Avaya Solution & Interoperability Test Lab

Application Notes for NetIQ AppManager 8.2 with Avaya Communication Server 1000 Release 7.6 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya Communication Server 1000 Release 7.6 and the NetIQ AppManager 8.2. During compliance testing, the AppManager was able to deliver systems management solution for the Communication Server 1000 system using File Transfer Protocol and Simple Network Management Protocol. This test was performed to verify the basic interaction between Avaya Communication Server 1000 and NetIQ AppManager to ensure there is no adverse impact on the Communication Server 1000 system or the quality of phone calls.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

This is the application notes for Avaya Communication Server 1000 Release 7.6 (hereafter referred to as Communication Server 1000) and the NetIQ AppManager 8.2 (hereafter referred to as AppManager). This test was performed to verify the basic interaction between Communication Server 1000 and AppManager to ensure that there is no adverse impact on the Communication Server 1000 system while AppManager is running and accessing Communication Server 1000 systems. The AppManager is a systems management tool that provides monitoring, reporting, analysis, diagnostics and resolution to the system it is connected to using File Transfer Protocol (FTP) and Simple Network Management Protocol (SNMP).

2. General Test Approach and Test Results

The focus of this interoperability compliance testing was primarily to verify the basic functionalities of AppManager such as System Discovery, Monitoring System Health, BMZ_CallQuality and Telephone Inventory. AppManager can work with the Communication Server 1000 system with no adverse impact on the Communication Server 1000 system or any other management interfaces.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

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

- Discovery of Avaya Communication Server 1000 devices, including CoRes (Call Server and Signaling Server) card and SIP Line Gateway card.
- Retrieving information from Avaya Communication Server 1000 devices such as software version, hardware platform.
- Monitor health of Avaya Communication Server 1000 devices (including SIP Line resources) such as HealthCheck and Alarms.
- Telephone Inventory is retrieved from Avaya Communication Server 1000.
- OM Reports are retrieved from Avaya Communication Server 1000.
- BMZ_CallQuality metrics is retrieved from Avaya Communication Server 1000.
- All AppManager module scripts are running at the same time with its default values.

2.2. Test Results

The objectives outlined in S**ection 2.1** were verified and met. All tests were executed and passed.

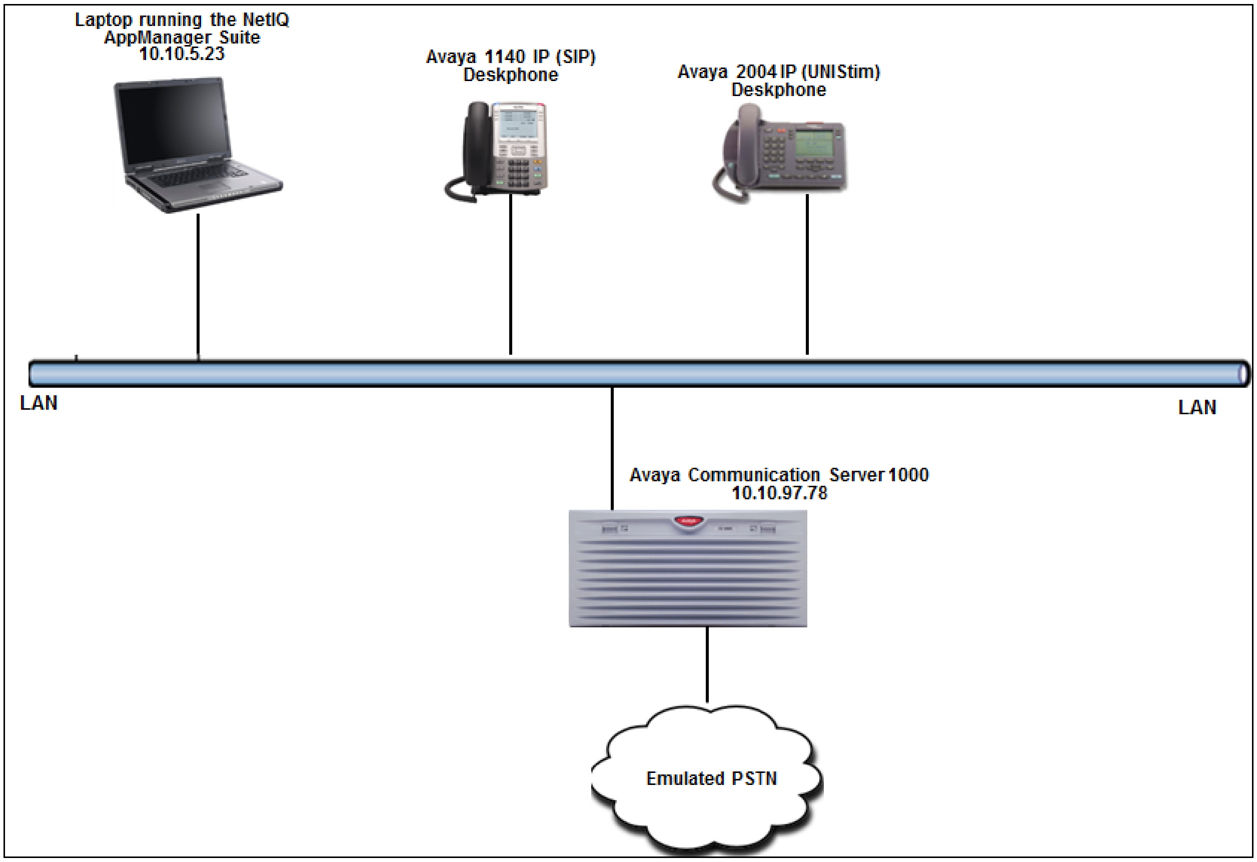
2.3. Support

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

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

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing event between Avaya Communication Server 1000 Release 7.6 and AppManager 8.2.



Laptop running the NetIQ AppManager Suite 10.10.5.23
Avaya 1140 IP (SIP) Deskphone
Avaya 2004 IP (UNIStim) Deskphone
LAN
LAN
Avaya Communication Server 1000 10.10.97.78
Emulated PSTN

Figure 1: Test Solution Configuration

4. Equipment and Software Validated

Equipment/Software	Release/Version
Avaya Communication Server 1000	SW Version : 7.65 SP3
Avaya IP Deskphones: 2004 (UNIStim) 1140E (SIP)	 0602B76 04.03.12
NetIQ AppManager Server: Server hosting AppManager AppManager NetIQ NortelCS module	 Windows Server 2003 SP2 SW Version 8.2 (Build 8.2.3.37) SW Version 7.4.78.0 (Hotfix 7015022)

5. Configuring the Communication Server 1000

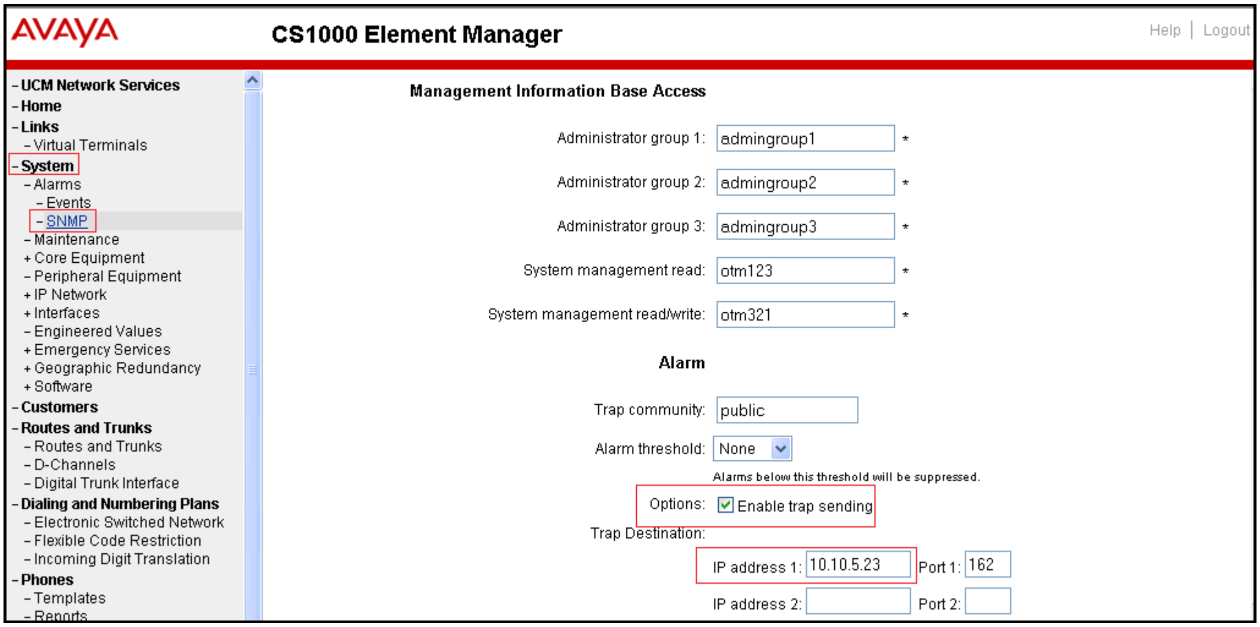
This section describes the steps to configure Communication Server 1000 to work with the AppManager.

Here is a summary of Communication Server 1000 Configuration:

- IP address of AppManager machine is configured as a trap receiver.
- Setting QoS Zone and Call Basis Threshold Parameters.
- Setting Zone Notification Levels.
- Insecure shell access enabled.
- Configuring the Call Server to inventory Phones.

5.1. AppManager Server Configured as a Trap Receiver

Access the Communication Server 1000 Element Manager via the Unified Communication Manager or System Manager (not shown). Navigate to **System → SNMP** and configure the IP address of the Server hosting the AppManager application as a trap receiver which is **Trap Destination** as shown below. Under the **Options** field check the box for E*nable trap sending*. All other fields are at default values. Click on **Save** (not shown) to complete the configuration.



Management Information Base Access

Administrator group 1: admingroup1 *

Administrator group 2: admingroup2 *

Administrator group 3: admingroup3 *

System management read: otm123 *

System management read/write: otm321 *

Alarm

Trap community: public

Alarm threshold: None

Alarms below this threshold will be suppressed.

Options: ☑ Enable trap sending

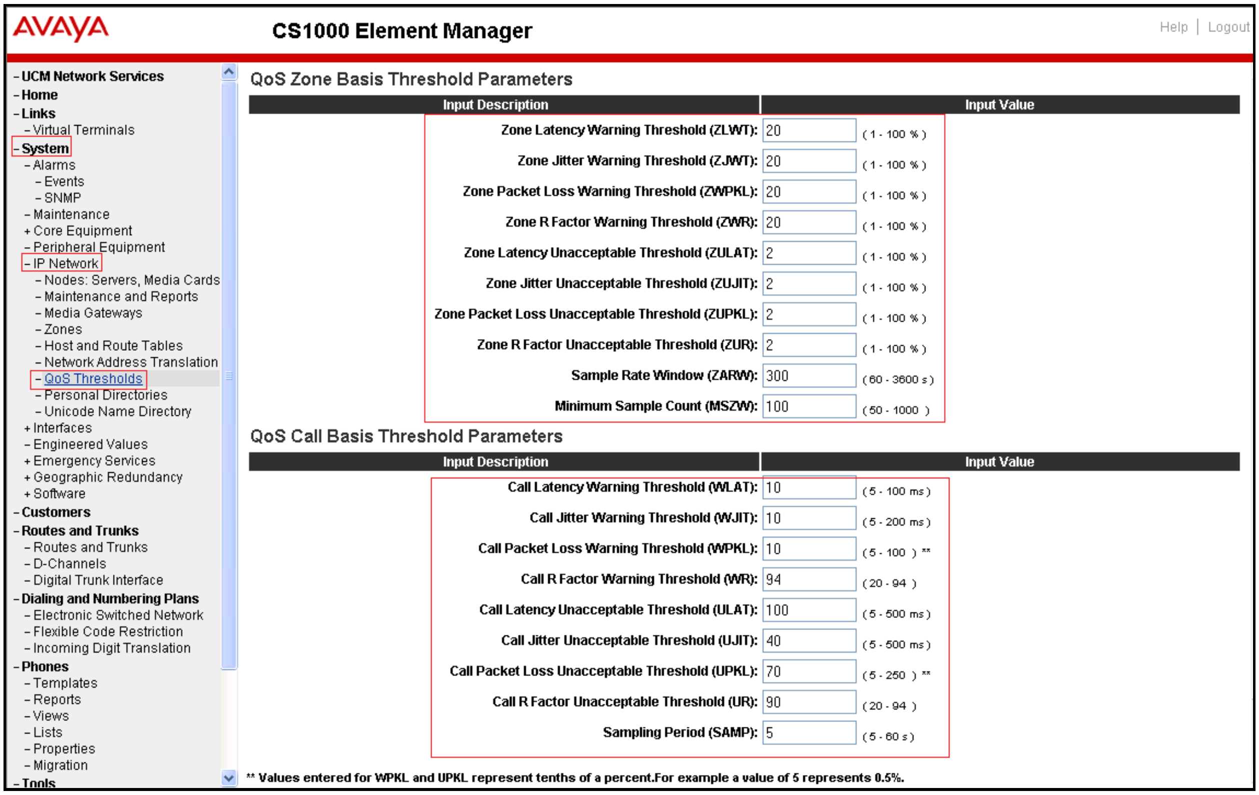
Trap Destination:

IP address 1: 10.10.5.23 Port 1: 162

IP address 2: Port 2:

5.2. Setting QoS Zone and Call Basis Threshold Parameters

Access the Communication Server 1000 Element Manager via the Unified Communication Manager or System Manager (not shown). Navigate to **System → IP Network → QoS Thresholds**. Configure the values marked in red under the **QoS Zone Basis Threshold Parameters** and **QoS Call Basis Threshold Parameters** section as shown below. All quality metrics that fall outside of the thresholds are identified by the Alarms script. Click on **Save** (not shown) to complete the configuration.



QoS Zone Basis Threshold Parameters

Input Description	Input Value	
Zone Latency Warning Threshold (ZLWT):	20	(1 - 100 %)
Zone Jitter Warning Threshold (ZJWT):	20	(1 - 100 %)
Zone Packet Loss Warning Threshold (ZWPKL):	20	(1 - 100 %)
Zone R Factor Warning Threshold (ZWR):	20	(1 - 100 %)
Zone Latency Unacceptable Threshold (ZULAT):	2	(1 - 100 %)
Zone Jitter Unacceptable Threshold (ZUJIT):	2	(1 - 100 %)
Zone Packet Loss Unacceptable Threshold (ZUPKL):	2	(1 - 100 %)
Zone R Factor Unacceptable Threshold (ZUR):	2	(1 - 100 %)
Sample Rate Window (ZARW):	300	(60 - 3600 s)
Minimum Sample Count (MSZW):	100	(50 - 1000)

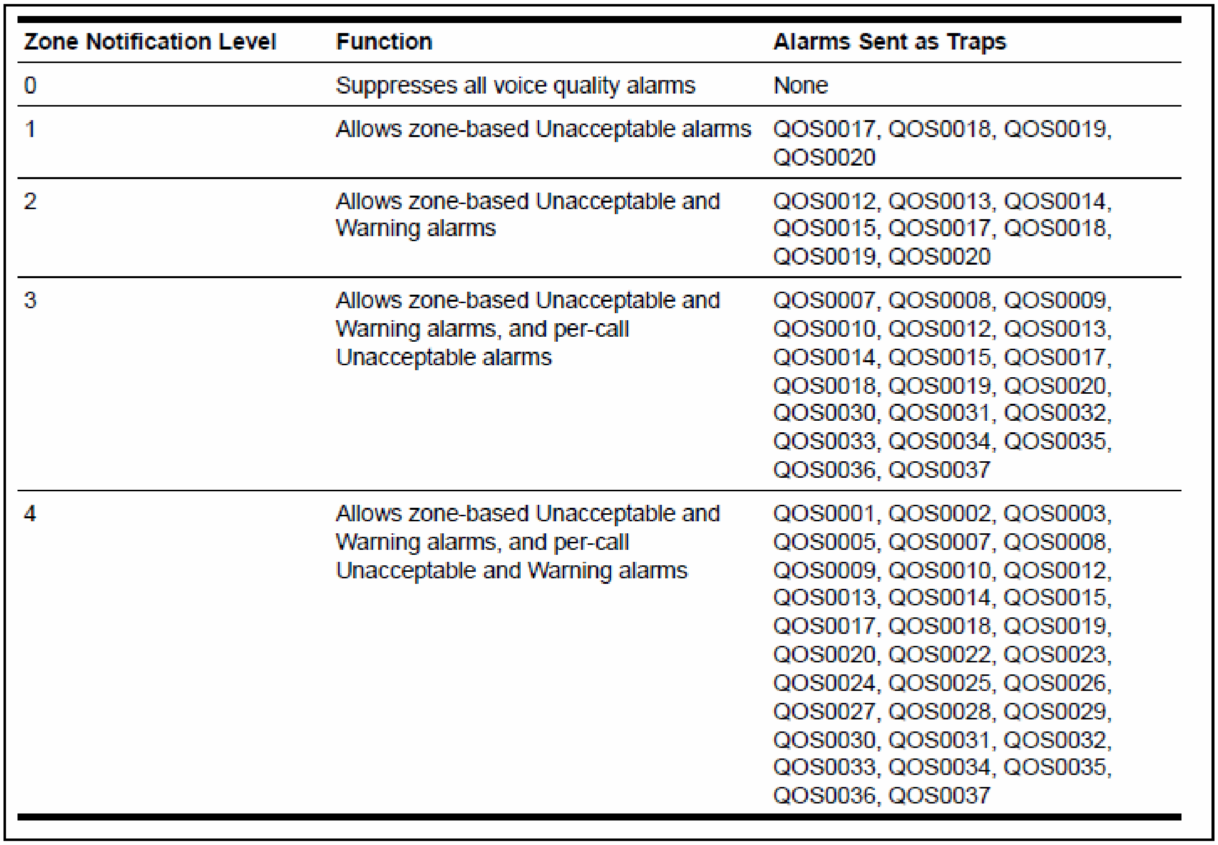
QoS Call Basis Threshold Parameters

Input Description	Input Value	
Call Latency Warning Threshold (WLAT):	10	(5 - 100 ms)
Call Jitter Warning Threshold (WJIT):	10	(5 - 200 ms)
Call Packet Loss Warning Threshold (WPKL):	10	(5 - 100) **
Call R Factor Warning Threshold (WR):	94	(20 - 94)
Call Latency Unacceptable Threshold (ULAT):	100	(5 - 500 ms)
Call Jitter Unacceptable Threshold (UJIT):	40	(5 - 500 ms)
Call Packet Loss Unacceptable Threshold (UPKL):	70	(5 - 250) **
Call R Factor Unacceptable Threshold (UR):	90	(20 - 94)
Sampling Period (SAMP):	5	(5 - 60 s)

** Values entered for WPKL and UPKL represent tenths of a percent.For example a value of 5 represents 0.5%.

5.3. Setting Zone Notification Levels

Zone notification levels determine which QoS alarms are sent to the AppManager as SNMP traps. The following **Table 1** below identifies the notification levels and the corresponding alarms sent as SNMP traps. User can refer to **Table 1** and set the Notification level accordingly as explained below.



Zone Notification Level	Function	Alarms Sent as Traps
0	Suppresses all voice quality alarms	None
1	Allows zone-based Unacceptable alarms	QOS0017, QOS0018, QOS0019, QOS0020
2	Allows zone-based Unacceptable and Warning alarms	QOS0012, QOS0013, QOS0014, QOS0015, QOS0017, QOS0018, QOS0019, QOS0020
3	Allows zone-based Unacceptable and Warning alarms, and per-call Unacceptable alarms	QOS0007, QOS0008, QOS0009, QOS0010, QOS0012, QOS0013, QOS0014, QOS0015, QOS0017, QOS0018, QOS0019, QOS0020, QOS0030, QOS0031, QOS0032, QOS0033, QOS0034, QOS0035, QOS0036, QOS0037
4	Allows zone-based Unacceptable and Warning alarms, and per-call Unacceptable and Warning alarms	QOS0001, QOS0002, QOS0003, QOS0005, QOS0007, QOS0008, QOS0009, QOS0010, QOS0012, QOS0013, QOS0014, QOS0015, QOS0017, QOS0018, QOS0019, QOS0020, QOS0022, QOS0023, QOS0024, QOS0025, QOS0026, QOS0027, QOS0028, QOS0029, QOS0030, QOS0031, QOS0032, QOS0033, QOS0034, QOS0035, QOS0036, QOS0037

Table 1: Zone Notification Level

If a zone notification level is not specifically designated, all QoS alarms fall into the default level which is **0**. Notification level **4** should be enabled in order to receive all possible QoS alarms for that zone. To set a zone notification level, issue the following command from the Communication Server 1000 command line in **LD 117**.

```
>ld 117
=>  CHG ZQNL 1  4; In this example 1 is the zone and 4 is the level.
```

5.4. Enabling Insecure Shell Access

For the integration to be successful between the Communication Server 1000 and AppManager, the Telnet Service on Communication Server 1000 has to be turned on. This is because AppManager does not support Secure Shell (SSH) access and requires Telnet access.

To enable Telnet, which is part of the insecure Shell access on Signalling Server (SS):
Log in to the Linux-based Signalling Server and issue the following command,

```
[admin@cpppm3 ~]$ harden telnet on
```

To enable Telnet, which is part of the insecure Shell access on Communication Server 1000, Log in to Communication Server 1000 command line and issue the following command from overlay **LD 117**,

```
      >ld 117
      => ENL SHELLS INSECURE
```

5.5. Configuring the Call Server to Count IP Phones

The PhoneInventory Knowledge Script job uses SNMP to query the Entity MIB on the Call Server and counts the number of IP telephones in the Entity MIB. This is used by the AppManager application for licensing the product against the number of sets that will be monitored in the Communication Server 1000. Inventory of the sets can be reported by running the following commands in **LD 117** of the Communication Server 1000 through Command Line Interface.

- Communication Server 1000 to generate the inventory report once every midnight

```
INV MIDNIGHT SETS
```

- Communication Server 1000 to include the telephones from the inventory report in the Entity MIB

```
INV ENTITY SETS ON
```

- Optional: Communication Server 1000 can also generate the inventory report immediately if required. The two above mentioned commands generate an inventory report at midnight. If reports need to be run in real time, the following command from **LD 117** can be used.

```
INV GENERATE SETS
```

Note

- Issue these commands before running the **Discovery_NortelCS** Knowledge Script from the AppManager Application in **Section 6.3**.
- The inventory report can take hours to complete, based on the number of phones. The task normally runs at midnight at a low priority, and should not interfere with call processing.

6. AppManager Configuration

This section describes the steps to configure AppManager for Communication Server 1000. This section assumes that AppManager has been installed. For more information about installing AppManager or about AppManager system requirements, refer to **Section 9**. The configurations explained are,

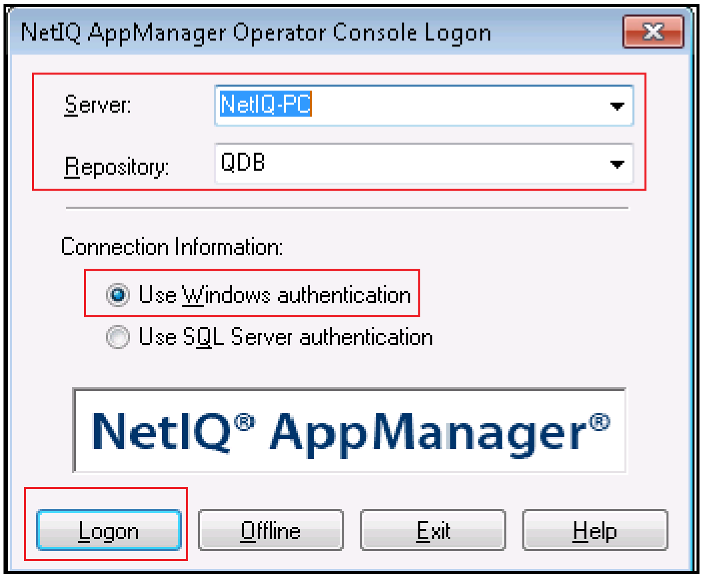
- Configuring SNMP community strings.
- Disabling NetIQ trap receiver.
- AppManager configuration for discovery of Communication Server 1000 devices.
- AppManager configuration to collect Health Check data of Communication Server 1000 devices.

6.1. Configuring SNMP Community Strings

To enable AppManager to use SNMP to access Avaya Communication Server 1000 devices, the SNMP community strings are required to be configured in the AppManager Security Manager.

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.



NetIQ AppManager Operator Console Logon

Server: NetIQ-PC

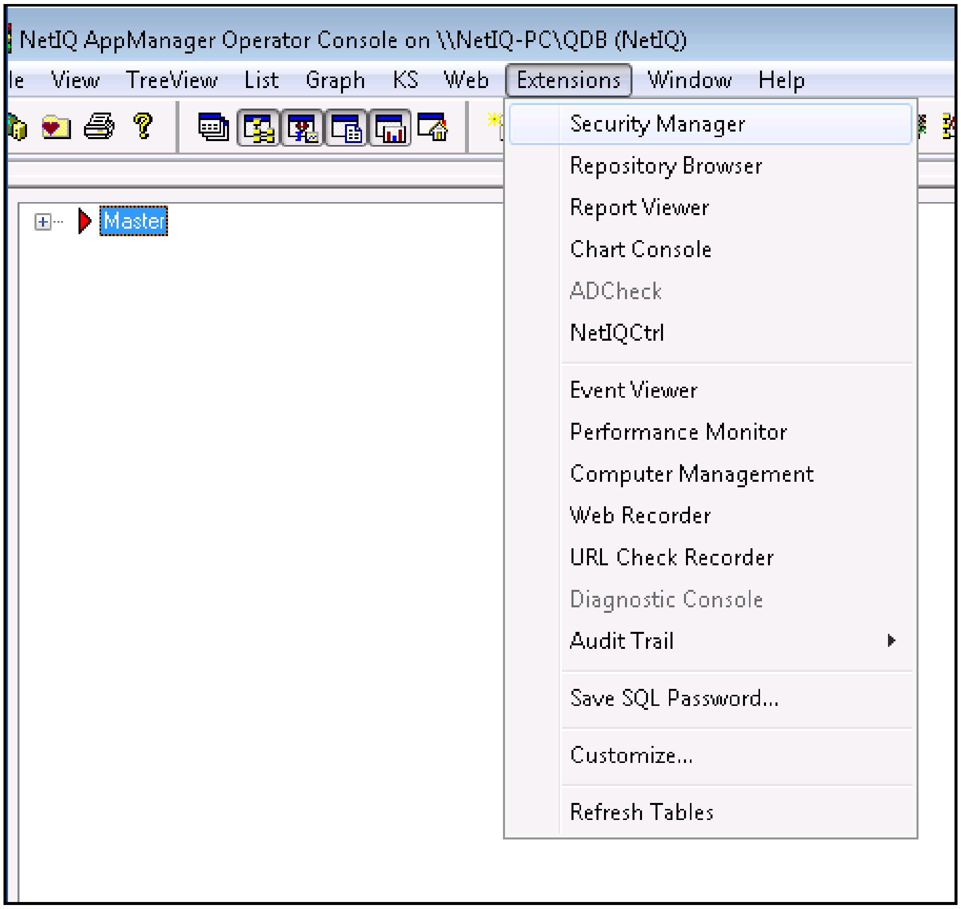
Repository: QDB

Connection Information:

● Use Windows authentication

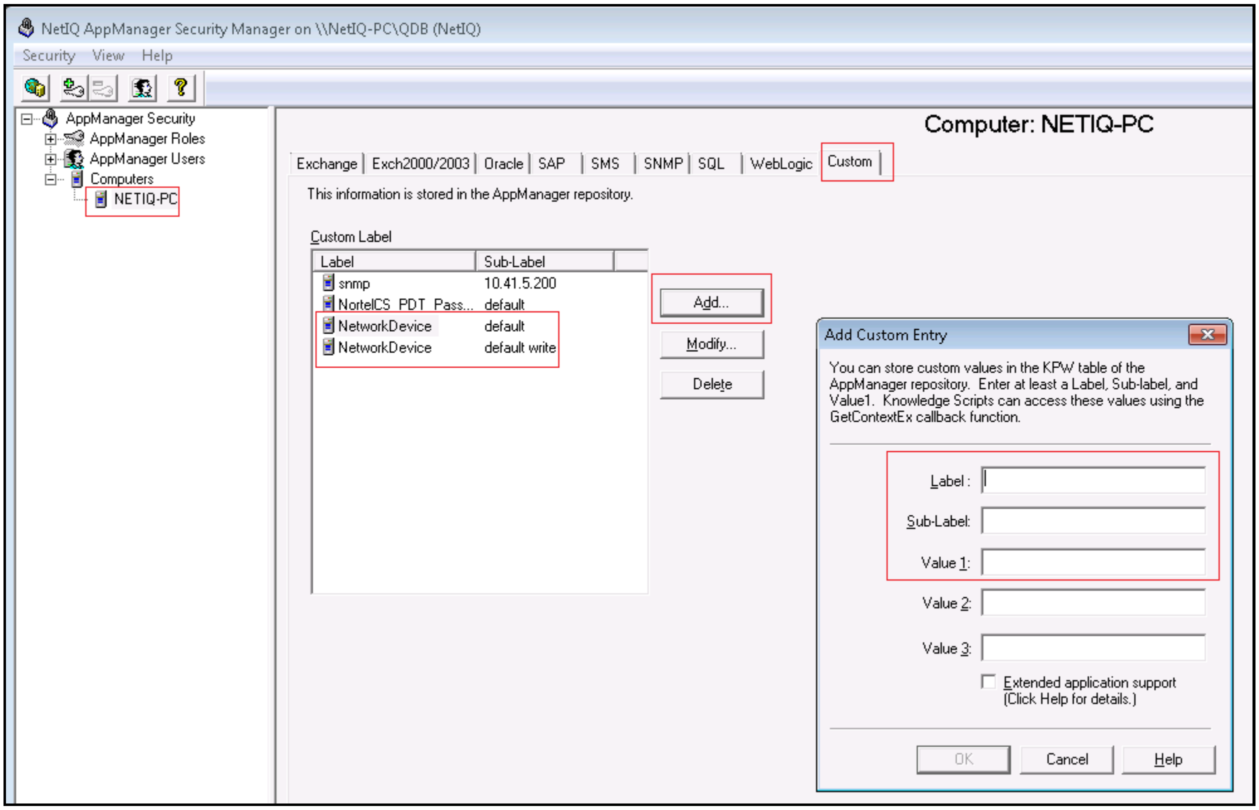
○ Use SQL Server authentication

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



Select the **NETIQ-PC** under **Computers** as seen on the left window pane of screen seen below. Under the **Custom** tab, add the **Custom Label** as required and the appropriate community string in **Value 1** (refer to **Section 5.1** for the System management values for read and read/write) and then click on the **Apply** (not shown) button when completed.

- For all devices that use the same read-only community string, type *default*.
  Use the *default* **Sub-Label** for Call Server, Network Routing Server (NRS), Element Manager (EM), and co-resident devices.
- For all devices that use the same read/write community string, type *default write*.
  Use the *default write* sub-label for all Signalling Servers, VGMCs, MGCs, and MC32Ss.



This information is stored in the AppManager repository.

Custom Label

Label	Sub-Label
snmp	10.41.5.200
NortelCS_PDT_Pass...	default
NetworkDevice	default
NetworkDevice	default write

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.)

6.2. Disabling NetIQ Trap Receiver

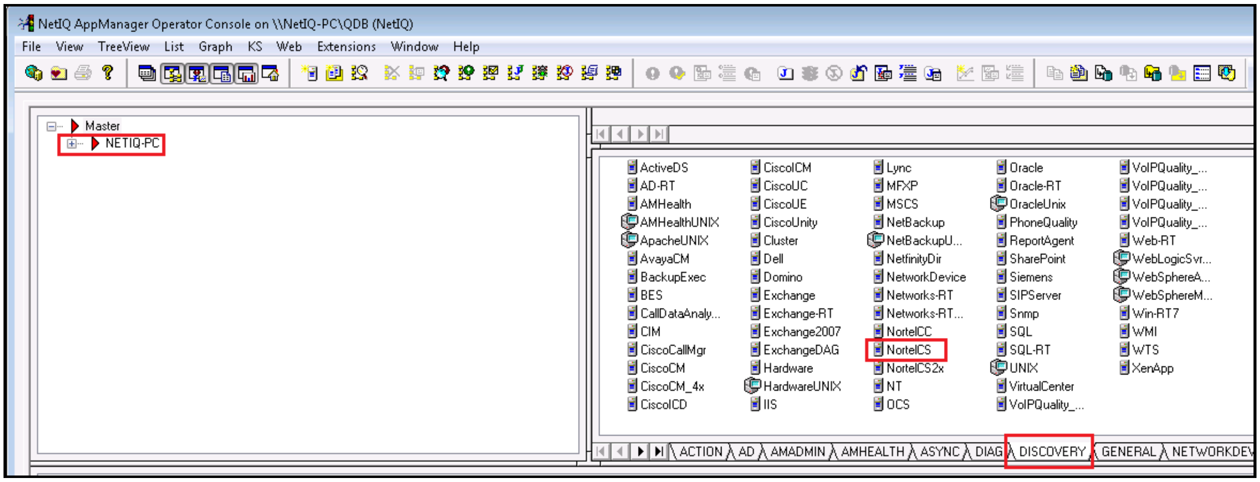
Disable the **NetIQ Trap Receiver** and enable the **SNMP Trap Service** on the AppManager server as follows,

- Access the **Services** of the NetIQ server by navigating to **Start → Administrative Tools → Services** (not shown).
- From the **Services** window select **NetIQ Trap Receiver** service and disable it (not shown).
- From the **Services** window select **SNMP Trap Service** and configure it to start automatically (not shown).
- From the **Services** window select **NetIQ AppManager Client Communication Manager** and **NetIQ App Manager Client Resource Monitor** and restart these two services (not shown).

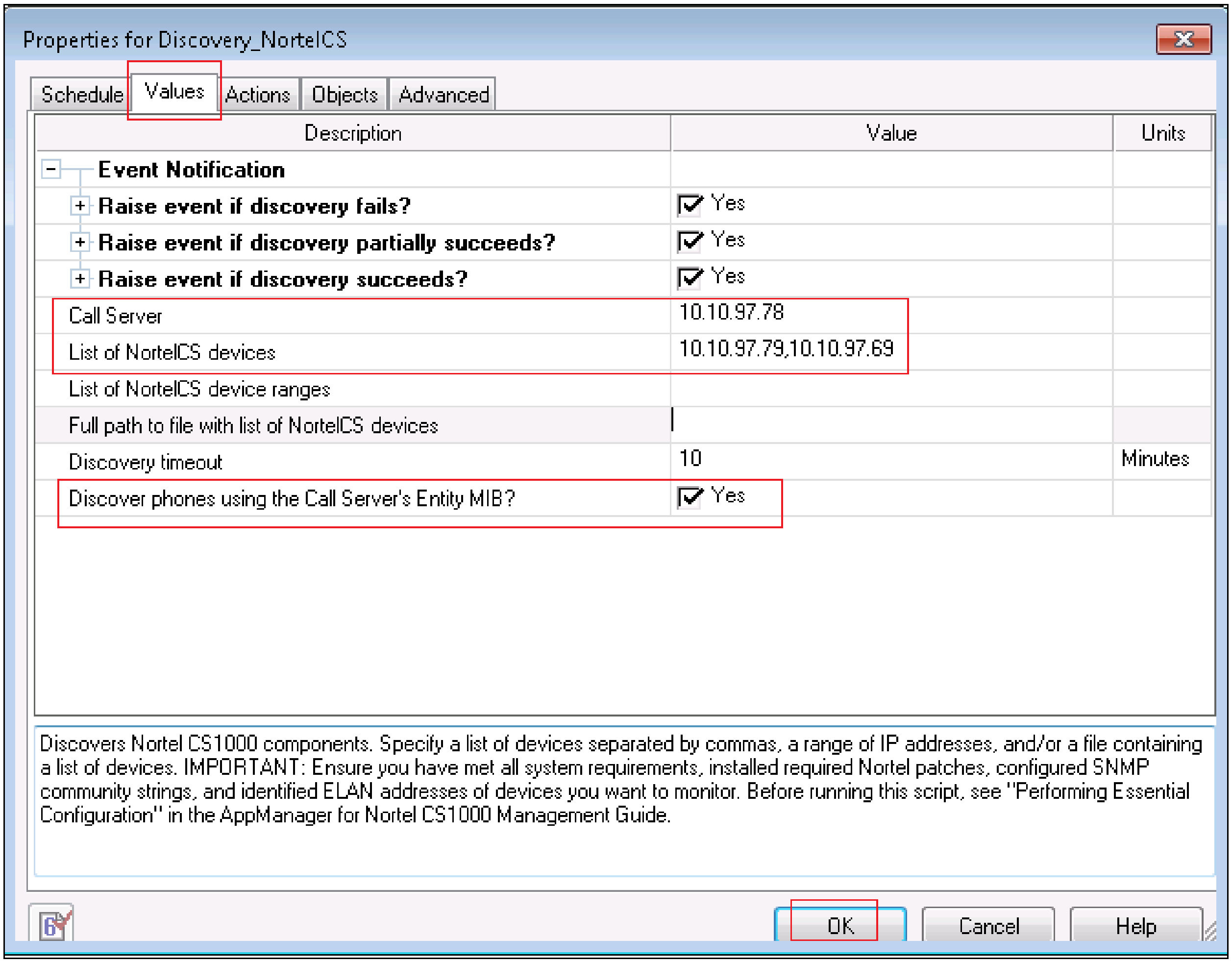
6.3. AppManager Configuration for Discovery of Communication Server 1000 Devices

This section explains the configuration in the AppManager where the required Knowledge Script is selected and the values configured so that the elements of Communication Server 1000 can be discovered.

During the compliance testing the **NortelCS** Knowledge Script was used. To access the **NortelCS** Knowledge Script, open the Operator Console window as explained in **Section 6.1**. Click on **DISCOVERY** tab shown below. Select **NortelCS** that is seen on the right hand window pane and drag it to the **NETIQ-PC** that is on the left hand window pane.



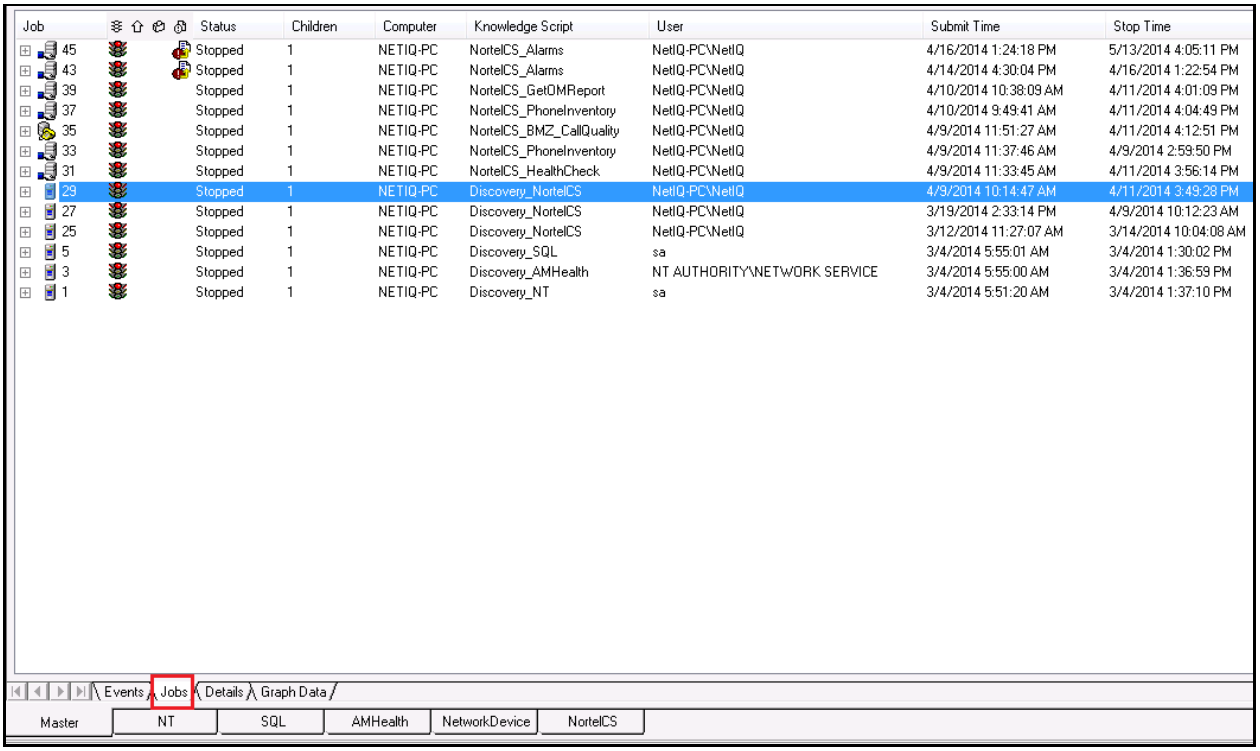
When the required Knowledge Script is selected and dragged the **Properties for Discovery_NortelCS** window automatically pops up as shown below. From this window select the **Values** tab and configure the **Call Server** IP address value and **List of NortelCS devices** values. Ensure the box for **Discover phones using the Call Server's Entity MIB?** is selected. Click on **OK** to continue.



Description	Value	Units
Event Notification		
Raise event if discovery fails?	☑ Yes	
Raise event if discovery partially succeeds?	☑ Yes	
Raise event if discovery succeeds?	☑ Yes	
Call Server	10.10.97.78	
List of NortelCS devices	10.10.97.79,10.10.97.69	
List of NortelCS device ranges		
Full path to file with list of NortelCS devices		
Discovery timeout	10	Minutes
Discover phones using the Call Server's Entity MIB?	☑ Yes	

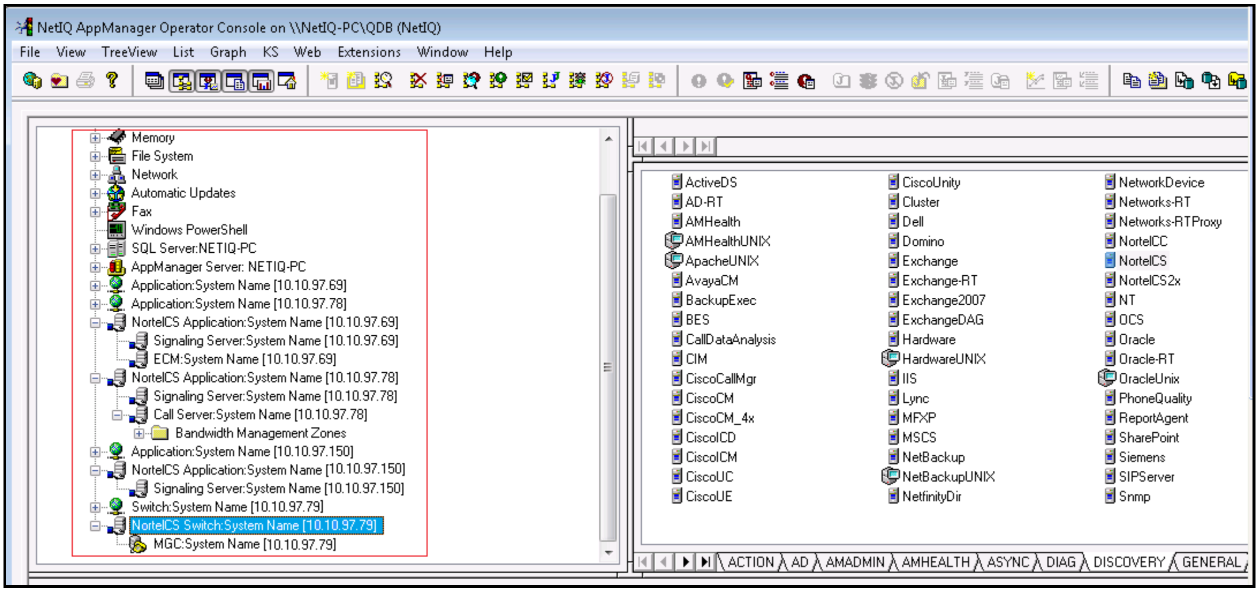
Discovers Nortel CS1000 components. Specify a list of devices separated by commas, a range of IP addresses, and/or a file containing a list of devices. IMPORTANT: Ensure you have met all system requirements, installed required Nortel patches, configured SNMP community strings, and identified ELAN addresses of devices you want to monitor. Before running this script, see "Performing Essential Configuration" in the AppManager for Nortel CS1000 Management Guide.

Once the properties are configured, a job is automatically created that will run and discovers all Communication Server 1000 elements. Screen below shows an example of the job whose status is stopped after the job has been completed. However, a user can start the job manually by clicking on the Traffic Light symbol.



Job	Status	Children	Computer	Knowledge Script	User	Submit Time	Stop Time
45	Stopped	1	NETIQ-PC	NortelCS_Alarms	NetIQ-PC\NetIQ	4/16/2014 1:24:18 PM	5/13/2014 4:05:11 PM
43	Stopped	1	NETIQ-PC	NortelCS_Alarms	NetIQ-PC\NetIQ	4/14/2014 4:30:04 PM	4/16/2014 1:22:54 PM
39	Stopped	1	NETIQ-PC	NortelCS_GetOMReport	NetIQ-PC\NetIQ	4/10/2014 10:38:09 AM	4/11/2014 4:01:09 PM
37	Stopped	1	NETIQ-PC	NortelCS_PhoneInventory	NetIQ-PC\NetIQ	4/10/2014 9:49:41 AM	4/11/2014 4:04:49 PM
35	Stopped	1	NETIQ-PC	NortelCS_BMZ_CallQuality	NetIQ-PC\NetIQ	4/9/2014 11:51:27 AM	4/11/2014 4:12:51 PM
33	Stopped	1	NETIQ-PC	NortelCS_PhoneInventory	NetIQ-PC\NetIQ	4/9/2014 11:37:46 AM	4/9/2014 2:59:50 PM
31	Stopped	1	NETIQ-PC	NortelCS_HealthCheck	NetIQ-PC\NetIQ	4/9/2014 11:33:45 AM	4/11/2014 3:56:14 PM
29	Stopped	1	NETIQ-PC	Discovery_NortelCS	NetIQ-PC\NetIQ	4/9/2014 10:14:47 AM	4/11/2014 3:49:28 PM
27	Stopped	1	NETIQ-PC	Discovery_NortelCS	NetIQ-PC\NetIQ	3/19/2014 2:33:14 PM	4/9/2014 10:12:23 AM
25	Stopped	1	NETIQ-PC	Discovery_NortelCS	NetIQ-PC\NetIQ	3/12/2014 11:27:07 AM	3/14/2014 10:04:08 AM
5	Stopped	1	NETIQ-PC	Discovery_SQL	sa	3/4/2014 5:55:01 AM	3/4/2014 1:30:02 PM
3	Stopped	1	NETIQ-PC	Discovery_AMHealth	NT AUTHORITY\NETWORK SERVICE	3/4/2014 5:55:00 AM	3/4/2014 1:36:59 PM
1	Stopped	1	NETIQ-PC	Discovery_NT	sa	3/4/2014 5:51:20 AM	3/4/2014 1:37:10 PM

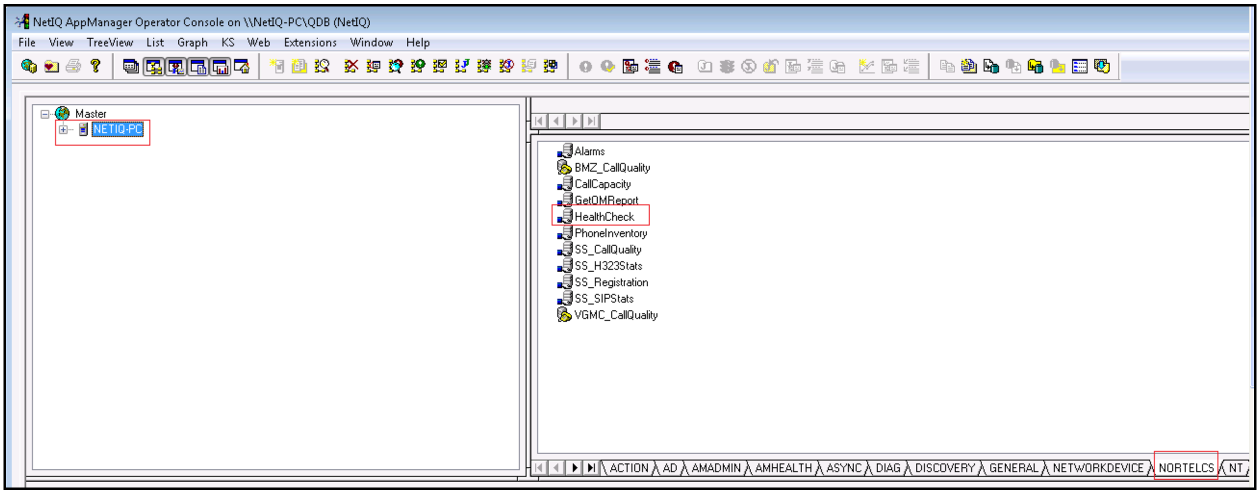
Screen below shows the window with the devices of Communication Server 1000 discovered during compliance testing.


NetIQ AppManager Operator Console on \\NetIQ-PC\QDB (NetIQ)
File View TreeView List Graph KS Web Extensions Window Help
Memory
File System
Network
Automatic Updates
Fax
Windows PowerShell
SQL Server:NETIQ-PC
AppManager Server: NETIQ-PC
Application:System Name [10.10.97.69]
Application:System Name [10.10.97.78]
NortelCS Application:System Name [10.10.97.69]
Signaling Server:System Name [10.10.97.69]
ECM:System Name [10.10.97.69]
NortelCS Application:System Name [10.10.97.78]
Signaling Server:System Name [10.10.97.78]
Call Server:System Name [10.10.97.78]
Bandwidth Management Zones
Application:System Name [10.10.97.150]
NortelCS Application:System Name [10.10.97.150]
Signaling Server:System Name [10.10.97.150]
Switch:System Name [10.10.97.79]
NortelCS Switch:System Name [10.10.97.79]
MGC:System Name [10.10.97.79]
ActiveDS
AD-RT
AMHealth
AMHealthUNIX
ApacheUNIX
AvayaCM
BackupExec
BES
CallDataAnalysis
CIM
CiscoCallMgr
CiscoCM
CiscoCM_4x
CiscoICD
CiscoICM
CiscoUC
CiscoUE
CiscoUnity
Cluster
Dell
Domino
Exchange
Exchange-RT
Exchange2007
ExchangeDAG
Hardware
HardwareUNIX
IIS
Lync
MFXP
MSCS
NetBackup
NetBackupUNIX
NetfinityDir
NetworkDevice
Networks-RT
Networks-RTProxy
NortelCC
NortelCS
NortelCS2x
NT
OCS
Oracle
Oracle-RT
OracleUnix
PhoneQuality
ReportAgent
SharePoint
Siemens
SIPServer
Snmp
ACTION
AD
AMADMIN
AMHEALTH
ASYNC
DIAG
DISCOVERY
GENERAL

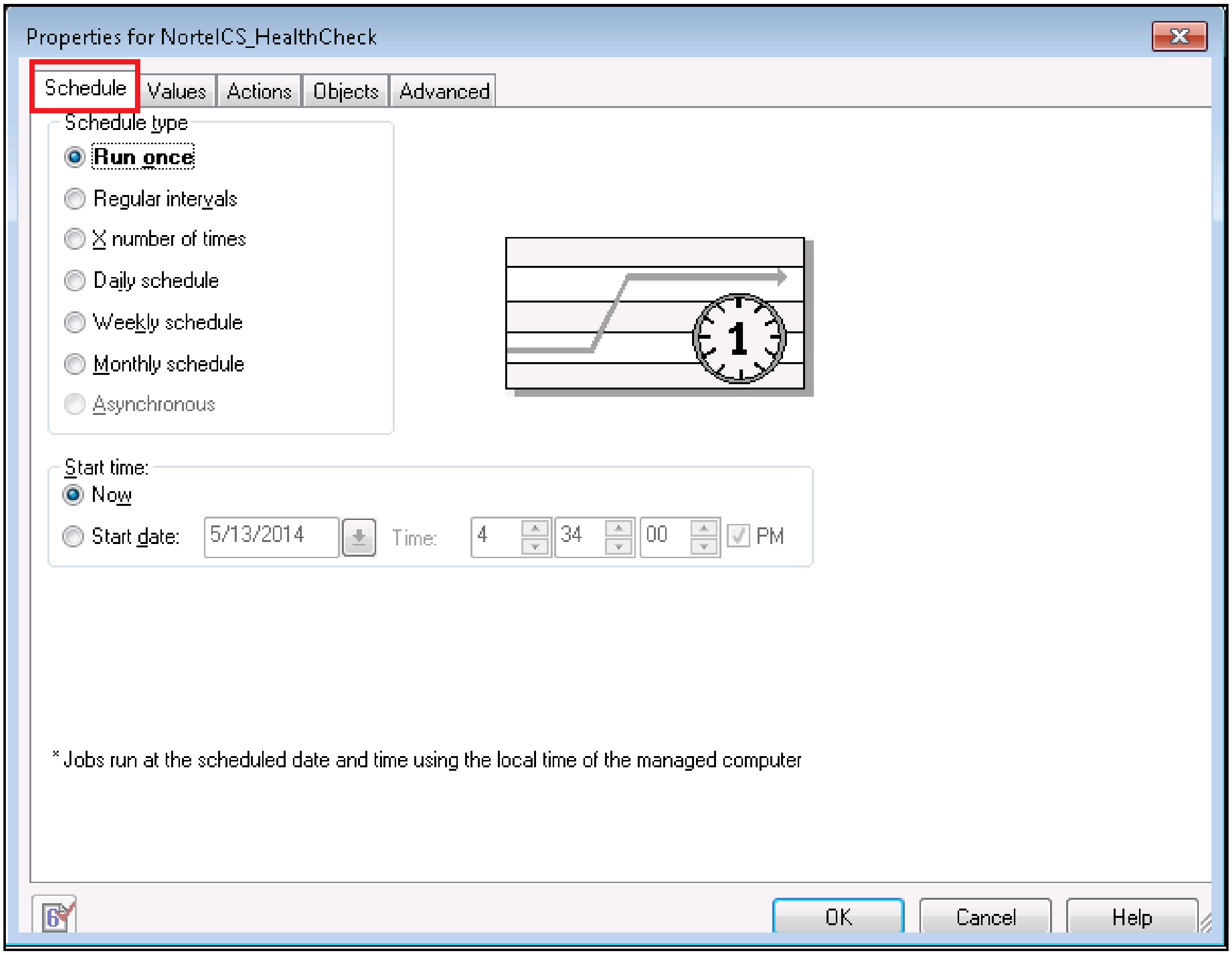
6.4. AppManager Configuration to Run Health Check Report

This section explains how to configure the AppManager to run the Health Check report. The Health Check report is one of the several Knowledge Scripts under the NortelCS module.

In the Operator Console window of the AppManager make sure that NortelCS Knowledge Script has been successfully executed and all CS 1000 devices can be found on the left hand pane and all the available Knowledge Scripts can be found on the right hand pane of the AppManager tree view as shown in screen below. Select the **HealthCheck** Knowledge Script seen on the right hand window pane and drag it to the **NETIQ-PC** that is seen on the left hand window pane of screen shown below.



When the required HealthCheck script is selected and dragged the **Properties for NortelCS_HealthCheck** window automatically pops up as shown below. From this window select the **Schedule** tab and select the job to **Run once**.



Properties for NortelCS_HealthCheck

Schedule type

● Run once

○ Regular intervals

○ X number of times

○ Daily schedule

○ Weekly schedule

○ Monthly schedule

○ Asynchronous

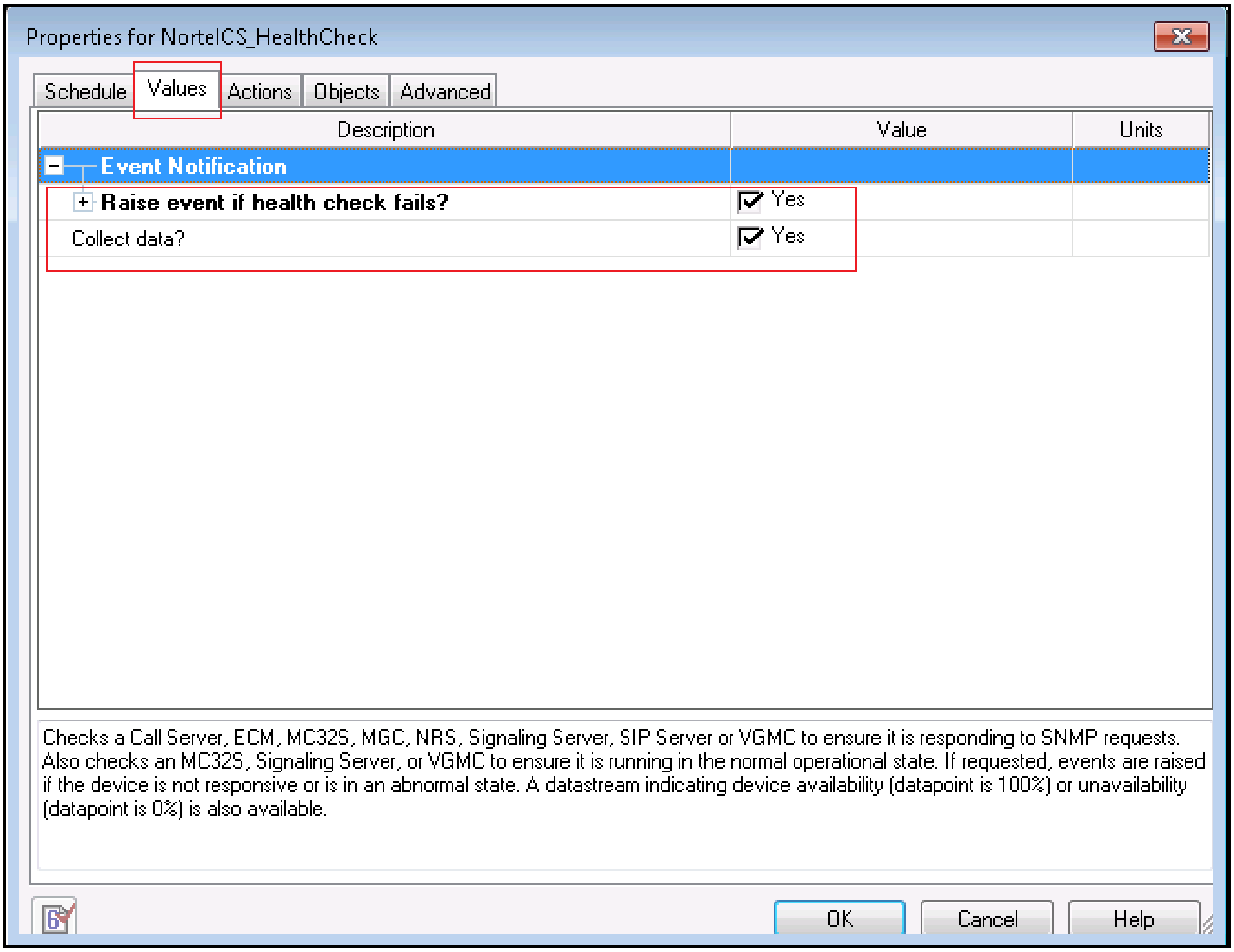
Start time:

● Now

○ Start date: 5/13/2014 Time: 4 34 00 ☑ PM

* Jobs run at the scheduled date and time using the local time of the managed computer

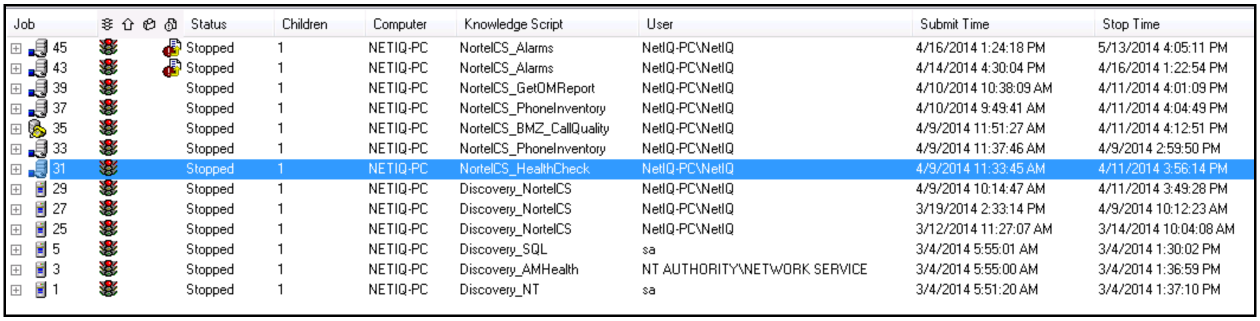
From the **Values** tab of the properties window, check the **Yes** box for **Raise event if health check fails** and **Collect data** fields. Leave the rest of the values at default. Click on **OK** to complete the configuration as shown below.



Description	Value	Units
Event Notification		
Raise event if health check fails?	☑ Yes	
Collect data?	☑ Yes	

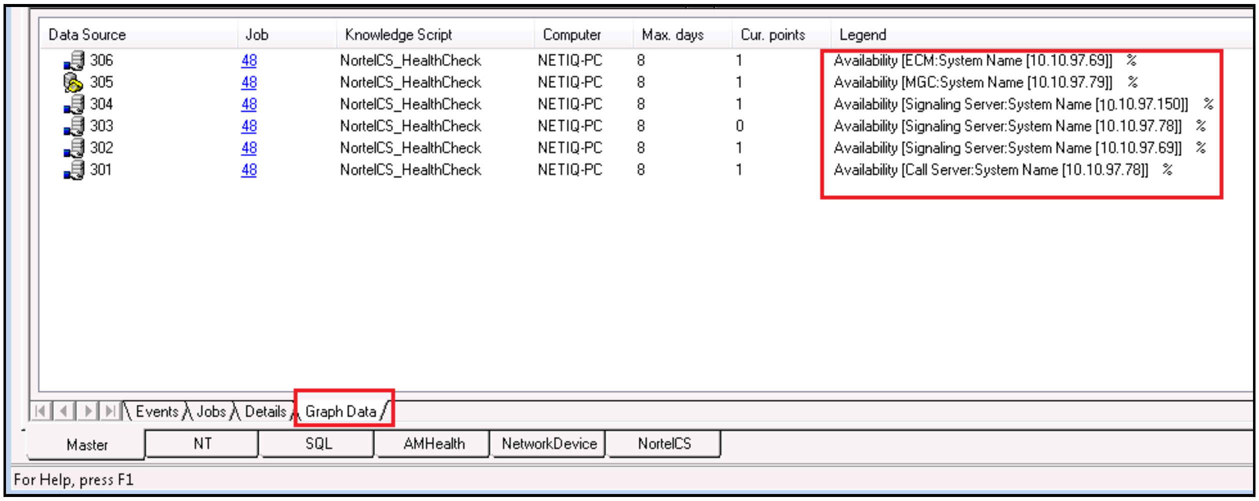
Checks a Call Server, ECM, MC32S, MGC, NRS, Signaling Server, SIP Server or VGMC to ensure it is responding to SNMP requests. Also checks an MC32S, Signaling Server, or VGMC to ensure it is running in the normal operational state. If requested, events are raised if the device is not responsive or is in an abnormal state. A datastream indicating device availability (datapoint is 100%) or unavailability (datapoint is 0%) is also available.

Once the properties are configured, a job is automatically created that will run and captures the data for the HealthCheck of the Communication Server 1000 devices. Screen below shows an example of the job that is completed and whose status now is stopped. However, a user can start the job manually by clicking on the Traffic Light symbol.



Job	Status	Children	Computer	Knowledge Script	User	Submit Time	Stop Time
45	Stopped	1	NETIQ-PC	NortelCS_Alarms	NetIQ-PC\NetIQ	4/16/2014 1:24:18 PM	5/13/2014 4:05:11 PM
43	Stopped	1	NETIQ-PC	NortelCS_Alarms	NetIQ-PC\NetIQ	4/14/2014 4:30:04 PM	4/16/2014 1:22:54 PM
39	Stopped	1	NETIQ-PC	NortelCS_GetOMReport	NetIQ-PC\NetIQ	4/10/2014 10:38:09 AM	4/11/2014 4:01:09 PM
37	Stopped	1	NETIQ-PC	NortelCS_PhoneInventory	NetIQ-PC\NetIQ	4/10/2014 9:49:41 AM	4/11/2014 4:04:49 PM
35	Stopped	1	NETIQ-PC	NortelCS_BMZ_CallQuality	NetIQ-PC\NetIQ	4/9/2014 11:51:27 AM	4/11/2014 4:12:51 PM
33	Stopped	1	NETIQ-PC	NortelCS_PhoneInventory	NetIQ-PC\NetIQ	4/9/2014 11:37:46 AM	4/9/2014 2:59:50 PM
31	Stopped	1	NETIQ-PC	NortelCS_HealthCheck	NetIQ-PC\NetIQ	4/9/2014 11:33:45 AM	4/11/2014 3:56:14 PM
29	Stopped	1	NETIQ-PC	Discovery_NortelCS	NetIQ-PC\NetIQ	4/9/2014 10:14:47 AM	4/11/2014 3:49:28 PM
27	Stopped	1	NETIQ-PC	Discovery_NortelCS	NetIQ-PC\NetIQ	3/19/2014 2:33:14 PM	4/9/2014 10:12:23 AM
25	Stopped	1	NETIQ-PC	Discovery_NortelCS	NetIQ-PC\NetIQ	3/12/2014 11:27:07 AM	3/14/2014 10:04:08 AM
5	Stopped	1	NETIQ-PC	Discovery_SQL	sa	3/4/2014 5:55:01 AM	3/4/2014 1:30:02 PM
3	Stopped	1	NETIQ-PC	Discovery_AMHealth	NT AUTHORITY\NETWORK SERVICE	3/4/2014 5:55:00 AM	3/4/2014 1:36:59 PM
1	Stopped	1	NETIQ-PC	Discovery_NT	sa	3/4/2014 5:51:20 AM	3/4/2014 1:37:10 PM

The collected HealthCheck data can be viewed from the **Graph Data** tab as shown below.



Data Source	Job	Knowledge Script	Computer	Max. days	Cur. points	Legend
306	48	NortelCS_HealthCheck	NETIQ-PC	8	1	Availability [ECM:System Name [10.10.97.69]] %
305	48	NortelCS_HealthCheck	NETIQ-PC	8	1	Availability [MGC:System Name [10.10.97.79]] %
304	48	NortelCS_HealthCheck	NETIQ-PC	8	1	Availability [Signaling Server:System Name [10.10.97.150]] %
303	48	NortelCS_HealthCheck	NETIQ-PC	8	0	Availability [Signaling Server:System Name [10.10.97.78]] %
302	48	NortelCS_HealthCheck	NETIQ-PC	8	1	Availability [Signaling Server:System Name [10.10.97.69]] %
301	48	NortelCS_HealthCheck	NETIQ-PC	8	1	Availability [Call Server:System Name [10.10.97.78]] %

User can similarly configure the properties for different available Knowledge Scripts using the AppManager as explained in **Section 6.4** above and thereby report, monitor and diagnose the Communication Server 1000 devices.

7. Verification Steps

The following tests were conducted to verify the solution between the Communication Server 1000 and AppManager Application.

- Ensure AppManager can run multiple Knowledge Scripts without interfering in the functioning of the Communication Server 1000. Run multiple Knowledge Scripts and at the same time perform various maintenance functions on the Communication Server 1000. Knowledge Scripts and Communication Server 1000 functions normally.
- Ensure AppManager does not impact phone calls when calls are made during running of a Knowledge Script. Make a call on the Communication Server 1000 and then start Knowledge Scripts. No calls were impacted while Knowledge Scripts were being executed.
- Ensure AppManager does not impact the voice quality when Knowledge Scripts are run while a phone call is in progress. Make a call on the Communication Server 1000 and then start Knowledge Scripts. Call Quality was not impacted while Knowledge Scripts were being executed.

8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 2**. The NetIQ AppManager 8.2 is considered compliant with Avaya Communication Server 1000 Release 7.65.

9. Additional References

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

Avaya:
Software Input Output Reference —Administration Avaya Communication Server 1000, NN43001-611
Software Input Output Reference —Maintenance Avaya Communication Server 1000, NN43001-711
Element Manager System Reference – Administration - Avaya Communication Server 1000, March 2013, Release 7.6, NN43001-632.

Product documentation for NetIQ AppManager may be found at:
https://www.netiq.com/support/default.asp?tab=ProductSupport&product=NONE

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.