unknown","Unknown","Unknown","Registered"
,"2016-11-11 15:15:50"
"56104","9611","OneOFour","Unknown","Unknown","Unknown","Registered",
"2016-11-11 15:15:50"
"56105","9611","StatioNameOneOFive","Unknown","Unknown","Unknown","Re
gistered","2016-11-11 15:15:50"
"56106","1608","OneSix","Unknown","Unknown","Unknown","Registered","2
016-11-11 15:15:50"
"56108","4620","Calibre Recorder
56108","Unknown","Unknown","Unknown","Registered","2016-11-11
15:15:50"
"56109","4620","Cablibre Recorder
56109","Unknown","Unknown","Unknown","UnRegistered","2016-11-11
15:15:50"
"56110","4620","Calibre Recorder
56110","Unknown","Unknown","Unknown","Registered","2016-11-11
15:15:50"
"56111","4620","Calibre
```

9.3.3. Verify CDR Connection

AppManager collects CDR data from Communication Manager. From the SAT, use the **status cdr-link** command to verify that the CDR primary link to AppManager is up as configured in **Section 7.4**.

status cdr-link		
CDR LINK STATUS		
Primary		Secondary
Link State: up		up
Date & Time: 2017/02/28 15:13:55		2017/02/28 15:14:03
Forward Seq. No: 0		111
Backward Seq. No: 0		0
CDR Buffer % Full: 0.00		0.00
Reason Code: OK		OK

Note: CDR link from Communication Manager to AppManager will only appear "up" if one or more call data Knowledge Scripts is running (CallActivity, CallQuality, CallFailures, CallQuery, PhoneQuality).

Once the AppManager configuration is complete as detailed in **Section 8.4**, scripts can be run against the various components in the TreeView. For example, to run the *CallQuery* script, which queries call detail records retrieved from Communication Manager and stored in the supplemental database, select the **AVAYACM** tab and drag the *CallQuery* script to the **Active SPE** in the TreeView (not shown). A pop-up window appears (not shown) that allows parameters of the script to be modified, such as the date/time range. An example of the script output is shown below, which displayed calls that matched the criteria specified in the script parameters pop-up window.

Event Properties: 1489

Event

Message

Comments

CallQuery: Results

The number of calls found (4) exceeds the threshold (0).

CallQuery: Summary

Number of records matching the query

4

Starting disconnect time

9/19/2016 3:12:00 PM

Ending disconnect time

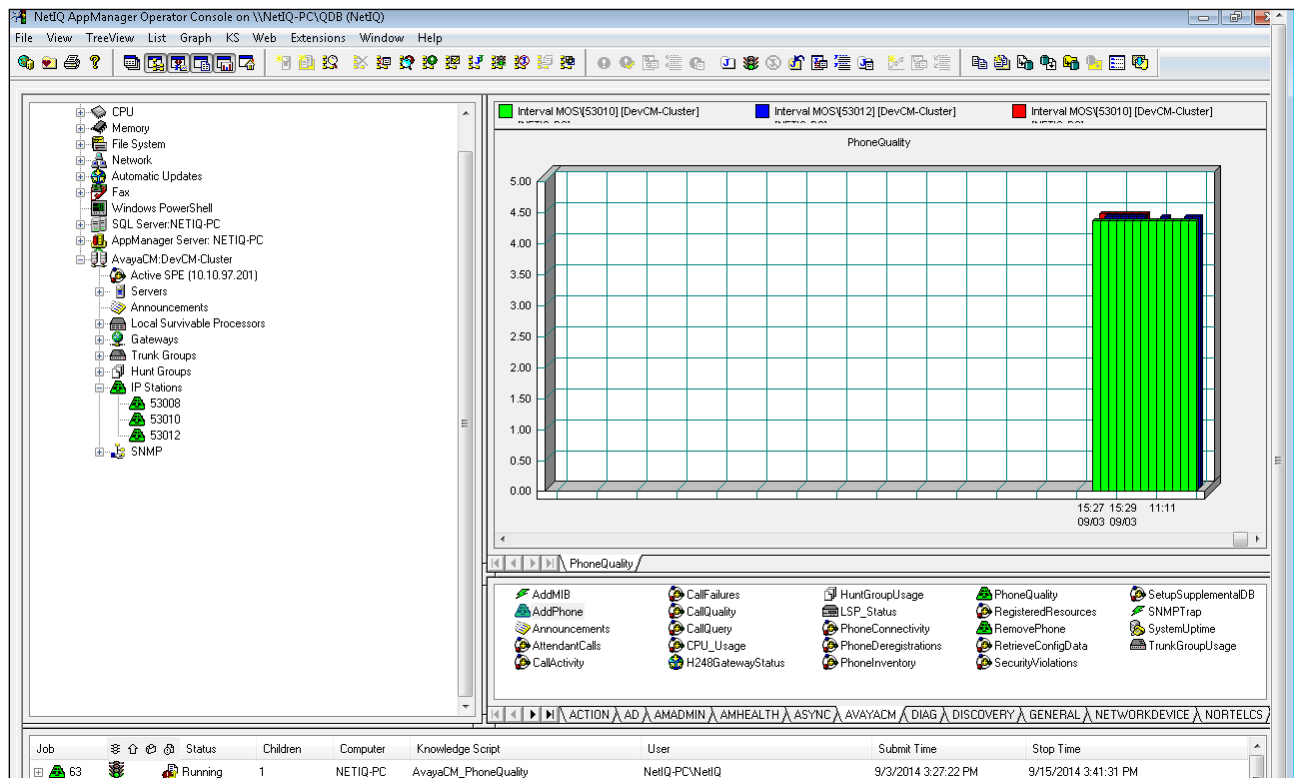
9/19/2016 3:13:00 PM

CallQuery: Details for the first 4 records.

	Condition Code	Calling Number	Called Number	Connect Time	Disconnect Time	Duration (seconds)
1	9 : Incoming or tandem call	6149754406	53012	9/19/2016 3:12:53 PM	9/19/2016 3:13:00 PM	7
2	7 : Call used the AAR or ARS feature	53012	16149754405	9/19/2016 3:11:54 PM	9/19/2016 3:12:00 PM	6
3	0 : No error	53012	53115	9/19/2016 3:11:57 PM	9/19/2016 3:12:00 PM	3
4	0 : No error	53010	53012	9/19/2016 3:11:57 PM	9/19/2016 3:12:00 PM	3

9.3.4. Verify RTCP Data from 9600 Series IP Deskphones

AppManager receives RTCP call quality data directly from 9600 Series SIP and H323 IP Deskphones. To run the *PhoneQuality* script, which collects real-time voice quality statistics for active calls 9600 Series IP Deskphones, select the **AvayaCM** tab and drag the **PhoneQuality** script to the **Active SPE** in the TreeView. A pop-up window appears (not shown) that allows parameters of the script to be modified. Select the data in the bottom half of the operator console and drag into the **Data Pane** to generate a graph (not shown). The following example shows a real-time graph of latency for an active call on a monitored IP station.



10. Conclusion

These Application Notes describe the steps required to configure NetIQ AppManager to interoperate with Avaya Aura® Session Manager, Avaya Aura® System Manager, Avaya Aura® Communication Manager, Avaya 1100 Series IP Deskphone, and Avaya 9600 Series IP Deskphone. All tests passed as noted in **Section 2.2**.

11. 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>.

- [1] *Administering Avaya Aura® Communication Manager* Release 7.0.1 03-300509 Issue 2.1 August 2016.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0.1 555-245-205 Issue 3 October 2016.
- [3] *Avaya Aura® Communication Manager Screen Reference* Release 7.0.1 03-602878 Issue 2 May 2016
- [4] *SIP Software for Avaya 1100 Series IP Deskphones-Administration* Release 4.4 NN43170-600 Issue 06.06 Standard, December 2015.
- [5] *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*, Release 6.5, 16-601944, Issue 1 January 2015.
- [6] *Administering 9608/9608G/9611G/9621G/9641G IP Deskphones H.323*, Release 6.4, 16-300698, Issue 19 June 2014
- [7] *Avaya 9621G and 9641G IP Deskphone H.323* Release 6.4 June 2014
- [8] *Administering Avaya Aura® Session Manager* Release 7.0.1 Issue 2 May 2016.
- [9] *Administering Avaya Aura® System Manager* Release 7.0.1
- [10] *NetIQ AppManager for Avaya Communication Manager Management Guide*, available at: <https://www.netiq.com/documentation/appmanager-modules/pdfdoc/appmanagerforavayacm/appmanagerforavayacm.pdf>

©2017 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.