



Avaya Solution & Interoperability Test Lab

Application Notes for NetIQ Vivinet Diagnostics 2.3 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 Vivinet Diagnostics 2.3. During the compliance testing, NetIQ Vivinet Diagnostics was able to work as a network diagnostic tool capable of determining the cause of failure in the case of degraded voice quality. This test was performed to verify the basic interaction between Avaya Communication Server 1000 and NetIQ Vivinet Diagnostics 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 interoperability test report for Avaya Communication Server 1000 Release 7.5 (hereafter referred to as CS1000) and the NetIQ Vivinet Diagnostics 2.3 (hereafter referred to as Vivinet Diagnostics). This test was performed to verify the basic interaction between CS1000 and NetIQ Vivinet Diagnostics to ensure that there is no adverse impact on the CS1000 system while NetIQ Vivinet Diagnostics is running and accessing CS1000 systems.

2. General Test Approach and Test Results

The focus of this interoperability compliance testing was primarily to verify Vivinet Diagnostics does not impact the quality of phone calls when diagnostics is run. For example, diagnostics were triggered and completed successfully when it receives a QoS0028 trap from the CS1000 Signaling Server.

2.1. Interoperability Compliance Testing

The focus of this compliant testing is to verify that NetIQ Vivinet Diagnostics was able to interoperate with Avaya CS1000 systems. The following interoperability areas were covered:

- Vivinet Diagnostics can successfully complete a diagnosis when triggered by a QoS0028 trap sent from CS1K Signaling Server.
- Vivinet Diagnostics correctly frees up the telnet session with the Signaling Server that it uses.
- Vivinet Diagnostics does not impact the quality of a phone call when diagnostics are running while a phone call is in progress.

The general test approach was to integrate the Vivinet Diagnostics into CS1000 system. The main objectives were to ensure that there is no adverse impact on the CS1000 system or any other management interfaces. The test did not focus on all the scenarios of CS1000 system failures and all the alarms from all CS1000 devices.

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 NetIQ Vivinet Diagnostics, 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 NetIQ Vivinet Diagnostics 2.3.

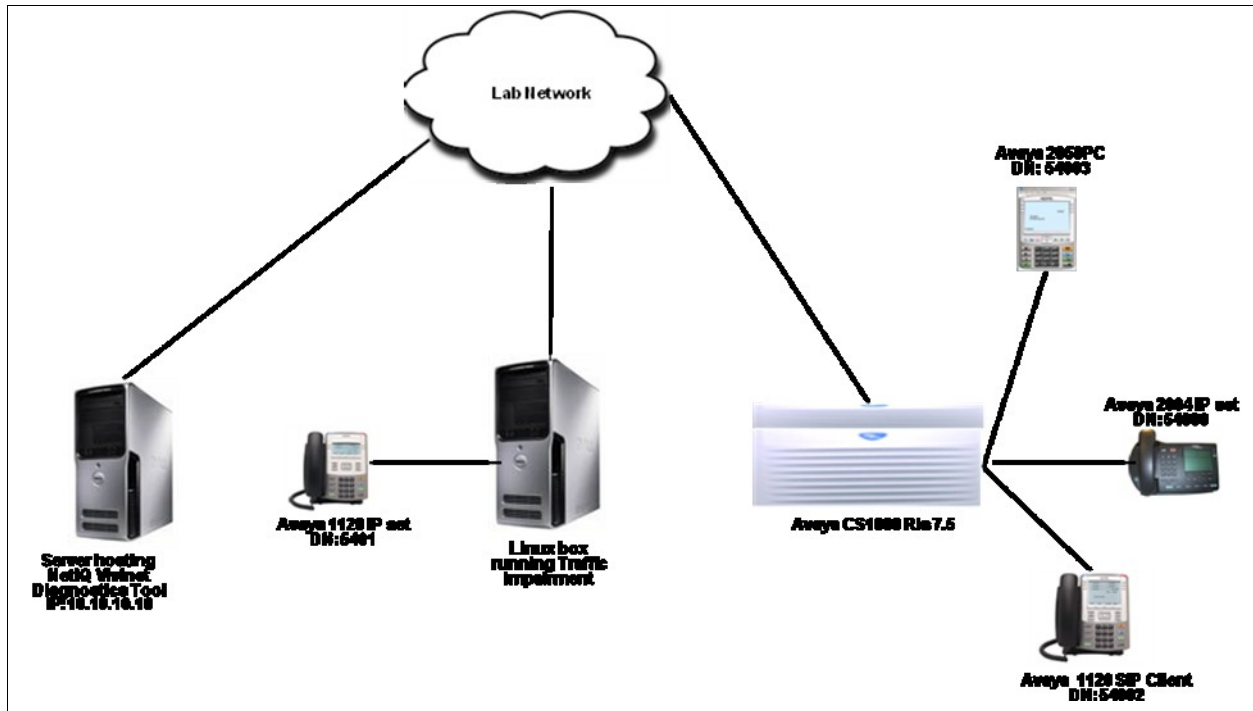


Figure 1: Test Solution Configuration

4. Equipment and Software Validated

Equipment	Software/Firmware
Avaya CS1000	SW Version : 7.50 Q
Avaya Telephones: i2004 (IP) 1120E (SIP) 1120E (IP) 2050PC (IP)	0602B76 04.01.13.00 0624C8A 3.04.0003
Server hosting Vivinet Diagnostics	Windows Server 2003 SP2
NetIQ Vivinet Diagnostics	SW Version 2.3.15304
NetIQ AppManager Suite	SW Version 7.0.1

5. Configuring the CS1000

This section describes the steps to configure CS1000 to work with the Vivinet Diagnostics.

Here is a summary of CS1000 Configuration:

- IP address of Vivinet Diagnostic's 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. Vivinet Diagnostics 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 Vivinet Diagnostics machine as a trap receiver as shown in **Figure 2** below. Under the **Options** field check the box for *Enable trap sending*. All other fields are at default values. Click on **Save** to complete the configuration.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with the following items: UCM Network Services, Home, Links, Virtual Terminals, System (highlighted), Alarms, Events, SNMP (highlighted), Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks, Routes and Trunks, D-Channels, Digital Trunk Interface, Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation, Phones, Templates, Reports, Views, Lists, Properties, Migration, Tools, Backup and Restore, Date and Time, Logs and reports, Security, Passwords, Policies, and Login Options. The main content area is titled 'CS1000 Element Manager' and includes a 'Help | Logout' link. The configuration fields are as follows: Administrator group 1: admingroup1, Administrator group 2: admingroup2, Administrator group 3: admingroup3, System management read: ctm123, System management read/write: ctm321, Alarm threshold: None, Trap community: public, 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: . The 'Save' button is circled in red.

Figure 2: Setting up Vivinet Diagnostics 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.

AVAYA CS1000 Element Manager Help | Logout

QoS Zone Basis Threshold Parameters

Input Description	Input Value	Range
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 (ZLAT):	2	(1 - 100 %)
Zone Jitter Unacceptable Threshold (ZJIT):	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	Range
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%.

Save Refresh Cancel

Copyright © 2002-2011 Avaya Inc. All rights reserved.

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 Vivinet Diagnostics as SNMP traps. The following **Table 1** below identifies the notification levels and the corresponding alarms sent as SNMP traps.

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

Vivinet Diagnostics does not support Secure Shell (SSH) access. Instead, it requires Telnet access.

To enable 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 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 Vivinet Diagnostics 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 above mentioned two 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 NetIQ AppManager Application in **Section 6.3**.
- The inventory report can take hours to complete, based on the number of phones, therefore it normally runs at midnight. As the task that generates the inventory report on the CS1000 runs at a low priority, it should not interfere with call processing.

6. NetIQ Vivinet Diagnostics Configuration

This section describes the steps to configure Vivinet Diagnostics for CS1000. This section assumes that Vivinet Diagnostics has been installed. For more information about installing Vivinet Diagnostics or about Vivinet Diagnostics system requirements, refer to **Section 9[2]**. NetIQ AppManager is required for Vivinet Diagnostics Configuration. During the compliance testing in the lab environment, both these applications were loaded on the same server. The configurations explained are,

- Configuring SNMP community strings.
- Disabling NetIQ trap receiver.
- AppManager configuration for discovery of CS1000 devices.
- AppManager configuration for receiving alarm traps of CS1000 devices.
- Vivinet diagnostics configuration.

6.1. Configuring SNMP Community Strings

To enable NetIQ 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)**. From the AppManager Operator Console window navigate to **Extensions > Security Manager** as shown in **Figure 4** below.

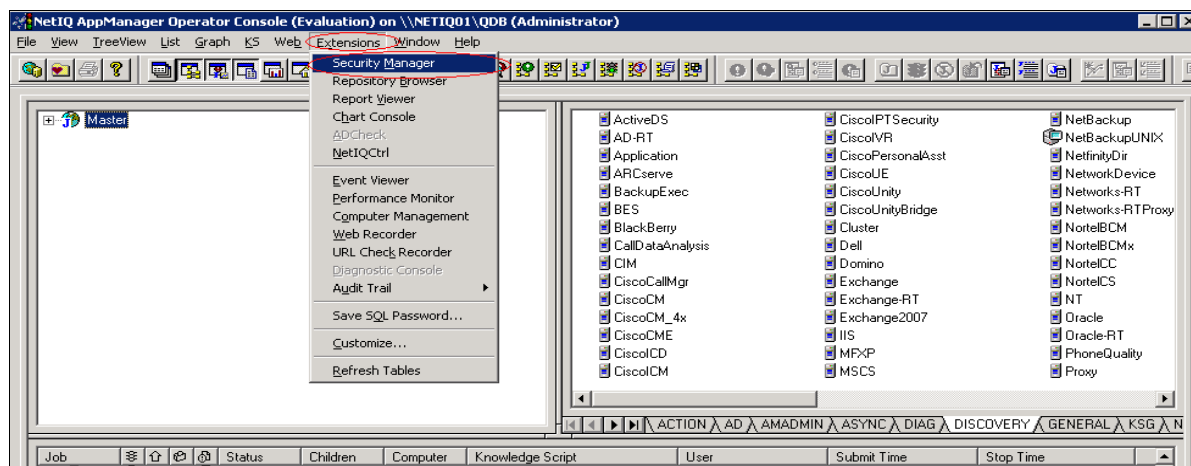


Figure 4: Accessing Security Manager

Select the **NETIQ01** under **Computers** as seen on the left window pane of **Figure 5**. 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 Signaling Servers, VGMCs, MGCs, and MC32Ss.

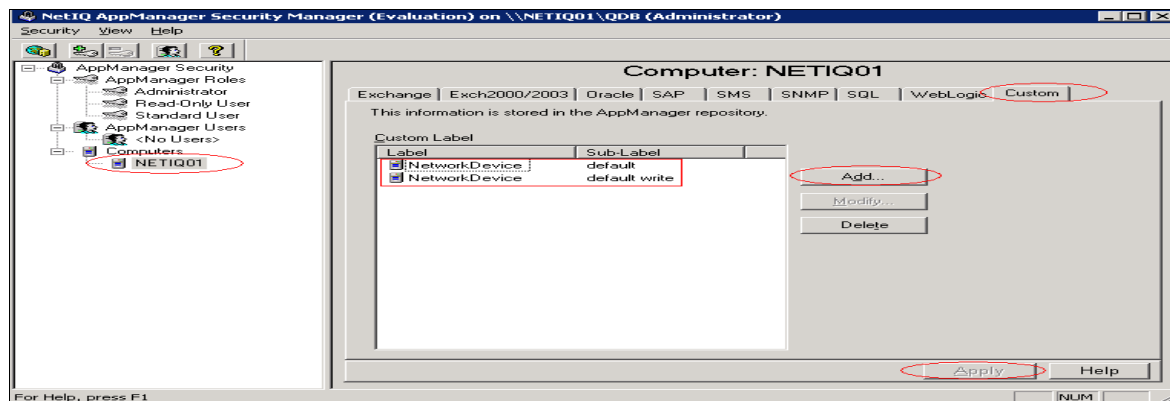


Figure 5: Adding Custom Labels

6.2. Disabling NetIQ Trap Receiver

This section describes disabling **NetIQ Trap Receiver** and enabling **SNMP Trap Service** on the Vivinet Diagnostics server.

- 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 6** 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.

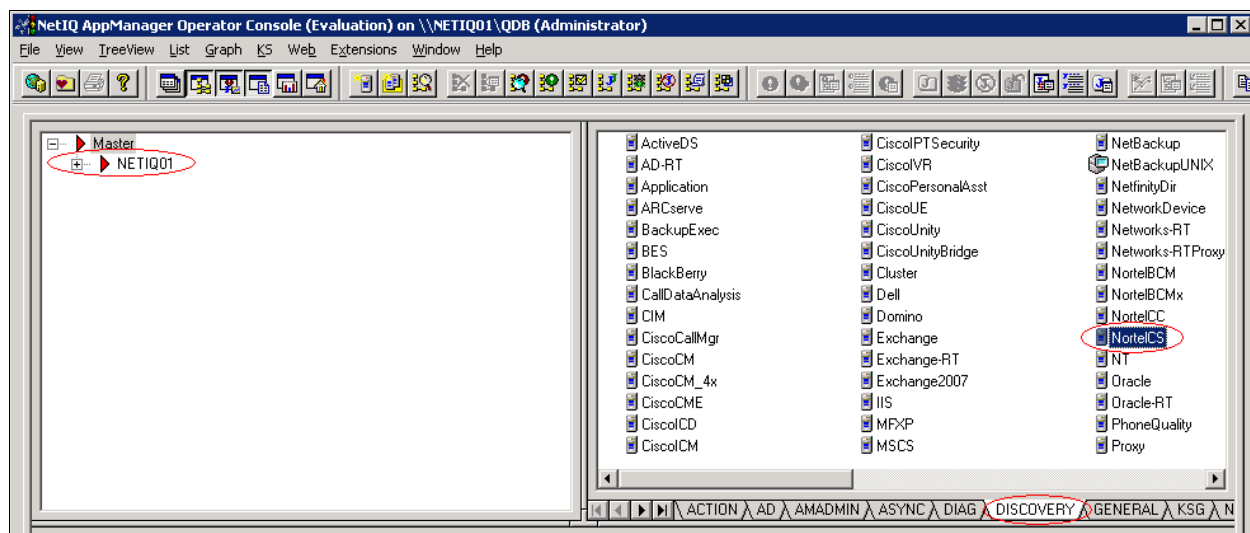


Figure 6: Selecting the required Knowledge Script for CS1000

When the required Knowledge Script is selected and dragged the **Properties for Discovery_NortelCS** window automatically pops up as shown in **Figure 7** 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?	<input checked="" type="checkbox"/> Yes	
Raise event if discovery partially succeeds?	<input checked="" type="checkbox"/> Yes	
Raise event if discovery succeeds?	<input type="checkbox"/> Yes	
Call Server		
List of NortelCS devices		
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?	<input checked="" type="checkbox"/> 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.

OK Cancel Help

Figure 7: Configuring the values of Discovery_NortelCS

Once the properties are configured a job is automatically created that will run and discover all the CS1000 elements. **Figure 8** below shows an example of the job whose status 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
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

Master NT NetworkDevice Report NortelCS

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

Figure 8: Window showing the Job Discovery_NortelCS

6.4. AppManager Configuration for Alarm of CS1000 Devices

This section explains the configuration in the AppManager where once the CS1000 elements are discovered the Alarms can be configured so that the Vivinet Diagnostics reports these alarms when they are triggered by CS1000.

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 in the AppManager tree view as shown in **Figure 9** below. Select the **NORTELCS** tab and drag the **Alarms** script seen on the right hand window pane to the **NortelCS Application System Name** that is seen on the left hand window pane.

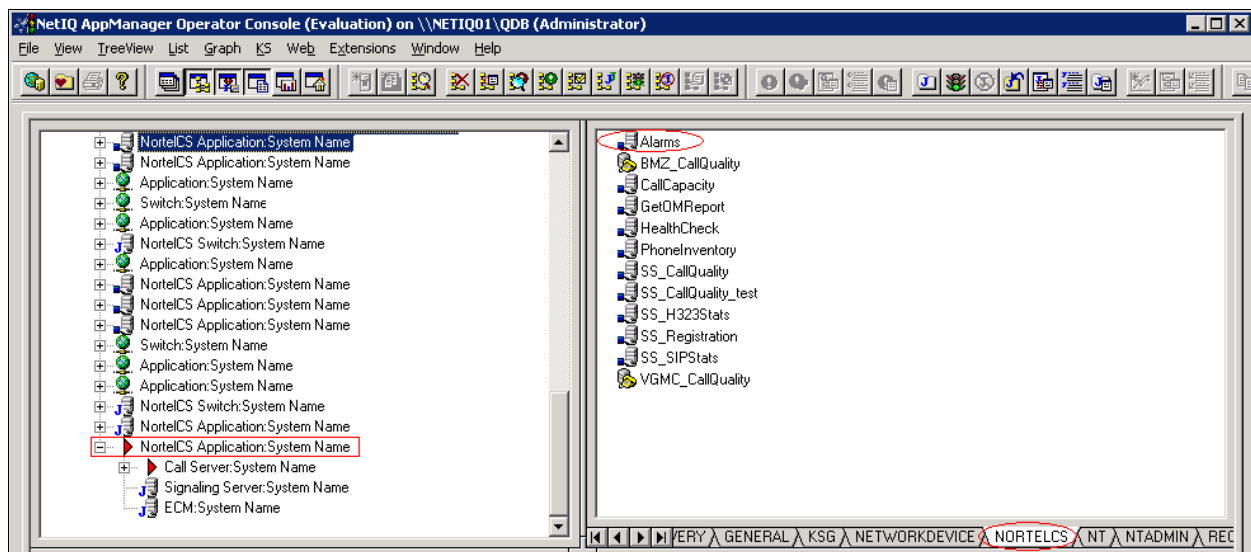


Figure 9: Selecting the required Alarm Script for CS1000

When the required Alarm script is selected and dragged the **Properties for NortelCS_Alarms** window automatically pops up as shown in **Figure 10** below. From this window select the **Values** tab and configure the required alarms. During compliance testing all alarms under the **Launch Diagnostics when the following alarms are received** was selected. Click on **OK** to continue.

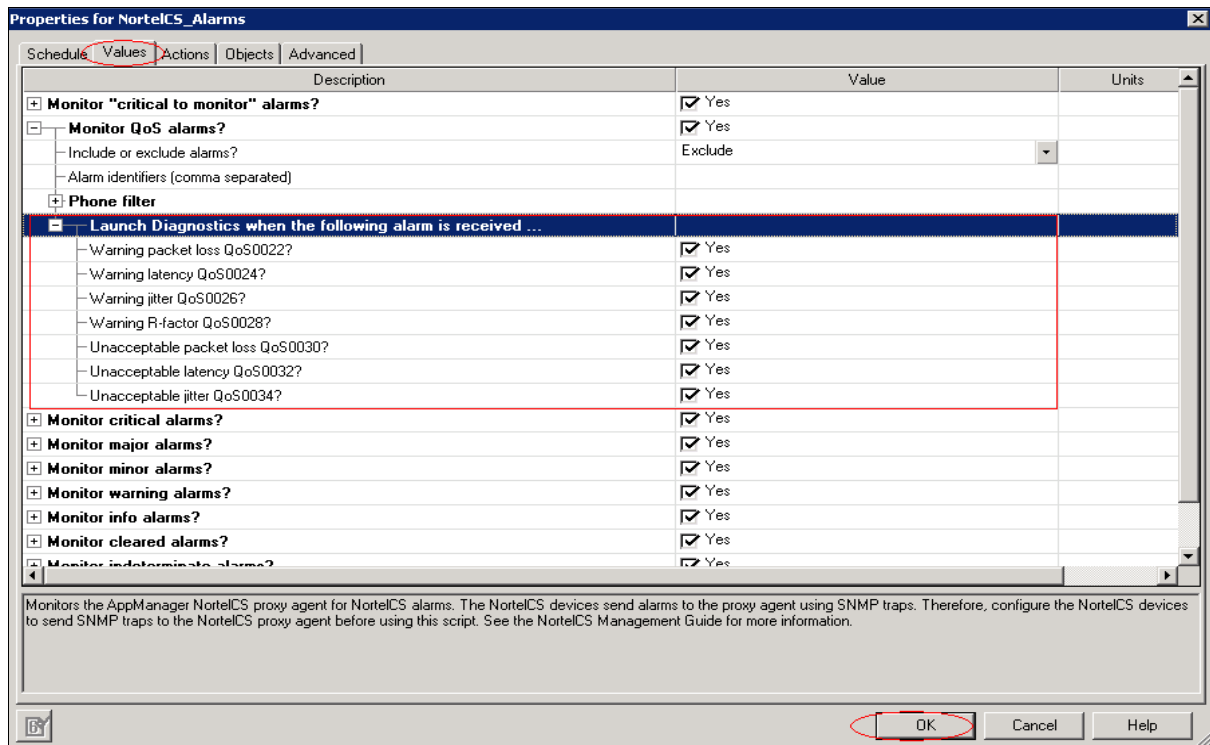


Figure 10: Configuring the values of NortelCS_Alarms

Once the properties are configured, a job is automatically created that will run and capture all the alarms that are defined. **Figure 11** below shows an example of the job whose status 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
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

Figure 11: Window showing the Job NortelCS_Alarms

6.5. Vivinet Diagnostics Configuration

This section explains the configuration in the Vivinet Diagnostics of the SNMP, Call Server and Signaling Server values of the CS1000.

Access the NetIQ Vivinet Diagnostics window by navigating to **Start > All Programs > NetIQ Vivinet Diagnostics**. Select **Options** as shown in **Figure 12** below. From the **Options** menu user can select **SNMP**, **Call Server** and **Signaling Server** to configure their respective values.

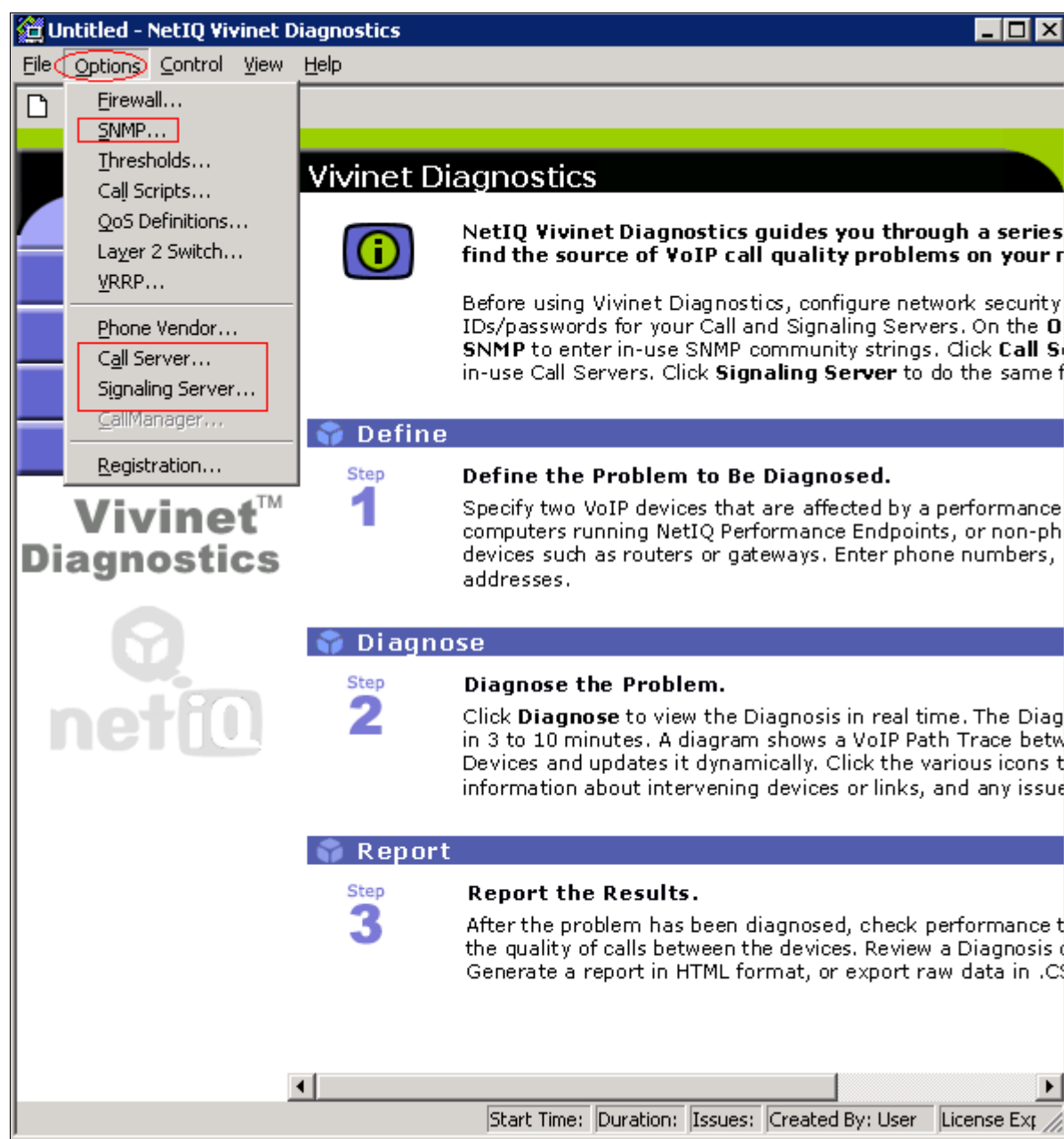


Figure 12: NetIQ Vivinet Diagnostics main screen

To configure the SNMP values, select the **SNMP v1/v2** tab and **Add** the required values as shown in **Figure 13** below. Click on **OK** to complete the configuration.

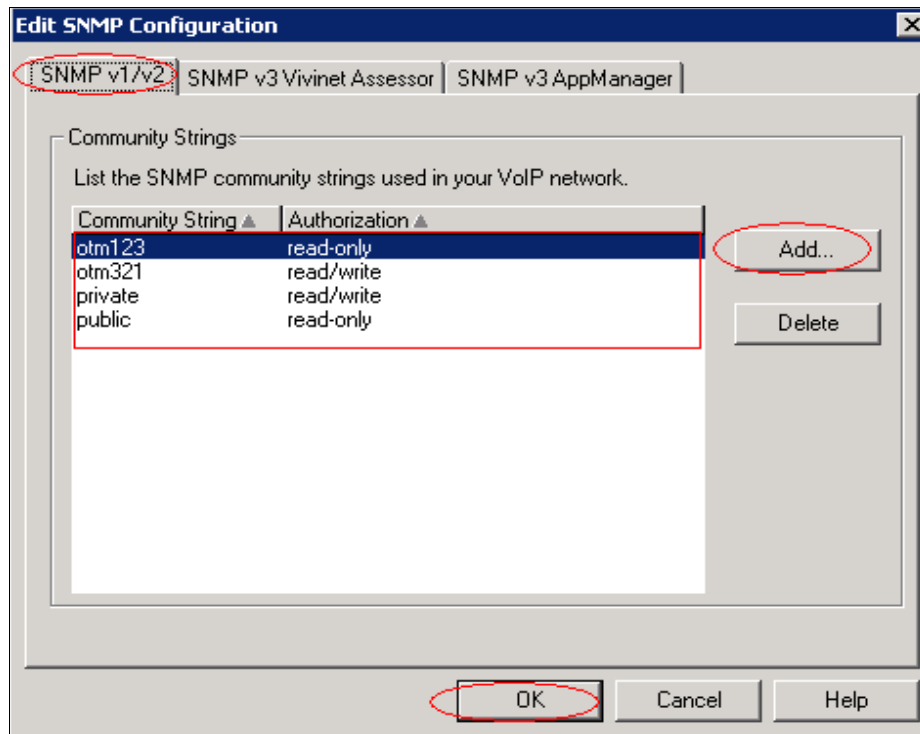


Figure 13: Editing the SNMP Configuration

To configure the Call Server value, select the **Call Server** option as shown in **Figure 12** above. Call Server window is presented as shown in **Figure 14** below. Click on **Add** button. Input the **Call Server** IP address, **User ID** and **Password**. Click on **OK** to complete the configuration.

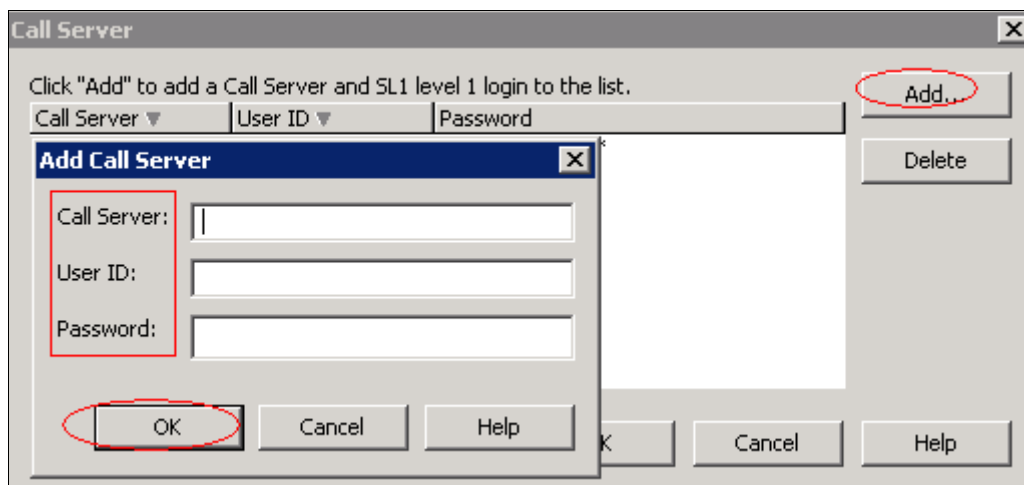


Figure 14: Editing the Call Server Configuration

To configure the Signaling Server value, select the **Signaling Server** option as shown in **Figure 12** above. Signaling Server window is presented as shown in **Figure 15** below. Click on **Add**

button. Input the **Signaling Server** IP address, **User ID** and **Password**. Click on **OK** to complete the configuration.

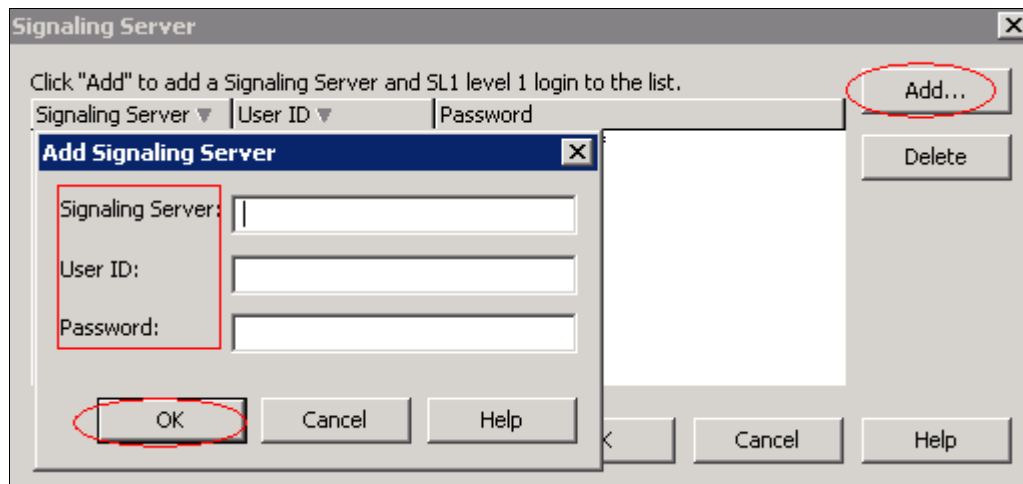


Figure 15: Window showing the Job NortelCS_Alarms

7. Verification Steps

The following tests were conducted to verify the solution between the CS1000 and Vivinet Diagnostics Application,

- QoS0028 alarm was triggered by the CS1000 and Vivinet Diagnostics captured this trap and provided the details.
- Ensure Vivinet Diagnostics does not interfere with the CS1000 Signaling Server's capability of processing commands using Telnet.
- Ensure Vivinet Diagnostics does not impact phone calls when calls are made during a diagnosis.
- Ensure Vivinet Diagnostics does not impact the quality of a phone call when diagnostics are run while a phone call is in progress.

8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 2**. The NetIQ Vivinet Diagnostics 2.3 is considered compliant with Avaya CS1000 Rls 7.5.

9. Additional References

[1] Product documentation for Avaya products may be found at:

<https://support.avaya.com/css/Products/>

[2] Product documentation for NetIQ Vivinet Diagnostics may be found at:

<https://www.netiq.com/support/default.asp?tab=ProductSupport&product=NONE>

©2011 Avaya Inc. All Rights Reserved.

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

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