



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring NetIQ AppManager with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring NetIQ AppManager with Avaya Communication Manager.

AppManager is an end-to-end systems management solution including monitoring, reporting/analysis, diagnostics and resolution. AppManager is designed to manage a variety of components – from physical hardware to server applications to end-user response time. This list of components includes Avaya Communication Manager and associated Avaya IP Telephones comprising the Voice Over IP (VoIP) telephony environment. AppManager performs event monitoring of the call server and gathers call quality data in real-time that can be used to accurately and quickly reflect the end user call experience. In addition, AppManager monitors call activity in order to track call usage and call failures.

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

1. Introduction

These Application Notes describe the procedures for configuring NetIQ AppManager with Avaya Communication Manager.

AppManager is an end-to-end systems management solution including monitoring, reporting/analysis, diagnostics and resolution. AppManager is designed to manage a variety of components – from physical hardware to server applications to end-user response time. This list of components includes Avaya Communication Manager and associated Avaya IP Telephones comprising the Voice Over IP (VoIP) telephony environment. AppManager performs event monitoring of the call server and gathers call quality data in real-time that can be used to accurately and quickly reflect the end user call experience. In addition, AppManager monitors call activity in order to track call usage and call failures.

To perform the monitoring functions, AppManager uses the following interfaces into the Avaya IP Telephony environment.

- Simple Network Management Protocol (SNMP) – AppManager uses SNMP to collect configuration and status information from Avaya Communication Manager.
- Real-time Transport Control Protocol (RTCP) – AppManager uses RTCP data from the Avaya IP Telephones to gather call quality metrics.
- Call Detail Recording (CDR) records - AppManager uses CDR records from Avaya Communication Manager to track call usage.

1.1. Configuration

Figure 1 illustrates the configuration used in these Application Notes. In the sample configuration, two sites are connected via an H.323 trunk. AppManager only monitors the VoIP infrastructure at site 1. Site 2 is present simply to generate inter-site traffic across the H.323 trunk.

Site 1 has a redundant pair of Avaya S8720 Servers running Avaya Communication Manager with an Avaya G650 Media Gateway. Also at this site is NetIQ AppManager running on a Windows 2003 Server. The AppManager installation includes the Operator Console which is used to perform AppManager configuration. In addition to the main AppManager installation, a proxy agent must also be installed which collects data from Avaya Communication Manager. This AppManager agent may be installed on the same Windows server as the main installation or on a separate PC. In the case of the compliance test, the AppManager agent was installed on the same server as the main installation. Endpoints at this site include Avaya 4600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), and an Avaya 6400 Series Digital Telephone.

Site 2 has an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Endpoints at this site include Avaya 4600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), and an Avaya 6400 Series Digital Telephone.

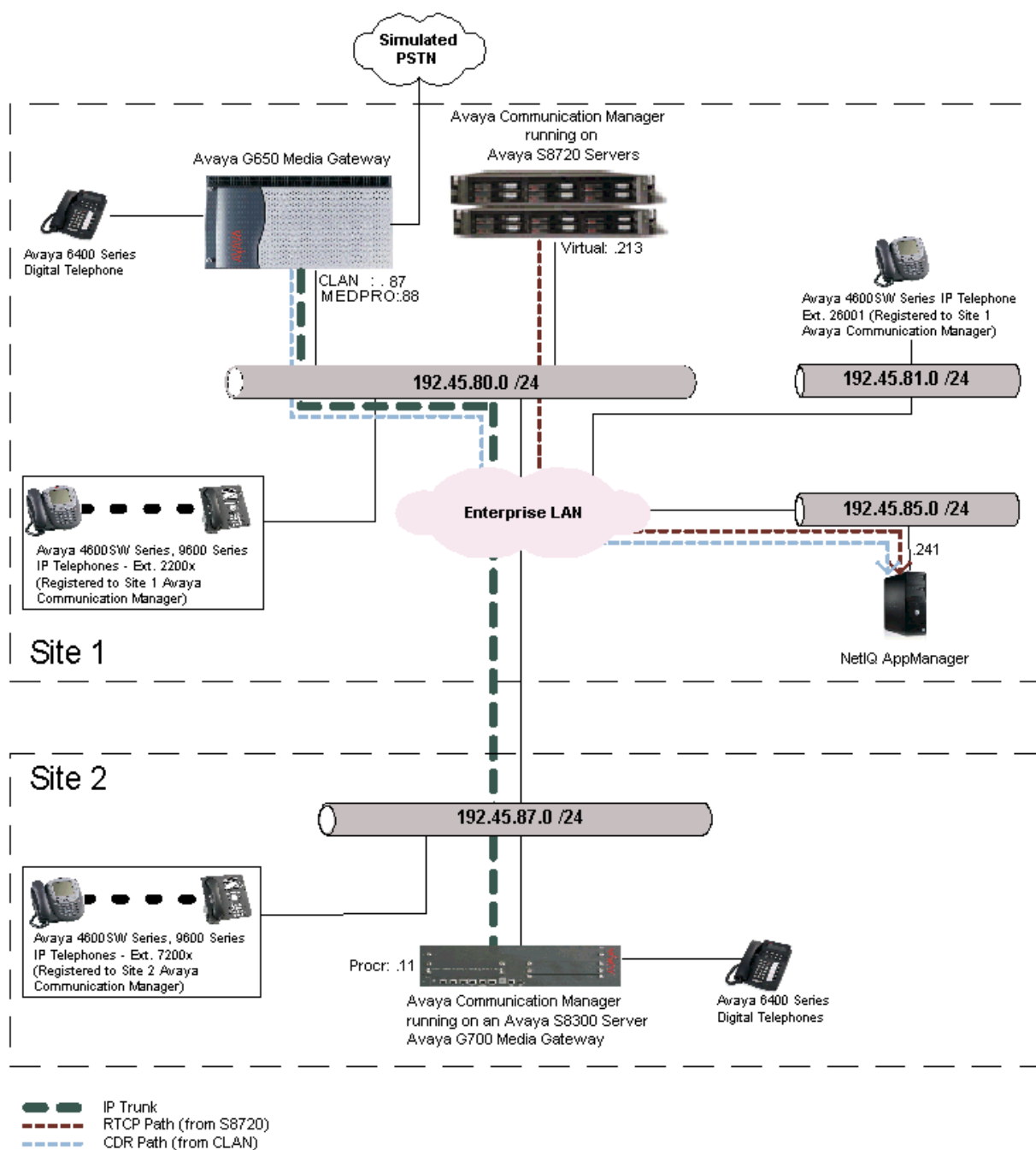


Figure 1: AppManager Test Configuration

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya S87200 Servers (at site1)	Avaya Communication Manager 4.0.1
Avaya G650 Media Gateway (at site 1) - CLAN - MedPro	TN799DP - HW 01 FW 26 TN2302AP - HW 20 FW 118
Avaya S8300 Server (at site 2)	Avaya Communication Manager 4.0.1
Avaya G700 Media Gateway (at site 2)	28.17.0
Avaya 4600 Series IP Telephones (H.323)	2.8.3
Avaya 9600 Series IP Telephones (H.323) - Avaya one-X Deskphone Edition	1.5
Avaya 6400 Series Digital Telephones	-
Windows Server	Windows 2003 Server SP2
NetIQ AppManager (on Windows 2003 Server)	7.1

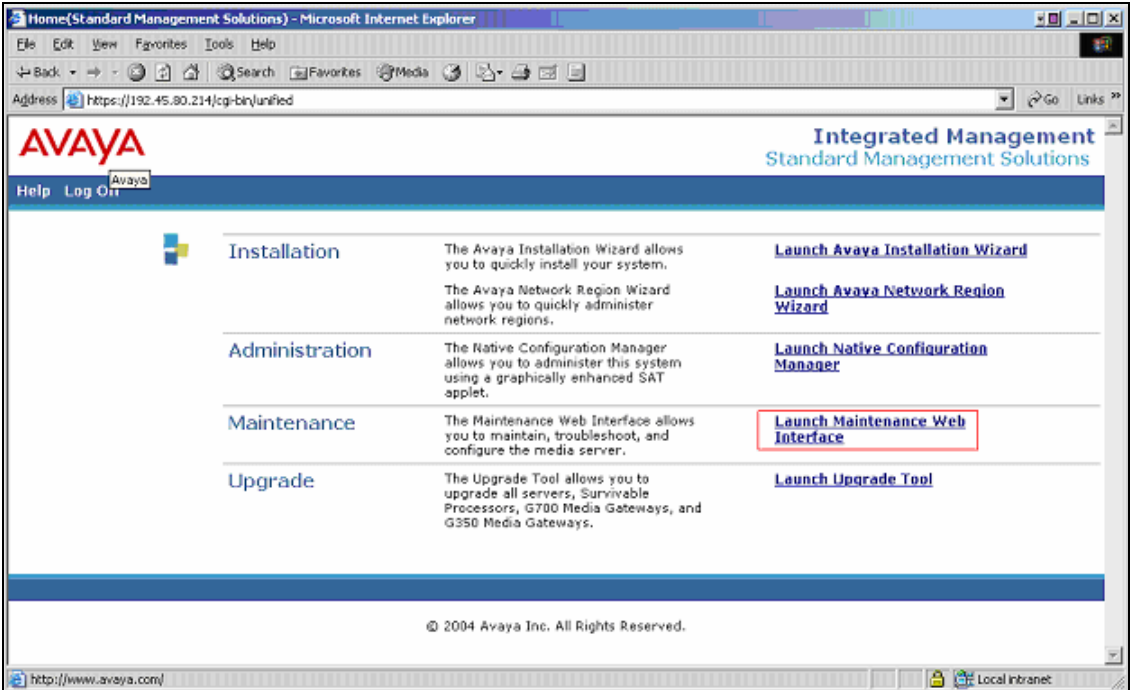
3. Configure Avaya Communication Manager

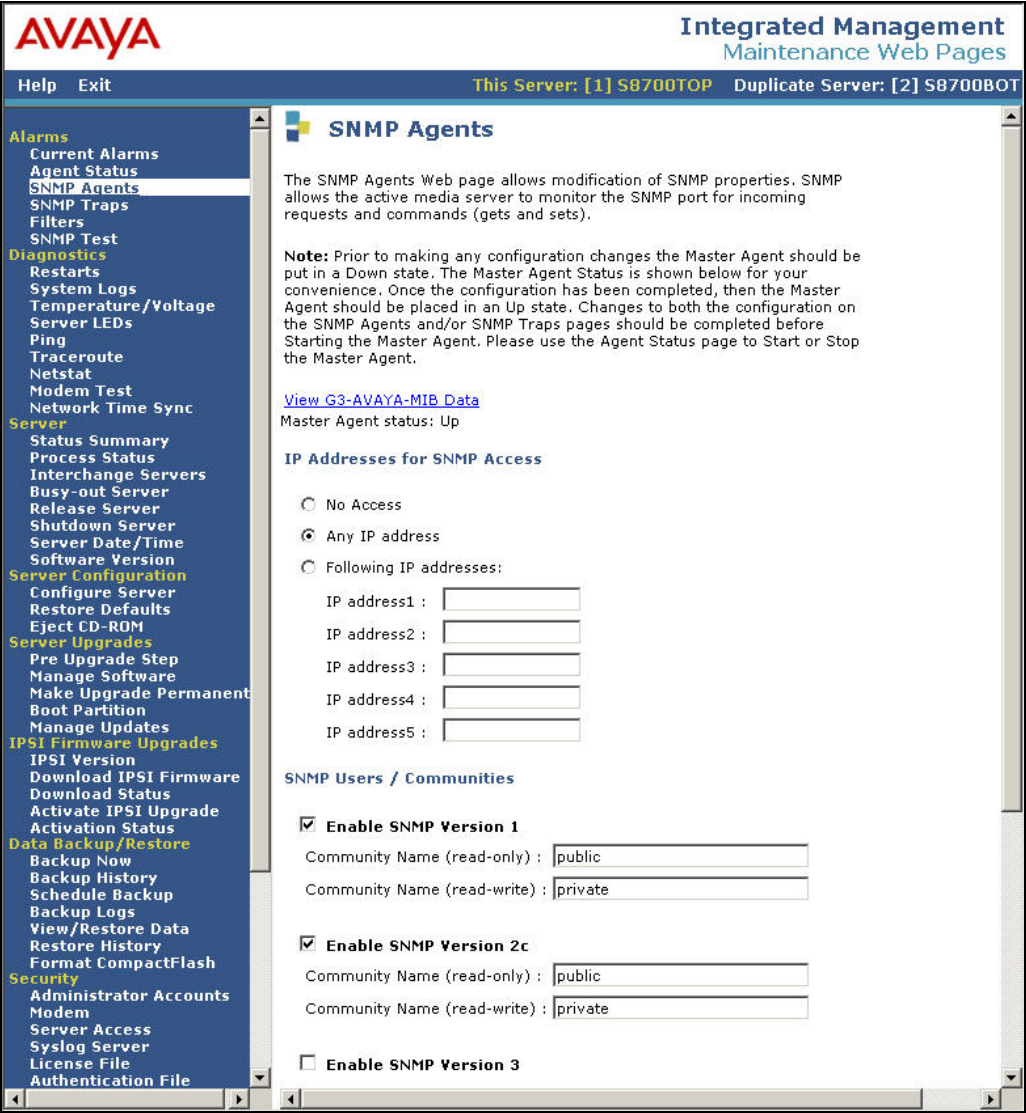
This section describes the Avaya Communication Manager configuration at site 1 necessary to interoperate with AppManager. In the test configuration, AppManager did not monitor site 2 so no configuration of Avaya Communication Manager at that site is necessary. This section is divided into three sub-sections describing the three interfaces used by AppManager to gather data on the VoIP infrastructure. **Section 3.1** describes the SNMP configuration, **Section 3.2** describes the RTCP configuration and **Section 3.3** describes the CDR configuration.


The configuration of Avaya Communication Manager in **Section 3.1** was performed using the Web interface. The configuration described in **Sections 3.2** and **3.3** was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

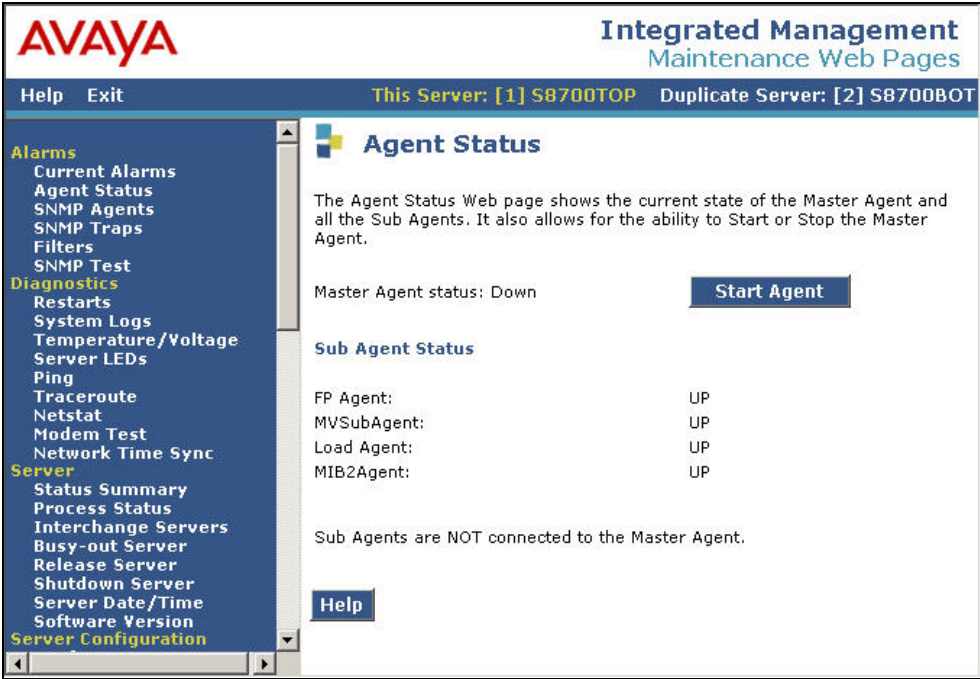
3.1. SNMP

Step	Description
1.	<p>Login</p> <p>To access the Avaya Communication Manager Web interface enter the IP address of the Avaya Server into a web browser. Login using appropriate credentials. The following page will appear. Click on Launch Maintenance Web Interface.</p>



Step	Description
2.	<p>SNMP Agent</p> <p>Navigate to Alarms→SNMP Agents in the left-hand menu pane. Under IP Addresses for SNMP Access, select <i>Any IP address</i>. Under SNMP Users / Communities, select <i>Enable SNMP Version 1</i> and enter <i>public</i> for the read-only community name. Repeat this for SNMP Version 2c.</p> 

Step	Description																																																																
3.	<p>Firewall</p> <p>The Avaya Server firewall must also be configured to allow SNMP traffic. To do this, navigate to Security→Firewall from the left-hand menu pane. Locate <i>snmp</i> in the Service column, then select both the Input to Server and Output from Server boxes.</p> <div><div><div>AVAYA</div><div>Integrated Management Maintenance Web Pages</div><div>Help Exit This Server: [1] S8700TOP Duplicate Server: [2] S8700BOT</div><div><div>Shutdown Server Server Date/Time Software Version Server Configuration Configure Server Restore Defaults Eject CD-ROM Server Upgrades Pre Upgrade Step Manage Software Make Upgrade Permanent Boot Partition Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Format CompactFlash Security Administrator Accounts Modem Server Access Syslog Server License File Authentication File Firewall Tripwire Tripwire Commands Install Root Certificate SSH Keys Ethernet Switch Ports Web Access Mask Media Gateways Configuration Miscellaneous File Synchronization IP Phones Download Files CM Phone Message File Serial Numbers</div><div><div>Firewall</div><div>The Firewall Web page lets you enable network services on the corporate LAN interface to the Avaya media server. Unselected services are automatically disabled.</div><div><div> WARNING: Some network services are required for proper operation of or access to the server. For additional details, click Help.</div><div>Please wait...</div></div><div><table><thead><tr><th>Input to Server</th><th>Output from Server</th><th>Service</th><th>Port/Protocol</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>ftp</td><td>21/tcp</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>ssh</td><td>22/tcp</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>telnet</td><td>23/tcp</td></tr><tr><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>domain</td><td>53/udp</td></tr><tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>bootps</td><td>67/udp</td></tr><tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>bootpc</td><td>68/udp</td></tr><tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>tftp</td><td>69/udp</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>http</td><td>80/tcp</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>ntp</td><td>123/udp</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>snmp</td><td>161/udp</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>snmptrap</td><td>162/udp</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>https</td><td>443/tcp</td></tr><tr><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>syslog</td><td>514/udp</td></tr><tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>ldap</td><td>389/tcp</td></tr><tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>ldaps</td><td>636/tcp</td></tr></tbody></table></div></div></div></div></div>	Input to Server	Output from Server	Service	Port/Protocol	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ftp	21/tcp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ssh	22/tcp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	telnet	23/tcp	<input type="checkbox"/>	<input checked="" type="checkbox"/>	domain	53/udp	<input type="checkbox"/>	<input type="checkbox"/>	bootps	67/udp	<input type="checkbox"/>	<input type="checkbox"/>	bootpc	68/udp	<input type="checkbox"/>	<input type="checkbox"/>	tftp	69/udp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	http	80/tcp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ntp	123/udp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	snmp	161/udp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	snmptrap	162/udp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	https	443/tcp	<input type="checkbox"/>	<input checked="" type="checkbox"/>	syslog	514/udp	<input type="checkbox"/>	<input type="checkbox"/>	ldap	389/tcp	<input type="checkbox"/>	<input type="checkbox"/>	ldaps	636/tcp
Input to Server	Output from Server	Service	Port/Protocol																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ftp	21/tcp																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ssh	22/tcp																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	telnet	23/tcp																																																														
<input type="checkbox"/>	<input checked="" type="checkbox"/>	domain	53/udp																																																														
<input type="checkbox"/>	<input type="checkbox"/>	bootps	67/udp																																																														
<input type="checkbox"/>	<input type="checkbox"/>	bootpc	68/udp																																																														
<input type="checkbox"/>	<input type="checkbox"/>	tftp	69/udp																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	http	80/tcp																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ntp	123/udp																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	snmp	161/udp																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	snmptrap	162/udp																																																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	https	443/tcp																																																														
<input type="checkbox"/>	<input checked="" type="checkbox"/>	syslog	514/udp																																																														
<input type="checkbox"/>	<input type="checkbox"/>	ldap	389/tcp																																																														
<input type="checkbox"/>	<input type="checkbox"/>	ldaps	636/tcp																																																														

Step	Description
4.	<p>Start Agent</p> <p>Lastly, the SNMP agent must be started. Navigate to Alarms→Agent Status. If the Master Agent status is <i>Down</i> then click the Start Agent button. If the Master Agent status is <i>Up</i>, then the agent must be stopped and restarted.</p>  <p>The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The left sidebar contains a navigation menu with categories: Alarms (Current Alarms, Agent Status, SNMP Agents, SNMP Traps, Filters, SNMP Test), Diagnostics (Restarts, System Logs, Temperature/Voltage, Server LEDs, Ping, Traceroute, Netstat, Modem Test, Network Time Sync), Server (Status Summary, Process Status, Interchange Servers, Busy-out Server, Release Server, Shutdown Server, Server Date/Time, Software Version), and Server Configuration. The main content area is titled 'Agent Status' and includes a description: 'The Agent Status Web page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.' It displays 'Master Agent status: Down' with a 'Start Agent' button. Below, 'Sub Agent Status' lists FP Agent, MVSubAgent, Load Agent, and MIB2Agent, all with 'UP' status. A message states 'Sub Agents are NOT connected to the Master Agent.' and a 'Help' button is at the bottom.</p>

3.2. RTCP

This section describes the RTCP configuration. It is performed using the Avaya Communication Manager SAT interface.

Step	Description
1.	<p>IP Options</p> <p>Use the change system-parameters ip-options command to set the RTCP Monitor Server parameters. These values will be sent from Avaya Communication Manager to each Avaya IP Telephone so the telephones will know where to send RTCP data. Set the Default Server IP Address to the IP address of the AppManager agent that will collect the data. The Default Server Port and Default RTCP Report Period must match the AppManager configuration in Section 4, Step 5. In the case of the compliance test, the default values of 5005 and 5 were used respectively.</p> <div><pre>change system-parameters ip-options Page 1 of 3 IP-OPTIONS SYSTEM PARAMETERS IP MEDIA PACKET PERFORMANCE THRESHOLDS Roundtrip Propagation Delay (ms) High: 800 Low: 400 Packet Loss (%) High: 40 Low: 15 Ping Test Interval (sec): 20 Number of Pings Per Measurement Interval: 10 RTCP MONITOR SERVER Default Server IP Address: 192.45.85.241 Default Server Port: 5005 Default RTCP Report Period(secs): 5 AUTOMATIC TRACE ROUTE ON Link Failure? y H.248 MEDIA GATEWAY H.323 IP ENDPOINT Link Loss Delay Timer (min): 5 Link Loss Delay Timer (min): 5 Primary Search Time (sec): 75 Periodic Registration Timer (min): 20</pre></div>

3.3. CDR

This section describes the CDR configuration. It is performed using the Avaya Communication Manager SAT interface.

Step	Description																																							
1.	<p>IP Node Names</p> <p>Use the change node-names ip command to associate the IP address of the AppManager agent to a node name. In the case of the compliance test, the node name netIQ was assigned to IP address 192.45.85.241. Also, highlighted in the example below is the node name CLAN which will be used in the next step. This node name represents the IP address of the CLAN circuit pack used as the source of the CDR data.</p> <div><pre>change node-names ip</pre><table><tr><th colspan="2">IP NODE NAMES</th><th>Page 1 of 2</th></tr><tr><th>Name</th><th>IP Address</th><td></td></tr><tr><td>CLAN</td><td>192.45.80.87</td><td></td></tr><tr><td>CLAN-AES</td><td>192.45.80.89</td><td></td></tr><tr><td>MEDPRO</td><td>192.45.80.88</td><td></td></tr><tr><td>MEDPRO2</td><td>192.45.80.161</td><td></td></tr><tr><td>RDTT</td><td>192.45.80.254</td><td></td></tr><tr><td>S8300G700</td><td>192.45.87.11</td><td></td></tr><tr><td>SIP</td><td>192.45.80.101</td><td></td></tr><tr><td>VAL</td><td>192.45.80.85</td><td></td></tr><tr><td>default</td><td>0.0.0.0</td><td></td></tr><tr><td>netIQ</td><td>192.45.85.241</td><td></td></tr><tr><td>procr</td><td>192.45.80.214</td><td></td></tr></table></div>	IP NODE NAMES		Page 1 of 2	Name	IP Address		CLAN	192.45.80.87		CLAN-AES	192.45.80.89		MEDPRO	192.45.80.88		MEDPRO2	192.45.80.161		RDTT	192.45.80.254		S8300G700	192.45.87.11		SIP	192.45.80.101		VAL	192.45.80.85		default	0.0.0.0		netIQ	192.45.85.241		procr	192.45.80.214	
IP NODE NAMES		Page 1 of 2																																						
Name	IP Address																																							
CLAN	192.45.80.87																																							
CLAN-AES	192.45.80.89																																							
MEDPRO	192.45.80.88																																							
MEDPRO2	192.45.80.161																																							
RDTT	192.45.80.254																																							
S8300G700	192.45.87.11																																							
SIP	192.45.80.101																																							
VAL	192.45.80.85																																							
default	0.0.0.0																																							
netIQ	192.45.85.241																																							
procr	192.45.80.214																																							
2.	<p>IP Services</p> <p>Use the change ip-services command to define the CDR link between Avaya Communication Manager and AppManager. In the Service Type field, enter CDR1 for the primary CDR link. In the Local Node field, enter the node name that will terminate the CDR link on Avaya Communication Manager. In the case of the compliance test, which used an Avaya G650 Media Gateway, the near-end node was the CLAN circuit pack discussed in Step 1. The Remote Node field is set to the node name defined in Step 1 for AppManager. The Remote Port may be set to a value between 5000 and 64500 inclusive and must match the port configured on AppManager in Section 4, Step 5.</p> <div><pre>change ip-services</pre><table><tr><th colspan="6">IP SERVICES</th><th>Page 1 of 4</th></tr><tr><th>Service Type</th><th>Enabled</th><th>Local Node</th><th>Local Port</th><th>Remote Node</th><th>Remote Port</th><td></td></tr><tr><td>CDR1</td><td></td><td>CLAN</td><td>0</td><td>netIQ</td><td>9000</td><td></td></tr></table></div>	IP SERVICES						Page 1 of 4	Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		CDR1		CLAN	0	netIQ	9000																			
IP SERVICES						Page 1 of 4																																		
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																																			
CDR1		CLAN	0	netIQ	9000																																			

Step	Description																
3.	<p>IP Services – Continued</p> <p>On Page 3, set the Reliable Protocol field to <i>n</i> to disable the use of Avaya’s Reliable Session Protocol (RSP) for CDR transmission. In this case, the CDR link will use TCP without RSP.</p> <div><div>change ip-services</div><div>Page3 of 4</div><table><tr><th rowspan="2">Service Type</th><th rowspan="2">Reliable Protocol</th><th colspan="4">SESSION LAYER TIMERS</th></tr><tr><th>Packet Resp Timer</th><th>Session Connect Message Cntr</th><th>SPDU Cntr</th><th>Connectivity Timer</th></tr><tr><td>CDR1</td><td>n</td><td>30</td><td>3</td><td>3</td><td>60</td></tr></table></div>	Service Type	Reliable Protocol	SESSION LAYER TIMERS				Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	CDR1	n	30	3	3	60
Service Type	Reliable Protocol			SESSION LAYER TIMERS													
		Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer												
CDR1	n	30	3	3	60												

Step	Description
4.	<p>CDR parameters</p> <p>Use the change system-parameters cdr command to set the parameters for the type of calls to track and the format of the CDR data. The settings for the compliance test are described below. AppManager requires a customized CDR format which is defined in Step 5.</p> <ul style="list-style-type: none"> • CDR Date Format: <i>month/day</i> • Primary Output Format: <i>customized</i> • Primary Output Endpoint: <i>CDR1</i> <p>The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.</p> <ul style="list-style-type: none"> • Record Outgoing Calls Only? <i>n</i> This allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls. • Suppress CDR for Ineffective Call Attempts? <i>y</i> This prevents calls that are blocked from appearing in the CDR record. • Intra-switch CDR? <i>y</i> This allows call records for internal calls involving specific stations. • Outg Trk Call Splitting? <i>y</i> This allows a separate call record for any portion of an outgoing call that is transferred or conferenced. • Inc Trk Call Splitting? <i>y</i> This allows a separate call record for any portion of an incoming call that is transferred or conferenced. <p>Default values may be used for all other fields.</p> <div data-bbox="331 1115 1417 1656" style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <pre> change system-parameters cdr CDR SYSTEM PARAMETERS Page 1 of 2 Node Number (Local PBX ID): 1 CDR Date Format: month/day Primary Output Format: customized Primary Output Endpoint: CDR1 Secondary Output Format: Use ISDN Layouts? n Enable CDR Storage on Disk? y Use Enhanced Formats? n Condition Code 'T' For Redirected Calls? y Use Legacy CDR Formats? n Remove # From Called Number? n Modified Circuit ID Display? n Intra-switch CDR? y Record Outgoing Calls Only? n Outg Trk Call Splitting? y Suppress CDR for Ineffective Call Attempts? y Outg Attd Call Record? n Disconnect Information in Place of FRL? y Interworking Feat-flag? n Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n Calls to Hunt Group - Record: group-ext Record Called Vector Directory Number Instead of Group or Member? n Record Agent ID on Incoming? y Record Agent ID on Outgoing? n Inc Trk Call Splitting? y Inc Attd Call Record? n Record Non-Call-Assoc TSC? n Call Record Handling Option: warning Record Call-Assoc TSC? n Digits to Record for Outgoing Calls: dialed Privacy - Digits to Hide: 0 CDR Account Code Length: 6 </pre> </div>

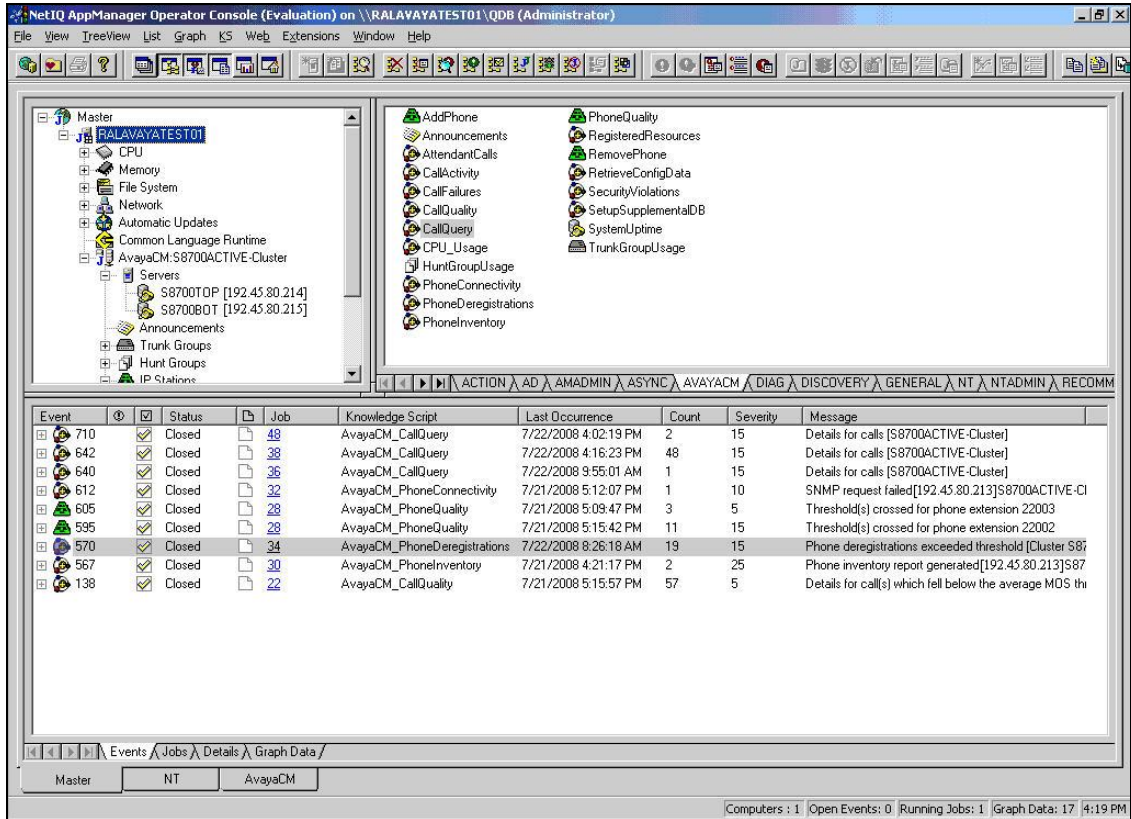
Step	Description																																																			
5.	<div><div>CDR custom format</div><div>On Page 2, the customized CDR format used by AppManager is defined. Each field in the CDR record is entered in the Data Item column, followed by the expected length of the field in the Length column. This is the format that Avaya Communication Manager will use when sending CDR records to AppManager.</div><div><div><div>change system-parameters cdr</div><div>Page2 of2</div><div><div>CDR SYSTEM PARAMETERS</div><table><thead><tr><th>Data Item - Length</th><th>Data Item - Length</th><th>Data Item - Length</th></tr></thead><tbody><tr><td>1: acct-code - 15</td><td>17: -</td><td>33: -</td></tr><tr><td>2: atttd-console - 2</td><td>18: -</td><td>34: -</td></tr><tr><td>3: auth-code - 13</td><td>19: -</td><td>35: -</td></tr><tr><td>4: clg-num/in-tac - 15</td><td>20: -</td><td>36: -</td></tr><tr><td>5: code-dial - 4</td><td>21: -</td><td>37: -</td></tr><tr><td>6: code-used - 4</td><td>22: -</td><td>38: -</td></tr><tr><td>7: cond-code - 1</td><td>23: -</td><td>39: -</td></tr><tr><td>8: date - 6</td><td>24: -</td><td>40: -</td></tr><tr><td>9: dialed-num - 23</td><td>25: -</td><td>41: -</td></tr><tr><td>10: in-crt-id - 3</td><td>26: -</td><td>42: -</td></tr><tr><td>11: in-trk-code - 4</td><td>27: -</td><td>43: -</td></tr><tr><td>12: out-crt-id - 3</td><td>28: -</td><td>44: -</td></tr><tr><td>13: sec-dur - 5</td><td>29: -</td><td>45: -</td></tr><tr><td>14: time - 4</td><td>30: -</td><td>46: -</td></tr><tr><td>15: return - 1</td><td>31: -</td><td>47: -</td></tr><tr><td>16: line-feed - 1</td><td>32: -</td><td>48: -</td></tr></tbody></table><div>Record length = 104</div></div></div></div></div>	Data Item - Length	Data Item - Length	Data Item - Length	1: acct-code - 15	17: -	33: -	2: atttd-console - 2	18: -	34: -	3: auth-code - 13	19: -	35: -	4: clg-num/in-tac - 15	20: -	36: -	5: code-dial - 4	21: -	37: -	6: code-used - 4	22: -	38: -	7: cond-code - 1	23: -	39: -	8: date - 6	24: -	40: -	9: dialed-num - 23	25: -	41: -	10: in-crt-id - 3	26: -	42: -	11: in-trk-code - 4	27: -	43: -	12: out-crt-id - 3	28: -	44: -	13: sec-dur - 5	29: -	45: -	14: time - 4	30: -	46: -	15: return - 1	31: -	47: -	16: line-feed - 1	32: -	48: -
Data Item - Length	Data Item - Length	Data Item - Length																																																		
1: acct-code - 15	17: -	33: -																																																		
2: atttd-console - 2	18: -	34: -																																																		
3: auth-code - 13	19: -	35: -																																																		
4: clg-num/in-tac - 15	20: -	36: -																																																		
5: code-dial - 4	21: -	37: -																																																		
6: code-used - 4	22: -	38: -																																																		
7: cond-code - 1	23: -	39: -																																																		
8: date - 6	24: -	40: -																																																		
9: dialed-num - 23	25: -	41: -																																																		
10: in-crt-id - 3	26: -	42: -																																																		
11: in-trk-code - 4	27: -	43: -																																																		
12: out-crt-id - 3	28: -	44: -																																																		
13: sec-dur - 5	29: -	45: -																																																		
14: time - 4	30: -	46: -																																																		
15: return - 1	31: -	47: -																																																		
16: line-feed - 1	32: -	48: -																																																		
6.	<div><div>Intra-Switch CDR</div><div>If the Intra-switch CDR field is set to y in Step 4, use the change intra-switch-cdr command to define the extensions that will be subject to call detail records. In the Assigned Members field, enter a specific extension whose usage will be tracked with a CDR record. Add an entry for each additional extension of interest.</div><div><div><div>change intra-switch-cdr</div><div>Page1 of3</div><div><div>INTRA-SWITCH CDR</div><table><thead><tr><th>Extension</th><th>Assigned Members:</th><th>5</th><th>of 5000</th><th>administered</th></tr><tr><th>Extension</th><th>Extension</th><th>Extension</th><th>Extension</th><th>Extension</th></tr></thead><tbody><tr><td>22001</td><td></td><td></td><td></td><td></td></tr><tr><td>22002</td><td></td><td></td><td></td><td></td></tr><tr><td>22003</td><td></td><td></td><td></td><td></td></tr><tr><td>22007</td><td></td><td></td><td></td><td></td></tr><tr><td>26001</td><td></td><td></td><td></td><td></td></tr></tbody></table></div></div></div></div>	Extension	Assigned Members:	5	of 5000	administered	Extension	Extension	Extension	Extension	Extension	22001					22002					22003					22007					26001																				
Extension	Assigned Members:	5	of 5000	administered																																																
Extension	Extension	Extension	Extension	Extension																																																
22001																																																				
22002																																																				
22003																																																				
22007																																																				
26001																																																				

Step	Description
7.	<p>Trunk Group</p> <p>For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. To do this, use the change trunk-group <i>n</i> command, where <i>n</i> is the trunk group number, to verify that the CDR Reports field is set to y. This applies to all trunk group types. The example below shows the H.323 trunk between site 1 and 2.</p> <div data-bbox="339 401 1409 741" style="border: 1px solid black; padding: 10px;"> <pre> display trunk-group 10 Page 1 of 21 TRUNK GROUP Group Number: 10 Group Type: isdn CDR Reports: y Group Name: To G700 COR: 1 TN: 1 TAC: 111 Direction: two-way Outgoing Display? y Carrier Medium: H.323 Dial Access? y Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: tie Auth Code? n Member Assignment Method: auto Signaling Group: 10 Number of Members: 10 </pre> </div>

4. Configure NetIQ AppManager

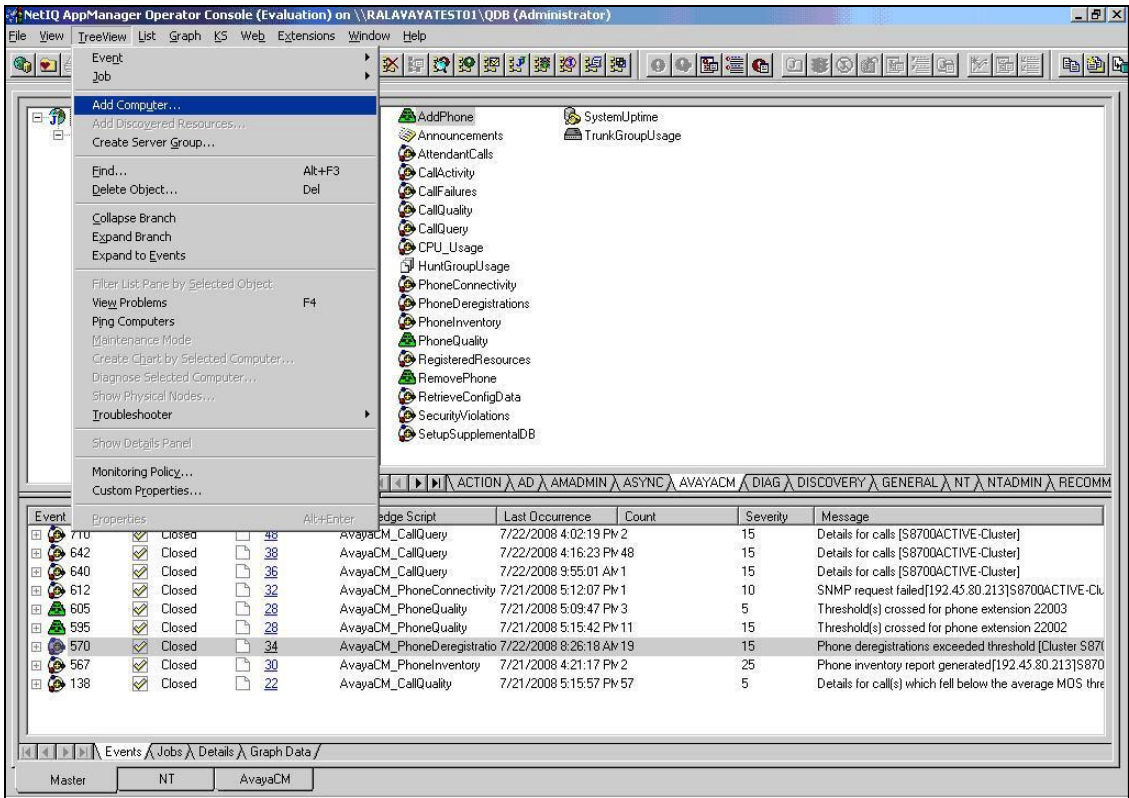
This section describes the configuration of AppManager. It assumes that the application and all required software components have been installed. It also assumes all components have been properly licensed.

Step	Description
1.	<p>Launch NetIQ AppManager Operator Console</p> <p>The AppManager configuration is performed using the NetIQ AppManager Operator Console. Launch the Operator Console from the Windows Start menu by navigating to All Programs→NetIQ→AppManager→Operator Console.</p> <p>The main Operator Console window appears as shown below. The example below shows the Operator Console window after all the system components have been configured/discovered and thus appear in the tree view in the upper left pane. Steps 2 - 11 describe how these components are added to the configuration shown in the tree view.</p>

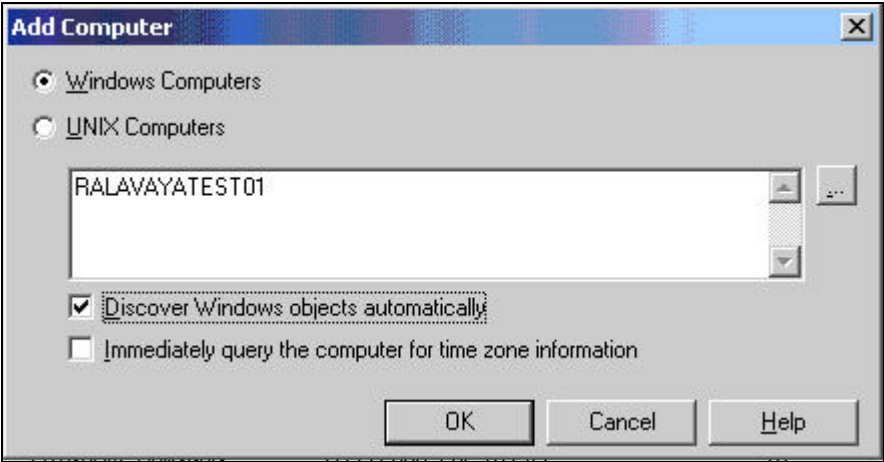


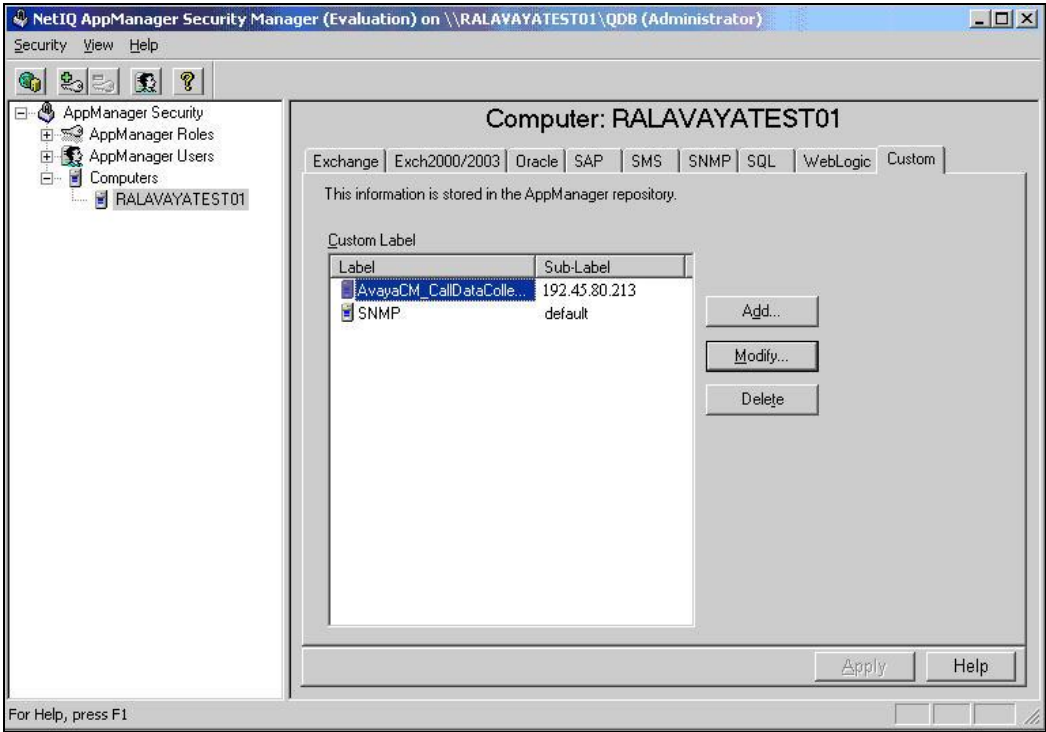
Event	Status	Job	Knowledge Script	Last Occurrence	Count	Severity	Message
710	Closed	48	AvayaCM_CallQuery	7/22/2008 4:02:19 PM	2	15	Details for calls [S8700ACTIVE-Cluster]
642	Closed	38	AvayaCM_CallQuery	7/22/2008 4:16:23 PM	48	15	Details for calls [S8700ACTIVE-Cluster]
640	Closed	36	AvayaCM_CallQuery	7/22/2008 9:55:01 AM	1	15	Details for calls [S8700ACTIVE-Cluster]
612	Closed	32	AvayaCM_PhoneConnectivity	7/21/2008 5:12:07 PM	1	10	SNMP request failed[192.45.80.213]S8700ACTIVE-Cluster
605	Closed	28	AvayaCM_PhoneQuality	7/21/2008 5:09:47 PM	3	5	Threshold(s) crossed for phone extension 22003
595	Closed	28	AvayaCM_PhoneQuality	7/21/2008 5:15:42 PM	11	15	Threshold(s) crossed for phone extension 22002
570	Closed	34	AvayaCM_PhoneDeregistrations	7/22/2008 8:26:18 AM	19	15	Phone deregistrations exceeded threshold [Cluster S8700ACTIVE-Cluster]
567	Closed	30	AvayaCM_PhoneInventory	7/21/2008 4:21:17 PM	2	25	Phone inventory report generated[192.45.80.213]S8700ACTIVE-Cluster
138	Closed	22	AvayaCM_CallQuality	7/21/2008 5:15:57 PM	57	5	Details for call(s) which fell below the average MOS threshold

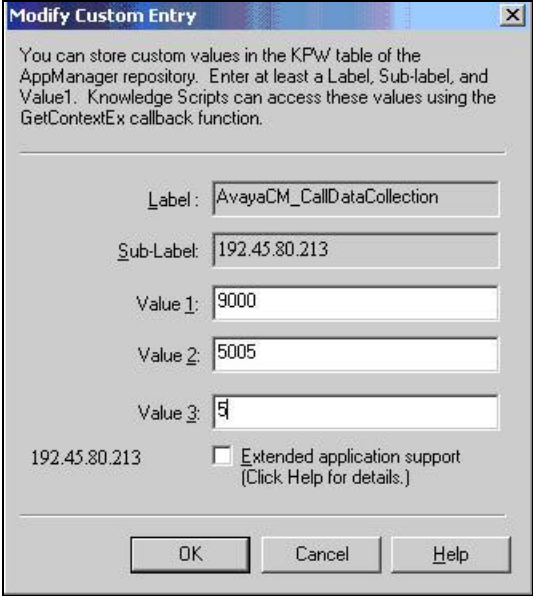
Step	Description
2.	<p>Add Computer</p> <p>Initially, a host computer must be added to the tree view that will serve as the proxy agent for gathering data from Avaya Communication Manager. In the case of the compliance test, this proxy agent (known as the AppManager agent) is running on the same computer as the Operator Console but this is not necessary. In order to add an agent computer to the Operator Console, navigate to TreeView→Add Computer.</p>

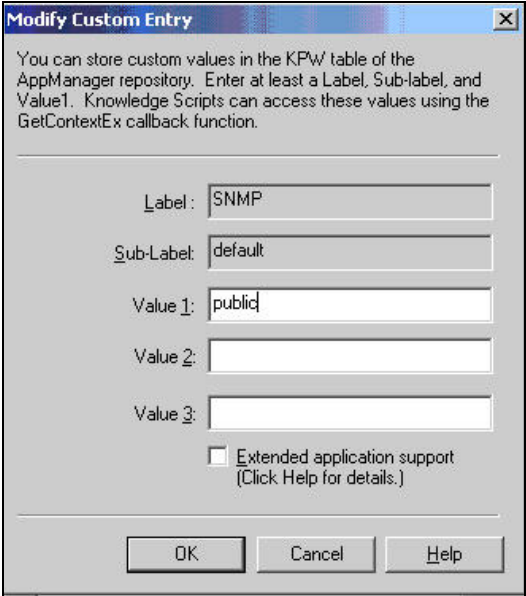


Event	Properties	Alert	Edge Script	Last Occurrence	Count	Severity	Message
710	Closed	48	AvayaCM_CallQuery	7/22/2008 4:02:19 PM 2		15	Details for calls [S8700ACTIVE-Cluster]
642	Closed	38	AvayaCM_CallQuery	7/22/2008 4:16:23 PM 48		15	Details for calls [S8700ACTIVE-Cluster]
640	Closed	36	AvayaCM_CallQuery	7/22/2008 9:55:01 AM 1		15	Details for calls [S8700ACTIVE-Cluster]
612	Closed	32	AvayaCM_PhoneConnectivity	7/21/2008 5:12:07 PM 1		10	SNMP request failed[192.45.80.213]S8700ACTIVE-Cl
605	Closed	28	AvayaCM_PhoneQuality	7/21/2008 5:09:47 PM 3		5	Threshold(s) crossed for phone extension 22003
595	Closed	28	AvayaCM_PhoneQuality	7/21/2008 5:15:42 PM 11		15	Threshold(s) crossed for phone extension 22002
570	Closed	34	AvayaCM_PhoneDeregistratio	7/22/2008 8:26:18 AM 19		15	Phone deregistrations exceeded threshold [Cluster S870
567	Closed	30	AvayaCM_PhoneInventory	7/21/2008 4:21:17 PM 2		25	Phone inventory report generated[192.45.80.213]S870
138	Closed	22	AvayaCM_CallQuality	7/21/2008 5:15:57 PM 57		5	Details for call(s) which fell below the average MOS thre

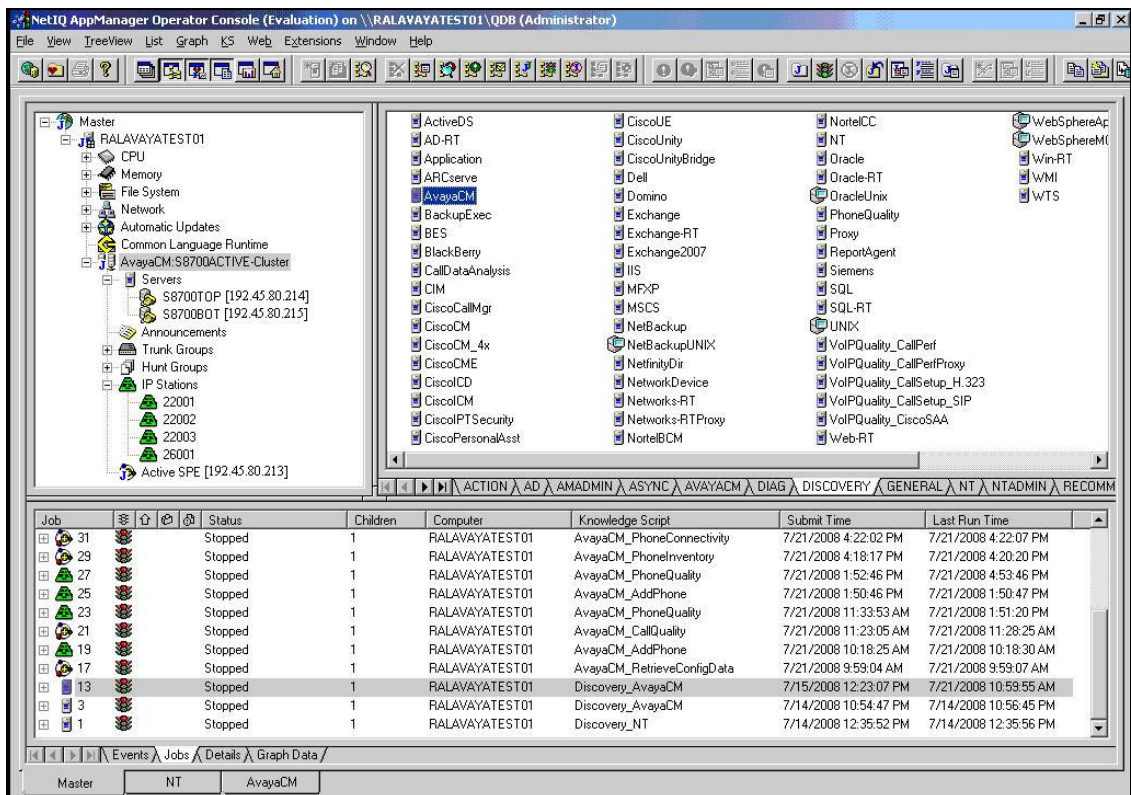
Step	Description
3.	<p>Computer Details</p> <p>The following pop-up window appears. Select the appropriate radio button for Windows Computers or Unix Computers. Enter the host name of the agent computer in the center box. In the case of Window Computers, click the box for Discover Windows objects automatically. Click OK.</p> <p>This will populate the tree view in Step 1 with the following Window objects for the agent computer.</p> <ul style="list-style-type: none"> • CPU • Memory • File System • Network • Automatic Updates • Common Language Runtime 

Step	Description
4.	<p>Agent Computer Connection Parameters</p> <p>The agent computer created in Step 2 – 3, must be configured to connect to Avaya Communication Manager. From the main window shown in Step 1, navigate to Extensions→Security Manager from the tool bar across the top of the window. The following window appears. Highlight the agent host name RALAVAYATEST01 and click on the Custom tab.</p> <p>The example below shows the two custom entries required to communicate to Avaya Communication Manager. These were originally created by clicking the Add button. The details of these entries can be changed by highlighting an entry and clicking the Modify button.</p> 

Step	Description
5.	<p>CDR and RTCP Parameters</p> <p>The first entry is the configuration of the CDR and RTCP connection parameters. Enter AvayaCM_CallDataCollection for the Label field. Enter the IP address of the Avaya Server in the Sub-Label field. In the case of redundant servers, enter the virtual server IP address. Value 1 is the port number used for CDR data. This must match the value configured on Avaya Communication Manager in Section 3.3, Step 2. Value 2 is the port number used for RTCP data. Value 3 is the RTCP report period in seconds. These values must match the values configured on Avaya Communication Manager in Section 3.2, Step 1. Click OK.</p> 

Step	Description
6.	<p>SNMP Parameters</p> <p>The second entry is the configuration of the SNMP connection parameters. Enter SNMP for the Label field. Enter <i>default</i> in the Sub-Label field. The value of <i>default</i> will allow the value entered in the Value 1 field to be used as the SNMP password for any IP address. Click OK.</p> 

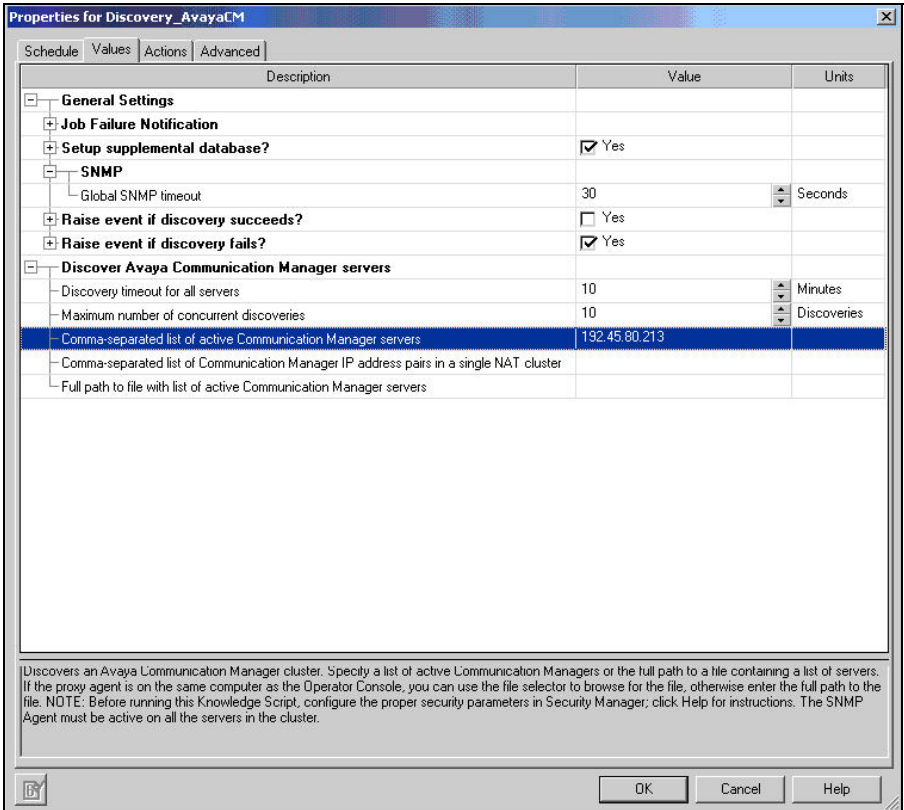
Step	Description
7.	<p>Discovery</p> <p>Once the connection parameters have been defined (Steps 4 - 6), then the components of Avaya Communication Manager can be discovered using SNMP. To do this, select the DISCOVERY tab. Drag the AvayaCM script to the agent host name (RALAVAYATEST01) in left pane tree view.</p>

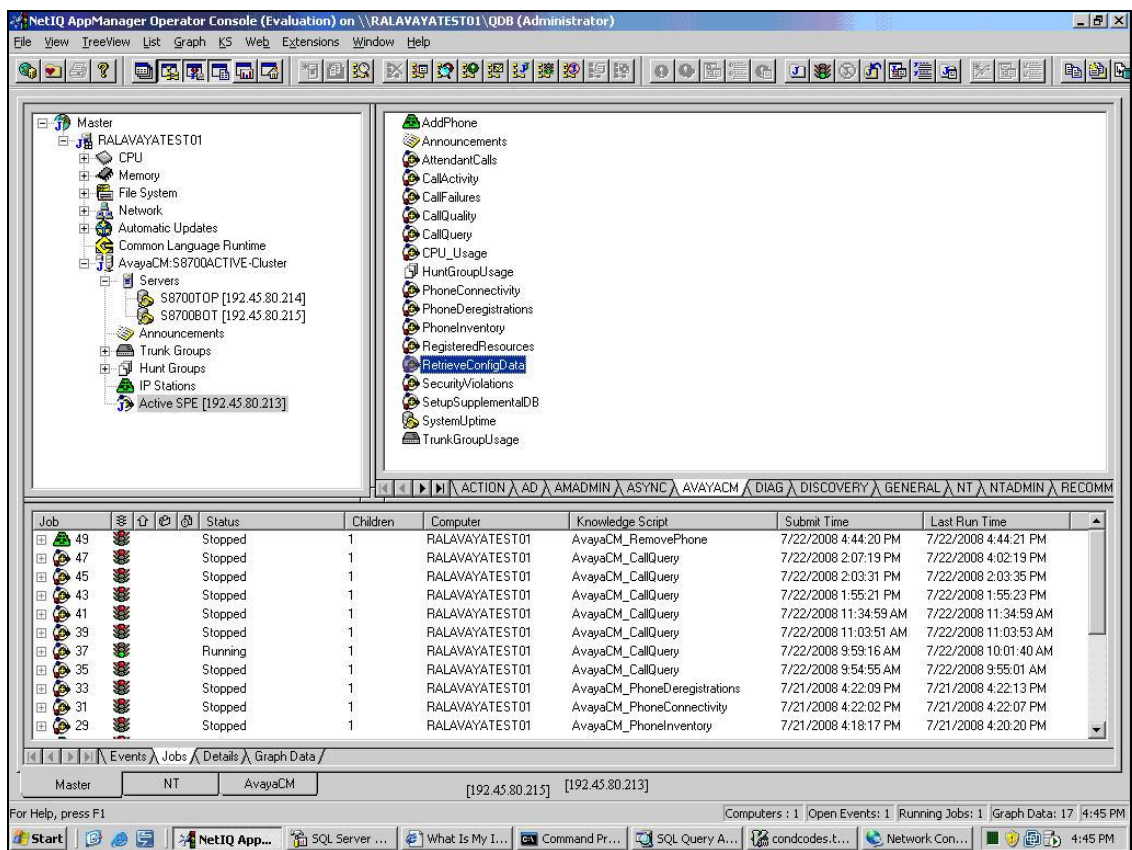


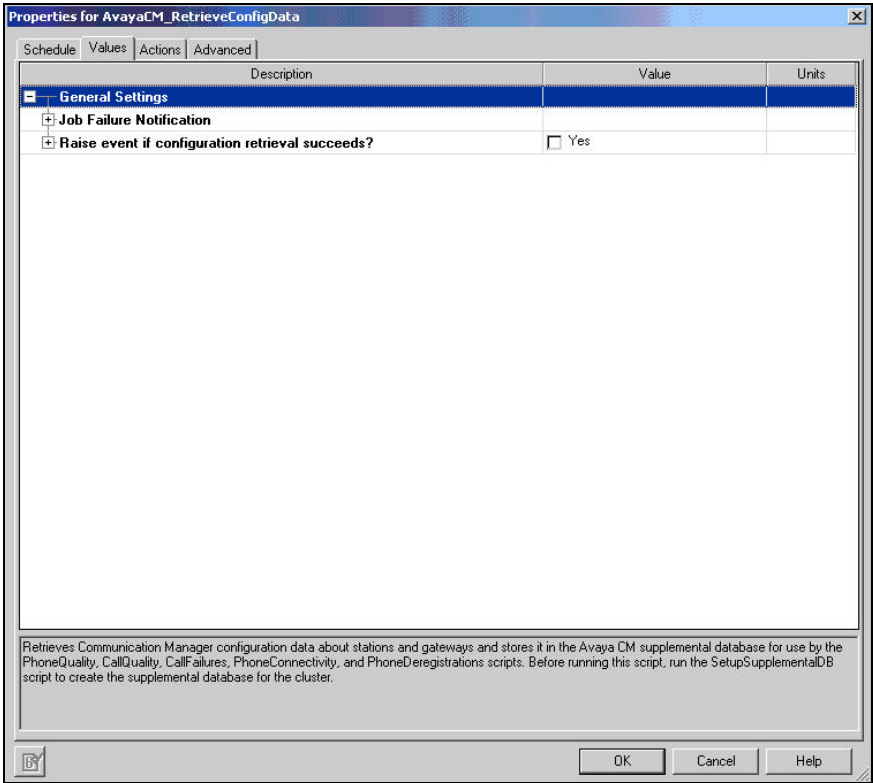
The screenshot displays the NetIQ AppManager Operator Console interface. The title bar indicates the console is running on 'RALAVAYATEST01\QDB (Administrator)'. The interface is divided into three main sections:

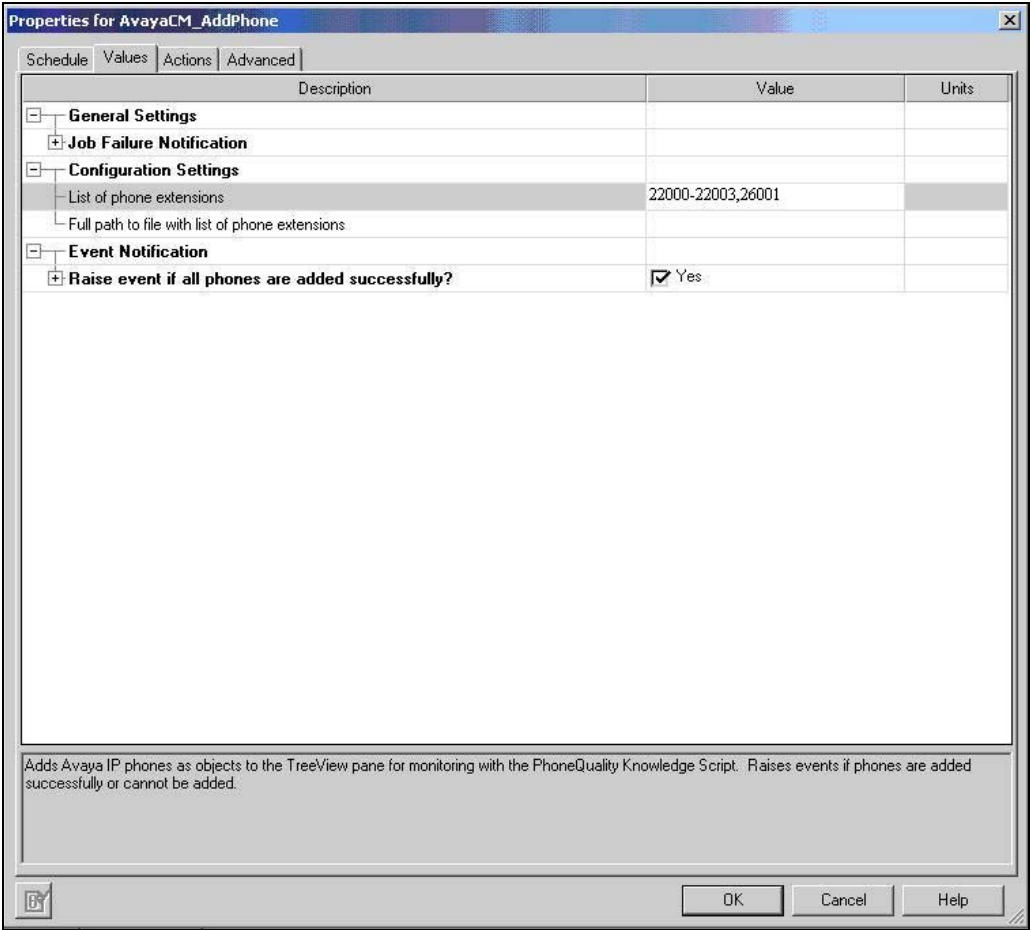
- Left Pane (Tree View):** Shows a hierarchical tree structure under 'Master'. The 'RALAVAYATEST01' node is expanded, showing sub-nodes like CPU, Memory, File System, Network, Automatic Updates, Common Language Runtime, and 'AvayaCM:S8700ACTIVE-Cluster'. The 'AvayaCM:S8700ACTIVE-Cluster' node is further expanded, showing 'Servers' (S8700TOP, S8700BOT), 'Announcements', 'Trunk Groups', 'Hunt Groups', 'IP Stations' (22001, 22002, 22003, 26001), and 'Active SPE'.
- Right Pane (Script List):** Displays a list of available scripts for discovery. The 'AvayaCM' script is highlighted. Other scripts include ActiveDS, AD-RT, Application, ARCServe, BackupExec, BES, BlackBerry, CallDataAnalysis, CIM, CiscoCallMgr, CiscoCM, CiscoCM_4x, CiscoCME, CiscoCD, CiscoCM, CiscoPTS security, CiscoPersonalAsst, CiscoUE, CiscoUnity, CiscoUnityBridge, Dell, Domino, Exchange, Exchange-RT, Exchange2007, IIS, MFXP, MSCS, NetBackup, NetBackupUNIX, NetfinityDir, NetworkDevice, Networks-RT, Networks-RTProxy, NortelBCM, NortelCC, NT, Oracle, Oracle-RT, OracleUnix, PhoneQuality, Proxy, ReportAgent, Siemens, SQL, SQL-RT, UNIX, VolPQuality_CallPerf, VolPQuality_CallPerfProxy, VolPQuality_CallSetup_H.323, VolPQuality_CallSetup_SIP, VolPQuality_CiscoSAA, and Web-RT.
- Bottom Pane (Job Table):** Displays a table of discovery jobs. The table has columns for Job, Status, Children, Computer, Knowledge Script, Submit Time, and Last Run Time. The table shows several jobs, with the most recent ones being 'Discovery_AvayaCM' and 'Discovery_NT'.

Job	Status	Children	Computer	Knowledge Script	Submit Time	Last Run Time
31	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneConnectivity	7/21/2008 4:22:02 PM	7/21/2008 4:22:07 PM
29	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneInventory	7/21/2008 4:18:17 PM	7/21/2008 4:20:20 PM
27	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneQuality	7/21/2008 1:52:46 PM	7/21/2008 4:53:46 PM
25	Stopped	1	RALAVAYATEST01	AvayaCM_AddPhone	7/21/2008 1:50:46 PM	7/21/2008 1:50:47 PM
23	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneQuality	7/21/2008 11:33:53 AM	7/21/2008 1:51:20 PM
21	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuality	7/21/2008 11:23:05 AM	7/21/2008 11:28:25 AM
19	Stopped	1	RALAVAYATEST01	AvayaCM_AddPhone	7/21/2008 10:18:25 AM	7/21/2008 10:18:30 AM
17	Stopped	1	RALAVAYATEST01	AvayaCM_RetrieveConfigData	7/21/2008 9:59:04 AM	7/21/2008 9:59:07 AM
13	Stopped	1	RALAVAYATEST01	Discovery_AvayaCM	7/15/2008 12:23:07 PM	7/21/2008 10:59:55 AM
3	Stopped	1	RALAVAYATEST01	Discovery_AvayaCM	7/14/2008 10:54:47 PM	7/14/2008 10:56:45 PM
1	Stopped	1	RALAVAYATEST01	Discovery_NT	7/14/2008 12:35:52 PM	7/14/2008 12:35:56 PM

Step	Description
8.	<p>Discovery Parameters</p> <p>The following pop-up window will appear. Enter the active server IP address in the field labeled Comma-separated list of active Communication Manager servers. Click OK.</p> <p>This action will fill out the tree view with all the Avaya Communication Manager components shown in the tree view in Step 1 except for the individual IP telephones.</p>  <p>The screenshot shows a dialog box titled "Properties for Discovery_AvayaCM" with tabs for "Schedule", "Values", "Actions", and "Advanced". The "Values" tab is active. On the left is a tree view under "General Settings" with the following items: "Job Failure Notification", "Setup supplemental database?", "SNMP" (expanded), "Raise event if discovery succeeds?", "Raise event if discovery fails?", "Discover Avaya Communication Manager servers" (selected), "Discovery timeout for all servers", "Maximum number of concurrent discoveries", "Comma-separated list of active Communication Manager servers", "Comma-separated list of Communication Manager IP address pairs in a single NAT cluster", and "Full path to file with list of active Communication Manager servers". On the right is a table with columns "Description", "Value", and "Units". The table contains the following rows: "Global SNMP timeout" (30, Seconds), "Raise event if discovery succeeds?" (Yes, checkbox), "Raise event if discovery fails?" (Yes, checkbox), "Discovery timeout for all servers" (10, Minutes), "Maximum number of concurrent discoveries" (10, Discoveries), "Comma-separated list of active Communication Manager servers" (192.45.80.213), "Comma-separated list of Communication Manager IP address pairs in a single NAT cluster", and "Full path to file with list of active Communication Manager servers". At the bottom of the dialog is a text box with instructions: "Discovers an Avaya Communication Manager cluster. Specify a list of active Communication Managers or the full path to a file containing a list of servers. If the proxy agent is on the same computer as the Operator Console, you can use the file selector to browse for the file, otherwise enter the full path to the file. NOTE: Before running this Knowledge Script, configure the proper security parameters in Security Manager; click Help for instructions. The SNMP Agent must be active on all the servers in the cluster." and buttons for "OK", "Cancel", and "Help".</p>

Step	Description																																																																																				
9.	<p>Retrieve Configuration Data</p> <p>Even though the tree view is now populated with the Avaya Communication Manager components, additional detailed information must be retrieved using SNMP and stored in a supplemental database. To do this, select the AVAYACM tab and drag the RetrieveConfigData script to the Active SPE in left pane menu tree.</p>  <p>The screenshot shows the NetIQ AppManager Operator Console interface. On the left, a tree view displays the hierarchy: Master > RALAVAYATEST01 > AvayaCM:S8700ACTIVE-Cluster > Servers > Active SPE [192.45.80.213]. On the right, a list of scripts is shown, with 'RetrieveConfigData' highlighted. Below the tree and script list, a table displays the status of various jobs. At the bottom, the 'AVAYACM' tab is selected, and the 'Active SPE' is highlighted in the tree.</p> <table><tr><th>Job</th><th>Status</th><th>Children</th><th>Computer</th><th>Knowledge Script</th><th>Submit Time</th><th>Last Run Time</th></tr><tr><td>49</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_RemovePhone</td><td>7/22/2008 4:44:20 PM</td><td>7/22/2008 4:44:21 PM</td></tr><tr><td>47</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_CallQuery</td><td>7/22/2008 2:07:19 PM</td><td>7/22/2008 4:02:19 PM</td></tr><tr><td>45</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_CallQuery</td><td>7/22/2008 2:03:31 PM</td><td>7/22/2008 2:03:35 PM</td></tr><tr><td>43</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_CallQuery</td><td>7/22/2008 1:55:21 PM</td><td>7/22/2008 1:55:23 PM</td></tr><tr><td>41</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_CallQuery</td><td>7/22/2008 11:34:59 AM</td><td>7/22/2008 11:34:59 AM</td></tr><tr><td>39</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_CallQuery</td><td>7/22/2008 11:03:51 AM</td><td>7/22/2008 11:03:53 AM</td></tr><tr><td>37</td><td>Running</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_CallQuery</td><td>7/22/2008 9:59:16 AM</td><td>7/22/2008 10:01:40 AM</td></tr><tr><td>35</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_CallQuery</td><td>7/22/2008 9:54:55 AM</td><td>7/22/2008 9:55:01 AM</td></tr><tr><td>33</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_PhoneDeregistrations</td><td>7/21/2008 4:22:09 PM</td><td>7/21/2008 4:22:13 PM</td></tr><tr><td>31</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_PhoneConnectivity</td><td>7/21/2008 4:22:02 PM</td><td>7/21/2008 4:22:07 PM</td></tr><tr><td>29</td><td>Stopped</td><td>1</td><td>RALAVAYATEST01</td><td>AvayaCM_PhoneInventory</td><td>7/21/2008 4:18:17 PM</td><td>7/21/2008 4:20:20 PM</td></tr></table>	Job	Status	Children	Computer	Knowledge Script	Submit Time	Last Run Time	49	Stopped	1	RALAVAYATEST01	AvayaCM_RemovePhone	7/22/2008 4:44:20 PM	7/22/2008 4:44:21 PM	47	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 2:07:19 PM	7/22/2008 4:02:19 PM	45	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 2:03:31 PM	7/22/2008 2:03:35 PM	43	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 1:55:21 PM	7/22/2008 1:55:23 PM	41	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 11:34:59 AM	7/22/2008 11:34:59 AM	39	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 11:03:51 AM	7/22/2008 11:03:53 AM	37	Running	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 9:59:16 AM	7/22/2008 10:01:40 AM	35	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 9:54:55 AM	7/22/2008 9:55:01 AM	33	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneDeregistrations	7/21/2008 4:22:09 PM	7/21/2008 4:22:13 PM	31	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneConnectivity	7/21/2008 4:22:02 PM	7/21/2008 4:22:07 PM	29	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneInventory	7/21/2008 4:18:17 PM	7/21/2008 4:20:20 PM
Job	Status	Children	Computer	Knowledge Script	Submit Time	Last Run Time																																																																															
49	Stopped	1	RALAVAYATEST01	AvayaCM_RemovePhone	7/22/2008 4:44:20 PM	7/22/2008 4:44:21 PM																																																																															
47	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 2:07:19 PM	7/22/2008 4:02:19 PM																																																																															
45	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 2:03:31 PM	7/22/2008 2:03:35 PM																																																																															
43	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 1:55:21 PM	7/22/2008 1:55:23 PM																																																																															
41	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 11:34:59 AM	7/22/2008 11:34:59 AM																																																																															
39	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 11:03:51 AM	7/22/2008 11:03:53 AM																																																																															
37	Running	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 9:59:16 AM	7/22/2008 10:01:40 AM																																																																															
35	Stopped	1	RALAVAYATEST01	AvayaCM_CallQuery	7/22/2008 9:54:55 AM	7/22/2008 9:55:01 AM																																																																															
33	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneDeregistrations	7/21/2008 4:22:09 PM	7/21/2008 4:22:13 PM																																																																															
31	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneConnectivity	7/21/2008 4:22:02 PM	7/21/2008 4:22:07 PM																																																																															
29	Stopped	1	RALAVAYATEST01	AvayaCM_PhoneInventory	7/21/2008 4:18:17 PM	7/21/2008 4:20:20 PM																																																																															

Step	Description
10.	<p>RetrieveConfigData Script Parameters</p> <p>The following pop-up window appears. Retain the default values and click OK.</p> 

Step	Description
11.	<p>Add Phone</p> <p>Lastly, in order to run a script (specifically the PhoneQuality script) on an individual IP telephone, that IP telephone must be entered in the tree view. To add an IP Telephone to the tree view, select the AVAYACM tab shown in Step 9 and drag the AddPhone script to IP Stations in left pane menu tree. The following pop-up will appear. Enter the IP telephone extension or list of extensions in the List of phone extensions field. Click OK.</p> <p>This action will fill out the tree view with the individual IP telephones shown in the tree view in Step 7.</p> 

Step	Description																																										
12.	<p>Call Quality</p> <p>Once the tree view is complete, scripts can be run against the various components in the tree view. For example, to run the Call Quality script, select the AvayaCM tab in Step 9 and drag the CallQuality script to the Active SPE in left pane menu tree. A pop-up window appears (not shown) that allows parameters of the script to be modified, such as event threshold levels. An example of the script output is shown below. It displays call quality metrics such as MOS, jitter and latency from both the calling and called parties.</p> <div><div>■ Event 517 : Details for call(s) which fell below the average MOS threshold [68.160.102.5] [58700ACTIVE-Cluster]</div><div><div>CallQuality: Results</div><div>1 calls fell below the average MOS threshold (5). The minimum average MOS for a call was 4.37.</div></div><div><div>CallQuality: Summary</div><table><tr><td>Number of records matching the query</td><td>1</td></tr><tr><td>Starting dateTimeDisconnect</td><td>7/21/2008 4:00:43 PM</td></tr><tr><td>Ending dateTimeDisconnect</td><td>7/21/2008 4:00:59 PM</td></tr></table></div><div><div>CallQuality: Details for the first 1 records.</div><table><thead><tr><th></th><th>Calling Number</th><th>Called Number</th><th>Connect Time</th><th>Disconnect Time</th><th>Duration (seconds)</th><th>Calling Avg MOS</th><th>Calling Avg R-Value</th><th>Calling Jitter (ms)</th><th>Calling Latency (ms)</th><th>Calling Lost Packets (%)</th><th>Calling Codec</th><th>Called Avg MOS</th><th>Called Avg R-Value</th><th>Called Jitter (ms)</th><th>Called Latency (ms)</th><th>Called Lost Packets (%)</th><th>Called Codec</th></tr></thead><tbody><tr><td>1</td><td>22002</td><td>22001</td><td>7/21/2008 4:00:53 PM</td><td>7/21/2008 4:00:59 PM</td><td>6</td><td>4.38</td><td>91.94</td><td>2</td><td>1</td><td>0.00</td><td>G711u</td><td>4.37</td><td>91.26</td><td>0</td><td>1</td><td>0.28</td><td>G711u</td></tr></tbody></table></div></div>	Number of records matching the query	1	Starting dateTimeDisconnect	7/21/2008 4:00:43 PM	Ending dateTimeDisconnect	7/21/2008 4:00:59 PM		Calling Number	Called Number	Connect Time	Disconnect Time	Duration (seconds)	Calling Avg MOS	Calling Avg R-Value	Calling Jitter (ms)	Calling Latency (ms)	Calling Lost Packets (%)	Calling Codec	Called Avg MOS	Called Avg R-Value	Called Jitter (ms)	Called Latency (ms)	Called Lost Packets (%)	Called Codec	1	22002	22001	7/21/2008 4:00:53 PM	7/21/2008 4:00:59 PM	6	4.38	91.94	2	1	0.00	G711u	4.37	91.26	0	1	0.28	G711u
Number of records matching the query	1																																										
Starting dateTimeDisconnect	7/21/2008 4:00:43 PM																																										
Ending dateTimeDisconnect	7/21/2008 4:00:59 PM																																										
	Calling Number	Called Number	Connect Time	Disconnect Time	Duration (seconds)	Calling Avg MOS	Calling Avg R-Value	Calling Jitter (ms)	Calling Latency (ms)	Calling Lost Packets (%)	Calling Codec	Called Avg MOS	Called Avg R-Value	Called Jitter (ms)	Called Latency (ms)	Called Lost Packets (%)	Called Codec																										
1	22002	22001	7/21/2008 4:00:53 PM	7/21/2008 4:00:59 PM	6	4.38	91.94	2	1	0.00	G711u	4.37	91.26	0	1	0.28	G711u																										

Step	Description														
13.	<p>Call Query</p> <p>Another example of a script that is applicable to Avaya Communication Manager is the Call Query script. To run this script, select the AVAYACM tab in Step 9 and drag the CallQuality script to the Active SPE in left pane menu tree. A pop-up window appears (not shown) that allows parameters of the script to be modified. An example of the script output is shown below. It displays calls that match the criteria specified in the script parameters pop-up window. The example below shows an outbound trunk call from 22002 to 72001 that lasted 70 secs.</p> <div><div>Event 656 : Details for calls [58700ACTIVE-Cluster]</div><div><div>CallQuery: Results</div><div>The number of calls found (1) exceeds the threshold (0).</div></div><div><div>CallQuery: Summary</div><div><div>Number of records matching the query1</div><div>Starting dateTimeDisconnect7/22/2008 11:07:19 AM</div><div>Ending dateTimeDisconnect7/22/2008 11:19:41 AM</div></div></div><div><div>CallQuery: Details for the first 1 records.</div><table><thead><tr><th></th><th>Condition Code</th><th>Calling Number</th><th>Called Number</th><th>Connect Time</th><th>Disconnect Time</th><th>Duration (seconds)</th></tr></thead><tbody><tr><td>1</td><td>Call used the AAR or ARS feature</td><td>22002</td><td>72001</td><td>7/22/2008 11:17:50 AM</td><td>7/22/2008 11:19:00 AM</td><td>70</td></tr></tbody></table></div></div>		Condition Code	Calling Number	Called Number	Connect Time	Disconnect Time	Duration (seconds)	1	Call used the AAR or ARS feature	22002	72001	7/22/2008 11:17:50 AM	7/22/2008 11:19:00 AM	70
	Condition Code	Calling Number	Called Number	Connect Time	Disconnect Time	Duration (seconds)									
1	Call used the AAR or ARS feature	22002	72001	7/22/2008 11:17:50 AM	7/22/2008 11:19:00 AM	70									

5. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of NetIQ AppManager with Avaya Communication Manager. This section covers the general test approach and the test results.

5.1. General Test Approach

The general approach was to place various types of calls to and from stations, collect VoIP call quality data from AppManager, and compare collected values with Avaya IP Telephone's Network Audio Quality values. In addition, CDR data displayed in the call query output from AppManager was compared to the CDR data received by an Avaya CDR test tool. For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, and conferenced calls. During the compliance test, a network impairment tool was utilized to simulate network delay and packet drop. Verification of each call was made by performing queries into the AppManager data and looking at the results recorded. For serviceability testing, failures such as cable pulls and resets were applied.

5.2. Test Results

AppManager successfully passed compliance testing. The following observations were made during the compliance test:

- AppManager does not display the correct Avaya Communication Manager version from its SNMP query of this data.
- In the Call Quality script, it is not always possible for AppManager to determine accurately which number was the calling party and which number was the called party. So in some instances, these numbers are reversed in the output. In the Call Query script which relies on CDR output from Avaya Communication Manager for this data, these two values are displayed correctly.
- In the Call Quality script output, some call entries appeared with a colon (:) in the extension name. This also had the side effect of causing two entries for a single call in the call output.
- CDR records with the condition code of “G” (calls that terminate to a ringing station) were not displayed properly in the Call Query script output.

6. Verification Steps

The following steps may be used to verify the configuration.

- Use the **ping** command to verify connectivity from AppManager to all devices.
- Verify that calls can be successfully completed between the IP and digital telephones.
- Compare VoIP quality data from the following sources:
 - Network impairment tool settings
 - Avaya IP Telephone’s Network Audio Quality data
 - Avaya’s CDR test tool
 - AppManager

7. Support

For technical support on AppManager, contact NetIQ via the **Support & Services** link at www.netiq.com.

8. Conclusion

These Application Notes describe the procedures required to configure NetIQ AppManager to interoperate with Avaya Communication Manager. AppManager successfully passed compliance testing with the observations documented in **Section 5.2**.

9. Additional References

- [1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 6.0, January 2008.
- [2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4, January 2008.
- [3] *NetIQ AppManager For Avaya Communication Manager Management Guide*, May, 2008.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

Product documentation for AppManager may be found at <http://www.netiq.com>.

©2008 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.