Avaya Solution & Interoperability Test Lab

Application notes for NetIQ AppManager 7.0.1 with Avaya™ Communication Server 1000 Release 6.0 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya™ Communication Server 1000 Release 6.0 and the NetIQ AppManager 7.0. During the compliance testing, the AppManager was able to deliver systems management solution for the CS1000 system. This test was performed to verify the basic interaction between the CS1000 and the AppManager to ensure there is no adverse impact on the CS1000 system or any other management interfaces.

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

1. Introduction

This is the interoperability test report for Avaya Communication Server 1000 Release 6.0 (hereafter referred to as CS1000) and NetIQ AppManager 7.0.1 (hereafter referred to as AppManager). This test was performed to verify the basic interaction between CS1000 and NetIQ AppManager to ensure that there is no adverse impact on the CS1000 system or any other management interfaces while NetIQ AppManager is running and accessing CS1000 systems. During the compliance testing, the AppManager was able to provide system administrators with managing, reporting, analyzing performance and health check for the CS1000 system. It was also able to gather performance data for real-time and historical reporting and analysis.

1.1. Interoperability Compliance Testing

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

- Discovery of Avaya CS1000 devices, including CoRes system and SIP Line.
- Retrieving information from Avaya CS1000 devices.
- Monitor health of Avaya CS1000 devices (including SIP Line resources) such as HealthCheck and Alarms.
- Phone Inventory is retrieved from Avaya CS1000.
- BMZ_CallQuality metrics are retrieved from Avaya CS1000.

1.2. Support

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

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

2. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing event between the Avaya CS1000 Release 6.0 and NetIQ AppManager 7.0.1.

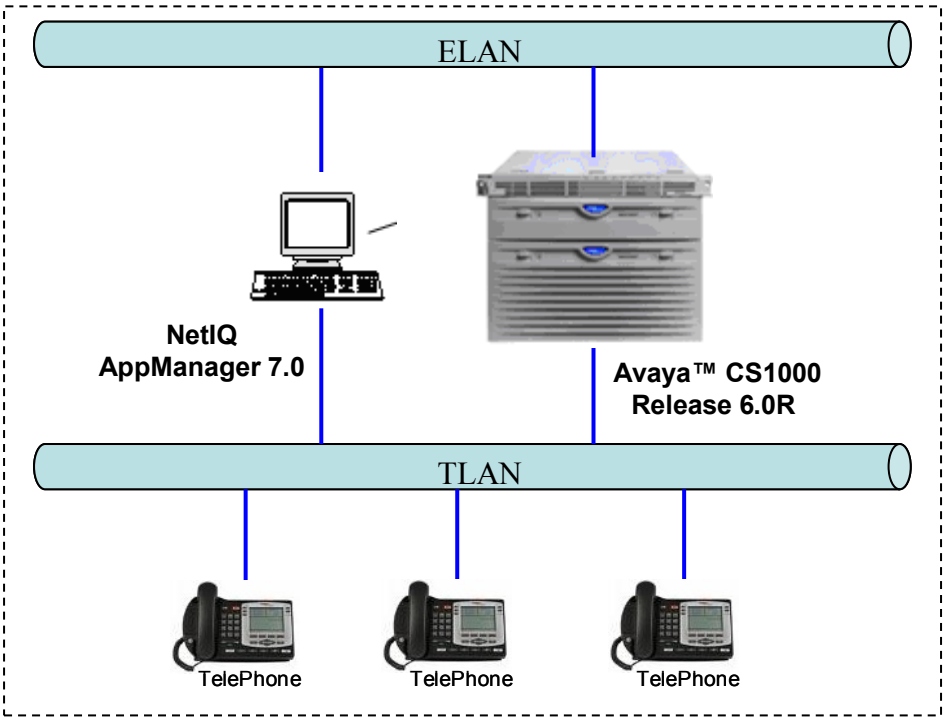


Figure 1: Avaya Interoperability Lab configuration.

3. Equipment and Software Validated

System	Software/Loadware Version
Avaya™ Communication Server 1000	• Call Server (CPPM): 6.00R + latest deplist • Signalling Server (HP DL320): 6.00.18 + latest deplist • Signalling Server (CPPM): 6.00.18 + latest deplist
IP phones	• 1230 - Model NTYS20 • 1140E - Model NTYS05 • 2004 – Model NTDU82
NetIQ AppManager	• Version of AppManager is 7.0.1 build 7.0.11256 • Version of the CS1000 monitoring module is 7.4.30 • Version of the Network Device is 7.4.55.0

4. Avaya CS1000 Configuration

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

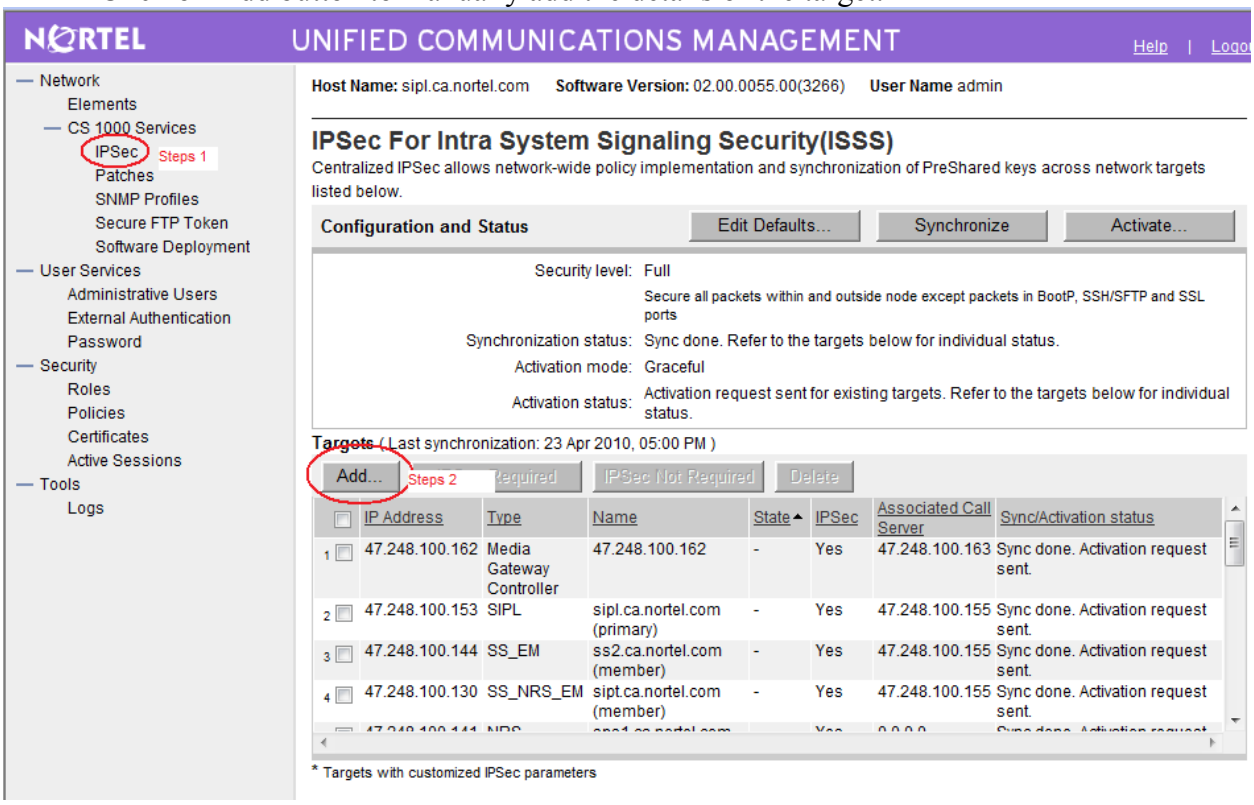
Here is a summary of CS1000 Configuration:

a. ELAN and TLAN IP addresses of AppManager machine are added to IPSec in CS1000 system. See **Section 4.1.**

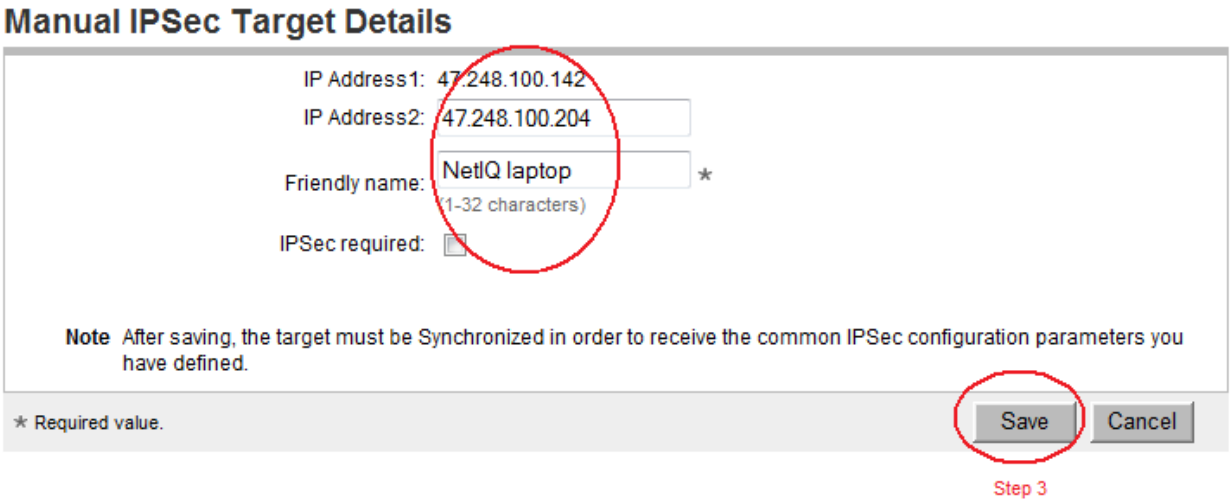
b. ELAN IP address of AppManager machine is configured as a trap receiver. See **Section 4.2.**
c. "snmpqosq" account (can be found in the "QOS MIB Access Setup" section of NTP NN43001-719_03.02_Fault-Management-SNMP.pdf). In the releases prior to Release 6.0, to access QOS MIB on Signalling Server (SS), user had to create special LAPW user account with user name as 'snmpqosq'. In Release 6.0, QOS MIB as well as QOS-TRAFFIC MIB can be accessed with regular ADMIN_COMM(2) community string. Creation of LAPW user account with user name 'snmpqosq' is not required.
d. Setting QoS Call Basis Thresholds. See **Section 4.3.**
e. Setting Zone Notification Levels. LD 117: chg zqnl <zone> 4 (on all zones). See **Section 4.4.**
f. Insecure shell access enabled. If disabled, enable it by the command "enl shells insecure" in LD 117. See **Section 4.5.**
g. Setting Bandwidth Management Zone Thresholds. See **Section 4.6.**
h. LD 117: inv midnight sets; inv entity sets on; inv generate sets. See **Section 4.6.**

4.1. IPSec configuration on CS1000

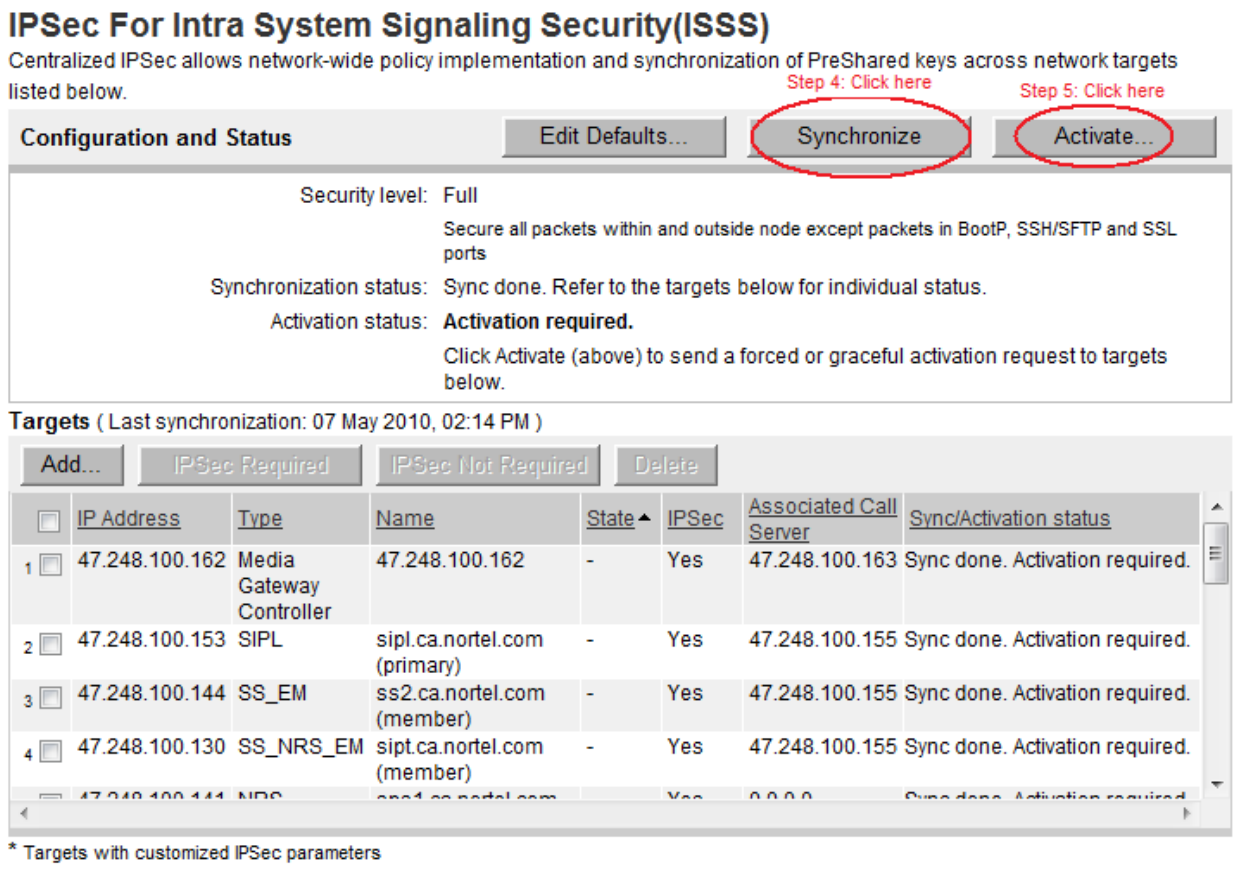
- Login to UCM and then add all IP addresses of NetIQ AppManager machine to IPSec table.
- Launch ISSS Page by clicking on IPSec on the UCM Page.
- Click on Add button to manually add the details of the target.



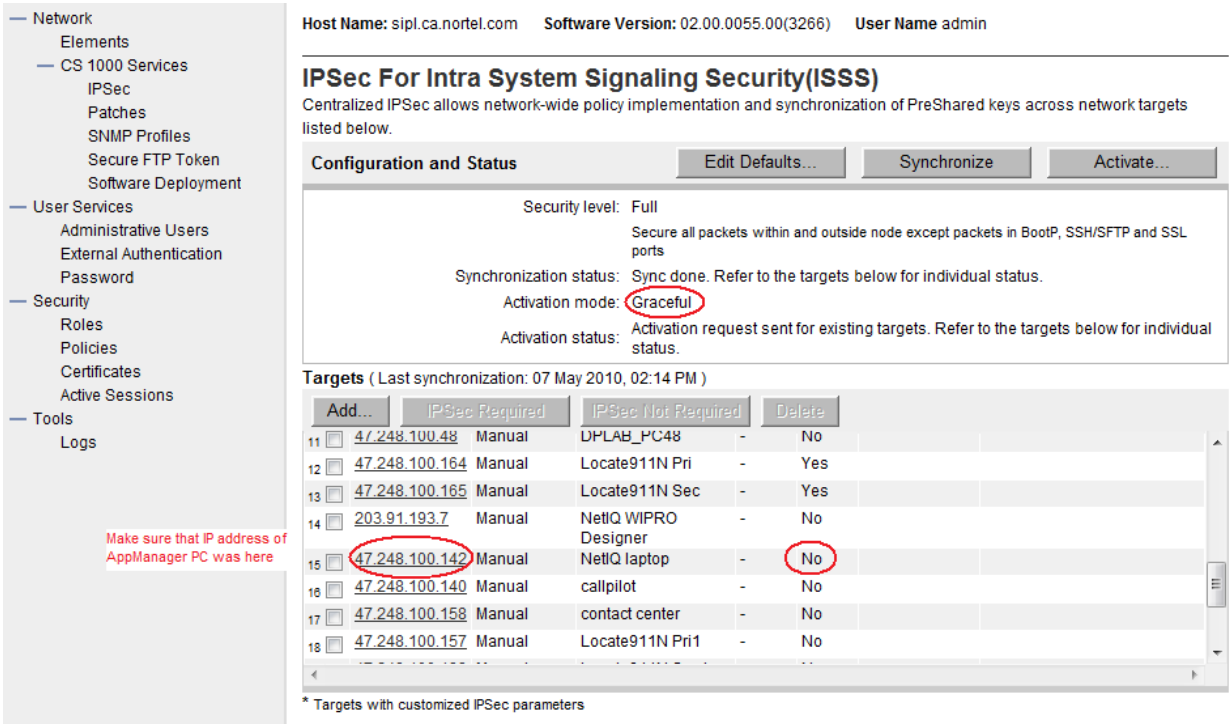
- Enter the details of the target as displayed below and Click on Save button.



- Click on synchronize button.

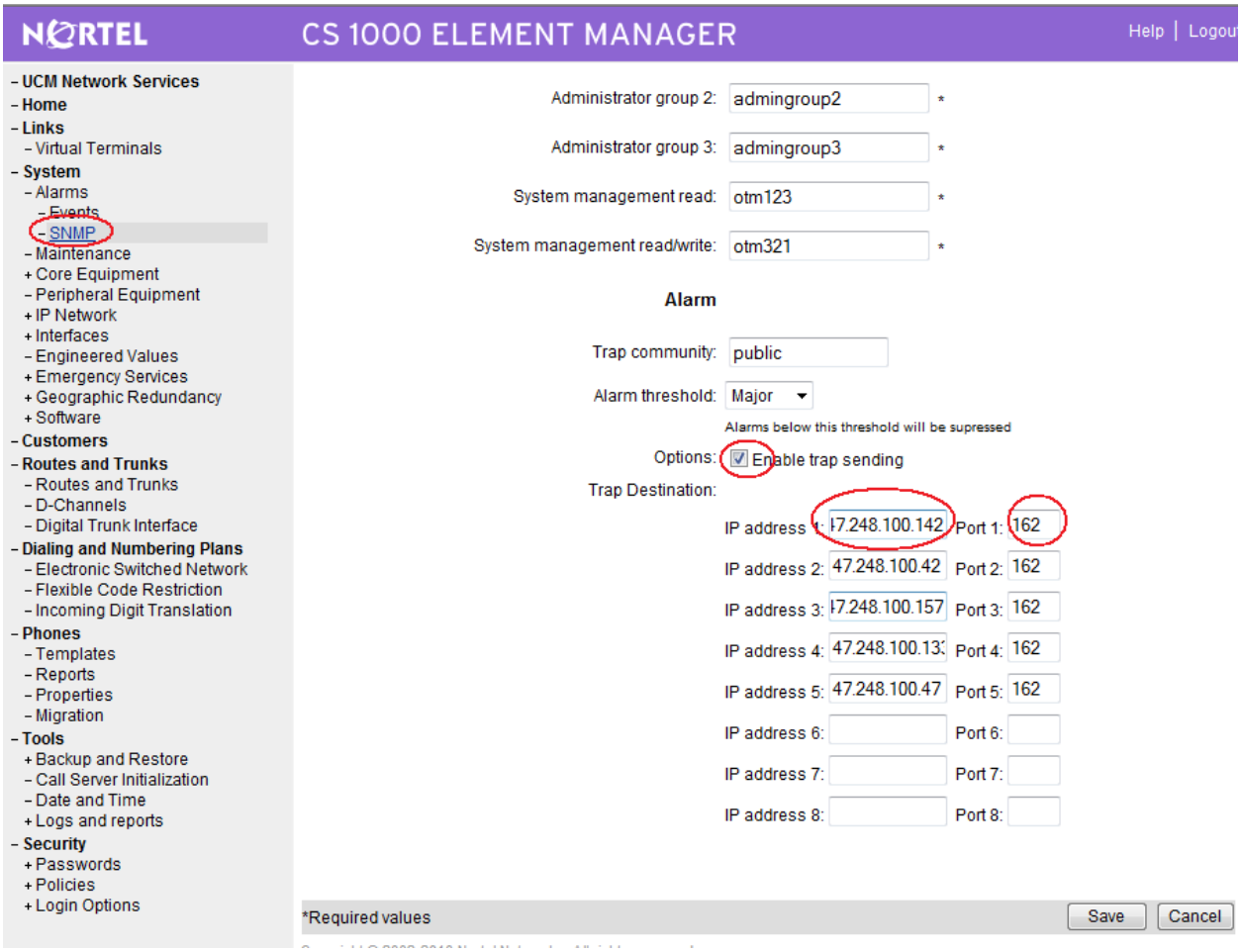


- Click on Activate button after successful synchronization to activate ISSS on the target.



4.2. AppManager is configured as a trap receiver

- Login Element Manager.
- Navigate to **System**, click **SNMP**, and then configure ELAN IP address of AppManager machine as a trap receiver.

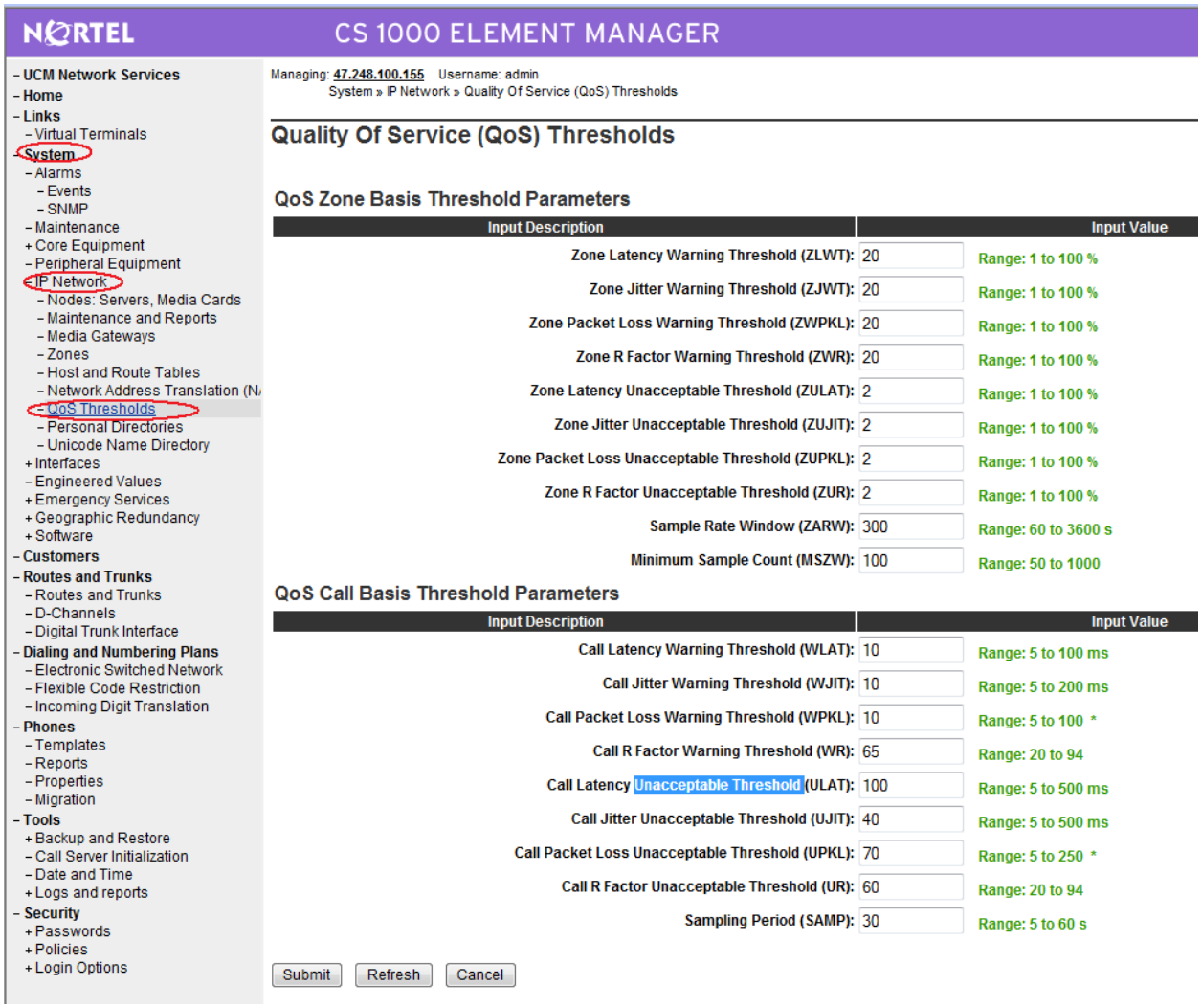


4.3. Setting QoS Call Basis Thresholds

Configure QoS call basis threshold levels in Avaya CS1000 Element Manager. All quality metrics that fall outside of the thresholds are identified by the Alarms script.

To configure **QoS thresholds**:

1. Navigate to **System**, click **IP Network**, and then click **QoS Thresholds**.
2. In the **QoS Call Basis Threshold Parameters** section, set the Warning and Unacceptable thresholds appropriate for current environment.
3. Click Submit. A message indicates that all changes will not take effect until after a Call Server data dump has been performed.
4. Click OK.
5. Use Element Manager or Overlay 43 to perform a Call Server data dump.



4.4. Setting Zone Notification Levels

Zone notification levels determine which QoS alarms are sent to the AppManager as SNMP traps. The following table 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

If a zone notification level is not specified, all QoS alarms will fall into the default level, which is 0. The 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 in Overlay 117: CHG ZQNL (ex: LD 117: chg zqnl 0 4).

4.5. Enabling Insecure Shell Access

The AppManager does not support Secure Shell (SSH) access. Instead, it requires Telnet access.

To enable insecure Shell access on SS:

1. Log in to the Linux-based Signaling Server.
2. Issue the following command: harden telnet on.

To enable insecure Shell access on CS:

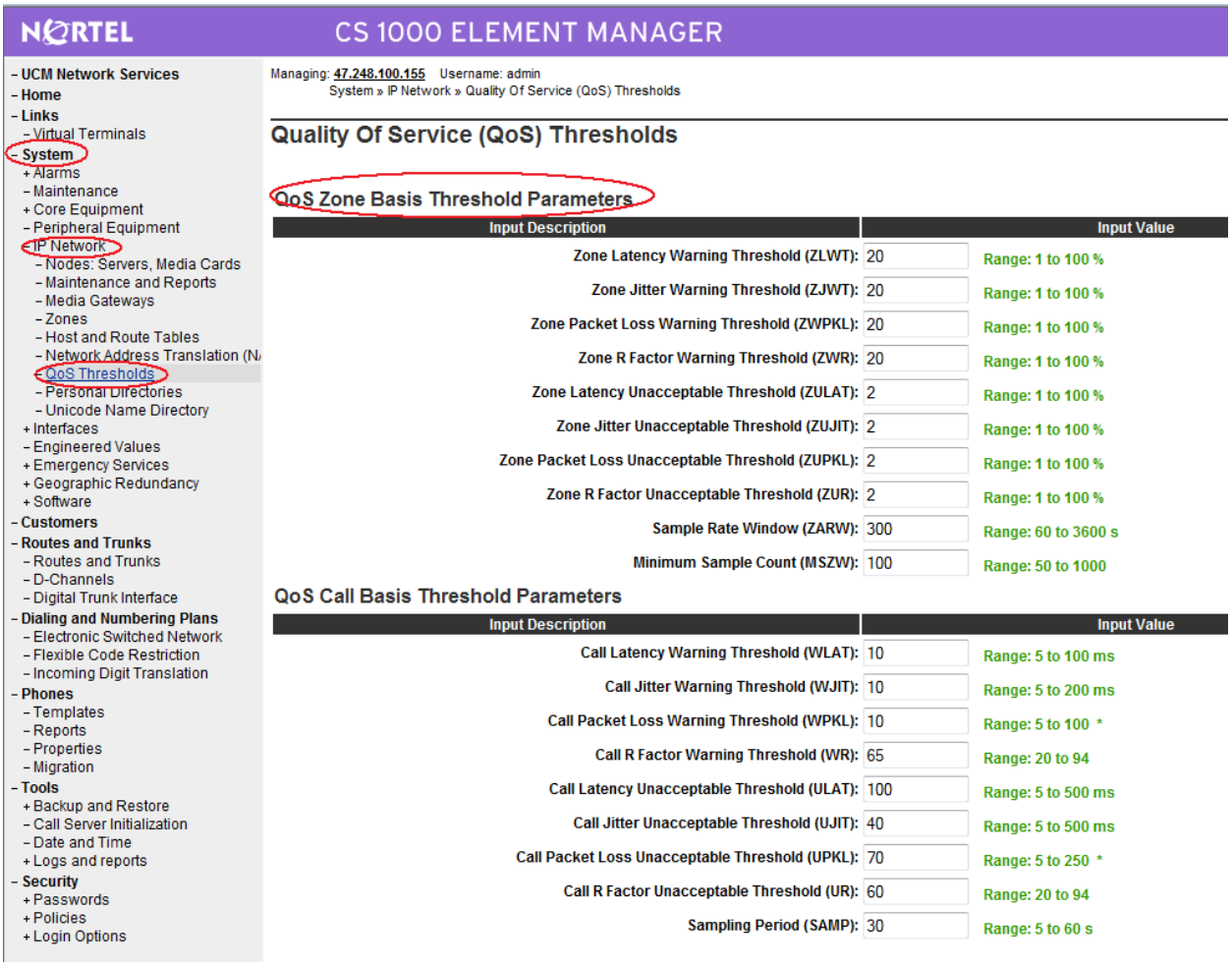
1. Log in to Overlay 117:
2. Issue the following command: ENL SHELLS INSECURE.

4.6. Setting Bandwidth Management Zone Thresholds

Before gathering Bandwidth Management Zone (BMZ) call quality metrics with the BMZ_CallQuality script, manually configure QoS zone basis threshold levels in Avaya CS1000 Element Manager.

To configure BMZ QoS thresholds:

1. Navigate to **System**, click **IP Network**, and then click **QoS Thresholds**.
2. In the **QoS Zone Basis Threshold Parameters** section, set the **Warning** and **Unacceptable** thresholds appropriate for current environment. Call quality metrics that fall outside of the thresholds more than *n* times in an hour will be identified by the BMZ_CallQuality script.
3. Click **Submit**. A message indicates your changes will not take effect until after a Call Server data dump has been performed.
4. Click **OK**.
5. Use Element Manager or Overlay 43 to perform a CallServer data dump.



4.7. Configuring the Call Server to count IP Phones

The Phone Inventory 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. However, for this process to work, two or three commands should be issued in Overlay 117:

• Tell the Call Server to generate the inventory report once every midnight.

INV MIDNIGHT SETS

• Tell the Call Server to include the IP telephones from the inventory report in the Entity MIB.
INV ENTITY SETS ON

• Optional: Tell the Call Server to generate the inventory report immediately. Two above commands generate an inventory report at midnight. If user does not want to wait until midnight to generate the inventory report and add the phones to the Entity MIB, issue a third Overlay 117 command: INV GENERATE SETS.

Note
- Issue these commands before running Discovery_NortelCS.
- The inventory report can take hours to complete, based on the number of phones, which is why it normally runs at midnight. Because the task that generates the inventory report on the CS1000 runs at a low priority, it should not interfere with call processing.

5. NetIQ AppManager configuration

This section describes the steps to configure the AppManager for CS1000. This section assumes that AppManager has been installed. For more information about installing AppManager or about AppManager system requirements, please see the Installation Guide for AppManager, reference [3].

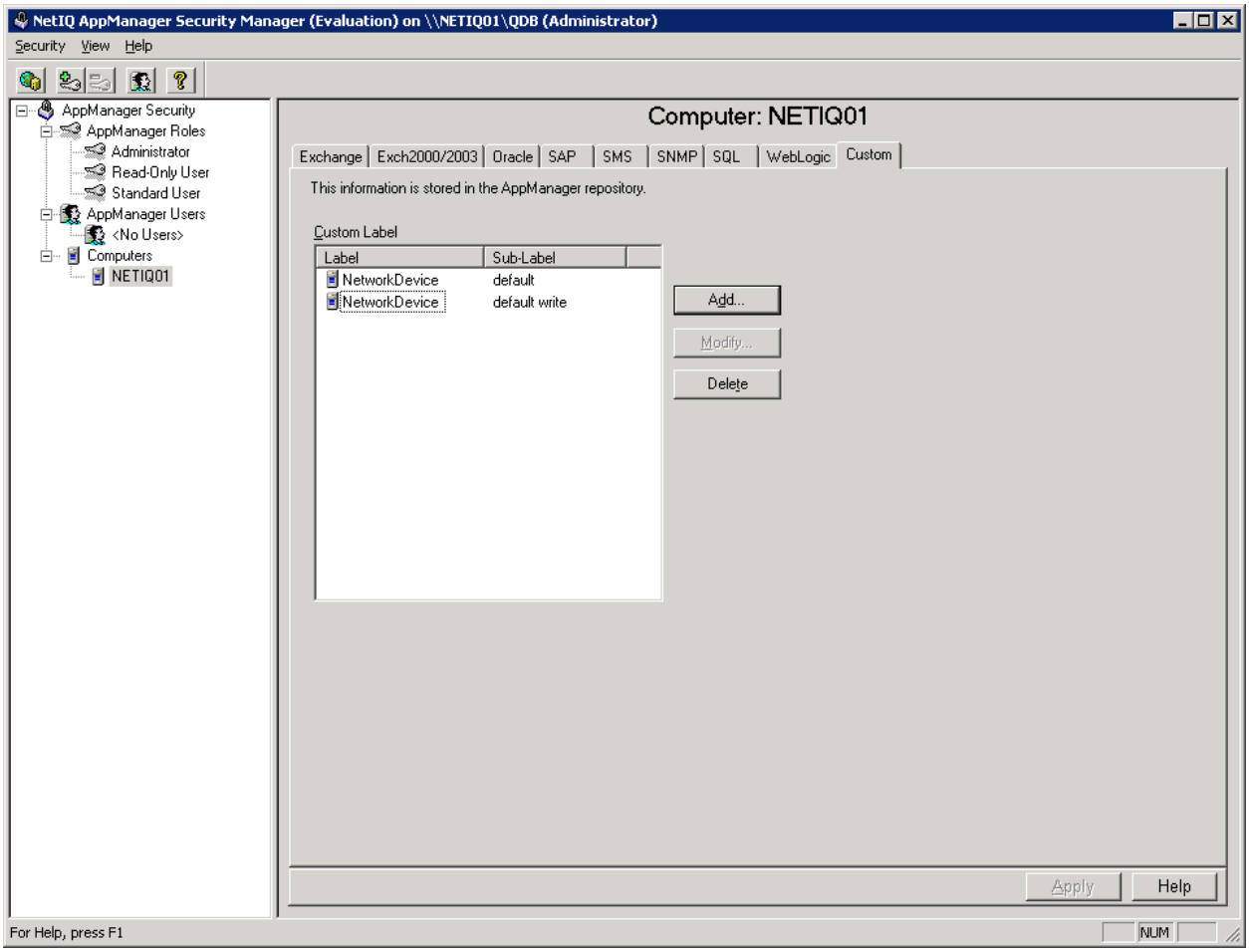
After installing AppManager, the following configuration must be performed to provide AppManager to access Avaya CS1000 as SNMP traps and the phone inventory on the Call Server. The user guide is available via the following link:
- The user guide is c:\Program Files\NetIQ\AppManagerforNortelCS1000.pdf
- The readme is: c:\Program Files\NetIQ\AppManagerforNortelCS1000_ReadMe.htm

5.1. Configuring SNMP Community Strings

To enable AppManager to use SNMP to access Avaya CS1000 devices, the SNMP community strings needs to be configured in AppManager Security Manager as follows:

On the Custom tab in Security Manager, complete the following fields:

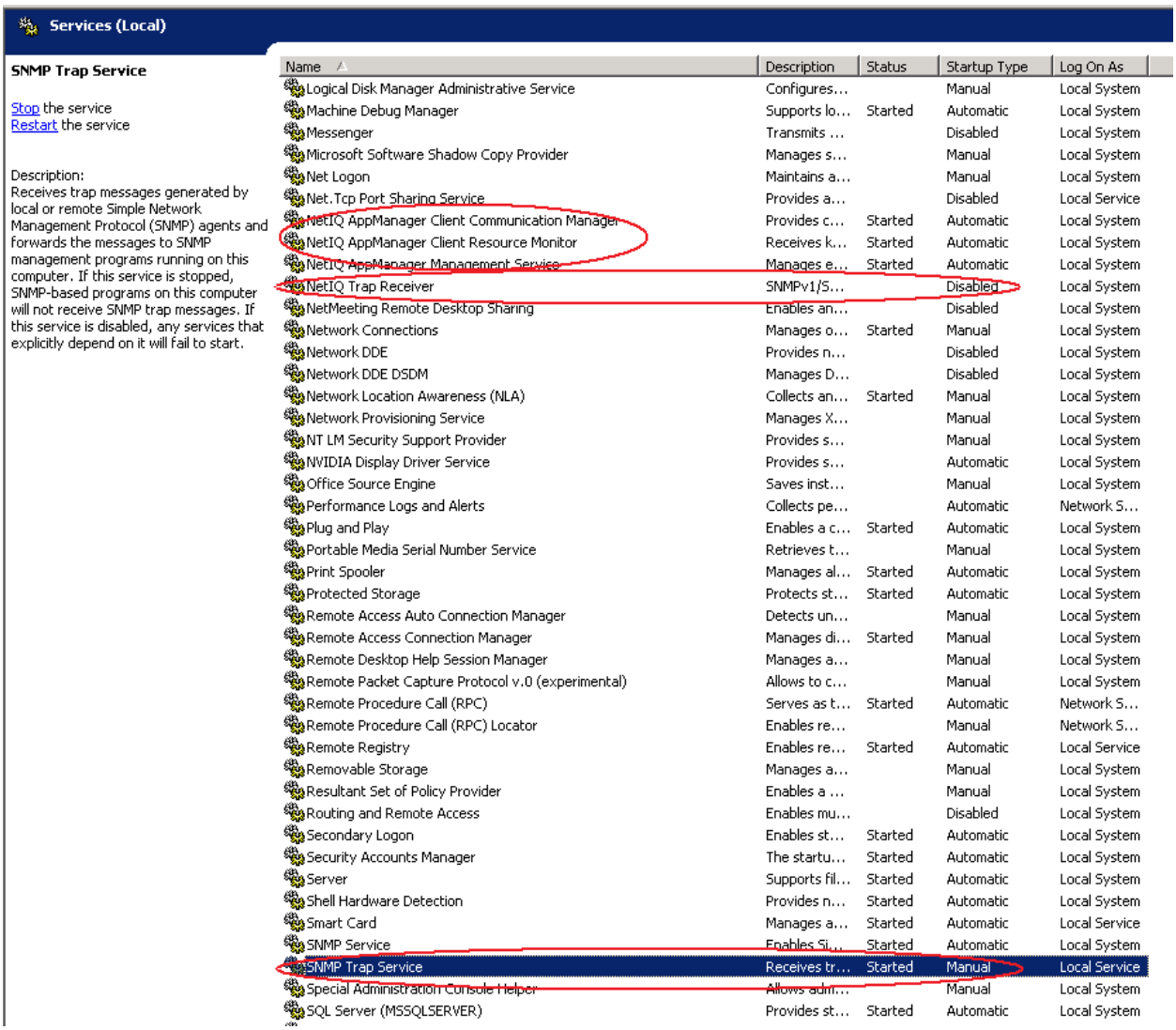
- For all devices that use the same read-only community string, type default.
  Use the default sub-label for Call Server, Network Routing Server (NRS), Enterprise Common Manager (ECM).
- For all devices that use the same read/write community string, type default write.
  Use the default write sub-label for all Signaling Servers, VGMCs, MGCs, and MC32Ss



5.2. Disabling NetIQ Trap Receiver

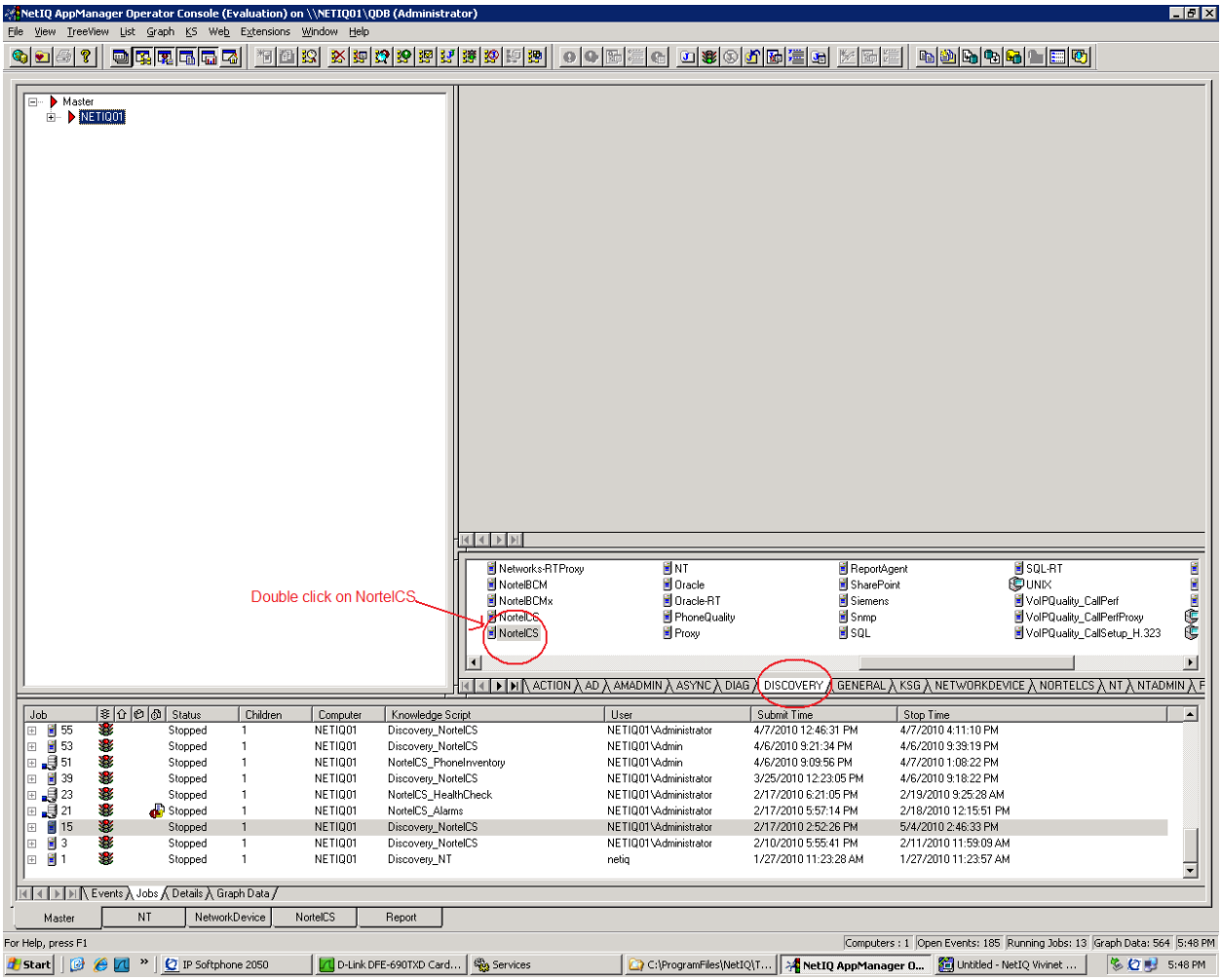
To disable **Trap Receiver** and enable **SNMP Trap Service** on the AppManager machine:

1. On the AppManager computer, navigate to **Control Panel > Administrative Tools > Services**.
2. On the list of services, right-click **NetIQ Trap Receiver** and select **Stop**.
3. Right-click **NetIQ Trap Receiver** again and select **Properties**.
4. In the **Startup type** field, select **Disabled**.
5. Click **OK**.
6. On the list of services, right-click **SNMP Trap Service** and select **Properties**.
7. In the **Startup type** field, select **Automatic**.
8. Click **Start**, and then click **OK**.
9. On the list of services, right-click **NetIQ AppManager Communication Manager** and select **Restart**.
10. On the list of services, right-click **NetIQ Client Resource Monitor** and select **Restart**.

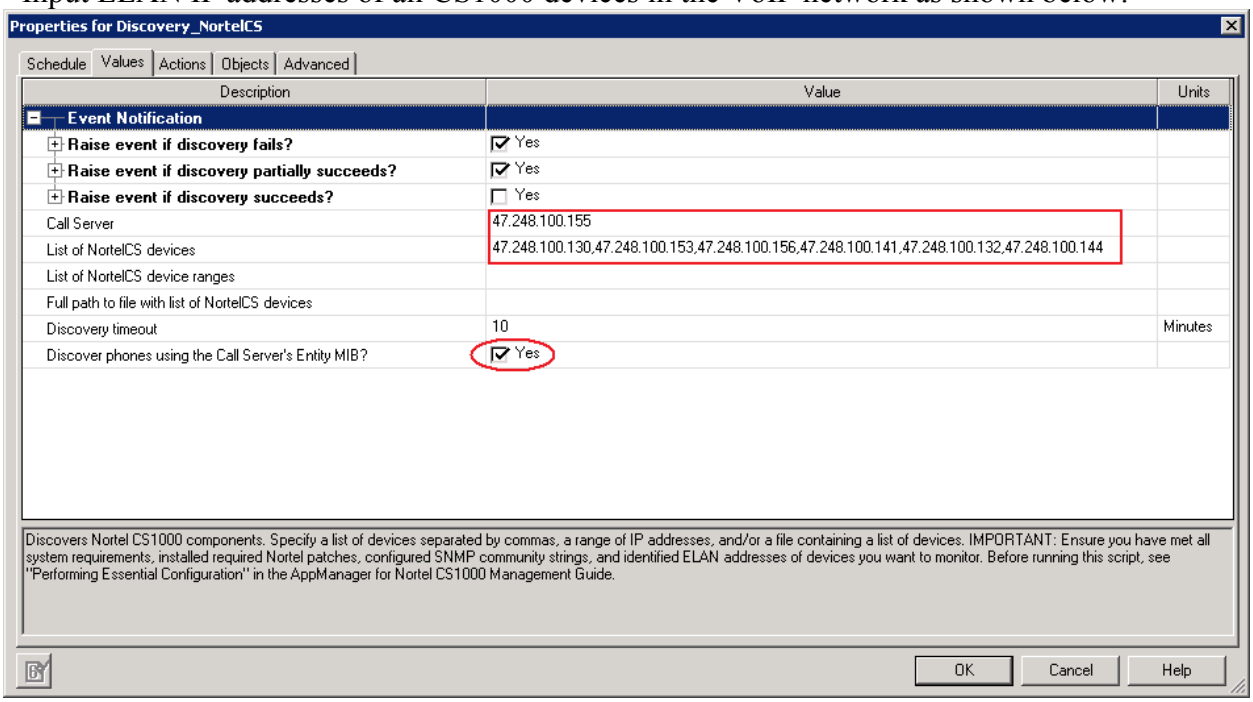


5.3. NetIQ AppManager Configuration for Discovery of Avaya CS1000 devices.

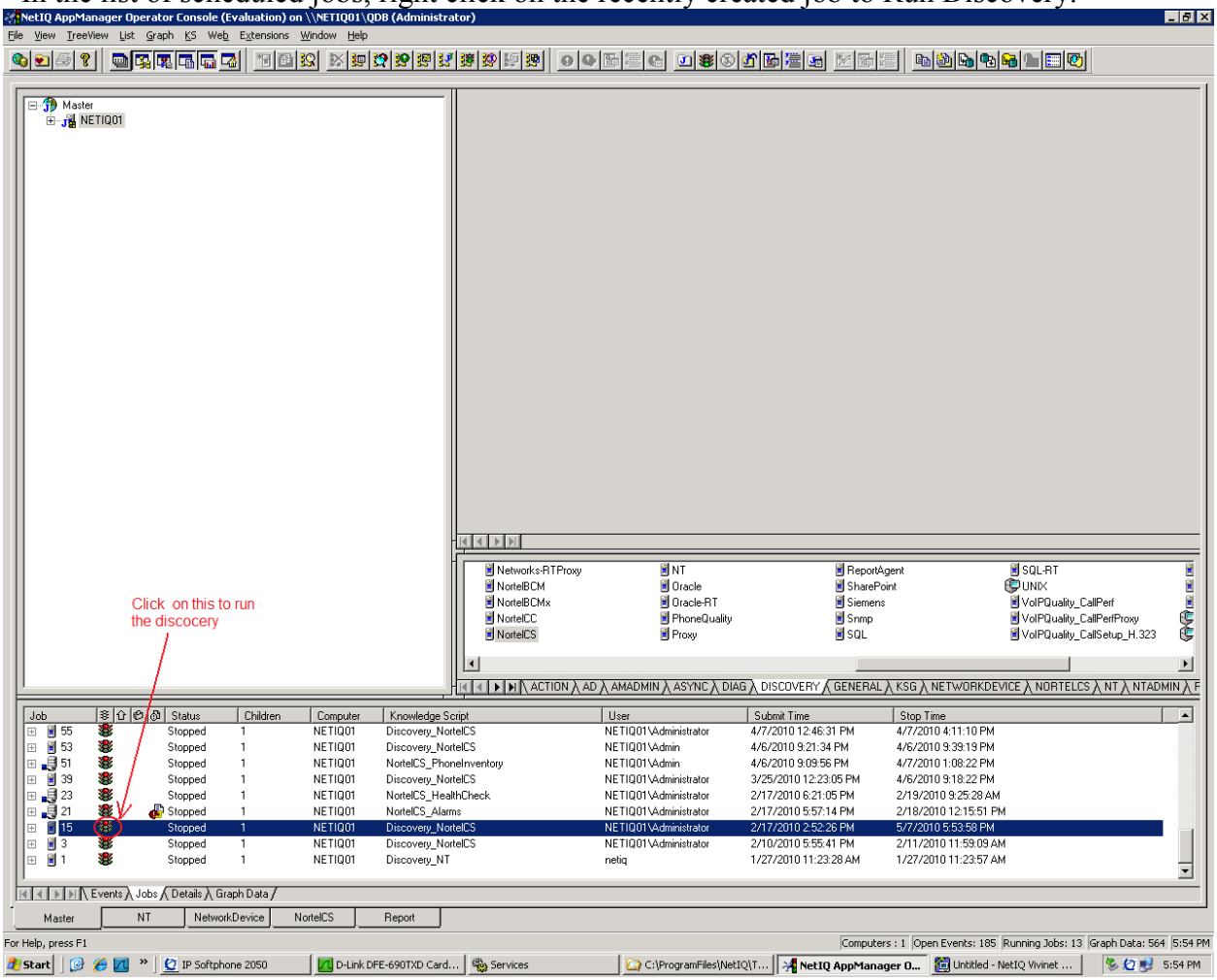
- Double click on NortelCS as shown below.



- Input ELAN IP addresses of all CS1000 devices in the VoIP network as shown below:



- In the list of scheduled jobs, right click on the recently created job to Run Discovery.



6. 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.

6.1. General Test Approach

The general test approach was to integrate the NetIQ 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:

- Discovery of Avaya CS1000 devices, including CoRes system and SIP Line.

- 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.
- BMZ_CallQuality metrics is retrieved from Avaya CS1000.
- All AppManager module scripts are running at the same time with its default values.

6.2. Test Results

The objectives outlined in **section 6.1** were verified and met. All tests were executed and passed. The following limitations have been noted during the compliance test:

- The Phone Inventory report only includes "IP phones" that are counted towards the licensing. The IP phones that are designated as "<Unavailable>" are not counted.
- The CallCapacity script only supports for Avaya CS1000 Call Server version 4.50 or 5.0 and it does not support other versions of the Call Server.
- The AppManager is sometimes crashed after user changes some parameters in NortelCS_Alarms while it is running. This issue was seen intermittently. It was also observed for HealthCheck script and others. Below are the steps to reproduce this issue.
  - Step 1: Open the NortelCS_Alarms when it's running.
  - Step 2: Select Objects
  - Step 3: Click **ok** and then an error message will appear and the application will be terminated.

7. Verification Steps

This section provides some steps that can be followed to verify that the Avaya CS1000 and NetIQ AppManager configuration steps have been done correctly.

7.1. Configure SNMP community strings.

For more information, refer to "Configuring SNMP Community Strings" in **section 5.1**.

7.2. Set up phone inventory process

Issue the following commands in Overlay 117 to check the phone inventory process on CS:

```
=> INV ?
INV ENTITY SETS - Include phone set inventory in Entity MIB, ON, OFF or STATUS
INV GENERATE - Generate inventory CARDS, SETS, LOCRPT, ALL or ABORT
INV MIDNIGHT - Generate inventory CARDS, SETS, LOCRPT, ALL, OFF or STATUS
INV PRT - Print STATUS, CARDS, SETS, LOCRPT or ALL

=> INV ENTITY SETS STATUS
Phone set inventory in Entity MIB is ON

=> INV MIDNIGHT STATUS
Generate inventory file for CARD SETS LOCRPT at midnight
```

For more information, refer to "Configuring the Call Server to Count IP Phones" in **section 4.7.**

7.3. Identify the SNMP trap receiver

Identify the AppManager computer as an SNMP trap receiver to receive Avaya CS1000 Alarms.
Issue the following commands in Overlay 117 to check SNMP configuration:

```
=> PRT SNMP_SYSGRP
System Description: PR:"CS1000E" SW:"Call Server, Sys 4021" BN:"6.00R" HW:"CP-PM" (c) Nortel
Networks
System Name       : sipt.ca.nortel.com
System Contact    : datna@nortel.com
System Location   : Belleville, ON, Canada
System Object ID  : 1.3.6.1.4.1.562.3
System Uptime     : 34 days, 0 hours, 30 minutes, 14 seconds

=> PRT OPEN_ALARM
Open Alarm destination #0 is 47.248.100.142:162
Open Alarm destination #1 is 47.248.100.42:162
Open Alarm destination #2 is 47.248.100.157:162
Open Alarm destination #3 is 47.248.100.133:162
Open Alarm destination #4 is 47.248.100.47:162

=> PRT ADMIN_COMM
Administrator community string (1): admingroup1
Administrator community string (2): admingroup2
Administrator community string (3): admingroup3

=> PRT ENABLE_TRAPS
ENABLE_TRAPS ON

=> PRT SYSMGMT_COMM
System Management Read Community : otm123
System Management Write Community: otm321
System Management Trap Community: public
```

For more information, please refer to **section 4.2.**

7.4. Set QoS thresholds

Issue the following commands in Overlay 117: => PRT QSTHS
For more information, refer to “Setting QoS Call Basis Thresholds” in **section 4.3**.

7.5. Set zone notification levels

Zone notification levels determine which CS1000 QoS alarms are sent to the AppManager.
Issue the following commands in Overlay 117 to make sure that all zone notification levels are 4.

```
=> PRT ZQNL all
 _____________________________________________
|     |                         |
| ZONE |    QoS Alarm Notification Level     |
|     |                         |
|     |                         |
|---------------------------------------------|
|  0  |            4            |
```

```
|-----------------------------------------------|
|  1  |            4                |
|-----------------------------------------------|
|  2  |            4                |
|-----------------------------------------------|
| 251 |            4                |
|-----------------------------------------------|
| 252 |            4                |
|-----------------------------------------------|
| 253 |            4                |
|-----------------------------------------------|
| 254 |            4                |
|-----------------------------------------------|
| 255 |            4                |
|-----------------------------------------------|
 Number of Zones configured = 8

=>
```

For more information, see "Setting Zone Notification Levels" in **section 4.4.**

7.6. Set BMZ QoS thresholds

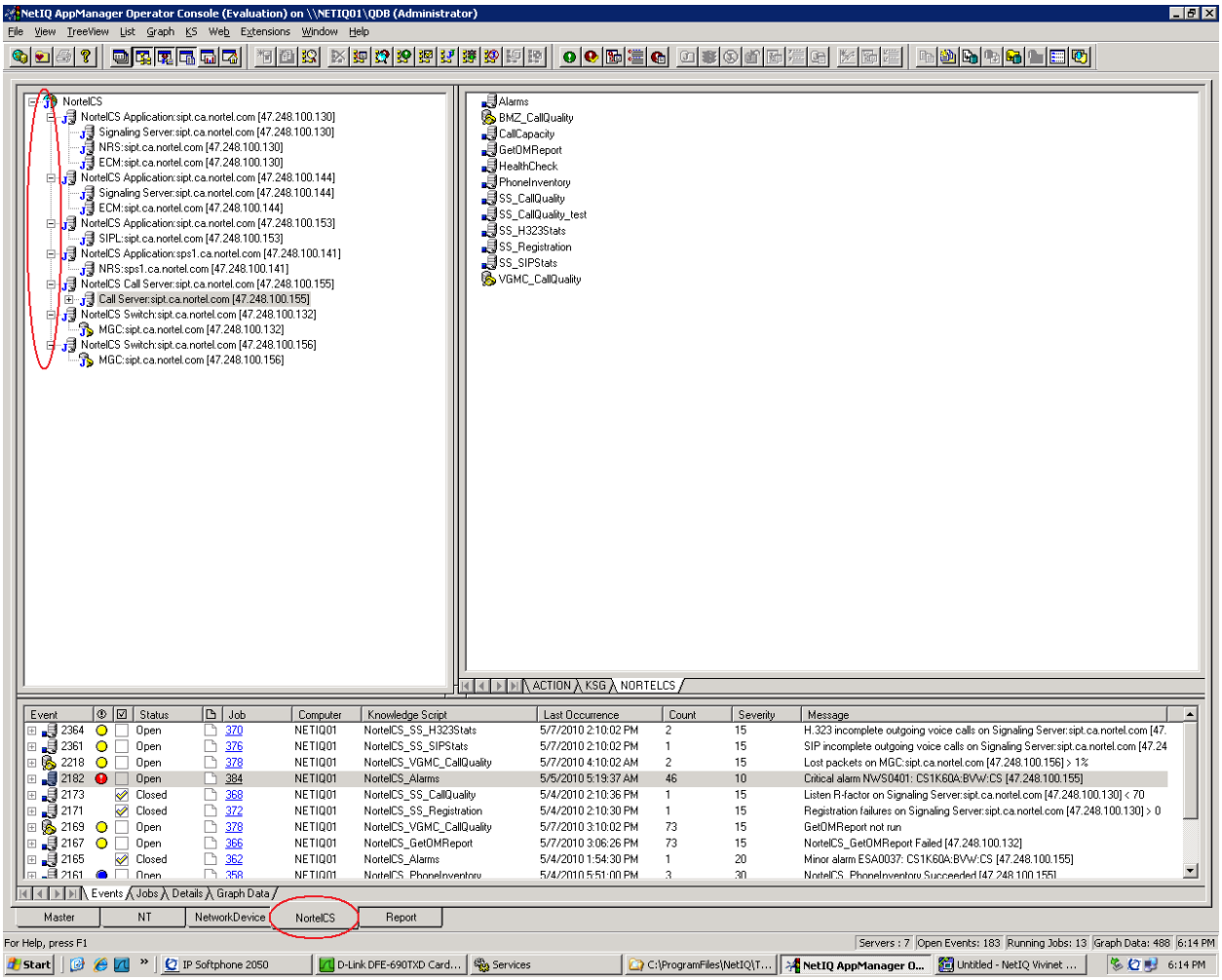
Issue the following commands in Overlay 117: => PRT QSTHS
For more information, see "Setting Bandwidth Management Zone Thresholds" in **Section 4.6.**

7.7. Enable insecure Shell access

Ensure the insecure Shell access is enabled on CS and SS. For more information, refer to **section 4.5**.

7.8. NortelCS objects

Verify that NetworkDevice and NortelCS objects are created in the AppManager treeview for each CS1000 device.



8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 6.1**, with some limitations/exceptions outlined in **Section 6.2**.

9. Additional References

[1] Product documentation for Avaya products may be found at:
http://support.nortel.com/go/main.jsp

[2] The AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site :
www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation

[3] Installation Guide for AppManager,
https://www.netiq.com/support/am/extended/documentation/default.asp

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.