Avaya Solution & Interoperability Test Lab

Application Notes for NetIQ AppManager with Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe the steps required to allow NetIQ AppManager to monitor Avaya Aura® Communication Manager. NetIQ AppManager provides monitoring, management and reporting for Avaya Aura® Communication Manager, including capturing call records, configuration data using SNMP, SNMP traps, and call quality metrics using RTCP. NetIQ AppManager performs event monitoring of the call server and gathers call quality data in real-time to accurately and quickly reflect the end user call experience. NetIQ AppManager also monitors call activity in order to track call usage and call failures.

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 to allow NetIQ AppManager to monitor Avaya Aura® Communication Manager. NetIQ AppManager provides monitoring, management and reporting for Avaya Aura® Communication Manager, including capturing call records, configuration data using SNMP, SNMP traps, and call quality metrics using RTCP. NetIQ AppManager performs event monitoring of the call server and gathers call quality data in real-time to accurately and quickly reflect the end user call experience. NetIQ AppManager also monitors call activity in order to track call usage and call failures.

NetIQ AppManager uses Knowledge Scripts to create jobs that gather data for call quality and call activity metrics and stores the data in the Avaya CM supplemental 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:

- *CallQuery* script monitors call activity via the CDR link.
- *CallQuality* and *PhoneQuality* scripts capture call quality metrics received in RTCP packets.
- *AvayaCM* script to discover Avaya Aura® Communication Manager components via SNMP.
- *RetrieveConfigData* and *PhoneInventory* scripts retrieve the phone inventory on Avaya Aura® Communication Manager using SNMP. Inventory data may then be used by other Knowledge Scripts that require it.
- *SNMPTrap* script captures SNMP traps from Avaya Aura® Communication Manager. The *AddMIB* script is used to install the Avaya MIBs in NetIQ AppManager.

To perform the monitoring functions, NetIQ AppManager uses the following interfaces on Avaya Aura® Communication Manager.

- Simple Network Management Protocol (SNMP) – NetIQ AppManager uses SNMP to collect configuration and status information and SNMP traps from Avaya Aura® Communication Manager.
- Real-time Transport Control Protocol (RTCP) – NetIQ AppManager uses RTCP data from Avaya IP telephones to gather call quality metrics for H.323 and SIP calls. 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.
- Call Detail Recording (CDR) – NetIQ AppManager uses CDR records from Avaya Aura® Communication Manager to track call activity.

2. General Test Approach and Test Results

This section describes the compliance testing used to verify the interoperability of AppManager with Communication Manager. This section covers the general test approach and the test results. The testing covered feature and serviceability test cases. The feature testing covered the ability of AppManager to capture call records, configuration data, and SNMP traps from Communication Manager. In addition, call quality metrics from H.323 and SIP calls were also captured.

The CDR data displayed using the *CallQuery* script in AppManager was compared to the CDR data received by an Avaya CDR test tool. CDR's for various call types were generated, including internal calls, inbound trunk calls, outbound trunk calls, transferred calls, and conference calls.

To verify the accuracy of the configuration data in AppManager, stations were added and removed from Communication Manager to verify that AppManager updated its inventory information accordingly after running the *RetrieveConfigData* and *PhoneInventory* scripts.

To verify call quality metrics, the general approach was to place various types of calls to and from stations, inject errors, collect VoIP call quality data on AppManager using the CallQuality and PhoneQuality script, and compare the quality data on AppManager with values displayed on the Avaya IP telephones. During the compliance test, a network impairment tool was used to simulate network delay and packet drop conditions in the LAN.

Lastly, SNMP traps were generated on Communication Manager and the G650 Media Gateway to verify that AppManager displayed the SNMP traps properly using the *SNMPTrap* script.

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:

- Sending CDR from Communication Manager to AppManager for various call types.
- Displaying CDR on AppManager.
- Sending RTCP data from H.323 and SIP phones to AppManager.
- Displaying RTCP data in real-time on AppManager.
- Retrieving phone inventory from Communication Manager using SNMP.
- Capturing phone inventory in text file by AppManager.
- Sending SNMP traps from Communication Manager and G650 Media Gateway to AppManager.
- Displaying SNMP traps in AppManager.
- Proper system recovery after loss of network connectivity and power loss .

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 NetIQ. CDR test cases were run with RSP disabled. NetIQ AppManager for Avaya Aura® Communication Manager requires that a custom CDR format be applied. CDR test cases were run with a custom CDR format as described in the AppManager for Avaya Aura® Communication Manager Management guide.
  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 the AppManager application 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 the *PhoneInventory* knowledge script, the default path for the inventory file is, *C:\Program Files\NetIQ\Temp\NetIQ_Debug*. When running AppManager from a 64 bit machine, the path needs to be updated to *C:\Program Files (x86)\NetIQ\Temp\NetIQ_Debug*

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 7.2**.

2.3. Support

For technical support on AppManager, contact NetIQ Support by phone, through their website, or email.

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, two sites, Sites A and B, are connected via a SIP trunk. AppManager only monitors the VoIP calls and SNMP traps at Site A. Site B is present primarily to generate inter-site traffic across the SIP trunk. Site A has an Avaya S8800 server running Communication Manager with an Avaya G650 Media Gateway. Site A also includes Avaya Aura® Session Manager and Avaya 9600 Series H.323 and SIP Telephones. The configuration at Site B is similar to Site A. AppManager connects to Site A via the corporate LAN. In this configuration AppManager is running on a Windows 7 Professional SP1 server. The AppManager installation includes the following core components on the same server:

- **Operator Console** is used to perform AppManager configuration
- **Management Server** manages the data and communicates with agents to start/stop jobs
- **Repository** includes a Microsoft SQL database
- **Agent** is the managed client

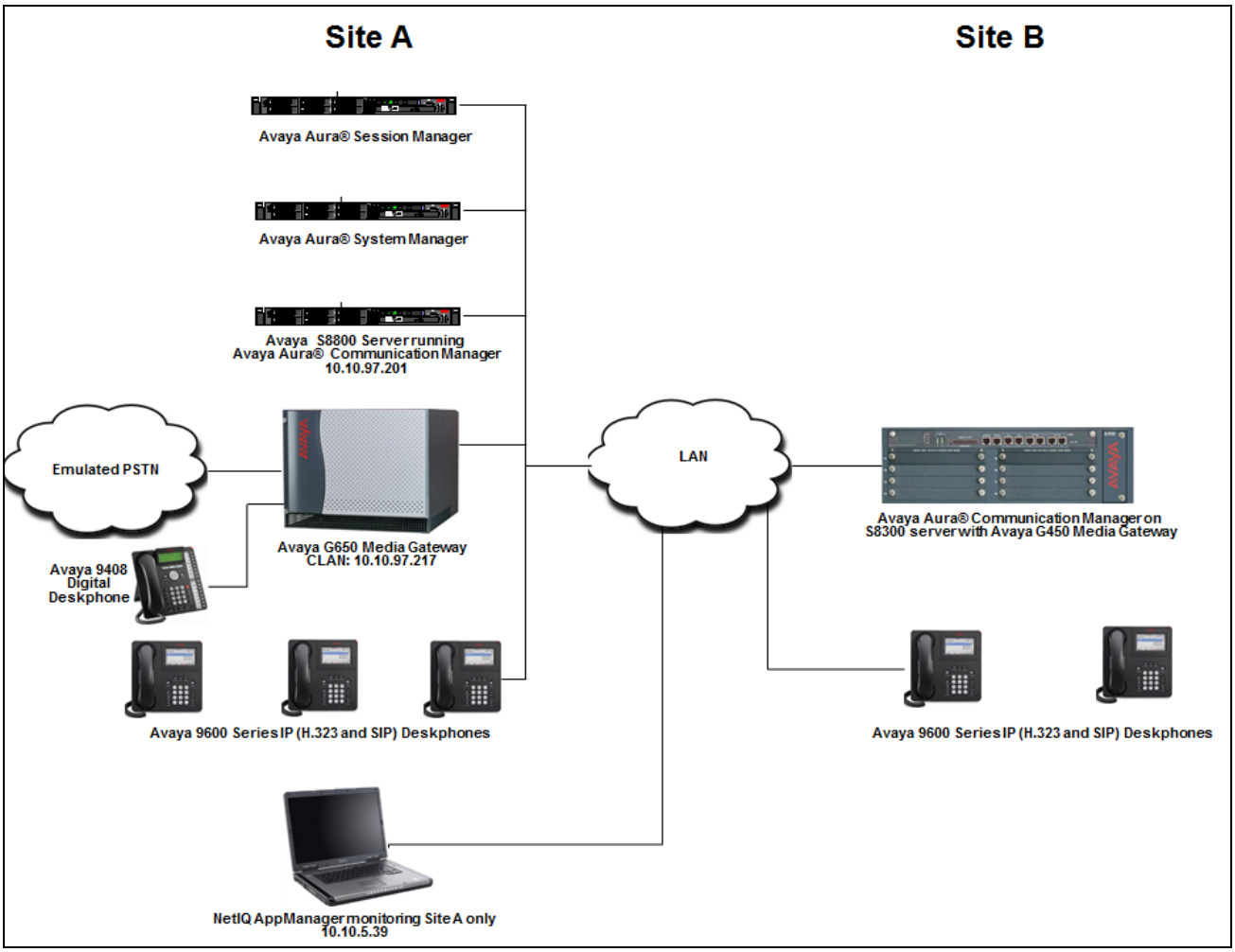


Figure 1: NetIQ AppManager with Avaya Aura® Communication Manager

4. Equipment and Software Validated

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

Equipment	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server with Avaya G650 Media Gateway.	6.3-03.0.124.0
Avaya Aura® Communication Manager running on Avaya S8300D Server with Avaya G450 Media Gateway.	R016x.03.0.124.0
Avaya Aura® Session Manager	6.3.2.0.632023
Avaya Aura® System Manager	6.3.0.8.5682-6.3.8.1627
Avaya 9600 Series IP Telephones Avaya 9408 Digital Phone	S3.220A (H.323) 6.4014 (H.323) 2.6.11.4 (SIP) FW 12 Boot 29
NetIQ AppManager running on Windows 7 Professional SP1	8.2 (Build 8.2.3.37)

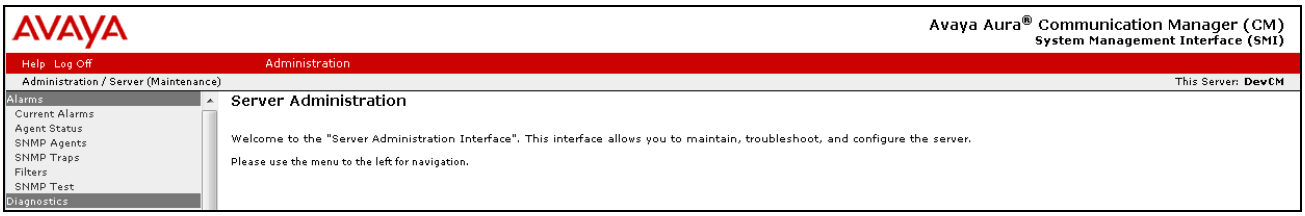
5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration at Site A that is required to interoperate with AppManager. In the test configuration, AppManager did not monitor Site B so no configuration of Communication Manager at that site is required. This section is divided into three sub-sections describing the three interfaces used by AppManager to gather data on the VoIP infrastructure. **Section 5.1** describes the SNMP configuration, **Section 5.2** describes the RTCP configuration, and **Section 5.3** describes the CDR configuration.

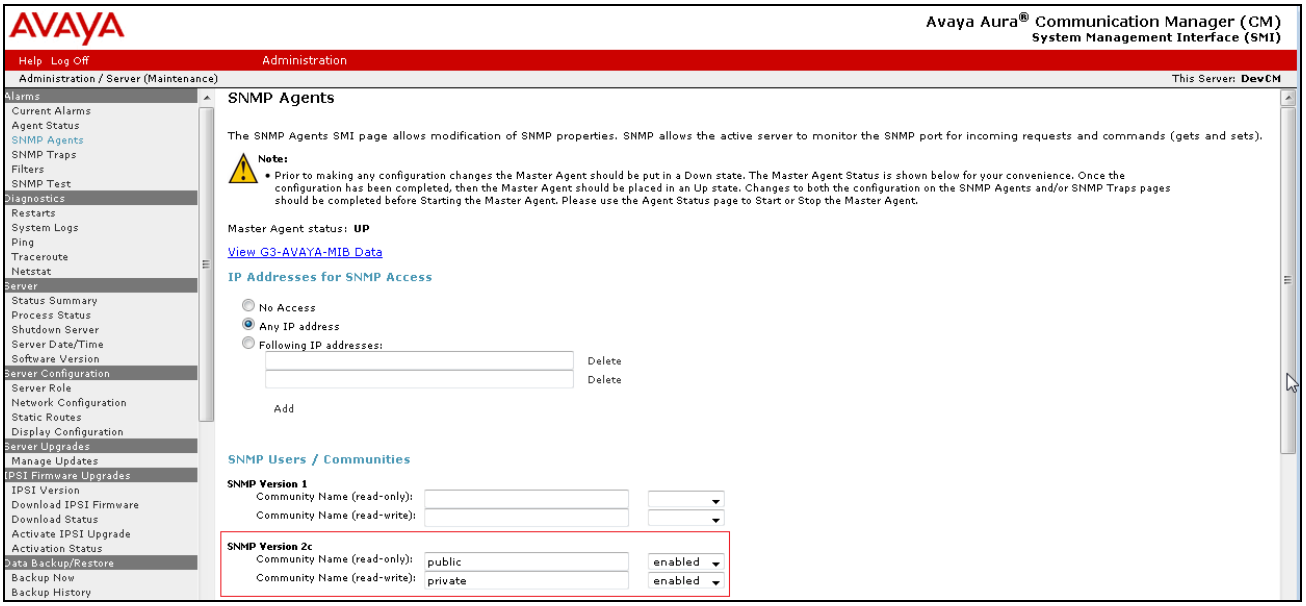
The configuration of Communication Manager in **Section 5.1** was performed using the Web interface. The configuration described in **Sections 5.2** and **5.3** was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

5.1. Configure SNMP

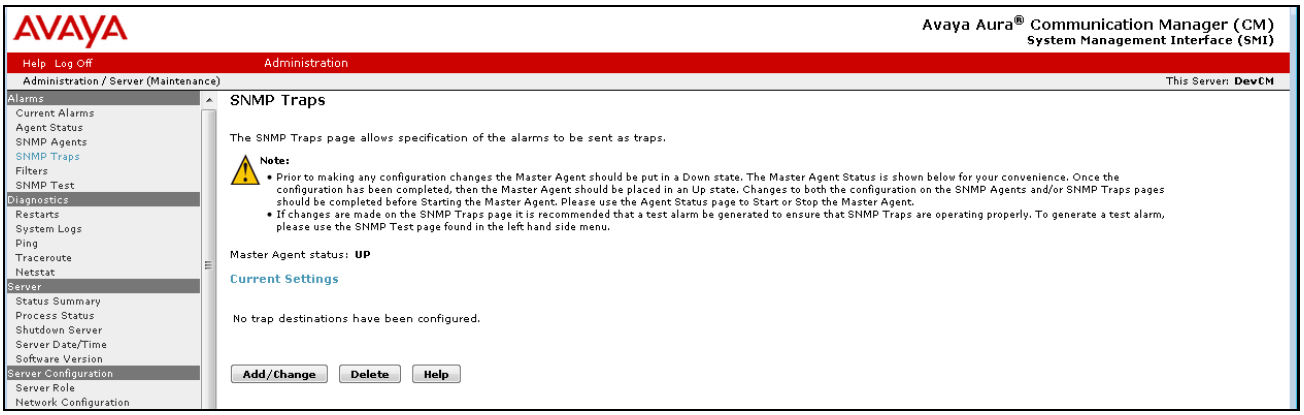
To access the **Avaya Aura® Communication Manager System Management Interface**, enter the IP address of the Avaya Server into a web browser. Log in using appropriate credentials. Navigate to **Administration → Server (Maintenance)** (not shown) to display the following web page.



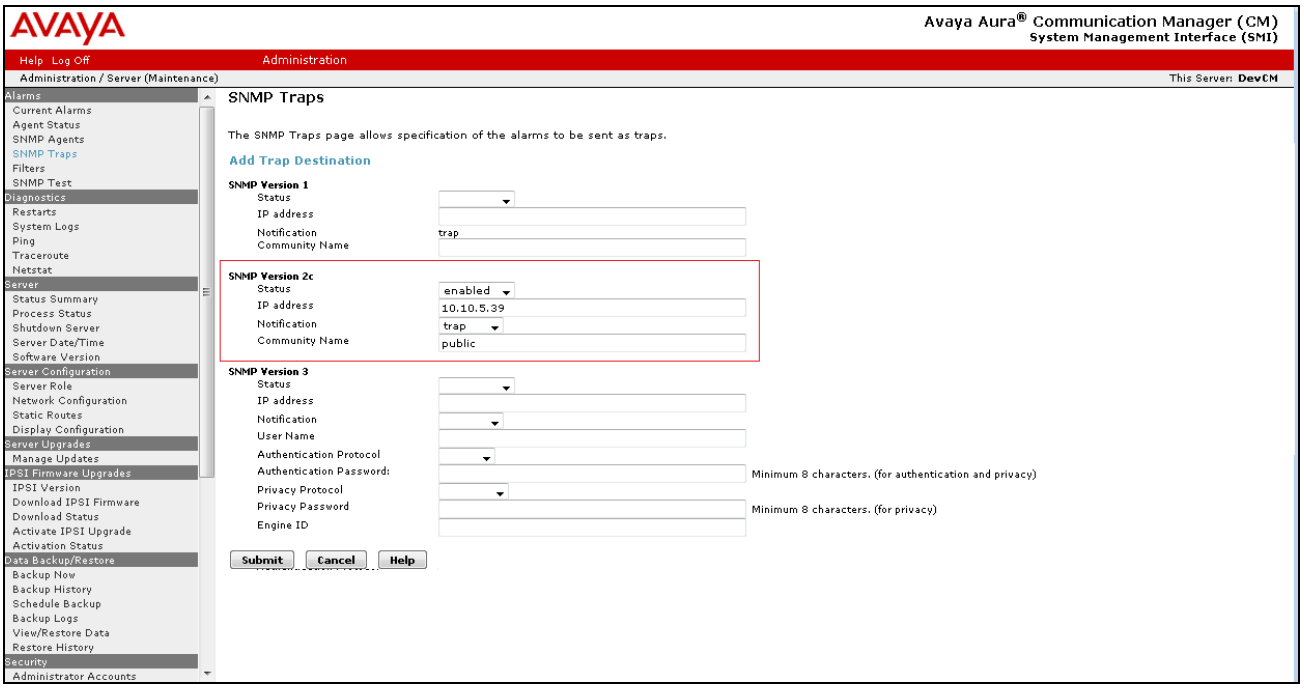
To allow AppManager to use SNMP to collect configuration and status information from Communication Manager, navigate to **Alarms → SNMP Agents** in the left pane. Under **IP Addresses for SNMP Access**, select *Any IP address*. Under **SNMP Users / Communities**, configure the **SNMP Version 2c** section. Set the **Community Name (read-only)** field to *public* and the drop-down box to the right to *enabled*. Click **Submit** at the bottom of the web page (not shown in the figure).



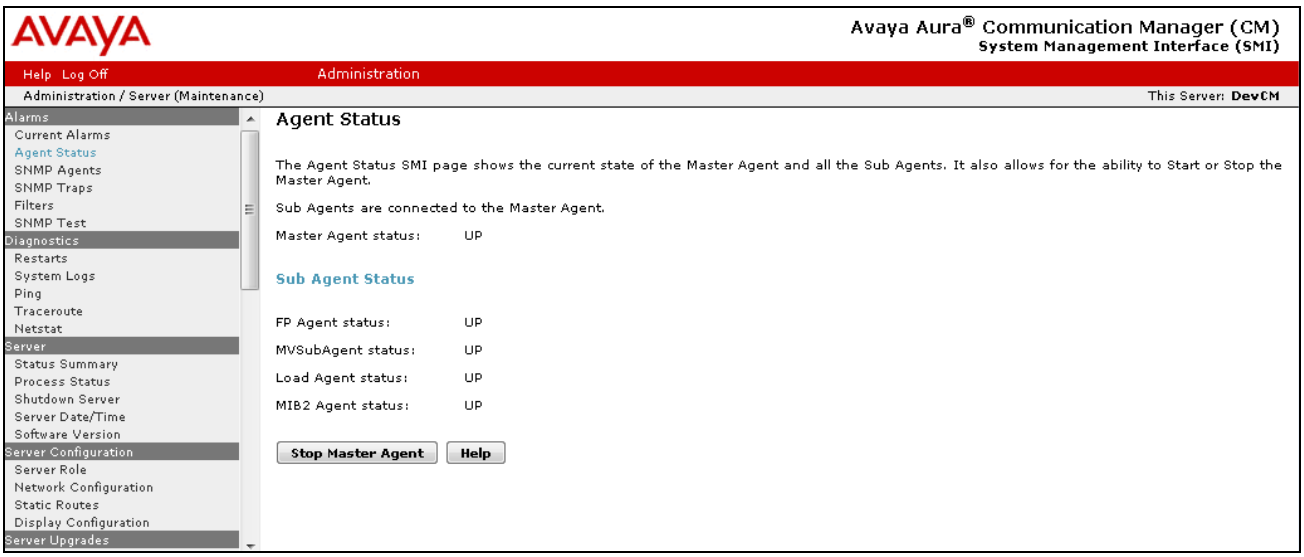
To configure AppManager as an SNMP trap receiver, navigate to **Alarms → SNMP Traps** in the left pane. In the **SNMP Traps** web page, click the **Add/Change** button shown below.



In the subsequent SNMP Traps web page below, configure AppManager as an SNMP trap receiver under the **Add Trap Destination** section, including the **SNMP Version 2c** parameters. Set the **Status** field to *enabled*, specify the **IP address** of AppManager, set the **Notification** field to *trap*, and set the **Community Name** to *public*. Click the **Submit** button.



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



5.2. 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 H.323 IP telephone so that the telephones will know where to send RTCP data. Set the **Server IPV4 Address** to the IP address of the AppManager agent that will collect the data. The **IPV4 Server Port** and **RTCP Report Period(secs)** fields must match the AppManager configuration in **Section 6.2**. In the compliance test, the default values of *5005* and *5* were used, respectively.

Note: For an Avaya SIP telephone, the RTCP configuration is specified in the 46xxsettings.txt file. The **RTCPMON** parameter must be set to the IP address of the AppManager server.

```
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: 10.10.5.39      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 H.323 IP telephones. In the compliance test, the H.323 IP telephones 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
```

5.3. 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 *10.10.5.39*. Also, highlighted in the example below is the node name *CLAN1*, which represents the IP address of the CLAN circuit pack used as the source of the CDR data.

```
change node-names ip                                            Page   1 of   2
                                IP NODE NAMES
    Name              IP Address
AES63               10.10.98.17
AVAYARDTT           10.10.98.71
CLAN1               10.10.97.217
CLAN2               10.10.97.238
GW                  10.10.97.193
MedPro1             10.10.97.218
MedPro2             10.10.97.233
NetIQ               10.10.5.39
SM61                10.10.97.198
default             0.0.0.0
procr               10.10.97.201
( 16 of 17   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Use the **change ip-services** command to define the CDR link between Communication Manager and AppManager. In the **Service Type** field, enter ***CDR1*** for the primary CDR link. In the **Local Node** field, enter the node name that will terminate the CDR link on Communication Manager. In the compliance test, which used an Avaya G650 Media Gateway, the **Local Node** was the CLAN circuit pack discussed above. The **Remote Node** field is set to the node name defined above *NetIQ* for AppManager. The **Remote Port** may be set to a value between 5000 and 64500 inclusive and must match the port configured on AppManager in **Section 6.2**.

```
change ip-services                                              Page   1 of   4

                                  IP SERVICES
 Service      Enabled     Local        Local        Remote       Remote
  Type                    Node         Port         Node         Port
AESVCS         y       CLAN2           8765
CDR1                   CLAN1           0        NetIQ            9000
CDR2                   CLAN1           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      Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type        Protocol     Timer        Message Cntr    Cntr     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. AppManager used a customized CDR format which is defined below. Other standard CDR formats may be used, but would require the **AvayaCDRFormat.txt** file to be modified with the appropriate CDR format on AppManager (see reference **[3]** for more details).

- **CDR Date Format:** ***month/day***
- **Primary Output Format**: ***customized***
- **Primary Output Endpoint**: ***CDR1***

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference **[1]** and **[2]** for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Intra-switch CDR?** ***y*** This allows call records for internal calls involving specific stations.
- **Record Outgoing Calls Only?** ***n*** This allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.
- **Outg Trk Call Splitting?** ***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?** ***y*** This prevents calls that are blocked from appearing in the CDR record.
- **Inc Trk Call Splitting?** ***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? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: 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 set to *y* as seen earlier, use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the **Assigned Members** field, enter a specific extension whose usage will be tracked with a CDR record. Add an entry for each additional extension of interest. During compliance testing 53010, 53012 and 53116 were monitored

```
change intra-switch-cdr                                           Page   1 of   3
                           INTRA-SWITCH CDR

                                Assigned Members:   15   of 5000   administered
   Extension          Extension          Extension          Extension
   53008
   53010
   53012
   53013
   53014
   53016
   53045
   53100
   53101
   53102
   53104
   53105
   53106
   53107
   53116
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, to 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-CS1K 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 Sites A and B.

```
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
```

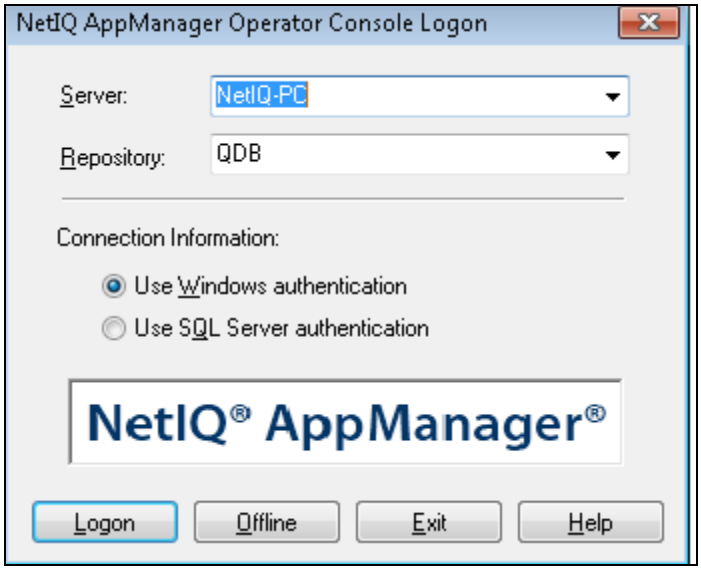
6. Configure NetIQ AppManager

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:

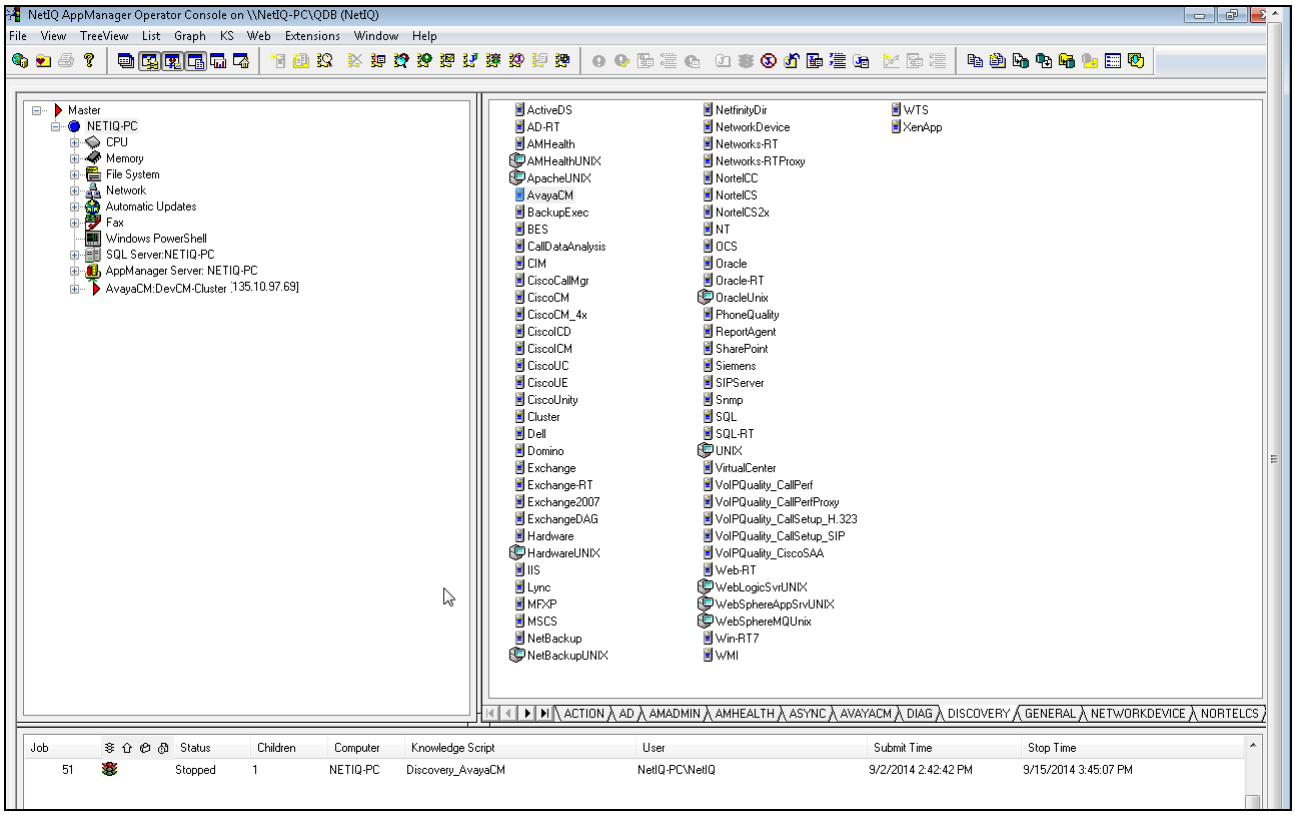
- Launch AppManager for Communication Manager
- Add Computer
- Configure SNMP, CDR, and RTCP Parameters
- Discover Avaya Communication Manager
- Retrieve Configuration Data
- Add Avaya IP Telephones

6.1. Launch NetIQ AppManager for Avaya Aura® Communication Manager

AppManager is configured using the **Operator Console**. Launch the **Operator Console** from the Windows Start menu by navigating to **All Programs → NetIQ → AppManager → Operator Console**. The logon screen is displayed as shown below. Enter the appropriate values for **Server** and **Repository** fields and then click on the **Logon** button.

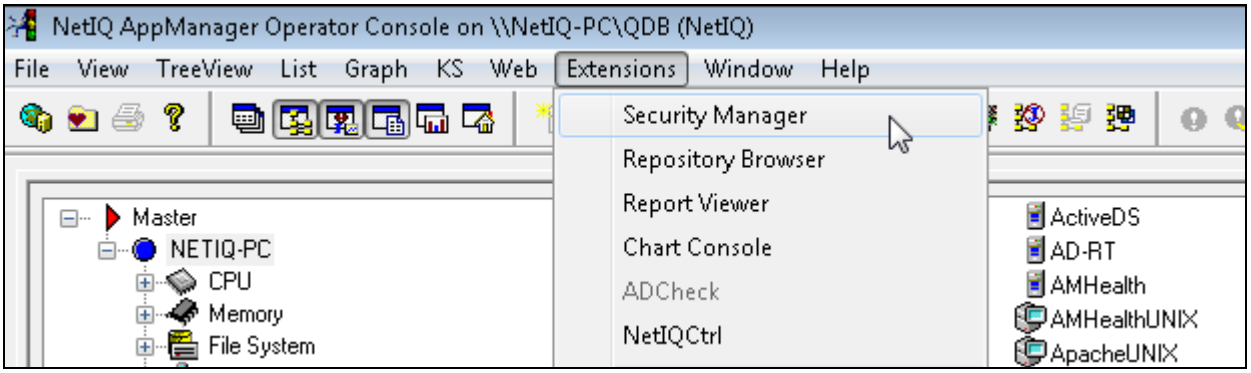


The main **NetIQ AppManager Operator Console** window appears as shown below.

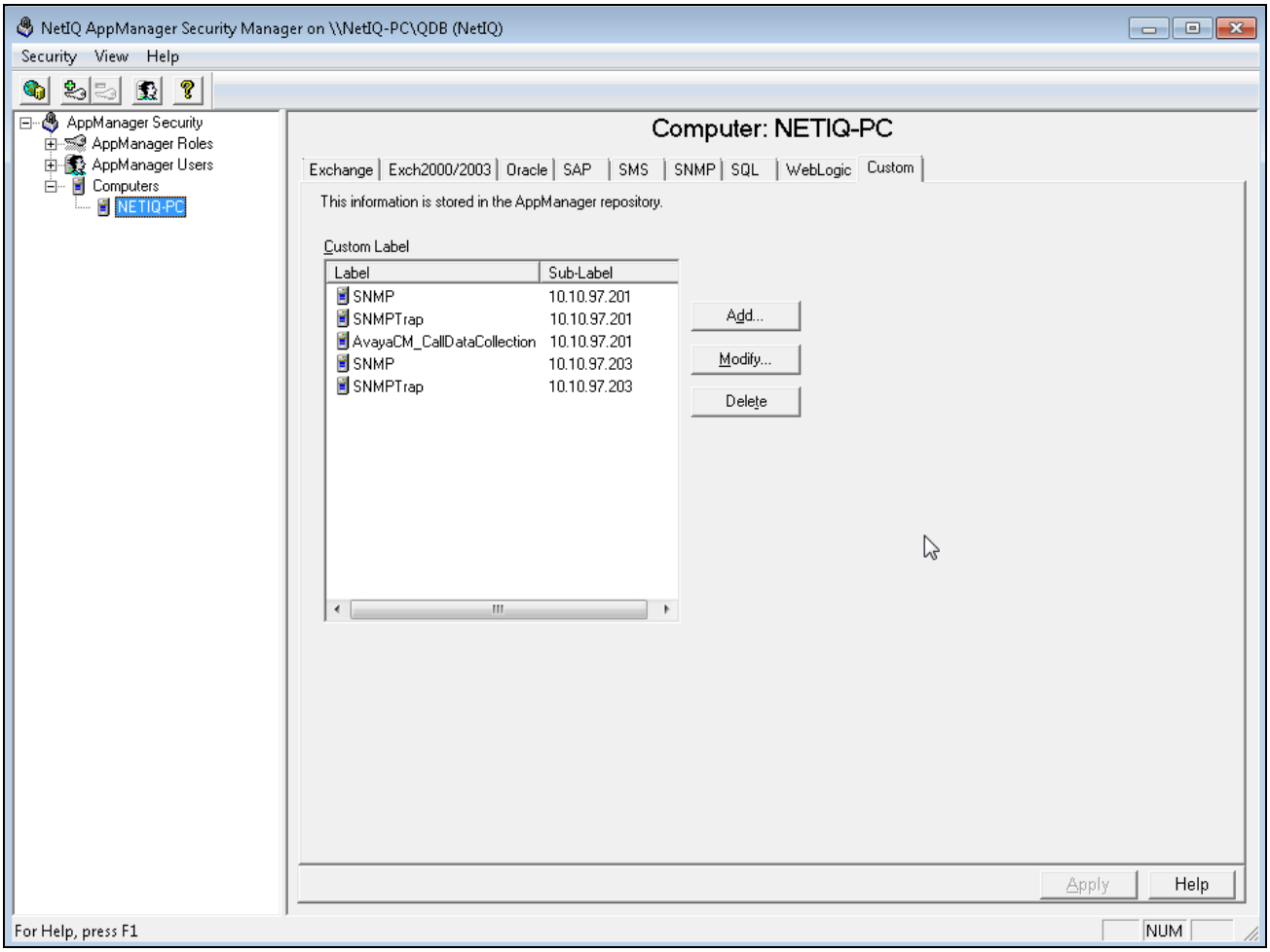


6.2. Configure SNMP, SNMP Traps, CDR and RTCP Parameters

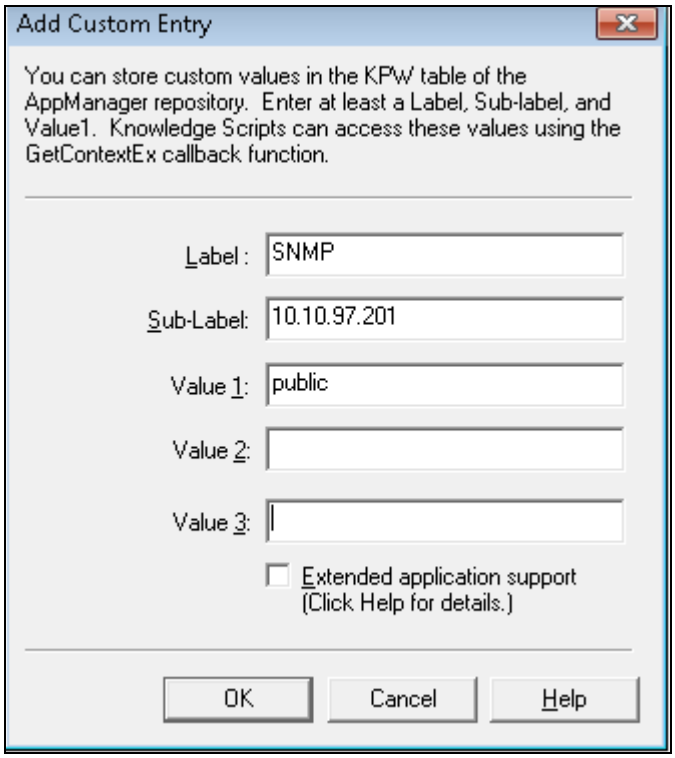
AppManager must be configured to connect to Communication Manager. From the **Operator Console**, navigate to **Extensions → Security Manager** from the menu across the top of the window as shown below.



The following window appears. Highlight the agent host name **NETIQ-PC** and click on the **Custom** tab. The example below shows custom entries to communicate with Communication Manager via SNMP, CDR, and RTCP. The **AvayaCM_CallDataCollection** entry covers CDR and RTCP. These entries were originally created by clicking the **Add** button and will be covered next.

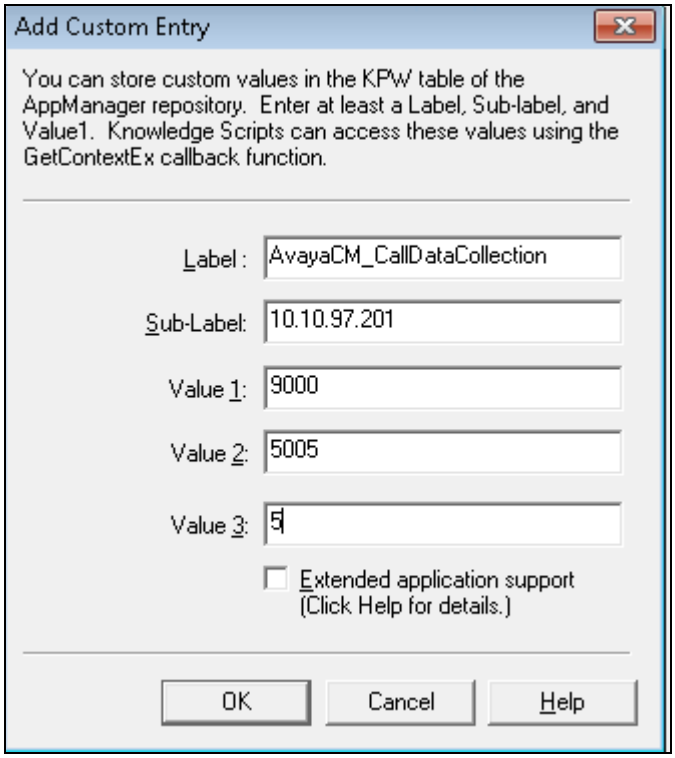


Click on the **Add** button in the Security Manager window shown in the screen above to configure the SNMP connection parameters. The dialog box as shown below is displayed. Enter *SNMP* for the **Label** field. Enter the IP address of Communication Manager in the **Sub-Label** field. Enter the SNMP community string (read-only) configured in **Section 5.1** in the **Value 1** field. Click **OK**.



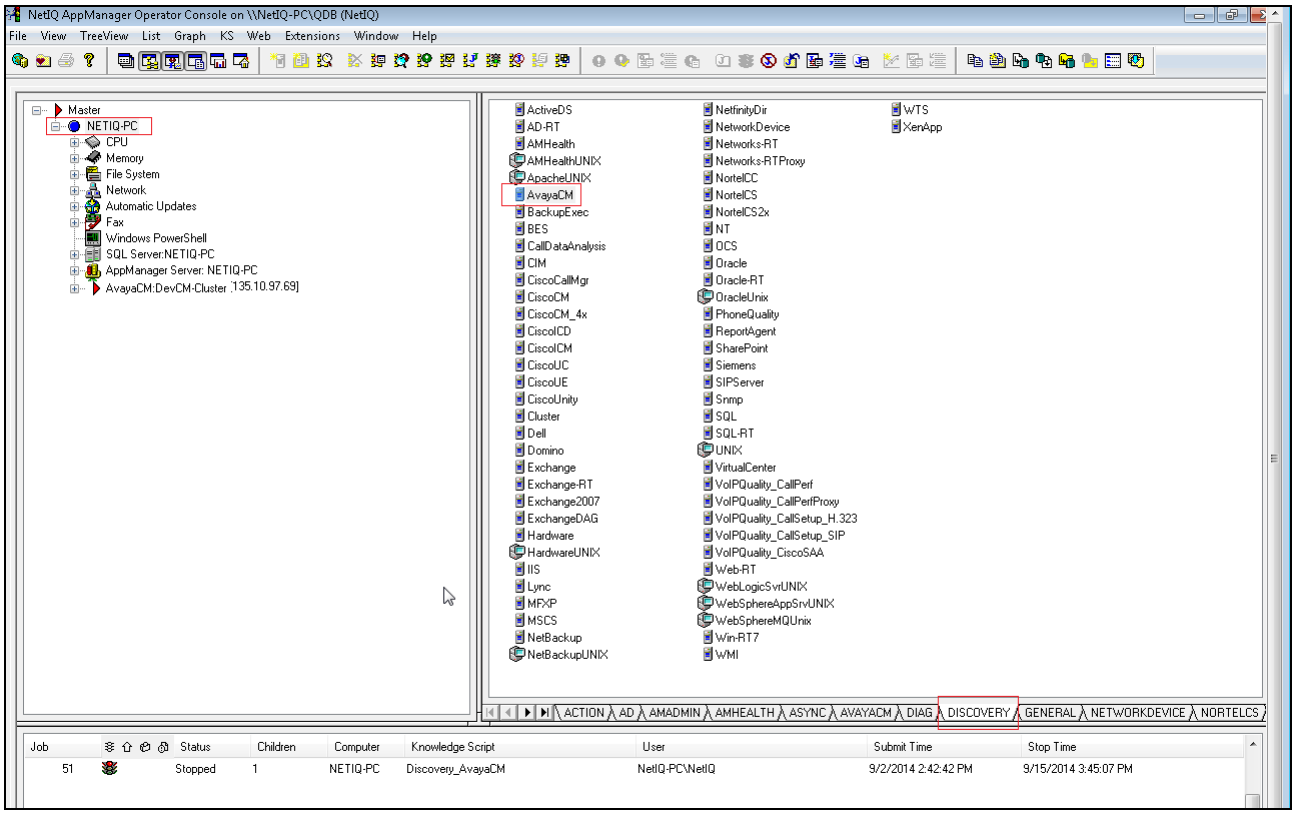
Similarly click on the **Add** button in the Security Manager window to configure the SNMP connection parameters. Enter *SNMPTrap* for the **Label** field. Enter the IP address of Communication Manager in the **Sub-Label** field. Enter the SNMP community string (read-only) configured in **Section 5.1** in the **Value 1** field. Click **OK**. (not shown).

Click the **Add** button in the Security Manager window again to configure the CDR and RTCP connection parameters and enter *AvayaCM_CallDataCollection* for the **Label** field. Enter the IP address of Communication Manager in the **Sub-Label** field. **Value 1** is the port number used for CDR data. This must match the value configured on Communication Manager in **Section 5.3**. **Value 2** is the port number used for RTCP data. **Value 3** is the RTCP report period in seconds. These values must match the values configured on Communication Manager in **Section 5.2**. Click **OK**.



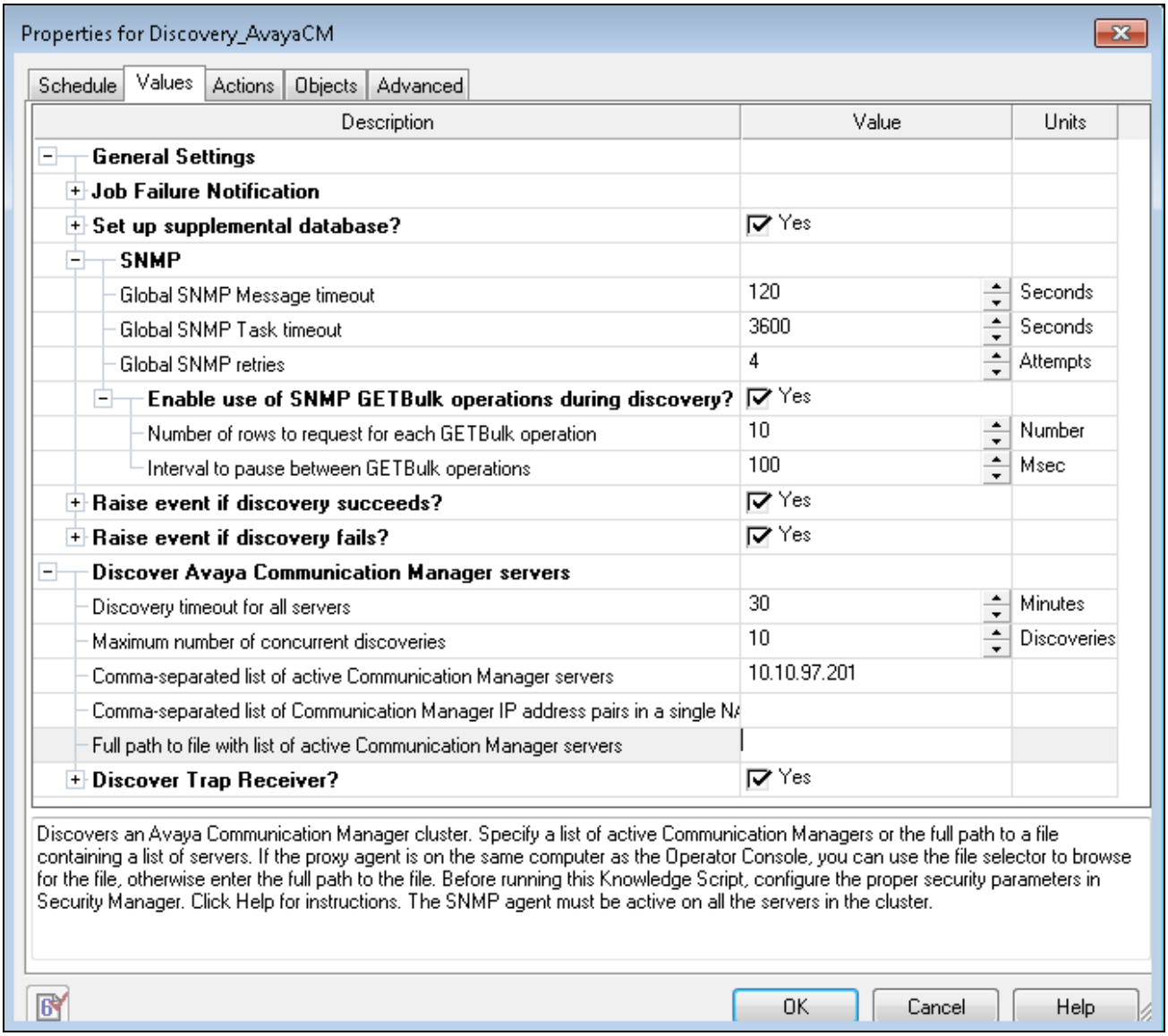
6.3. Discover Avaya Aura® Communication Manager

Once the connection parameters have been defined as shown in **Section 6.2**, then the components of Communication Manager can be discovered using SNMP. To do this, select the **DISCOVERY** tab. Drag the **AvayaCM** script to the agent host name (**NETIQ-PC**) in the tree view.



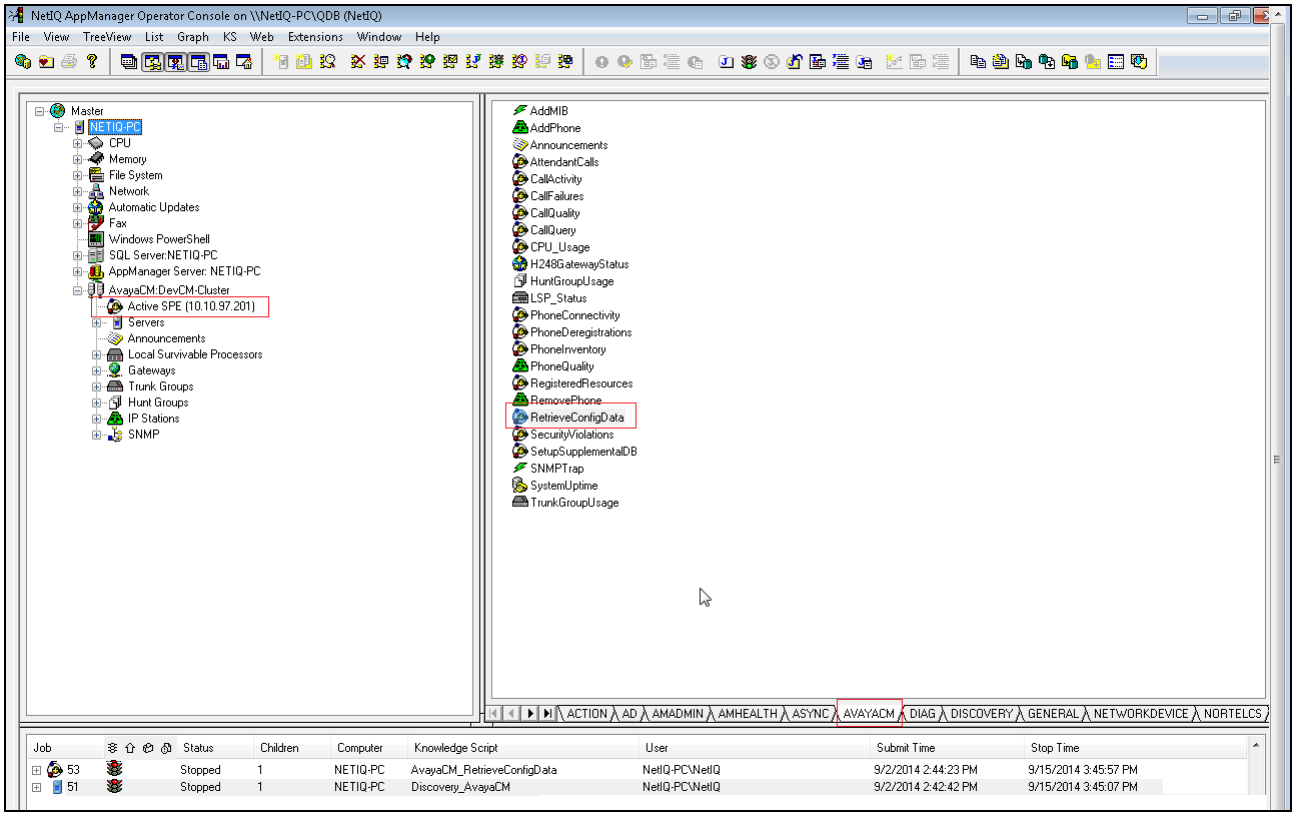
The following pop-up window will appear. Enter the IP address of Communication Manager in the field labeled **Comma-separated list of active Communication Manager servers**. Enable **Discover Trap Receiver?**. Optionally, the **Raise event if discovery succeeds?** option may be enabled. Click **OK**.

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

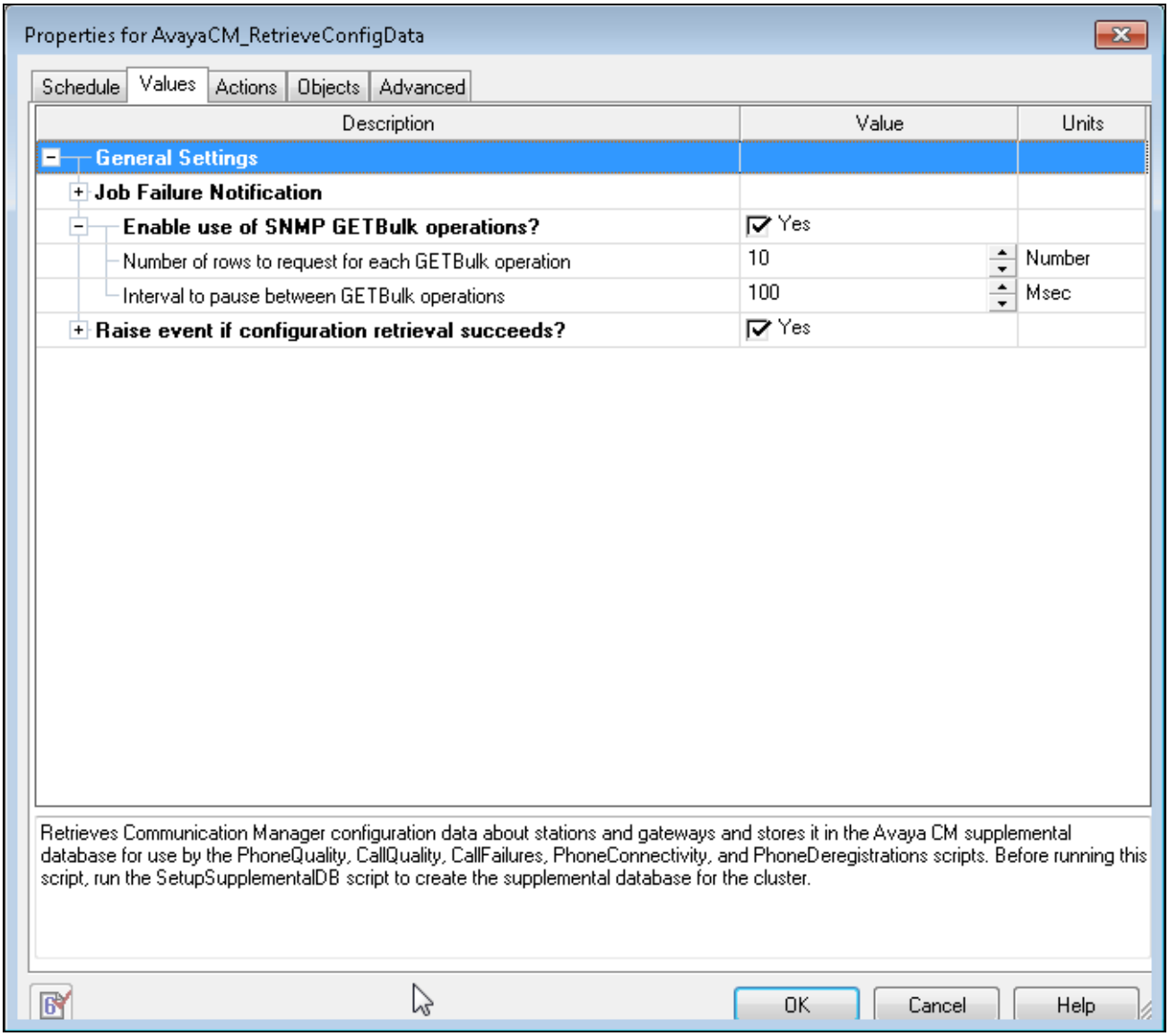


6.4. Retrieve Configuration Data

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

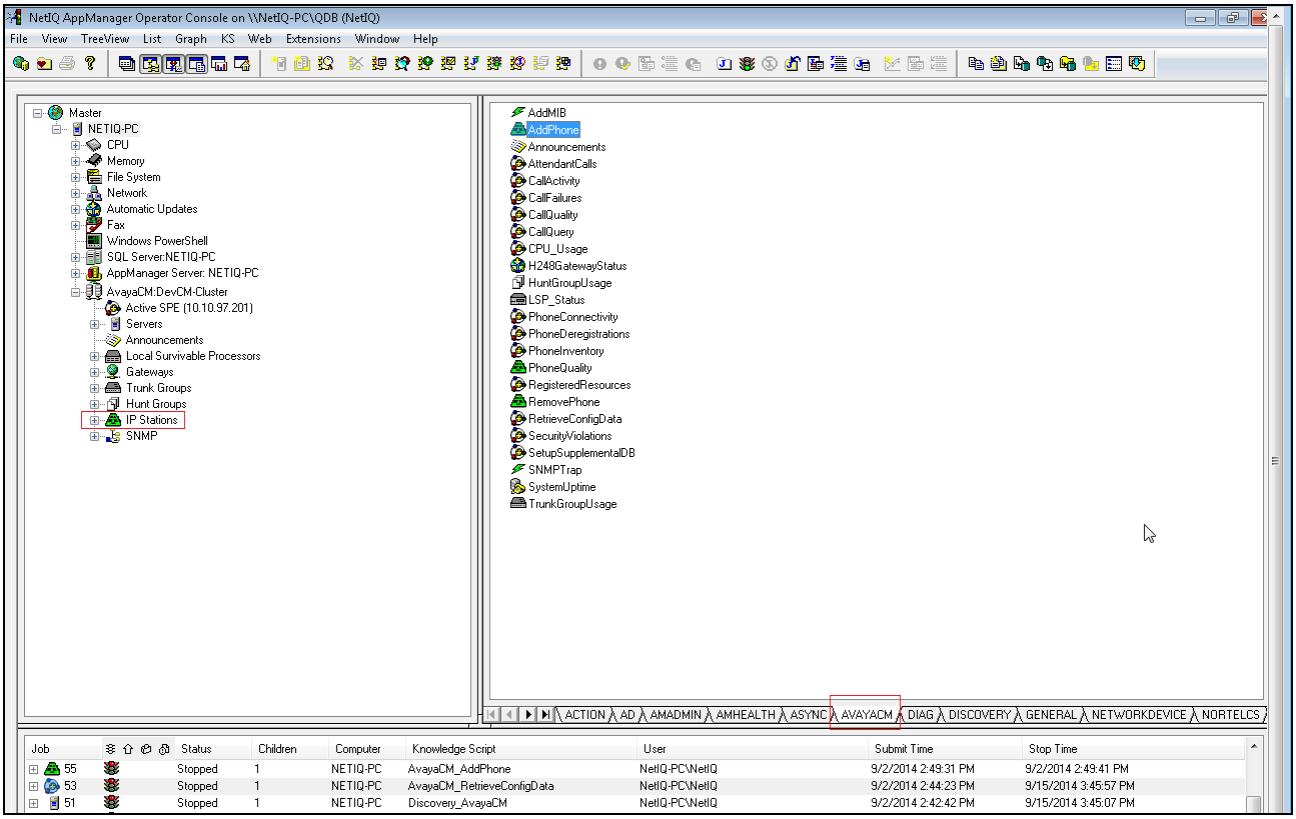


The following pop-up window appears. Retain the default values. Optionally, the **Raise event if configuration retrieval succeeds?** option may be enabled. Click **OK**.

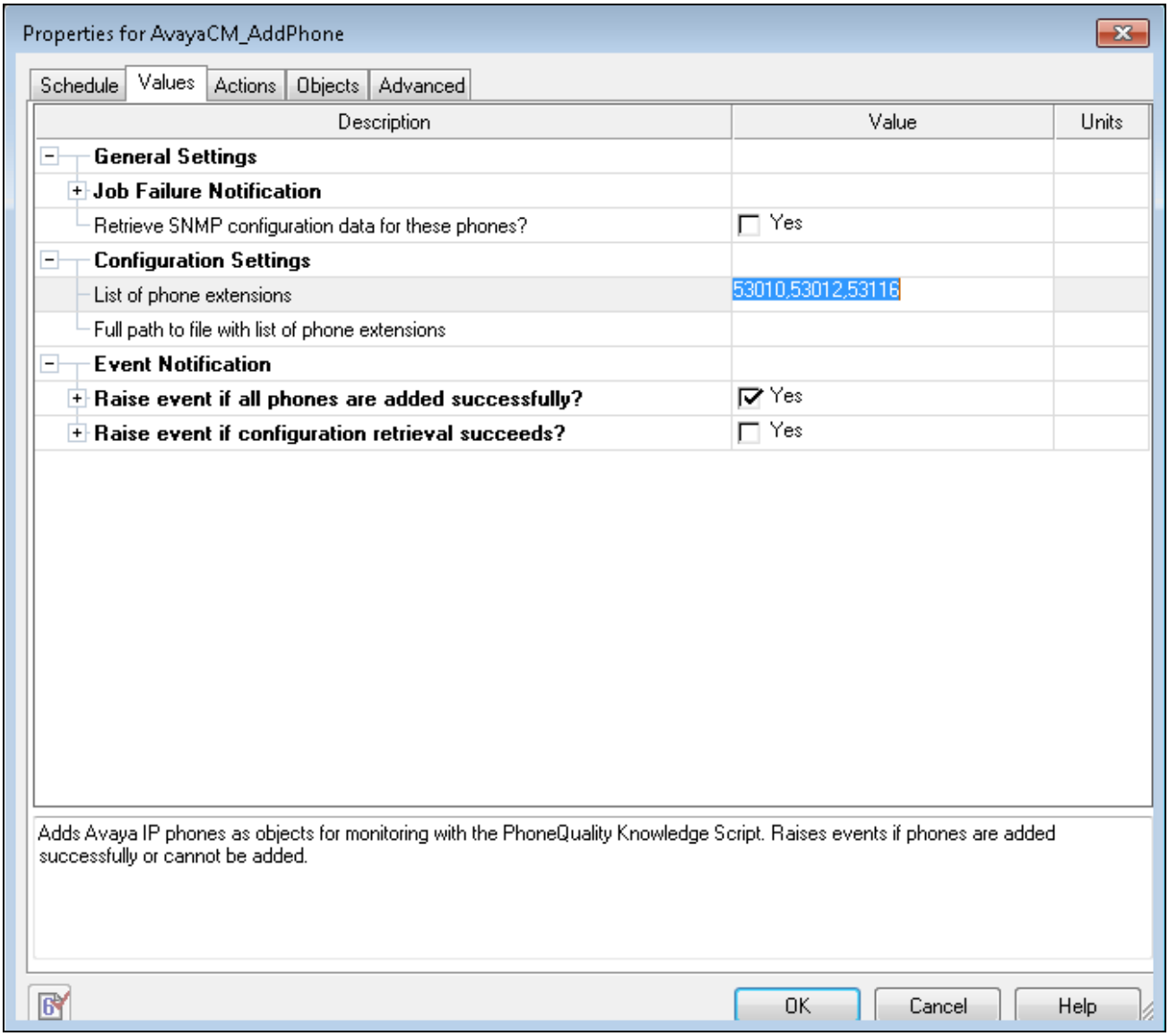


6.5. Add Avaya IP Telephones

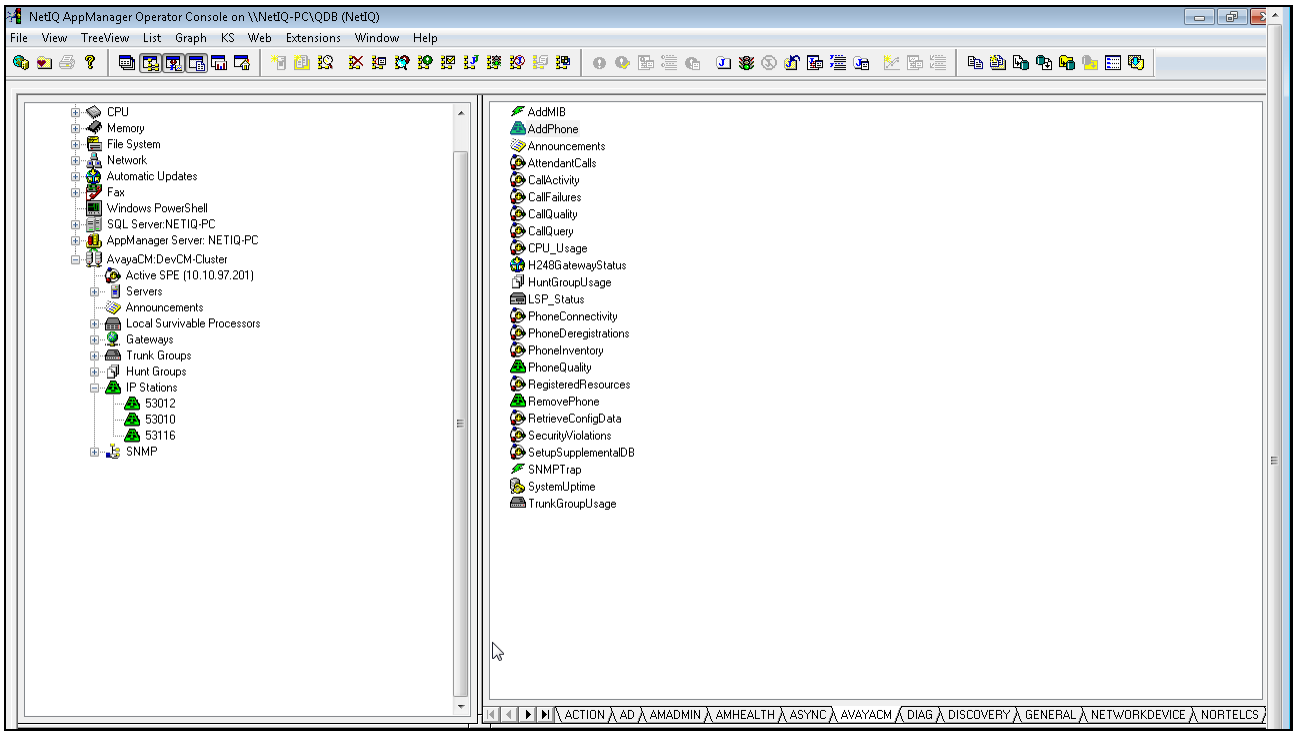
Lastly, in order to run a script (specifically the *PhoneQuality* script) on an individual IP telephone, that IP telephone must be entered in the tree view. To add an IP telephone to the tree view, select the **AVAYACM** tab and drag the **AddPhone** script to **IP Stations** in the left pane. The pop-up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



Enter the IP telephone extension or list of 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 tree view with the individual IP telephones shown in the tree view as seen in the next screen. Sample AppManager reports are shown in **Section 7.2**.



After adding the Avaya IP telephones using the procedure above, the IP extensions are then displayed under **IP Stations** in the tree view as shown below. Note that extensions *53012*, *53010*, and *53116* are displayed under **IP Stations**. During the compliance testing these were the extensions that were monitored as mentioned in **Section 5.3**.



7. Verification Steps

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

7.1. Verify Avaya Aura® Communication Manager

The following steps may be used to verify the configuration on Communication Manager.

- Use the **ping** command to verify network connectivity from AppManager to all devices.
- Verify that calls can be successfully completed between the IP and digital telephones.
- From the SAT, use the **status cdr-link** command to verify that the CDR link to AppManager is up.

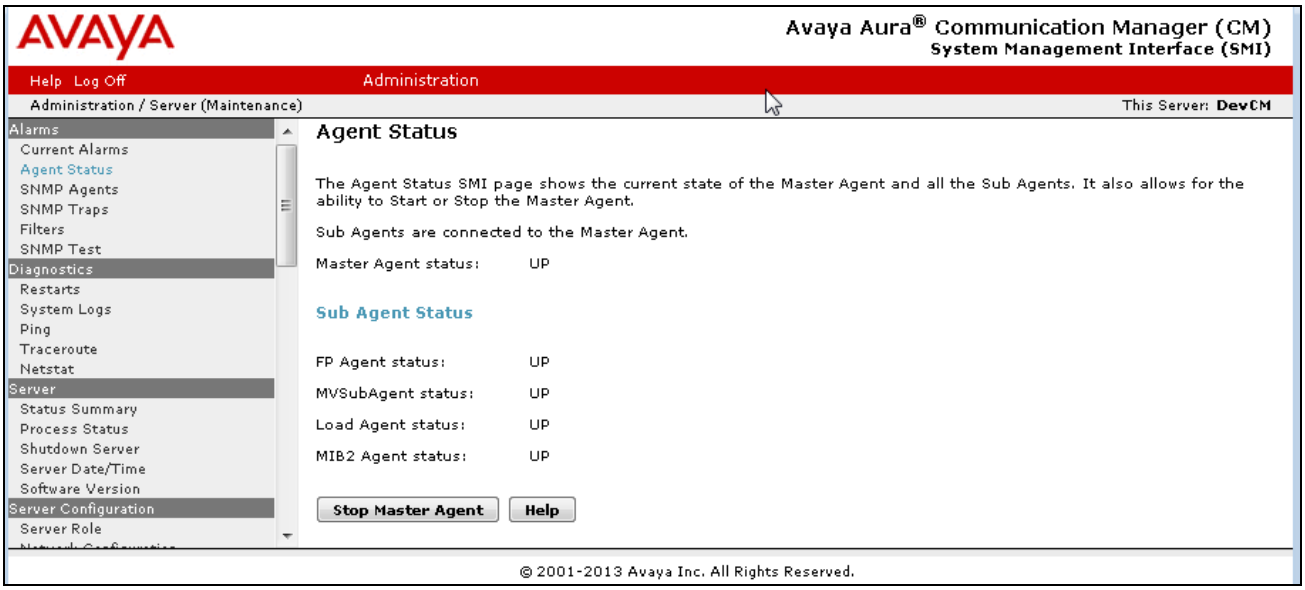
```
status cdr-link
                                CDR LINK STATUS
                    Primary                       Secondary

        Link State: up                            up

       Date & Time: 2014/09/19 15:13:55           2014/09/19 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 using Knowledge Scripts is running (CallActivity, CallQuality, CallFailures, CallQuery, PhoneQuality).

- From the Communication Manager Web interface, click on the **Agent Status** link on the left pane to verify that the **Master Agent Status** is up as shown in the screen below.



7.2. Verify NetIQ 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.

- Once the AppManager configuration is complete as detailed in **Section 6**, scripts can be run against the various components in the tree view. For example, to run the *CallQuery* script, which queries call detail records retrieved from Communication Manager and stored in the Avaya CM supplemental database, select the **AVAYACM** tab and drag the *CallQuery* script to the **Active SPE** in the tree view. 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. It displays calls that match the criteria specified in the script parameters pop-up window.

Event Properties: 1489

Event | Message | Comments

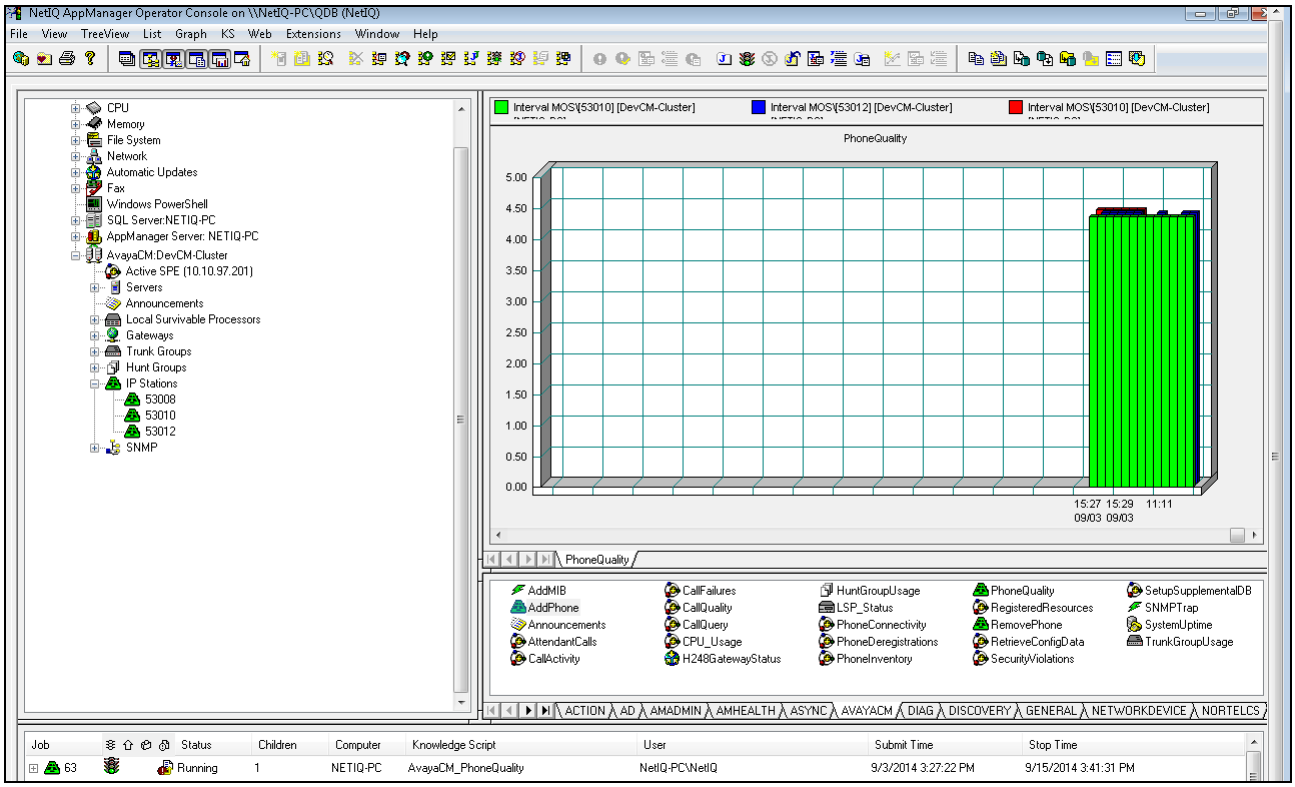
CallQuery: Results
The number of calls found (4) exceeds the threshold (0).

CallQuery: Summary	
Number of records matching the query	4
Starting disconnect time	9/19/2014 3:12:00 PM
Ending disconnect time	9/19/2014 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	9/19/2014 3:12:53 PM	9/19/2014 3:13:00 PM	7
2	7 : Call used the AAR or ARS feature	53012	16149754405	9/19/2014 3:11:54 PM	9/19/2014 3:12:00 PM	6
3	0 : No error	53012	53115	9/19/2014 3:11:57 PM	9/19/2014 3:12:00 PM	3
4	0 : No error	53010	53012	9/19/2014 3:11:57 PM	9/19/2014 3:12:00 PM	3

- To run the *PhoneQuality* script, which collects real-time voice quality statistics for active calls on Avaya IP phones, select the **AvayaCM** tab and drag the **PhoneQuality** script to the **Active SPE** to monitor in the tree view. 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. The following example shows a real-time graph of latency for an active call on a monitored IP station.



- In **Section 6.4**, the *RetrieveConfigData* script was run to retrieve Communication Manager configuration data about stations and store it in the Avaya CM supplemental database. To retrieve an inventory of all stations on Communication Manager, drag the *PhoneInventory* script to the **Active SPE** item in the tree view. This script generates a data file with the phone inventory as shown below. This data file is stored on the AppManager server in the **Program Files\NetIQ\Temp\NetIQ_debug** directory by default. If AppManager is installed on a 64 bit machine then the default path needs to be changed to **Program Files(x86)\NetIQ\Temp\NetIQ_debug** in the properties page of the *PhoneInventory* script.

```
|
==================================
Active SPE,Select By,Criteria,Status Filter,Start Time
----------,---------,--------,-------------,----------
DevCM,Extension,,Any,2014-09-03 15:58:36
==================================



Extension,StationType,Name,Building,Floor,Room,Status,Status Time
---------,-----------,----,--------,----,----,------,-----------
"3035389089","9611","Test9089","Unknown","Unknown","Unknown","UnR
egistered","2014-09-03 15:58:36"
"3035389090","9650SIP","Test9090,
Test","Unknown","Unknown","Unknown","UnRegistered","2014-09-03
15:58:36"
"3035389091","9650SIP","Test9091,
Test","Unknown","Unknown","Unknown","UnRegistered","2014-09-03
15:58:36"
"3035389092","9650SIP","Test9092,
Test","Unknown","Unknown","Unknown","UnRegistered","2014-09-03
15:58:36"
"3035389093","9650SIP","Test9093,
Test","Unknown","Unknown","Unknown","UnRegistered","2014-09-03
15:58:36"
"3035389094","9650SIP","Test9094,
Test","Unknown","Unknown","Unknown","UnRegistered","2014-09-03
15:58:36"
"3035389095","9650SIP","Test9095,
Test","Unknown","Unknown","Unknown","UnRegistered","2014-09-03
15:58:36"
"3035389096","9650SIP","9650SIP","9650SIP","9650SIP","9650SIP","U
nRegistered","2014-09-03 15:58:36"
"3035389097","9650SIP","Test9097,
Test","Unknown","Unknown","Unknown","UnRegistered","2014-09-03
15:58:36"
"3035389098","9650SIP","Test9098,
```

- To capture SNMP traps, drag *SNMPTrap* script into the **SNMP** item in the tree view. SNMP traps will be displayed in the **Events** tab of AppManager. To view a detailed message of the SNMP traps, right-mouse click on and SNMP trap and then select **Detailed Message** from the pop-up menu. Below is a sample SNMP detailed message.

Event Properties: 1345

Event | Message | Comments

Trap G3-AVAYA-TRAP::alarmResolved received on 9/7/2014 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	09/07/2014 @ 15:27:37
New/Modified alarm	New
Derived G3 Alarm Port	service crond was successfully restarted.

Varbinds		
OID	**Type**	**Value**
G3-AVAYA-MIB::g3clientExternalName [1.3.6.1.4.1.6889.2.8.2.1.1.1.4]	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]		
G3-AVAYA-MIB::g3alarmsErrorCodes [1.3.6.1.4.1.6889.2.8.1.4.6.1.28]		

8. Conclusion

These Application Notes describe the steps required to configure NetIQ AppManager to interoperate with Avaya Aura® Communication Manager, including establishing a CDR link, sending RTCP data from the Avaya H.323 and SIP Telephones to NetIQ AppManager, enabling SNMP for collecting configuration data, and enabling AppManager as an SNMP trap receiver. All tests passed as noted in **Section 2.2**.

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.

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

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, June 2014, Release 6.3, Issue 12.0, Document Number 555-245-205.

[3] *NetIQ AppManager for Avaya Communication Manager Management Guide*, December 2013, available at : https://www.netiq.com/documentation/appmanager-modules/pdfdoc/appmanagerforavayacm/appmanagerforavayacm.pdf

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.