Avaya Solution & Interoperability Test Lab

Application Notes for NetIQ AppManager 8.0 with Avaya Communication Server 1000 Release 7.5 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya Communication Server 1000 Release 7.5 (CS1000) and the NetIQ AppManager 8.0. During compliance testing, the AppManager was able to deliver systems management solution for the CS1000 system using FTP and SNMP. 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 CS1000 system or the quality of phone calls.

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 7.5 (hereafter referred to as CS1000) and the NetIQ AppManager 8.0 (hereafter referred to as AppManager). This test was performed to verify the basic interaction between CS1000 and AppManager to ensure that there is no adverse impact on the CS1000 system while AppManager is running and accessing CS1000 systems. The AppManager is a systems management tool that provides monitoring, reporting, analysis, diagnostics and resolution to the system it is connected to using FTP and SNMP Protocols.

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 CS1000 system with no adverse impact on the CS1000 system or any other management interfaces.

2.1. Interoperability Compliance Testing

The general test approach was to integrate the AppManager into Avaya CS1000 system. The main objectives were to ensure that there is no adverse impact on the CS1000 system or any other management interfaces. The following features were executed during active calls:

- Discovery of Avaya CS1000 devices, including CoRes (Call Server and Signaling Server) card and SIP Line Gateway card.
- Retrieving information from Avaya CS1000 devices such as software version, hardware platform.
- Monitor health of Avaya CS1000 devices (including SIP Line resources) such as HealthCheck and Alarms.
- Telephone Inventory is retrieved from Avaya CS1000.
- OM Reports are retrieved from Avaya CS1000.
- BMZ_CallQuality metrics is retrieved from Avaya CS1000.
- All AppManager module scripts are running at the same time with its default values.

2.2. Test Results

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

2.3. Support

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

- **Telephone:** 1-713-418-5555
- **Email:** 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 CS1000 Release 7.5 and AppManager 8.0.

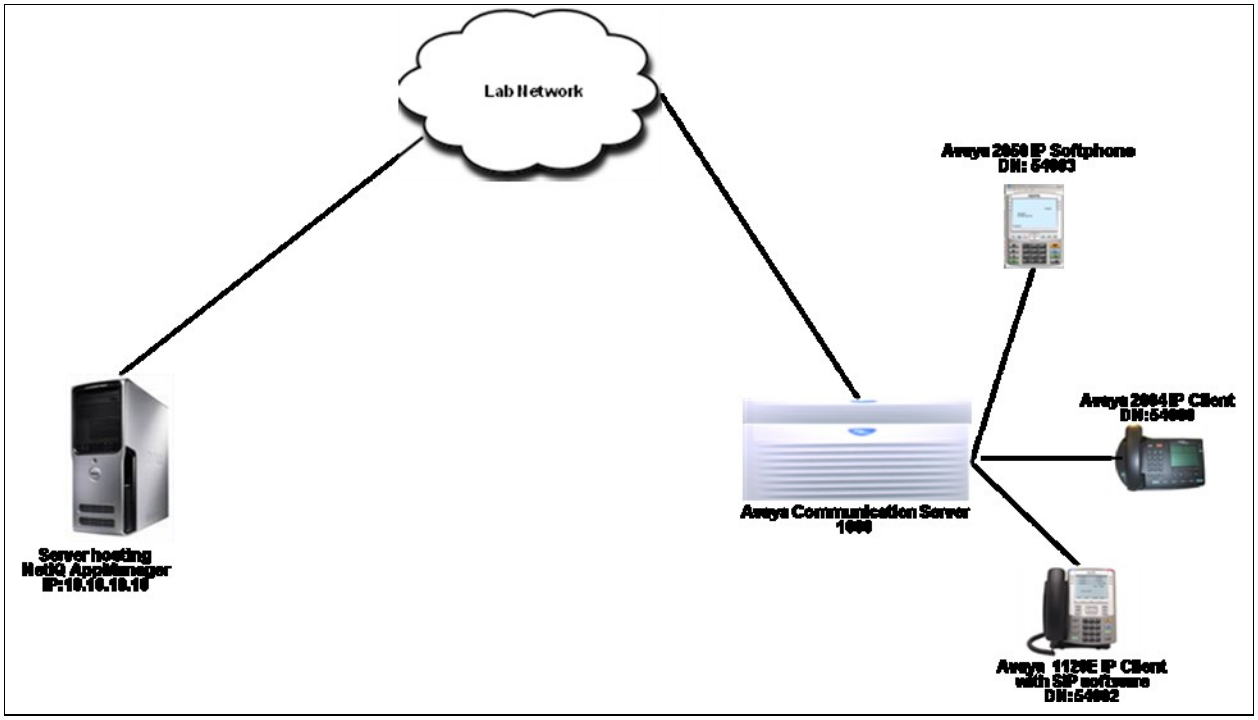


Figure 1: Test Solution Configuration

4. Equipment and Software Validated

Equipment	Software/Firmware
Avaya Communication Server 1000	SW Version : 7.50 Q
Avaya Telephones:	
2004 (IP)	0602B76
1120E (SIP)	04.01.13.00
2050 (IP)	3.04.0003
NetIQ AppManager Server:	
Server hosting AppManager	Windows Server 2003 SP2
AppManager	SW Version 8.0
NetIQ NortelCS module	SW Version 7.4.63

5. Configuring the CS1000

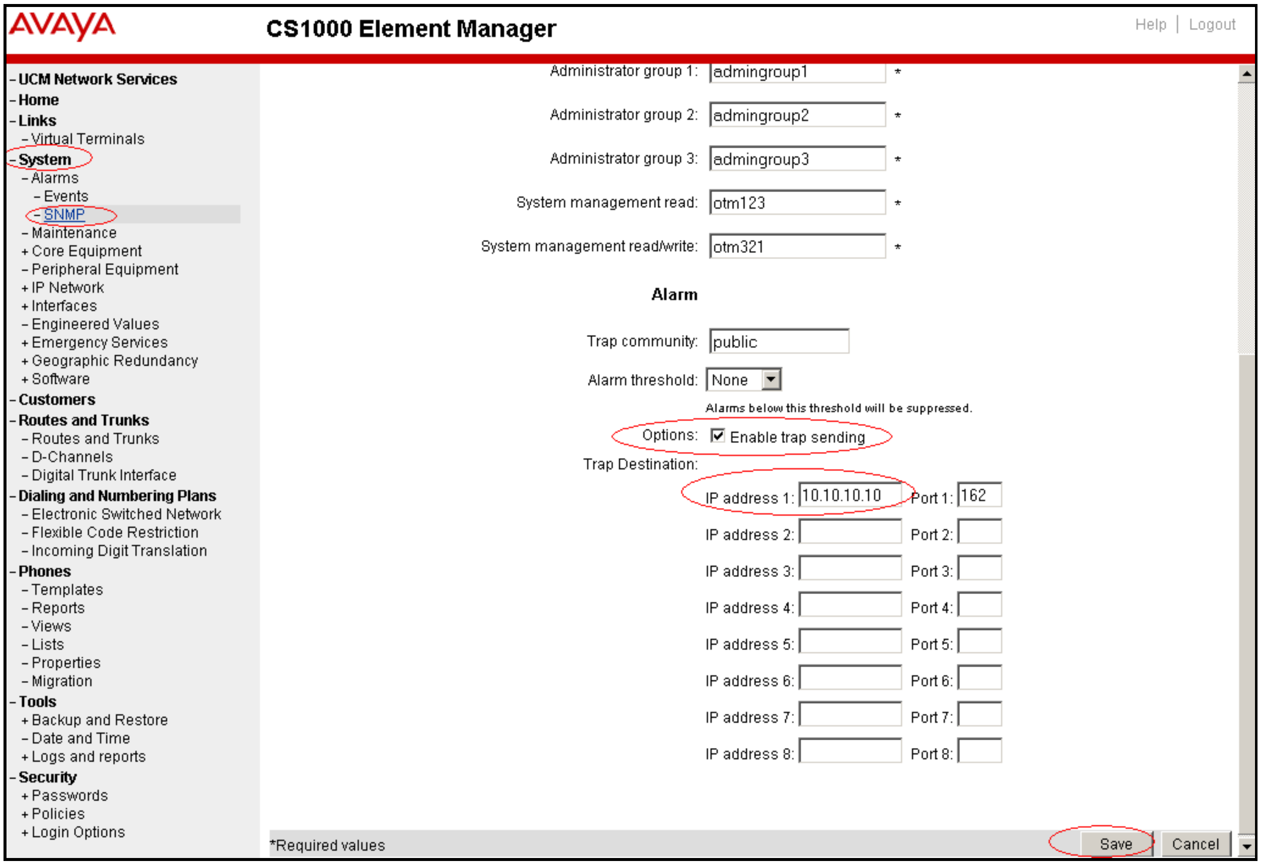
This section describes the steps to configure CS1000 to work with the AppManager.

Here is a summary of CS1000 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 is Configured as a Trap Receiver

Access the CS1000 Element Manager via the Unified Communication 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 in **Figure 2** below. Under the **Options** field check the box for E*nable trap sending*. All other fields are at default values. Click on **Save** to complete the configuration.



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: 10.10.10.10 Port 1: 162

IP address 2: Port 2:

IP address 3: Port 3:

IP address 4: Port 4:

IP address 5: Port 5:

IP address 6: Port 6:

IP address 7: Port 7:

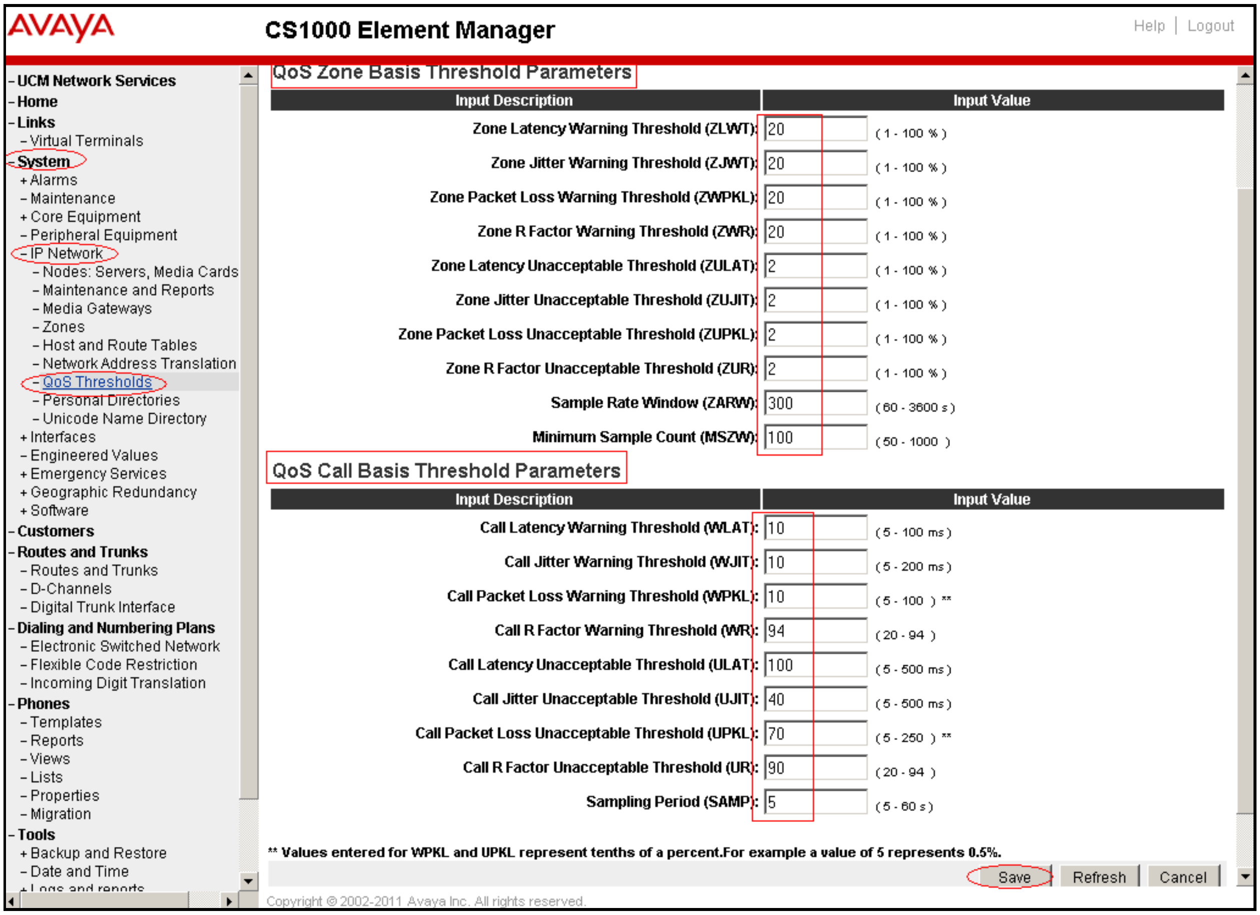
IP address 8: Port 8:

*Required values

Figure 2: Setting up AppManager Server as a Trap Receiver

5.2. Setting QoS Zone and Call Basis Threshold Parameters

Access the CS1000 Element Manager via the Unified Communication 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 in **Figure 3** below. All quality metrics that fall outside of the thresholds are identified by the Alarms script. Click on **Save** 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

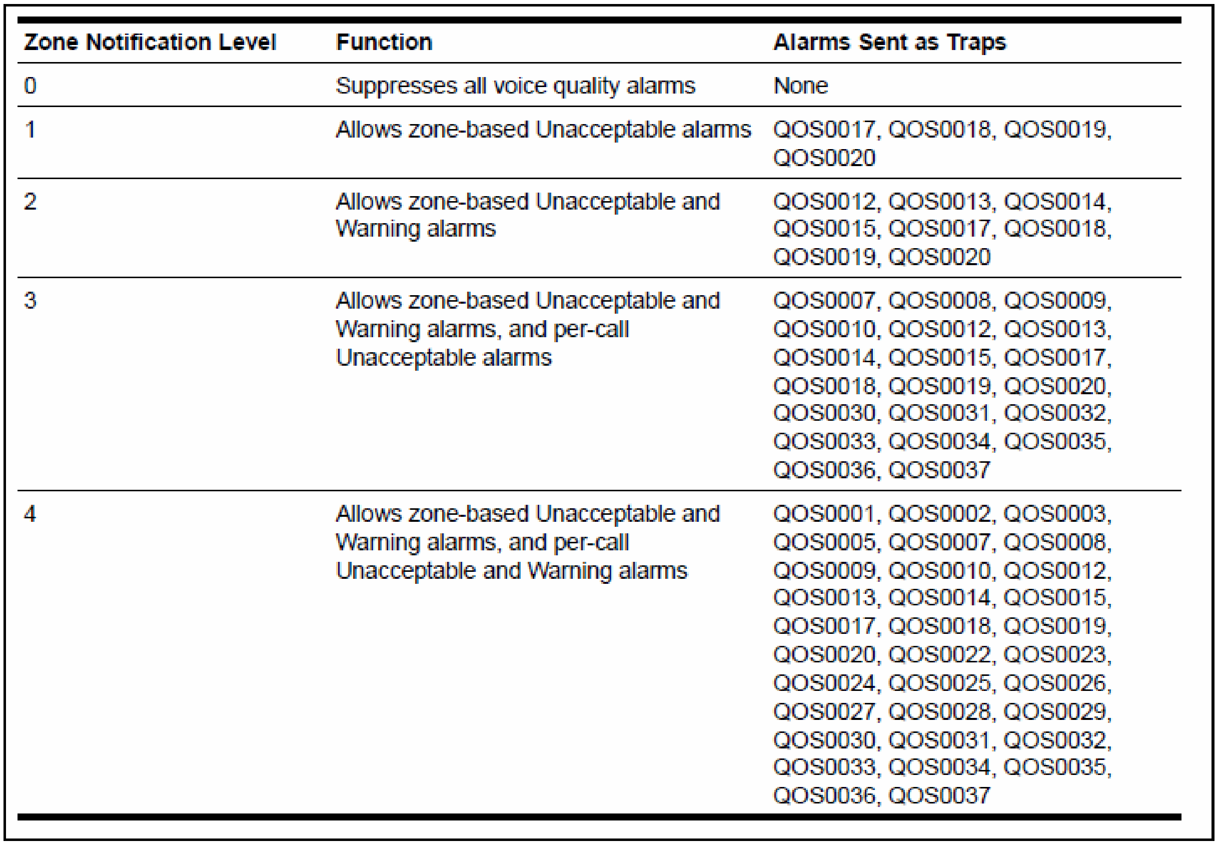
Input Description	Input Value	
Call Latency Warning Threshold (WLAT):	10	(5 - 100 ms)
Call Jitter Warning Threshold (WJIT):	10	(5 - 200 ms)
Call Packet Loss Warning Threshold (WPKL):	10	(5 - 100) **
Call R Factor Warning Threshold (WR):	94	(20 - 94)
Call Latency Unacceptable Threshold (ULAT):	100	(5 - 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%.

Figure 3: Configuration of QoS Zone/Call Basis Threshold Parameters

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 CS1000 command line in **LD117**.

>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 CS1000 and AppManager, the Telnet Service on CS1000 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 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 CS1000:
Log in to CS1000 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 CS1000. Inventory of the sets can be reported by running the following commands in **LD 117** of the CS1000 through Command Line Interface.

- CS1000 to generate the inventory report once every midnight

```
INV MIDNIGHT SETS
```

- CS1000 to include the telephones from the inventory report in the Entity MIB

```
INV ENTITY SETS ON
```

- Optional: CS1000 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 CS1000. This section assumes that AppManager has been installed. For more information about installing AppManager or about AppManager system requirements, refer to **[2] in Section 9**. The configurations explained are,

- Configuring SNMP community strings.
- Disabling NetIQ trap receiver.

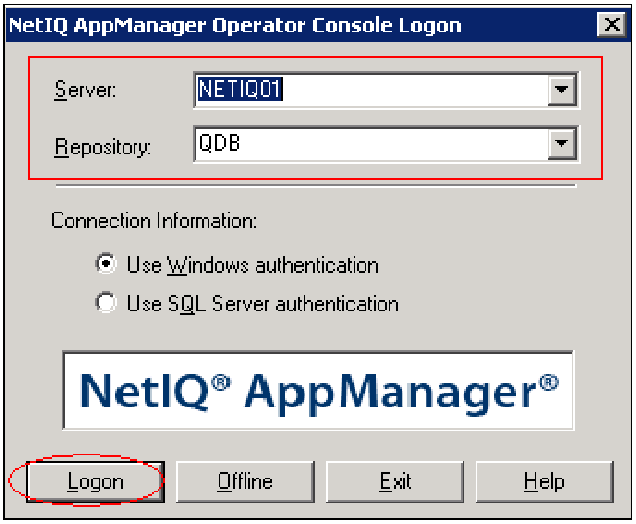
- AppManager configuration for discovery of CS1000 devices.
- AppManager configuration to collect Health Check data of CS1000 devices.

6.1. Configuring SNMP Community Strings

To enable AppManager to use SNMP to access Avaya CS1000 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 **Figure 4** below.



NetIQ AppManager Operator Console Logon

Server: NETIQ01

Repository: QDB

Connection Information:

● Use Windows authentication

○ Use SQL Server authentication

Figure 4: Operator Console Login

From the AppManager Operator Console window navigate to **Extensions > Security Manager** as shown in **Figure 5** below.

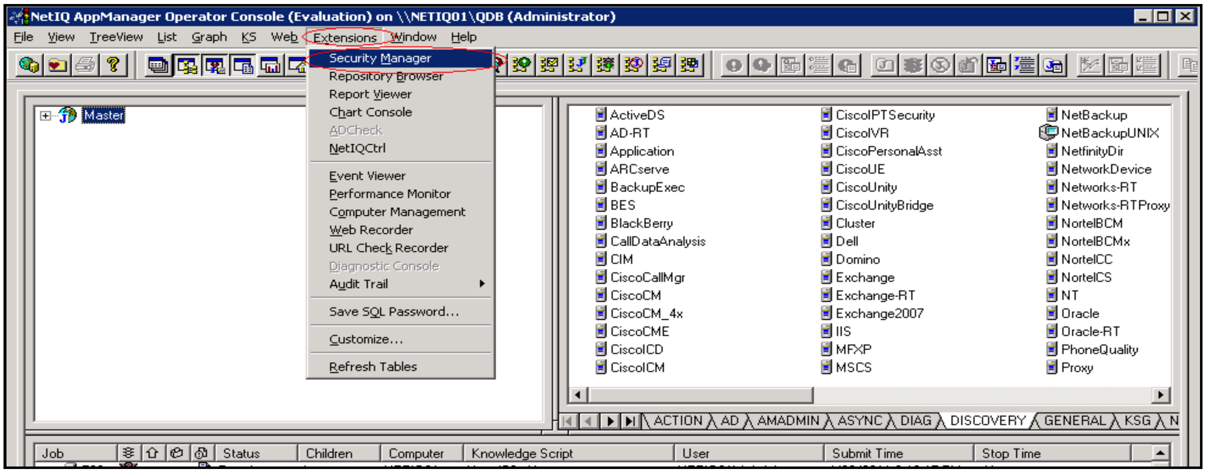
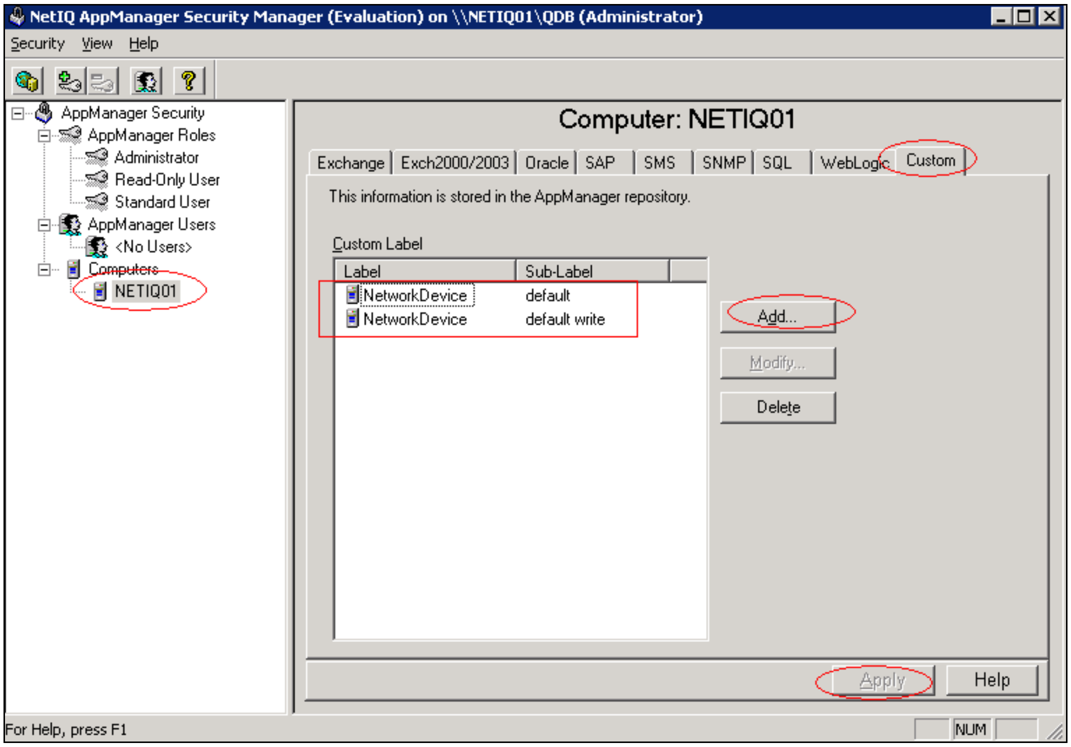


Figure 5: Accessing Security Manager

Select the **NETIQ01** under **Computers** as seen on the left window pane of **Figure 6**. Add the **Custom Label** as required and the appropriate community string in **Value 1** and then click on the **Apply** 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.

Label	Sub-Label
NetworkDevice	default
NetworkDevice	default write

Figure 6: Adding Custom Labels

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 CS1000 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 CS1000 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 in the **Figure 7** below. Select **NortelCS** that is seen on the right hand window pane and drag it to the **NETIQ01** that is on the left hand window pane.

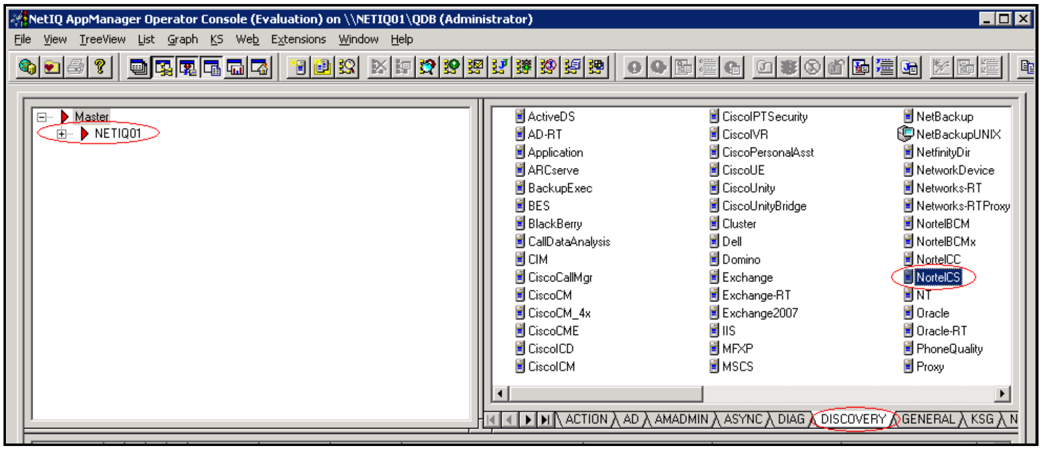
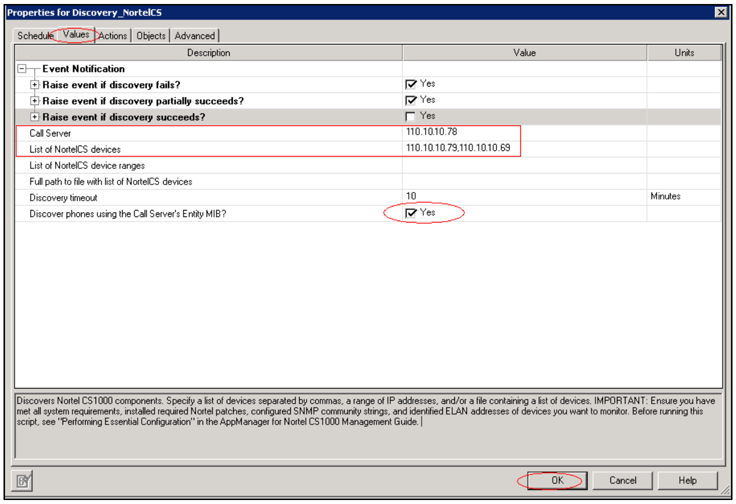


Figure 7: Selecting the Required Knowledge Script for CS1000

When the required Knowledge Script is selected and dragged the **Properties for Discovery_NortelCS** window automatically pops up as shown in **Figure 8** 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 checked. Click on **OK** to continue.

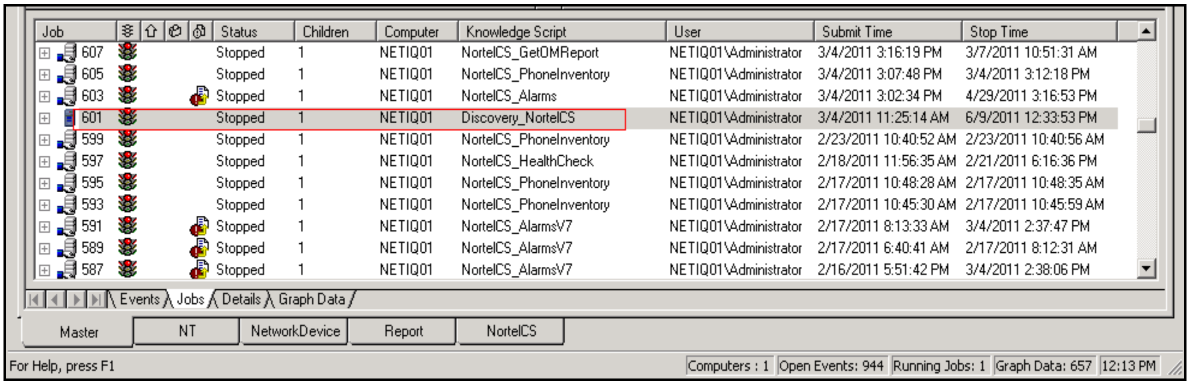


Description	Value	Units
Event Notification		
Raise event if discovery fails?	☑ Yes	
Raise event if discovery partially succeeds?	☑ Yes	
Raise event if discovery succeeds?	☐ Yes	
Call Server	110.10.10.78	
List of NortelCS devices	110.10.10.79,110.10.10.69	
List of NortelCS device ranges		
Full path to 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.

Figure 8: Configuring the values of Discovery_NortelCS

Once the properties are configured a job is automatically created that will run and discover all CS1000 elements. **Figure 9** 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
607	Stopped	1	NETIQ01	NortelCS_GetOMReport	NETIQ01\Administrator	3/4/2011 3:16:19 PM	3/7/2011 10:51:31 AM
605	Stopped	1	NETIQ01	NortelCS_PhoneInventory	NETIQ01\Administrator	3/4/2011 3:07:48 PM	3/4/2011 3:12:18 PM
603	Stopped	1	NETIQ01	NortelCS_Alarms	NETIQ01\Administrator	3/4/2011 3:02:34 PM	4/29/2011 3:16:53 PM
601	Stopped	1	NETIQ01	Discovery_NortelCS	NETIQ01\Administrator	3/4/2011 11:25:14 AM	6/9/2011 12:33:53 PM
599	Stopped	1	NETIQ01	NortelCS_PhoneInventory	NETIQ01\Administrator	2/23/2011 10:40:52 AM	2/23/2011 10:40:56 AM
597	Stopped	1	NETIQ01	NortelCS_HealthCheck	NETIQ01\Administrator	2/18/2011 11:56:35 AM	2/21/2011 6:16:36 PM
595	Stopped	1	NETIQ01	NortelCS_PhoneInventory	NETIQ01\Administrator	2/17/2011 10:48:28 AM	2/17/2011 10:48:35 AM
593	Stopped	1	NETIQ01	NortelCS_PhoneInventory	NETIQ01\Administrator	2/17/2011 10:45:30 AM	2/17/2011 10:45:59 AM
591	Stopped	1	NETIQ01	NortelCS_AlarmsV7	NETIQ01\Administrator	2/17/2011 8:13:33 AM	3/4/2011 2:37:47 PM
589	Stopped	1	NETIQ01	NortelCS_AlarmsV7	NETIQ01\Administrator	2/17/2011 6:40:41 AM	2/17/2011 8:12:31 AM
587	Stopped	1	NETIQ01	NortelCS_AlarmsV7	NETIQ01\Administrator	2/16/2011 5:51:42 PM	3/4/2011 2:38:06 PM

For Help, press F1 | Computers : 1 | Open Events: 944 | Running Jobs: 1 | Graph Data: 657 | 12:13 PM

Figure 9: Window showing the Job Discovery_NortelCS

Figure 10 below shows the window with the devices of CS1000 discovered during compliance testing.

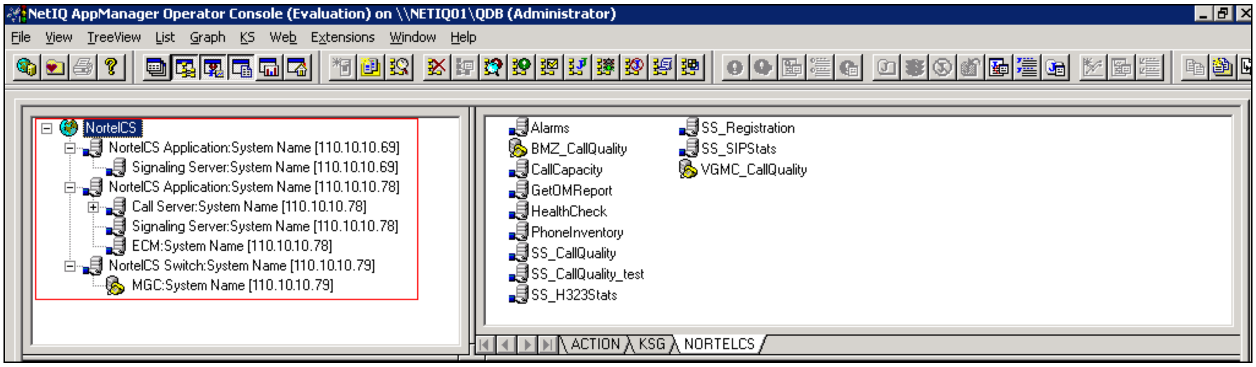

NetIQ AppManager Operator Console (Evaluation) on \\NETIQ01\QDB (Administrator)
File View TreeView List Graph KS Web Extensions Window Help
NortelCS
NortelCS Application:System Name [110.10.10.69]
Signaling Server:System Name [110.10.10.69]
NortelCS Application:System Name [110.10.10.78]
Call Server:System Name [110.10.10.78]
Signaling Server:System Name [110.10.10.78]
ECM:System Name [110.10.10.78]
NortelCS Switch:System Name [110.10.10.79]
MGC:System Name [110.10.10.79]
Alarms
BMZ_CallQuality
CallCapacity
GetOMReport
HealthCheck
PhoneInventory
SS_CallQuality
SS_CallQuality_test
SS_H323Stats
SS_Registration
SS_SIPStats
VGMC_CallQuality
ACTION
KSG
NORTELCS

Figure 10: CS1000 Discovered Devices

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 **Figure 10** above. Select the **HealthCheck** Knowledge Script seen on the right hand window pane and drag it to the **NortelCS** that is seen on the left hand window pane of **Figure 11** below.

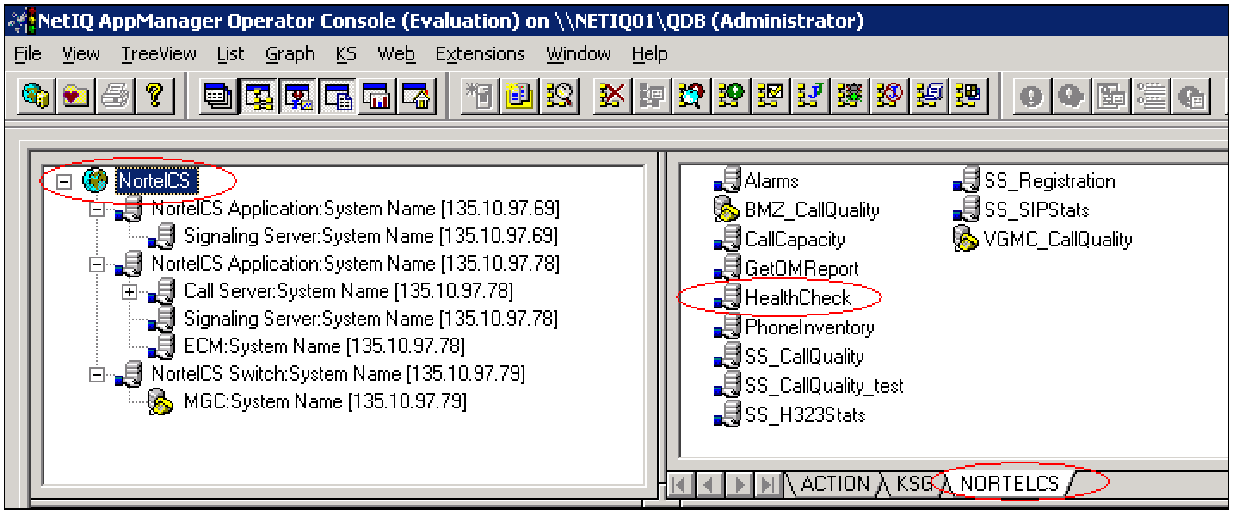
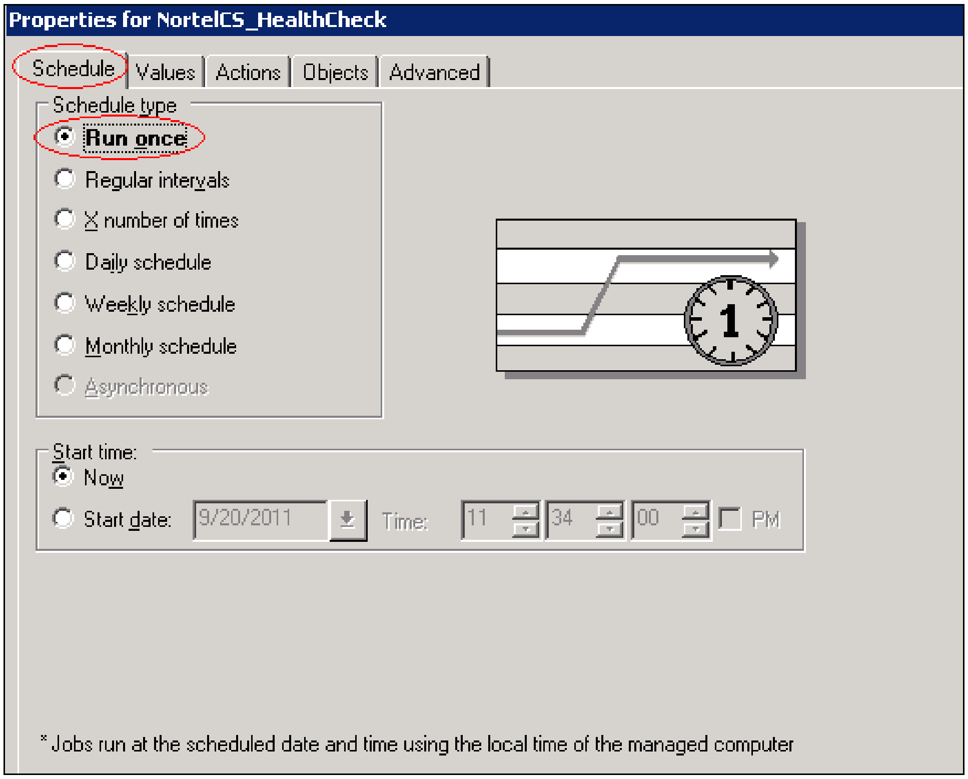

NetIQ AppManager Operator Console (Evaluation) on \\NETIQ01\QDB (Administrator)
File View TreeView List Graph KS Web Extensions Window Help
NortelCS
NortelCS Application:System Name [135.10.97.69]
Signaling Server:System Name [135.10.97.69]
NortelCS Application:System Name [135.10.97.78]
Call Server:System Name [135.10.97.78]
Signaling Server:System Name [135.10.97.78]
ECM:System Name [135.10.97.78]
NortelCS Switch:System Name [135.10.97.79]
MGC:System Name [135.10.97.79]
Alarms
BMZ_CallQuality
CallCapacity
GetOMReport
HealthCheck
PhoneInventory
SS_CallQuality
SS_CallQuality_test
SS_H323Stats
SS_Registration
SS_SIPStats
VGMC_CallQuality
ACTION
KSG
NORTELCS

Figure 11: Selecting the HealthCheck Knowledge Script

When the required HealthCheck script is selected and dragged the **Properties for NortelCS_HealthCheck** window automatically pops up as shown in **Figure 12** below. From this window select the **Schedule** tab and select the job to **Run once**.



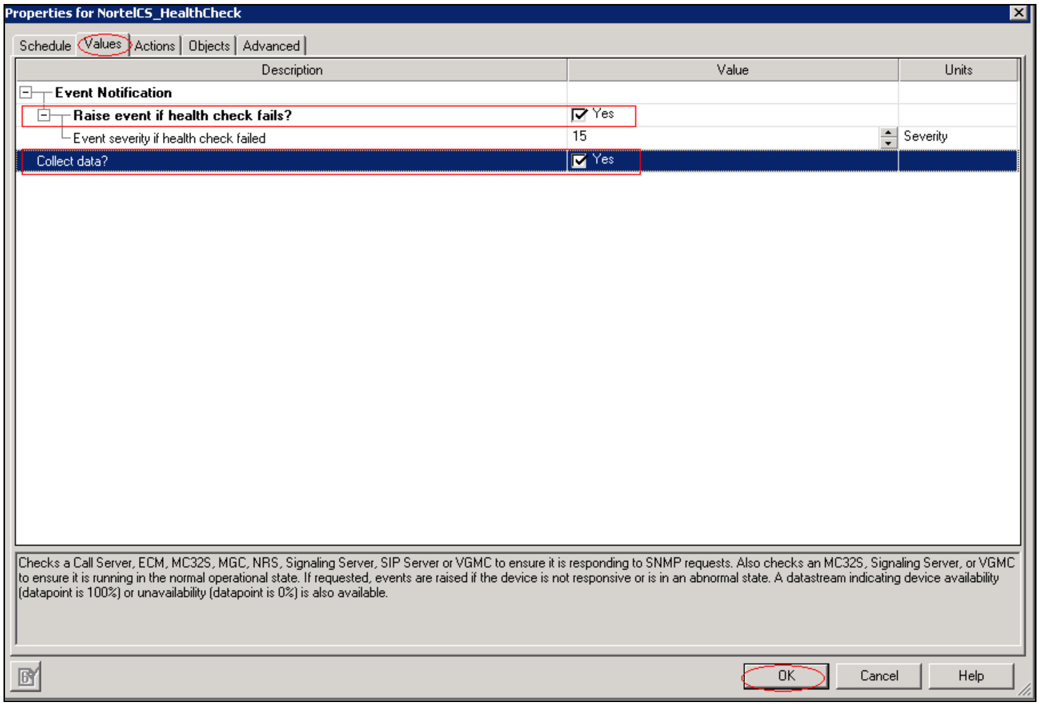
Schedule type
● Run once
○ Regular intervals
○ X number of times
○ Daily schedule
○ Weekly schedule
○ Monthly schedule
○ Asynchronous

Start time:
● Now
○ Start date: 9/20/2011 Time: 11 34 00 ☐ PM

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

Figure 12: Configuring the Schedule for NortelCS_HealthCheck

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 in **Figure 13** below.

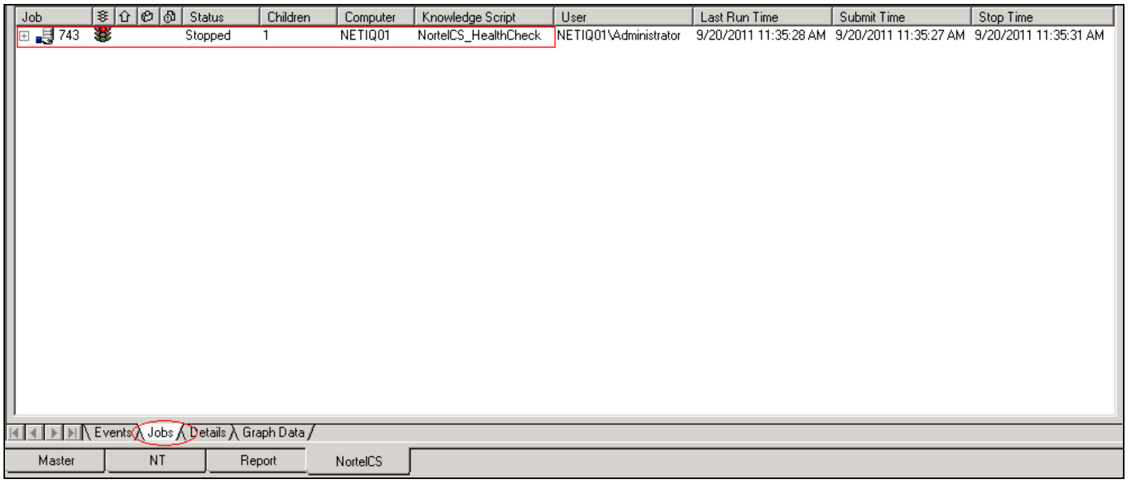


Description	Value	Units
Event Notification		
Raise event if health check fails?	☑ Yes	
Event severity if health check failed	15	Severity
Collect data?	☑ Yes	

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.

Figure 13: Configuring the Values for NortelCS_HealthCheck

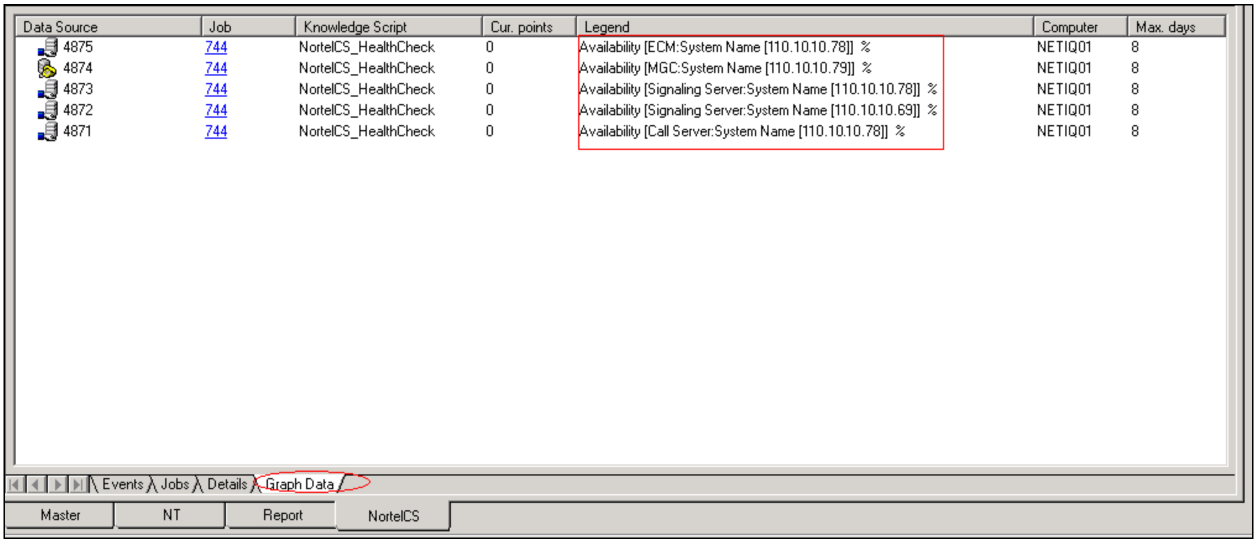
Once the properties are configured, a job is automatically created that will run and capture the data for the HealthCheck of the CS1000 devices. **Figure 14** below shows an example of the job that is completed and whose status now is stopped. However, a user can start the job manually by clicking on the Traffic Light symbol.



Job	Status	Children	Computer	Knowledge Script	User	Last Run Time	Submit Time	Stop Time
743	Stopped	1	NETIQ01	NortelCS_HealthCheck	NETIQ01\Administrator	9/20/2011 11:35:28 AM	9/20/2011 11:35:27 AM	9/20/2011 11:35:31 AM

Figure 14: Window showing the Job NortelCS_HealthCheck

The collected HealthCheck data can be viewed from the **Graph Data** tab as shown in **Figure 15** below.



Data Source	Job	Knowledge Script	Cur. points	Legend	Computer	Max. days
4875	744	NortelCS_HealthCheck	0	Availability [ECM:System Name [110.10.10.78]] %	NETIQ01	8
4874	744	NortelCS_HealthCheck	0	Availability [MGC:System Name [110.10.10.79]] %	NETIQ01	8
4873	744	NortelCS_HealthCheck	0	Availability [Signaling Server:System Name [110.10.10.78]] %	NETIQ01	8
4872	744	NortelCS_HealthCheck	0	Availability [Signaling Server:System Name [110.10.10.69]] %	NETIQ01	8
4871	744	NortelCS_HealthCheck	0	Availability [Call Server:System Name [110.10.10.78]] %	NETIQ01	8

Figure 15: Window showing the NortelCS_HealthCheck Data

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 CS1000 devices.

7. Verification Steps

The following tests were conducted to verify the solution between the CS1000 and AppManager Application.

- Ensure AppManager can run multiple Knowledge Scripts without interfering in the functioning of the CS1000. Run multiple Knowledge Scripts and at the same time perform various maintenance functions on the CS1000. Knowledge Scripts and CS1000 functions normally.
- Ensure AppManager does not impact phone calls when calls are made during running of a Knowledge Script. Make a call on the CS1000 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 CS1000 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 8.0 is considered compliant with Avaya CS1000 Release 7.5.

9. Additional References

[1] CS1000 7.50 Administering and System Programming documents available at:
https://support.avaya.com/css/Products/

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

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.