Management Guide

NetIQ® AppManager® for Avaya (Heritage-Nortel) Communication Server 1000

April 2017

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the AppManager Documentation page of the NetIQ Web site.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Introducing AppManager for Avaya (Heritage-Nortel) CS1000

Avaya CS1000, previously called Nortel CS1000, is a Voice over IP (VoIP) communication solution for the pure IP environment, as well as a mixed IP and circuit-switched solution for environments that are migrating to IP. This reliable, survivable IP telephony platform can be distributed across IP WANs and LANs.

You can find the AppManager for Avaya CS1000 Knowledge Scripts in the Nortel CS category.

1.1 Features and Benefits

AppManager is designed to help you gain easy access to CS1000 data, and to help you analyze and manage that data. The AppManager for Avaya CS1000 solution minimizes the cost of maintaining CS1000 services and functions, aids in capacity planning, and can prevent downtime.

With AppManager for Avaya CS1000, administrators gain access to a set of tools they can leverage to gather a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

The AppManager for Avaya CS1000 module includes Knowledge Scripts for creating jobs that monitor the health and status of key CS1000 components:

- Call Server, which provides call and connection management services for the IP network.
- Media Gateway, which acts as a bridge between IP and TDM-based telephony networks, such as the PSTN, supporting interfaces such as analog and digital trunks, and analog and digital lines.
- Signaling Server, which provides signaling interfaces to the IP network, and performs call control services such as the registration of terminals and gateways, admission control, IP address translation, and bandwidth control.
- Voice Gateway Media Card (VGMC), which packetizes and compresses voice for transmission over an IP data network.
- MC32S, an enhanced VGMC that supports 32-port DSPs (digital signal processors).
- Media Gateway Controller, which controls the Media Gateway chassis and cabinet in versions 4.50 and earlier. In versions 5.x and later, the MGC is a combination of controller for the Media Gateway chassis and a voice gateway.
- Network Routing Server, which runs on the Signaling Server in version 4.0, and on the Signaling Server or its own server in versions 5.x and later.
- Enterprise Common Manager, which runs on the COTS (commodity hardware) server platform
- Co-resident Call Servers, Signaling Servers, and Element Managers. Co-resident components reside on a single server.
- SIP Line (SIPL) Gateway application, which runs on its own COTS or Common Processor Pentium Mobile (CP PM) server.

Knowledge Scripts allow you to monitor and manage crucial services at a depth unparalleled by any other solution. You can configure each script to send an alert, collect data for reporting, and perform automated problem management when an event occurs. For more information about the Knowledge Scripts for monitoring CS1000, see the AppManager Help for any specific script.

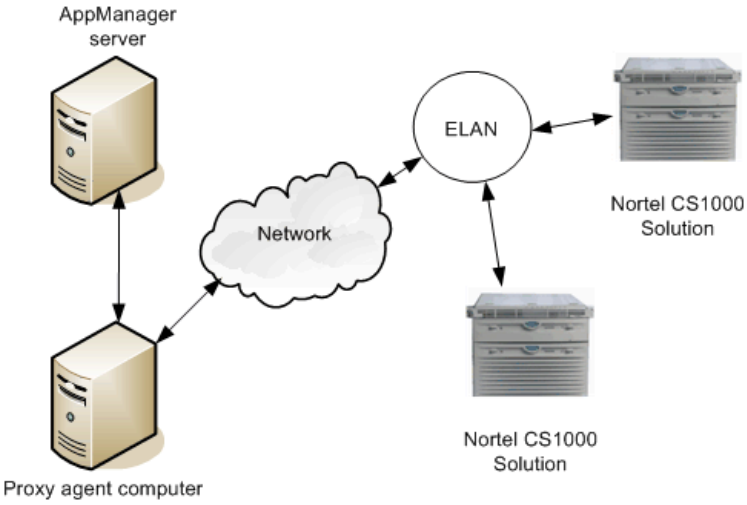
The following are just a few of the features and benefits of monitoring CS1000 with AppManager:

- Reduces the time that you spend diagnosing and resolving issues relating to fundamental call-processing functions
- Automates system management issues that could affect CS1000 performance
- Pinpoints problems wherever they originate
- Provides Knowledge Scripts for day-to-day and diagnostic monitoring
- Monitors system health, including the Call Server, Media Gateway, Signaling Server, VGMC, MGC, NRS, ECM, MC32S, and SIP Line (SIPL) Gateway
- Easily retrieves call quality statistics (jitter, latency, lost packets) from the Signaling Server, VGMC, MGC, and MC32S
- Monitors registration attempts and failures
- Creates an inventory of each phone in the Entity MIB
- Filters and reports on QoS alarms by subnet, using IP address or IP address range
- Retrieves current and historical Operational Management reports
- Monitors Host MIB attributes associated with CS1000 devices
- Monitors blocked calls, peak bandwidth, and call quality statistics for the Bandwidth Management Zone
- Interacts with NetIQ Vivinet Diagnostics to diagnose problems with VoIP quality between phones. For more information, see Section 2.15, “Working with Vivinet Diagnostics,” on page 32.
- Supports the Avaya and NetIQ Proactive Voice Quality Management (PVQM) solution on the 2050 model softphone. For more information, contact Nortel Technical Support.

1.2 Understanding the Proxy Architecture

With AppManager proxy architecture support for CS1000, the AppManager agent does not need to be installed on every device that you want to monitor.

The following diagram illustrates the relationship between Avaya CS1000, previously called Nortel CS1000, devices the AppManager repository (QDB) server, and the proxy agent computer.



AppManager uses SNMP over the network and the ELAN to tell the Call Server to use FTP to send Operational Measurement (OM) reports. AppManager also uses SNMP to receive traps from CS1000.

NOTE: If you use Vivinet Diagnostics to diagnose VoIP quality problems in your CS1000 environment, the proxy agent computer *must* also have TLAN connectivity. For more information, see Section 2.16.5, “GetOMReport Script Hangs in Running State,” on page 35.

1.3 Counting AppManager Licenses

Licensing for the module is based on the number of CS1000 soft phones and IP phones you have, excluding wireless IP phones.

Only phones with a physical description in the Entity MIB of “Internet Telephony Set” or “Internet Telephony PC Client” are counted for licensing. These phones are supported by Nortel PVQM and provide QoS statistics.

1.4 Using NetworkDevice Scripts

The AppManager for Network Device module provides Knowledge Scripts that can monitor and retrieve statistics about Ethernet interfaces and protocols from the MIB2 (management information base) of the Call Server, Media Gateway, Signaling Server, Media Gateway Controller, and VGMC.

In addition to using the Knowledge Scripts in the Nortel CS category, you can enhance your monitoring efforts by including the following Knowledge Scripts from the NetworkDevice category:

Knowledge Script	What It Does
NetworkDevice_Device_Ping	Checks the availability of network devices that respond to ICMP Echo requests.
NetworkDevice_Host_CPULoaded	This script monitors Nortel CS1000 version 4.50 Media Gateways only. Accesses the Host Resource MIB to monitor total CPU usage to determine whether the CPU is overloaded. ◆ **Call Server** Do not run this script on a Call Server — it will monitor call capacity usage rather than CPU usage. In version 4.50 devices, the MIB value for the CPU processor load represents call capacity usage. To monitor call capacity usage, use the NortelCS_CallCapacity Knowledge Script. ◆ **Media Gateway** The `hrProcessorload` value in the MIB is always -1, so the data stream value for this script is always 0.
NetworkDevice_Host_DeviceStatus	This script monitors CS1000 version 4.50 and later devices only. Accesses the Host Resource MIB to monitor the status and error count for Co-resident Servers, Call Servers, Media Gateways, VGMCs, Signaling Servers, and SIP Gateways.
NetworkDevice_Host_MemoryUsage	Accesses the Host Resource MIB to monitor memory usage on CS1000 version 4.50 and later Co-resident Servers, VGMCs, Signaling Servers, and SIP Gateways.
NetworkDevice_Host_ProcessDown	Accesses the Host Resource MIB to determine whether a specified process is not running on CS1000 version 4.50 and later Co-resident Servers, Call Servers, Media Gateways, VGMCs, Signaling Servers, and SIP Gateways.
NetworkDevice_Host_ProcessUp	Accesses the Host Resource MIB to determine whether a specified process is running on CS1000 version 4.50 and later Co-resident Servers, Call Servers, Media Gateways, VGMCs, Signaling Servers, and SIP Gateways.

Knowledge Script	What It Does
NetworkDevice_Host_StorageUsage	This script monitors CS1000 version 4.50 and later devices only. Accesses the Host Resource MIB to monitor storage usage on the following devices. ◆ **Call Server** This script monitors flash memory storage. ◆ **Media Gateway** This script monitors flash memory storage. ◆ **VGMC** This script monitors floppy disk storage. Flash memory is implemented on the VGMC Host MIB, but the value is always -1, so the data stream value for this script is always 0. ◆ **Signaling Server** This script monitors fixed disk, compact disk, and floppy disk storage. ◆ **MGC** This script monitors fixed disk storage. ◆ **Linux base server** This script monitors Linux file systems for CS1000 version 6.0.
NetworkDevice_Interface_Health	Monitors the parent resource for the interfaces on a network device.
NetworkDevice_IPSubsystem_Util	Monitors the IP subsystem of a network device.
NetworkDevice_LANLink_Util	Monitors the parent resource for the LAN links on a network device.

2 Installing and Configuring AppManager for Avaya (Heritage-Nortel) CS1000

This chapter provides system requirements and describes how to install and configure AppManager for Avaya (Heritage-Nortel) CS1000.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the AppManager Documentation page.

NOTE

- The AppManager for CS1000 module is incompatible with the Avaya Telephony Manager application, which competes with the module for UDP port 162.
- The AppManager for CS1000 module is incompatible with NetIQ Trap Receiver. For more information, see Section 2.12, “Disabling NetIQ Trap Receiver,” on page 28.

2.1 System Requirements

AppManager for Avaya (Heritage-Nortel) CS1000 has the following system requirements:

Requirement	Details
NetIQ AppManager installed on the AppManager repository (QDB) computers, on all proxy agent computers, and on all console computers	8.0.3, 8.2, 9.1, or later. One of the following AppManager agents are required: ◆ AppManager agent 7.0.4 with hotfix 72616 or later ◆ AppManager agent 8.0.3, 8.2, 9.1, or later The proxy agent computer’s network interface must be on the CS1000 ELAN, not the TLAN. **IMPORTANT:** If you use NetIQ Vivinet Diagnostics to diagnose VoIP quality problems in your CS1000 environment, the proxy agent computer must have *both* ELAN and TLAN connectivity. For more information, see the *AppManager for Avaya (Heritage-Nortel) Communication Server 1000 Management Guide*.

Requirement	Details
Microsoft Windows operating system on all proxy agent computers	One of the following: ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows 8 (32-bit and 64-bit) ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit and 64-bit) ◆ Windows 7 (32-bit and 64-bit) ◆ Windows Server 2003 R2 (32-bit and 64-bit)
AppManager for Microsoft Windows module installed on repository, agent, and console computers	7.6.170.0 or later. For more information, see the AppManager Module Upgrades & Trials page.
Avaya Communication Server 1000 (CS1000) version 7.65, 7.6, 7.5, 7.0, 6.0, 5.5, 5.0, 4.50, 4.0, or 3.0 installed on the computers you want to monitor	For **version 6.0** systems: ◆ Avaya **patch MPLR29703** must be installed. The patch supports OM Report retrieval. For **version 5.5** systems: ◆ Avaya **patch Q01857201-p25859_1.ss1** must be installed on **Signaling Servers**. The patch corrects a problem in which entries for unregistration attempts for model 2211 phones are missing in the OM Report. For **version 5.0** systems: ◆ Avaya **patch MPLR24316** must be installed on **Call Servers**. The patch corrects the `entityPhysicalDescr` MIB variable, which falsely reports IP telephony phones as Digital phones. ◆ Avaya **software load MGCCAD35 or later** must be installed on **Media Gateway Controllers**. The load enables OM Report retrieval. For **version 4.50** systems: ◆ Avaya **patch MPLR21714** must be installed on **Signaling Servers**. The patch enables BMZ support and requires manual configuration on the Call Server. For more information, see the patch ReadMe. ◆ Avaya **patch MPLR22309** must be installed on **VGMCs**. The patch enables VGMC trap retrieval. ◆ Avaya **patch MPLR23300** must be installed on **Call Servers**. The patch corrects a problem with Call Server QoS messages containing the wrong severities. ◆ Avaya **patch MPLR23560** must be installed on **Call Servers**. The patch corrects a problem with Zone statistics in which average bandwidth value may be higher than peak bandwidth value. **NOTE:** You can obtain all patches and software loads from your Avaya support and maintenance provider.

Requirement	Details
Microsoft Windows SNMP service installed and configured	Configure AppManager Security Manager as follows: ◆ For the Call Server, Media Gateway, ECM, NRS, and SIPL, configure the **read-only** SNMP community strings ◆ For the Signaling Server, VGMC, MC32S, and MGC, configure the **read/write** SNMP community strings. ◆ For a co-resident Call Server and Signaling Server, configure the **read/write** SNMP community strings. For more information, see Section 2.6, "Configuring SNMP Community Strings," on page 24.
SL1 Level 1 login ID and password configuration	For CS1000 **version 3.0 only**, configure AppManager Security Manager with the SL1 Level 1 login ID and password. For more information, see Section 2.8, "Configuring the SL1 Level 1 Login for Version 3.0," on page 26.
PDT password configuration	For CS1000 **version 3.0 only**, configure AppManager Security Manager with the PDT password. For more information, see Section 2.7, "Configuring the PDT Password for Version 3.0," on page 25.
ELAN IP addresses for all CS1000 devices that you want to monitor	Provide these addresses when setting up the Discovery_NortelCS Knowledge Script job. To identify the ELAN IP address of the Call Server, issue the following command from Overlay 117: `prt elnk`. Contact your CS1000 system administrator for the IP addresses of the other devices that you want to monitor. Each additional IP address needs to belong to the same subnet as the IP address of the Call Server. **NOTE:** Do not use a TLAN IP address in place of an ELAN IP address.
File Transfer Protocol	Ensure FTP (File Transfer Protocol) works in your environment. Ensure that no firewall prevents FTP from functioning on the ELAN. AppManager for Avaya CS1000 uses FTP to transfer OM reports. If you have special FTP requirements, see Section 4.4.5, "Configuring FTP Server Parameters," on page 61.
AppManager for Network Devices module	Although the AppManager for Network Devices module is not required, you can greatly enhance your monitoring efforts by using the NetworkDevice scripts to monitor your CS1000 devices. To download the latest AppManager for Network Devices module, see the AppManager Module Upgrades & Trials page.

2.2 Installing the Module

Run the module installer on the proxy agent computers you want to monitor to install the agent components, and run the module installer on all console computers to install the Help and console extensions.

Access the `AM70-NortelCS-7.x.x.0.msi` module installer from the `AM70_NortelCS_7.x.x.0` self-extracting installation package on the AppManager Module Upgrades & Trials page.

For Windows environments where User Account Control (UAC) is enabled, install the module using an account with administrative privileges. Use one of the following methods:

- Log in to the server using the account named Administrator. Then, run `AM70-NortelCS-7.x.x.0.msi` from a command prompt or by double-clicking it.
- Log in to the server as a user with administrative privileges and run `AM70-NortelCS.x.x.0.msi` as an administrator from a command prompt. To open a command-prompt window at the administrative level, right-click a command-prompt icon or a Windows menu item and select **Run as administrator**.

You can install the Knowledge Scripts and the Analysis Center reports into local or remote AppManager repositories (QDBs). The module installer installs Knowledge Scripts for each module directly into the QDB instead of installing the scripts in the `\AppManager\qdb\kp` folder as in previous releases of AppManager.

NOTE: Versions 7.1 and later of the module are incompatible with previous versions of the module. When you install version 7.1 or later, update all computers on which any previous version is installed.

To install the module:

1. Double-click the module installer `.msi` file.
2. Accept the license agreement.
3. Review the results of the pre-installation check. You can expect one of the following three scenarios:
   - **No AppManager agent is present:** In this scenario, the pre-installation check fails, and the installer does not install agent components.
   - **An AppManager agent is present, but some other prerequisite fails:** In this scenario, the default is to not install agent components because of one or more missing prerequisites. However, you can override the default by selecting Install agent component locally. A missing application server for this particular module often causes this scenario. For example, installing the AppManager for Microsoft SharePoint module requires the presence of a Microsoft SharePoint server on the selected computer.
   - **All prerequisites are met:** In this scenario, the installer installs the agent components.
4. To install the Knowledge Scripts into the QDB and to install the Analysis Center reports into the Analysis Center Configuration Database:
   - **4a** Select **Install Knowledge Scripts** to install the repository components, including the Knowledge Scripts, object types, and SQL stored procedures.
   - **4b** Select **Install report package** to install the Analysis Center reports.
   - **4c** Specify the SQL Server name of the server hosting the QDB, as well as the case-sensitive QDB name.
   - **4d** Specify the SQL Server name of the server hosting the Analysis Center Configuration Database.

5 (Conditional) If you use Control Center 7.x, run the module installer for each QDB attached to Control Center.

6 (Conditional) If you use Control Center 8.x, run the module installer only for the primary QDB. Control Center automatically replicates this module to secondary QDBs.

7 Run the module installer on all console computers to install the Help and console extensions.

8 Run the module installer on all proxy agent computers to install the agent components.

9 Before discovering CS1000 resources, perform all required configuration tasks for CS1000. For more information, see Section 2.5, “Checklists for Required Configuration Tasks,” on page 20.

10 If you have not discovered CS1000 resources, run the Discovery_NortelCS Knowledge Script on all proxy agent computers where you installed the module. For more information, see Section 2.13, “Discovering Avaya Communication Server Resources,” on page 29.

11 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.14, “Upgrading Knowledge Script Jobs,” on page 31.

After the installation has completed, the `ModuleName_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\ServerName` folder, lists any problems that occurred.

2.3 Deploying the Module with Control Center

You can use Control Center to deploy the module on a remote computer where an agent is installed. This topic briefly describes the steps involved in deploying a module and provides instructions for checking in the module installation package. For more information, see the *Control Center User Guide for AppManager*, which is available on the AppManager Documentation page.

2.3.1 Deployment Overview

This section describes the tasks required to deploy the module on an agent computer.

To deploy the module on an agent computer:

1 Verify the default deployment credentials.

2 Check in an installation package. For more information, see Section 2.3.2, “Checking In the Installation Package,” on page 19.

3 Configure an e-mail address to receive notification of a deployment.

4 Create a deployment rule or modify an out-of-the-box deployment rule.

5 Approve the deployment task.

6 View the results.

2.3.2 Checking In the Installation Package

You must check in the installation package, `AM70-NortelCS-7.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1 Log on to Control Center using an account that is a member of a user group with deployment permissions.

2 Navigate to the **Deployment** tab (for AppManager 8.x) or **Administration** tab (for AppManager 7.x).

3 In the Deployment folder, select **Packages**.

4 On the Tasks pane, click **Check in Deployment Packages** (for AppManager 8.x) or **Check in Packages** (for AppManager 7.x).

5 Navigate to the folder where you saved `AM70-NortelCS-7.x.x.0.xml` and select the file.

6 Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.

7 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.14, “Upgrading Knowledge Script Jobs,” on page 31.

2.4 Silently Installing the Module

To silently (without user intervention) install a module using the default settings, run the following command from the folder in which you saved the module installer:

```
msiexec.exe /i "AM70-NortelCS-7.x.x.0.msi" /qn
```

where *x.x* is the actual version number of the module setup program.

To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.14, “Upgrading Knowledge Script Jobs,” on page 31.

To create a log file that describes the operations of the module setup program, add the following flag to the command noted above:

```
/L* "AM70-NortelCS-7.x.x.0.msi.log"
```

The log file is created in the directory in which you saved the module setup program.

NOTE: To perform a silent install on an AppManager agent running Windows Server 2008 R2 or Windows Server 2012, open a command prompt at the administrative level and select **Run as administrator** before you run the silent install command listed above.

To silently install the module on a remote AppManager repository, you can use Windows authentication or SQL authentication.

Windows authentication:

```
AM70-NortelCS-7.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0
MO_B_SQLSVR_WINAUTH=1 MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

SQL authentication:

```
AM70-NortelCS-7.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0
MO_B_SQLSVR_WINAUTH=0 MO_SQLSVR_USER=SQLLogin MO_SQLSVR_PWD=SQLLoginPassword
MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

2.5 Checklists for Required Configuration Tasks

After you install the module, perform all required configuration tasks *before* you begin the discovery process. This configuration provides AppManager access to such CS1000 information as SNMP traps and the phone inventory on the Call Server. Much of the configuration also enables the functionality of the Alarms Knowledge Script.

The configuration tasks vary according to your version of CS1000.

2.5.1 Configuration for Versions 6.0 and Later

For CS1000 versions 6.0 and later, perform the following tasks *before* running the Discovery_NortelCS Knowledge Script.

	Task	Purpose
❑	Configure SNMP community strings	Configure SNMP community strings in AppManager Security Manager to allow AppManager to access CS1000 devices. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.
❑	Set up phone inventory process	Issue several commands in Overlay 117 to set up the phone inventory process on the Call Server. For more information, see Section 4.6.5, “Configuring the Call Server to Count IP Phones,” on page 65.
❑	Identify the SNMP trap receiver	Identify the proxy agent computer as an SNMP trap receiver to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 4.1.6, “Identifying the SNMP Trap Receiver,” on page 51.
❑	Set QoS thresholds	Set QoS thresholds to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.9, “Setting QoS Call Basis Thresholds,” on page 26.
❑	Set zone notification levels	Set zone notification levels to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.10, “Setting Zone Notification Levels,” on page 27.
❑	Set NIC binding order	Designate NIC binding order to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.11, “Setting NIC Binding Order,” on page 28.
❑	Set BMZ QoS thresholds	Configure QoS zone basis threshold levels to allow the BMZ_CallQuality script to gather Bandwidth Management Zone call quality metrics. For more information, see Section 4.2.6, “Setting Bandwidth Management Zone Thresholds,” on page 57.
❑	Enable insecure Shell access	To ensure AppManager for CS1000 interacts properly with NetIQ Vivinet Diagnostics, enable insecure Shell access. For more information, see Section 2.15, “Working with Vivinet Diagnostics,” on page 32.

2.5.2 Configuration for Versions 5.x

For CS1000 version 5.x, perform the following tasks *before* running the Discovery_NortelCS Knowledge Script.

	Task	Purpose
❑	Configure SNMP community strings	Configure SNMP community strings in AppManager Security Manager to allow AppManager to access CS1000 devices. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.
❑	Set up phone inventory process	Issue several commands in Overlay 117 to set up the phone inventory process on the Call Server. For more information, see Section 4.6.5, “Configuring the Call Server to Count IP Phones,” on page 65.
❑	Identify the SNMP trap receiver	Identify the proxy agent computer as an SNMP trap receiver to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 4.1.6, “Identifying the SNMP Trap Receiver,” on page 51.
❑	Set QoS thresholds	Set QoS thresholds to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.9, “Setting QoS Call Basis Thresholds,” on page 26.
❑	Set zone notification levels	Set zone notification levels to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.10, “Setting Zone Notification Levels,” on page 27.
❑	Set NIC binding order	Designate NIC binding order to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.11, “Setting NIC Binding Order,” on page 28.
❑	Set BMZ QoS thresholds	Configure QoS zone basis threshold levels to allow the BMZ_CallQuality script to gather Bandwidth Management Zone call quality metrics. For more information, see Section 4.2.6, “Setting Bandwidth Management Zone Thresholds,” on page 57.
❑	Enable QoS MIB access on the Signaling Server	Create a dedicated user account to enable SNMP to access the QoS MIB. For more information, see Section 4.2.7, “Enabling Access to the Signaling Server QoS MIB for CS1000 version 5.x,” on page 58.
❑	Enable insecure Shell access	To ensure AppManager for CS1000 interacts properly with NetIQ Vivinet Diagnostics, enable insecure Shell access. For more information, see Section 2.15, “Working with Vivinet Diagnostics,” on page 32.

2.5.3 Configuration for Versions 4.0 and 4.50

For CS1000 versions 4.0 and 4.50, perform the following tasks *before* running the Discovery_NortelCS Knowledge Script.

	Task	Purpose
❑	Configure SNMP community strings	Configure SNMP community strings in AppManager Security Manager to allow AppManager to access CS1000 devices. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.
❑	Issue Overlay 117 commands	Issue several commands in Overlay 117 to set up the phone inventory process on the Call Server. For more information, see Section 4.6.5, “Configuring the Call Server to Count IP Phones,” on page 65. **NOTE:** If you are upgrading from CS1000 version 3.0 or 4.0 to version 4.50, your previous PDT password and SL1 Level 1 login will continue to work. However, you should configure the Call Server to count IP phones so you can use the Entity MIB for the inventory report.
❑	Identify the SNMP trap receiver	Identify the proxy agent computer as an SNMP trap receiver to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 4.1.6, “Identifying the SNMP Trap Receiver,” on page 51.
❑	Set QoS thresholds	Set QoS thresholds to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.9, “Setting QoS Call Basis Thresholds,” on page 26.
❑	Set zone notification levels	Set zone notification levels to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.10, “Setting Zone Notification Levels,” on page 27.
❑	Set NIC binding order	Designate NIC binding order to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.11, “Setting NIC Binding Order,” on page 28.
❑	Set BMZ QoS thresholds	Configure QoS zone basis threshold levels to allow the BMZ_CallQuality script to gather Bandwidth Management Zone call quality metrics. For more information, see Section 4.2.6, “Setting Bandwidth Management Zone Thresholds,” on page 57.

2.5.4 Configuration for Version 3.0

For CS1000 version 3.0, perform the following tasks *before* running the Discovery_NortelCS Knowledge Script.

	Task	Purpose
❑	Configure SNMP community strings	Configure SNMP community strings in AppManager Security Manager to allow AppManager to access CS1000 devices. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.
❑	Configure the PDT password	Configure AppManager Security Manager with the PDT password to allow AppManager to ask the Call Server to generate the inventory report. For more information, see Section 2.7, “Configuring the PDT Password for Version 3.0,” on page 25.
❑	Configure the SL1 Level 1 login	Configure AppManager Security Manager with the SL1 Level 1 login to allow AppManager to ask the Call Server to generate the inventory report. For more information, see Section 2.8, “Configuring the SL1 Level 1 Login for Version 3.0,” on page 26.
❑	Set zone notification levels	Set zone notification levels to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.10, “Setting Zone Notification Levels,” on page 27.
❑	Set NIC binding order	Designate NIC binding order to allow the Alarms script to monitor the proxy agent computer for CS1000 alarms. For more information, see Section 2.11, “Setting NIC Binding Order,” on page 28.

2.6 Configuring SNMP Community Strings

To enable AppManager to use SNMP to access CS1000 devices, configure your SNMP community string information in AppManager Security Manager *before* you discover CS1000 devices.

Use the following guidelines to configure your community strings for one or more variations:

- If your read-only community string information is the same for all CS1000 devices, complete the following procedure once. Enter the following in the **Sub-label** field: `default`.
- If your read/write community string is the same for all Signaling Servers, VGMCs, MGCs, and MC32Ss, complete the following procedure once. Enter the following in the **Sub-label** field: `default write`.
- If your read-only or read/write community string information is different for different devices, complete the following procedure once for each different community string. Enter the device’s ELAN IP address in the **Sub-label** field.

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

Field	Description
Label	`NetworkDevice`

Field	Description
Sub-label	◆ For all devices that use the same read-only community string, type `default`. Use the `default` sub-label for the read-only community string used on the greatest number of 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 that use the same read/write community string. ◆ For a single device that uses a unique read-only community string, type the ELAN IP address of the Call Server, Media Gateway, NRS, ECM, or SIP Gateway. ◆ For a single device that uses a unique read/write community string, type <*IP address*> `write` where <*IP address*> is the ELAN IP address of the Signaling Server, VGMC, MGC, or MC32S
Value 1	The configured community string for the CS1000 device you want to monitor. ◆ To monitor a Call Server, Media Gateway (CS1000 version 4.50 and earlier), Network Routing Server (NRS), Enterprise Common Manager (ECM), or SIP Line server (SIPL), provide your configured SNMP read-only community string. ◆ To monitor a Signaling Server, VGMC, Media Gateway Controller (MGC), or MC32S, provide your configured SNMP read/write community string. The read/write community string gives AppManager SNMP access to the MIBs on these devices. ◆ To monitor a version 6.0 and later co-resident device that hosts a Signaling Server, provide your configured SNMP read/write community string.

Examples of community string configuration

- To monitor multiple Signaling Servers that have the same read/write community string, type `default write` in the **Sub-label** field and type the read/write community string in the **Value 1** field.
- To monitor a Call Server that has a unique read-only community string, type the ELAN IP address of the Call Server in the **Sub-label** field and type the read-only community string in the **Value 1** field.
- To monitor a VGMC that has a unique read/write community string, type <*IP address*> `write` in the **Sub-label** field (where `<IP address>` is the ELAN IP address of the VGMC) and type the read/write community string in the **Value 1** field.

2.7 Configuring the PDT Password for Version 3.0

To allow Discovery_NortelCS to retrieve the inventory report from CS1000 version 3.0, configure the PDT (Problem Determination Tool) password in AppManager Security Manager *before* you discover CS1000 devices.

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

Field	Description
Label	`NortelCS_PDT_Password`
Sub-label	`default`, or the IP address of the CS1000 Call Server
Value 1	PDT password

Field	Description
Extended application support	Encrypts the password in Security Manager. You must select this option.

2.8 Configuring the SL1 Level 1 Login for Version 3.0

To allow Discovery_NortelCS to retrieve the inventory report from CS1000 version 3.0, configure the Level 1 login in AppManager Security Manager *before* you discover CS1000 devices.

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

Field	Description
Label	`NortelCS_Login`
Sub-label	`default`, or the IP address of the CS1000 Call Server
Value 1	SL1 Level 1 user ID
Value 2	SL1 Level 1 password (PWD1)
Extended application support	Encrypts the user ID and password in Security Manager. You must select this option.

2.9 Setting QoS Call Basis Thresholds

Configure QoS call basis threshold levels in CS1000 Element Manager. Call quality metrics that exceed or fall below the thresholds are identified by the Alarms script.

2.9.1 Configuring QoS Thresholds for Versions 5.x and Later

Use Element Manager to configure QoS thresholds.

To configure QoS thresholds:

1. Navigate to **System**, click **IP Network**, and then click **QoS Thresholds**.
2. Set the **Warning** and **Unacceptable** thresholds appropriate for your environment.
3. Click **Submit**.
4. Use Element Manager or Overlay 43 to perform a Call Server data dump.

2.9.2 Configuring QoS Thresholds for Version 4.50

Use Element Manager to configure QoS thresholds.

To configure QoS thresholds:

1. Navigate to **IP Telephony** and click **QoS Thresholds**.
2. Set the **Warning** and **Unacceptable** thresholds appropriate for your environment.
3. Click **Submit**.
4. Use Element Manager or Overlay 43 to perform a Call Server data dump.

2.9.3 Configuring QoS Thresholds for Version 4.0

Use Element Manager to configure QoS thresholds.

To configure QoS thresholds:

1. Navigate to **Configuration**, click **IP Telephony**, and then click **Quality Of Service Thresholds**.
2. Set the **Warning** and **Unacceptable** thresholds appropriate for your environment.
3. Click **Submit**.
4. Use Element Manager or Overlay 43 to perform a Call Server data dump.

2.10 Setting Zone Notification Levels

Zone notification levels determine which QoS alarms are sent to the proxy agent computer as SNMP traps. The following table identifies the notification levels and the corresponding alarms.

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 you do not specifically designate a zone notification level, all QoS alarms fall into the default level, which is 0. Enable notification level 4 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`

NOTE: Enable notification level 4 if you use NetIQ Vivinet Diagnostics to diagnose problems between VoIP target devices. When running the Alarms Knowledge Script, AppManager can deploy the Action_DiagnoseNortelIPT Knowledge Script to trigger a diagnosis in your Avaya IP telephony

environment when the following alarms are raised: QOS0022, QOS0024, QOS0026, QOS0028, QOS0030, QOS0032, and QOS0034. Each of these alarms is in zone notification level 4. For more information, see the *User Guide for Vivinet Diagnostic*s.

2.11 Setting NIC Binding Order

Set the NIC *binding order* if your proxy agent computer uses two NICs (network interface cards): one on the ELAN and one on the TLAN. The binding order is the order in which the TCP/IP or other network service attempts to connect to a network interface.

If the binding order is set so the TLAN is contacted first, the Alarms script does not receive alarms because SNMP traps from CS1000 come in on the ELAN.

Set your binding order so the ELAN is contacted *before* the TLAN.

To set NIC binding order:

1. On the proxy agent computer, navigate to the Network Connections window.
2. On the Advanced menu, click **Advanced Settings**.
3. In the Connections panel, select a network connection, and then use the **Up** and **Down** buttons to sort the connections in the proper order.

2.12 Disabling NetIQ Trap Receiver

The AppManager for Avaya CS1000 module is incompatible with NetIQ Trap Receiver (Trap Receiver), which competes with the module for UDP port 162. Trap Receiver is installed with several AppManager modules, including AppManager for Network Devices. The Alarms Knowledge Scripts listens for SNMP traps on UDP port 162. To allow the Alarms script to function, disable Trap Receiver and enable Microsoft SNMP Trap Service.

To disable Trap Receiver and enable SNMP Trap Service:

1. On the proxy agent computer, navigate to **Control Panel > Administrative Tools > Services**.
2. In 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. In 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. In the list of services, right-click **NetIQ AppManager Communication Manager** and select **Restart**.
10. In the list of services, right-click **NetIQ Client Resource Monitor** and select **Restart**.

2.13 Discovering Avaya Communication Server Resources

Use the Discovery_NortelCS Knowledge Script to discover the various components of an Avaya CS1000 IP telephony system installation: Call Server, Signaling Server, Media Gateway Controller, Network Routing Server, MC32S, Enterprise Common Manager, Voice Gateway Media Card, and SIP Line Gateway.

The Discovery_NortelCS Knowledge Script also discovers co-resident Call Servers, Signaling Servers, and Element Managers. When co-resident, these components are installed on a single processor.

For CS1000 version 6.0 and later environments, the script discovers Bandwidth Management Zone (BMZ) objects on the Call Server. For earlier versions of CS1000, BMZ objects are discovered on the Signaling Server.

By default, Discovery_NortelCS runs weekly, on Sunday at 3 AM. The default schedule allows the discovery process to run at a time that is probably less busy for your Call Server.

If you delete or add a resource object, or if you make any other kind of change that might affect the monitoring of your resources, run the Discovery_NortelCS Knowledge Script again to update your list of resource objects. In addition, if you are running this module on AppManager 8 and later, you can use the delta discovery feature in Control Center to run discovery on a schedule to more quickly detect changes to your environment.

Set the parameters on the **Values** tab as needed:

Parameter	How to Set It
Event Notification	
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails for any reason. The default is Yes.
Event severity if discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when discovery fails. The default is 5.
Raise event if discovery partially succeeds?	Select **Yes** to raise an event if discovery is partially successful. A partially successful discovery is one in which, for example, AppManager can discover devices but cannot create an inventory report. Or one in which, for example, AppManager can discover all Signaling Servers, but not the Bandwidth Management Zones. The default is Yes.
Event severity if discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery is partially successful. The default is 15.
Raise event if discovery succeeds?	Select **Yes** to raise an event if discovery succeeds. The default is unselected.
Event severity if discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery succeeds. The default is 25.
Call Server	Provide the hostname or IP address of the CS1000 Call Server, such as `CS1000_CS`. Do not enter the IP address or hostname of the Call Server that is part of the Media Gateway. **Important** Provide *only one* Call Server hostname or IP address. Discovery is meant to discover only one CS environment.

Parameter	How to Set It
List of NortelCS devices	Use this parameter if you know which CS1000 devices you want to discover. Type a list of the devices you want to discover. Use a comma to separate the names in the list; for example: `CS1000_VGMC,CS1000_SS`. You can type hostnames (if you use DNS in your environment) or ELAN IP addresses. **Notes** ◆ Leave this field blank to discover only the Call Server, which you identified in the previous parameter. ◆ The community string information for each device you list in this field must be configured in Security Manager before you run this script. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.
List of NortelCS device ranges	Type a list of ELAN IP address ranges for the CS1000 devices you want to discover. Spaces are invalid in the list; only numbers, dashes, periods, and commas are allowed. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254`. **Notes** ◆ Leave this field blank to discover *only* the Call Server, which you identified in the *Call Server* parameter. ◆ Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.
Full path to file with list of NortelCS devices	Instead of listing each CS1000 device separately, you can specify the full path to a file on the proxy agent computer that contains a device name on each line of the file. **Notes** ◆ Leave this field blank to discover *only* the Call Server, which you identified in the *Call Server* parameter. ◆ The community string information for each device listed in the file must be configured in Security Manager before you run this script. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.
Discovery timeout	Specify the maximum amount of time (no more than 60 minutes) the script should attempt discovery before stopping as an unsuccessful discovery. The default is 10 minutes.
Discover phones using the Call Server’s Entity MIB?	Select **Yes** to use the Entity MIB (management information base) to count IP phones for the inventory report. AppManager will perform an SNMP query of this Call Server MIB to retrieve the inventory results. This parameter is applicable **only** for CS1000 4.0 and later. Disable this option if you use CS1000 3.0. For more information, see Section 4.6.5, “Configuring the Call Server to Count IP Phones,” on page 65.

2.14 Upgrading Knowledge Script Jobs

If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you might have made to the parameter settings for the Knowledge Scripts in the previous version of this module. Before AppManager 8.x, the module upgrade process *overwrote* any settings you might have made, changing the settings back to the module defaults.

As a result, if this module includes any changes to the default values for any Knowledge Script parameter, the module upgrade process ignores those changes and retains all parameter values that you updated. Unless you review the management guide or the online Help for that Knowledge Script, you will not know about any changes to default parameter values that came with this release.

You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

- Use the AMAdmin_UpgradeJobs Knowledge Script.
- Use the Properties Propagation feature.

2.14.1 Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

For more information, see the **Help** for the AMAdmin_UpgradeJobs Knowledge Script.

2.14.2 Propagating Knowledge Script Changes

You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups and renamed Knowledge Scripts.

Before propagating script changes, verify that the script parameters are set to your specifications. You might need to appropriately set new parameters for your environment or application.

If you are not using AppManager 8.x or later, customized script parameters might have reverted to default parameters during the installation of the module.

You can choose to propagate only properties (specified in the **Schedule** and **Values** tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate the properties and the script.

For more information about propagating Knowledge Script changes, see the “Running Monitoring Jobs” chapter of the *Control Center User Guide for AppManager*.

2.14.3 Propagating Changes to Ad Hoc Jobs or Knowledge Script Groups

You can propagate the properties and the logic (script) of a Knowledge Script to ad hoc jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

You can also propagate the properties and logic of a Knowledge Script to corresponding Knowledge Script Group members. After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

To propagate changes to ad hoc Knowledge Script jobs or Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script or Knowledge Script Group for which you want to propagate changes.
2. Right-click the script or group and select **Properties propagation** > **Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs or groups and click **OK**:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options. If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you might have made to the parameter settings for the Knowledge Scripts in the previous version of this module.

2.15 Working with Vivinet Diagnostics

NetIQ Vivinet Diagnostics diagnoses problems with the routing, connections, and performance of Voice over IP (VoIP) telephone calls on your network. With the data you receive from a Diagnosis, you can quickly resolve problems with VoIP hardware, software, and performance.

The integration of AppManager for Avaya CS1000 and Vivinet Diagnostics allows an Action script, Action_DiagnoseNortelIPT, to launch Vivinet Diagnostics when the Alarms script raises events for the following QoS alarms (SNMP traps): QOS0022, QOS0024, QOS0026, QOS0028, QOS0030, QOS0032, and QOS0034.

To prepare your CS1000 environment to interact properly with Vivinet Diagnostics, complete the tasks outlined in Section 2.5, “Checklists for Required Configuration Tasks,” on page 20. Then, perform the tasks in this topic.

2.15.1 Enabling Insecure Shell Access

For CS1000 versions 5.x and later, enable insecure Shell access. Vivinet Diagnostics does not support Secure Shell (SSH) access. Instead, Vivinet Diagnostics requires Telnet access.

To enable insecure Shell access for CS1000 versions 5.x and later on a Linux-based Signaling Server:

1. Log in to the Linux-based Signaling Server.
2. Issue the following command: `HARDEN TELNET ON`

To enable insecure Shell access for CS1000 versions 5.x and later on a Call Server:

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

2.15.2 Configuring Action_DiagnoseNortelIPT

The Action_DiagnoseNortelIPT Knowledge Script must be able to trigger Vivinet Diagnostics to run a diagnosis as often as problems occur. Therefore, disable or modify the “event collapsing” feature on the Alarms script. Event collapsing allows AppManager to suppress, or collapse, duplicate events. Vivinet Diagnostics cannot diagnose each problem if AppManager has collapsed all call quality events between the same targets into one event.

To disable or modify event collapsing:

1. Navigate to the Advanced tab of the Action_DiagnoseNortelIPT Properties dialog box.
2. To disable event collapsing, disable **Collapse duplicate events into a single event**.
3. To shorten the 20-minute collapsing interval, select a smaller number in the **Time interval for event collapsing** field.
4. Stop and then restart the Knowledge Script job to activate your changes.

For more information, see the *User Guide for Vivinet Diagnostics* and the AppManager Help for Action_DiagnoseNortelIPT.

2.16 Troubleshooting

Consult the topics in this section for solutions to problems and answers for frequently asked questions.

2.16.1 Discovery Does Not Create Resource Objects for Signaling Servers, VGMCs, MC32Ss, or MGCs

Problem: The Discovery_NortelCS Knowledge Script job created NetworkDevice and NortelCS1000 Call Server resource objects, but did not create CS1000 Signaling Server, VGMC, MC32S, or MGC objects.

Reason 1: TLAN IP addresses were used instead of ELAN IP addresses when specifying which devices to discover in Discovery_NortelCS.

Solution 1: Contact your CS1000 system administrator for the appropriate ELAN IP address. You cannot discover TLAN IP addresses.

Reason 2: The correct SNMP read/write community strings for the devices were not configured in AppManager Security Manager.

Solution 2: Contact your CS1000 system administrator for the correct SNMP read/write community strings. Then configure them in Security Manager. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.

2.16.2 Discovery Does Not Create Resource Objects for CS1000 or Network Device

Problem: The Discovery_NortelCS Knowledge Script job did not create NortelCS1000 or Network Device resource objects in the AppManager console. In addition, the Discovery job raised one of the following event messages:

```
NortelCSE1K.Discover returned -7
Failed to discover device.
device: 10.42.1.11
error:
Error was detected at Mon Sep 13 13:55:57 2004
Error was detected by the Console.
The return code was 1.
CHR0403: The request for Discover Device Vendor and Type from Device 10.42.1.11
failed.
CHR0392: AN SNMP request sent to 10.42.1.11 timed out.
```

or

```
NetworkDevice.Discover returned -7
Failed to discover device.
device: 10.42.1.11
error:
Error was detected at Mon Sep 13 13:53:25 2004
Error was detected by the Console.
The return code was 1.
CHR0403: The request for Discover Device Vendor and Type from device 10.42.1.11
failed.
CHR0386: AN SNMP request to 10.42.1.11 failed, returning Generic error (password
length too short.)
```

Reason: The SNMP community strings for the CS1000 devices were not specified or were specified incorrectly in AppManager Security Manager.

Solution: Contact your CS1000 system administrator for the correct SNMP community strings. Then configure them on the Custom tab of Security Manager. For more information, see Section 2.6, “Configuring SNMP Community Strings,” on page 24.

2.16.3 Entity MIB Does Not Contain Phones

Problem: For CS1000 versions 4.0 and later, the Discovery_NortelCS Knowledge Script job did not find IP phones in the Call Server Entity MIB.

Reason: The proper Overlay 117 commands were not issued.

Solution: Issue the proper Overlay 117 commands. For more information, see Section 4.6.5, “Configuring the Call Server to Count IP Phones,” on page 65.

2.16.4 GetOMReport Script Fails

Problem 1: The GetOMReport script failed with the following event message:

```
NortelCSE1K.GetOMReport returned -18
The AM agent’s built-in FTP server failed to start. Perhaps the IIS FTP server is
running.
```

Reason 1: The IIS FTP server is running and preventing the proxy agent computer’s FTP server from starting.

Solution 1: Open the Internet Information Services (IIS) Manager and stop the FTP service. Then rerun the GetOMReport script.

Problem 2: The GetOMReport script failed with the following event message:

```
NortelCSE1K.GetOMReport returned -18
CHR0412: FTP from Nortel CS server <IP address> to AM proxy agent <IP address>
failed with return code 4 (FTP error).
```

Reason 2: You installed Avaya software load `MGCCAD35` or later on the Media Gateway Controller. This software load prevents the retrieval of OM reports until after midnight on the day you install the software load.

Solution 2: Schedule the GetOMReport script to run after midnight.

2.16.5 GetOMReport Script Hangs in Running State

Problem: The GetOMReport script job remained in Running state and never completed its iteration or raised an event.

Reason: The proxy agent computer is attempting to access the CS1000 TLAN rather than the ELAN.

- ELAN (Embedded Virtual Private Local Area Network), which is the network CS1000 uses to communicate management information between servers and cards. ELAN performs the function of an Ethernet switch.
- TLAN (Telephony Local Area Network), which is the network CS1000 uses to communicate telephony signals and voice over IP (VoIP) between servers and cards.

Solution: Ensure you *cannot* reach the TLAN from the proxy agent computer. Ensure you installed and configured the IIS FTP service; and ensure you performed all required Security Manager configuration.

To troubleshoot the GetOMReport script:

1. From the proxy agent computer, ping the TLAN interface of the CS1000 device. If you *can* ping the interface, proceed with step 2. If you *cannot* ping the interface, skip to step 4.
2. Either change the network configuration or modify the route table on the CS1000 device to use the ELAN interface gateway to connect with the proxy agent computer. No route should exist between the ELAN and the TLAN. For assistance with changing your network configuration or modifying the route table, contact your Avaya support provider.
3. Ping the TLAN again to ensure you *cannot* access it from the proxy agent computer.
4. Ensure you performed the following tasks:
   - Install and configure the IIS FTP service on the proxy agent computer, which will prevent the FTP service from hanging while running GetOMReport. For more information, see "Configuration for Using IIS as the FTP Server" on page 62.
   - Configure the correct SNMP community strings for your CS1000 devices. For more information, see Section 2.6, "Configuring SNMP Community Strings," on page 24.
   - *If you use CS1000 version 3.0*, configure your PDT password in Security Manager. For more information, see Section 2.7, "Configuring the PDT Password for Version 3.0," on page 25.
   - *If you use CS1000 version 3.0*, configure your Level 1 login and password in Security Manager. For more information, see Section 2.8, "Configuring the SL1 Level 1 Login for Version 3.0," on page 26.
   - *If your proxy agent computer has more than one Network Interface Card (NIC)*, configure the correct address in Security Manager. For more information, see "Configuration for Using Two or More NICs" on page 61.
5. Restart the AppManager agent and rerun the GetOMReport script:
   - Stop and then delete all non-responsive GetOMReport jobs.
   - Restart the NetIQ AppManager Client Resource Monitor service (`netiqmc.exe`), using the `-oa` parameter.
   - Rerun the GetOMReport script.
6. If the GetOMReport script remains unresponsive in Running state, contact NetIQ Technical Support www.netiq.com/support.

2.16.6 Inventory Fails

Problem: An error message indicated the inventory process failed during discovery and that no IP phones could be counted.

Reason: You did not issue the Overlay 117 commands to set up the inventory process on the Call Server.

Solution: Run the proper commands. For more information, see Section 4.6.5, "Configuring the Call Server to Count IP Phones," on page 65.

NOTE: This topic applies only to CS1000 versions 4.0 and later.

2.16.7 Inventory Takes a Long Time

Problem: The inventory process of the Discovery_NortelCS Knowledge Script job took a long time to complete.

Reason: As part of the discovery process, AppManager takes an inventory of the phones in your CS1000 environment. The Call Server runs this task, which is low priority. If the Call Server is busy with higher priority items, it will not spend much time on inventory. Therefore, the inventory process could take a long time, perhaps up to two days depending on the number of phones.

Solution: Run Discovery_NortelCS at a less-busy time for your Call Server. By default, discovery runs weekly, on Sunday at 3 AM.

NOTE: This topic applies only to CS1000 version 3.0.

2.16.8 Signaling Server Scripts Do Not Generate Data

Problem: The SS_CallQuality, SS_H323Stats, SS_Registration, and SS_SIPStats Knowledge Scripts did not generate data streams or raise events.

Reason: By default, these scripts run at ten minutes past the hour. This default accommodates the schedule of the GetOMReport Knowledge Script, which runs at five minutes past the hour. In turn, the default for GetOMReport accommodates the schedule for the OM report, which is created at the top of each hour.

If you start a monitoring script job at 15 minutes past the hour, you will not see any action for another 55 minutes.

Solution 1: Wait. The scripts are operating as designed.

Solution 2: To see immediate results, run the GetOMReport Knowledge Script with a schedule of "Run Once." Then run the CallQuality, H323Stats, Registration, or SIPStats script with the same schedule. With this schedule, you receive immediate, one-time-only results.

2.16.9 BMZ_CallQuality Script Does Not Retrieve Data

Problem: The BMZ_CallQuality Knowledge Script did not retrieve call quality data from the Zone Traffic MIB.

Reason 1: You did not apply the prerequisite patch for the Signaling Server.

Solution 1: For Signaling Server version 4.50, apply Avaya patch `MPLR21714`. The patch requires configuration of the Call Server. For more information, see the patch Readme file. Obtain the patch and Readme from your Avaya support and maintenance provider.

Reason 2: A user or application is logged into the Call Server when the Signaling Server attempts to retrieve zone statistics from the Call Server. The Signaling Server uses a special login to issue Overlay commands that allow it to retrieve zone statistics. The Overlay commands cannot retrieve statistics from a Call Server that is in use at the time of retrieval.

Solution 2: None, except to understand why the zone statistics were not retrieved.

Reason 3: Access to the QoS MIB is not enabled.

Solution 3: Create the `snmpqosq` user account, which provides access to the QoS MIB. For more information, see Section 4.2.7, "Enabling Access to the Signaling Server QoS MIB for CS1000 version 5.x," on page 58.

2.16.10 SS_CallQuality and SS_Registration Scripts Do Not Monitor Specified Phone Models

Problem: The SS_CallQuality and SS_Registration Knowledge Scripts did not retrieve data for the phone models specified in the *Phone model selection* parameter.

Reason: The names of phone models changed with CS1000 versions 4.5, 5.0, and 6.0.

Solution: Before entering a regular expression in the *Phone model selection* parameter, verify the names of the phone models specific to the version of your Signaling Server.

3 Reporting with Analysis Center

NetIQ Analysis Center is designed to import raw data from multiple AppManager repositories, transform that data into useful information about the computing infrastructure that supports your business, and publish that information in the form of reports.

Beginning with version 2.6, Analysis Center ships with capacity planning, operational, and service level reports designed specifically for Avaya (heritage-Nortel) CS1000 VoIP data. With these reports, you can capture and distribute vital information, such as server availability, call activity trends and predictions for IP phone calls, real-time usage and performance, and call quality for the Signaling Server, VGMC, MC32S, and MGC.

You can find the reports within the **Reports > AppManager > Nortel CS** folder in the Analysis Center Navigation pane. These reports have been configured to filter for CS1000 data, so you can use them pretty much right out of the box.

3.1 Capacity Planning Report

Capacity planning reports should answer questions such as “How busy is this device” or “Is this device being used at all?”

The following table describes the capacity planning report available from Analysis Center for CS1000 data. For more information, see the Configuration Card details for the report.

Report Name	Description
Nortel CS Volume Trend and Prediction	Displays the trend of call volume for IP phones. This report uses the total number of calls each day over the specified range of existing data. Use the Metric context controls to select the types of calls to include in the trend report. Use the Group context controls to indicate whether you want to see trending data for all of your Signaling Servers or for an individual Signaling Server. Once you select the report in the Navigation pane, select the **Nortel Terminal Total Audio Setups** metric. We recommend that you set the **Parameters > PredictionDays** property to less than 180. The larger this value, the longer it takes to calculate the individual prediction values. If you set the property to a value greater than 730, the report will fail. You also can use this report to identify trends in trunk phone calls using the SIP and H.323 metrics.

3.2 Operational Reports

The operational side of your organization may be one of the most vital in terms of VoIP functionality. Operational reports provide the details behind the service-level management reports and help you isolate servers that are experiencing problems.

The following table describes the operational reports available from Analysis Center for Avaya CS1000 data. For more information, see the Configuration Card details for each report.

Report Name	Description
Nortel CS Call Volume	Displays at the total call volume made through Signaling Servers between IP phones for the time period you specify. This report uses the **Nortel Terminal Audio Setups** and **Nortel Terminal Total Voice Time** data stream generated by the SS_CallQuality Knowledge Script. Set the **Parameters > Time Units** property to select the units in which to show the total time duration. The report shows a table giving the total number of calls, total duration of all calls, and average duration per call.
Nortel CS Good-Acceptable-Poor Quality by Server	Examines the quality levels of individual CS1000 servers. Use the Metrics context to select the quality metric that you want to include in the report. The list of metrics contains quality metrics collected by the SS_CallQuality and VGMC_CallQuality Knowledge Scripts. Use the Group context to select the individual servers or groups that you want to include in the report. Check the **Show Instances** checkbox to see the individual CS1000 servers being managed by the proxy computer. Use the **Properties** tab to set thresholds for good and poor performance.
Nortel CS Performance Data	Examines CS1000 performance data by computer or computer group. Use the Group context to select the computer groups or individual computers that you want to include in the report; the computers or computer groups will be shown as rows in the report. Use the Metric context to select the metrics to include in the report; the metrics will be shown as columns in the report. Use the other context controls as data filters. For example, use the Time context to control the time range of the data. Use the Measures context to indicate whether you want to show the average, sum, or maximum for the measure. For metrics such as Jitter or Latency, average or maximum may be appropriate. For metrics that show volume, such as calls attempted or calls completed, selecting Sum may be appropriate.

Report Name	Description
Nortel CS Performance Data by Date and Time	Examines CS1000 performance data by date and time. The date and time are shown as rows in the report. By default, the report shows the data by day. You can show data by hour or minute by using the Time context and changing the **Interval** to hour or minute. Use the Group context to select the computer groups or individual computers that you want to include in the report; the computers or computer groups are shown as columns in the report. If you are including several computers or computer groups, you may want to change the **Chart Type** on the **Properties** tab from **Column** to **Line** to more easily represent many entities in the graph. Use the other context controls as data filters, including using the Metric context to select which metric should be shown in the report. For example, to create a report showing yesterday's average listening for each hour, use the Metric context to select **Nortel Terminal Average Listening MOS** and use the Time context to indicate **Yesterday** as the date range and **Hour** as the interval.
Nortel CS Performance Data by Hour	Examines CS1000 performance data by the hour of day. The hours of the day are shown as rows in the report. Use the Group context to select the computer groups or individual computers that you want to include in the report; the computers or computer groups are shown as columns in the report. If you are including several computers or computer groups, you may want to change the **Chart Type** on the **Properties** tab from **Column** to **Line** to more easily represent many entities in the graph. Use the other context controls as data filters, including using the Metric context to select which metric should be shown in the report. For example, to create a Busy Hour report for IP phone call volume, use the Metric context to select **Nortel Terminal Total Audio Setups** and use the Measures context to select **Sum**.
Nortel CS Performance Data Metrics by Date and Time	Compares multiple metrics by date and time — useful information to have when you are troubleshooting. For example, you can compare the **Nortel Terminal Average Listening MOS** data to that of **Nortel Terminal Minimum Listening MOS**. Or, you can compare the number of **Nortel Terminal Total Registration Attempts** to the number of **Nortel Terminal Total Registration Failures**. Use the Metric context to select one or more metrics to include in the report. Use the Time context to set the time range and interval (for example, **Last 28 Days** by **Day**). The interval you select determines the time aggregation. For example, if you select **Day**, there is one value for each date; if you select **Hour**, there are 24 values for each date. Use the other context controls as data filters. For example, use the Group context to select which computers or groups to include in the report.

3.3 Service Level Reports

The reporting capability of Analysis Center enables you to demonstrate the value of IT and how well IT is aligned with business objectives. To these ends, run service level management reports to reflect server availability and call quality.

The following table describes the service level reports available from Analysis Center for Nortel CS1000 data. For more information, see the Configuration Card details for each report.

Report Name	Description
Nortel CS Jitter Good-Acceptable-Poor	Creates a pie chart of good, acceptable, and poor values of jitter. This report uses the **Nortel Terminal Average Jitter** data stream generated by the SS_CallQuality Knowledge Script. Good jitter values are those less than 40 ms.; poor jitter values are those greater than 60 ms.
Nortel CS Latency Good-Acceptable-Poor	Creates a pie chart of good, acceptable, and poor values of latency. This report uses the **Nortel Terminal Average Latency** data stream generated by the SS_CallQuality Knowledge Script. Good latency values are those less than 150 ms.; poor latency values are those greater than 400 ms.
Nortel CS Listening MOS Good-Acceptable-Poor	Creates a pie chart of good, acceptable, and poor values of listening MOS. By default, this report uses the **Nortel Terminal Average Listening MOS** data stream generated by the SS_CallQuality Knowledge Script. Good listening MOS is greater than 4.03; poor listening MOS is less than 3.6. To change this report to show listening R-factor instead, use the Metric context to select **Nortel Terminal Average Listening R-factor** and change the **Good** and **Poor** standards defined in the Parameters section on the Properties tab. If you are using listening R-factor, you should set the good standard to scores greater than 80 and the poor standard to scores less than 70.
Nortel CS Lost Packets Good-Acceptable-Poor	Creates a pie chart of good, acceptable, and poor percentages of lost packets. This report uses the **Nortel Terminal Average Lost Packets** data stream generated by the SS_CallQuality Knowledge Script. The good standard is packet loss less than 0.50%; the poor standard is packet loss greater than 1.00%.
Nortel CS Server Availability	Creates an overview of the availability of all CS servers: Call Servers, Signaling Servers, Media Gateways, and VGMCs. This report uses the availability data collected by the HealthCheck Knowledge Script. You can use the **Nortel Call Server Availability** data stream to reflect availability data for Media Gateways. By default, this report shows the availability of all servers. **Tip** You can use this report to create an operational report that shows the availability of each server. This type of operational report is extremely valuable for isolating which servers are experiencing problems. Use the Group context to show the availability of individual servers or groups. Check the **Show Instances** box on the Group context to see the individual CS1000 server being managed from the proxy computers. The servers or groups are shown as rows in the report. Columns in the report display the available and unavailable percentages so that information can easily be graphed as a stacked column.
Nortel CS Service Levels Overview	Creates a dashboard report that provides an overview of underlying reports showing key service level metrics: server availability and good-acceptable-poor levels of listening MOS, jitter, latency, and lost packets. Click the title of any member report to see the full view of that report. When deploying this report, be sure to deploy each member report first.

4 NortelCS Knowledge Scripts

AppManager provides Knowledge Scripts that enable you to monitor CS1000 devices. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, select a Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Alarms	Monitors the proxy agent computer for CS1000 alarms.
BMZ_CallQuality	Monitors call quality statistics for Bandwidth Management Zones (BMZs) for CS1000 versions 4.50 and later.
CallCapacity	Retrieves the call capacity utilization calculation from a Call Server for CS1000 versions 4.50 and 5.0.
GetOMReport	Retrieves the most recent Operational Management (OM) report and the report from the previous day, if one exists.
HealthCheck	Monitors the state of the Call Server, Media Gateway Controller, Signaling Server, MC32S, Network Routing Server, VGMC, and SIP Gateway.
PhoneInventory	Creates an inventory of IP phones based on data from the Call Server Entity MIB.
SS_CallQuality	Monitors Signaling Server statistics: jitter, latency, voice time, audio setups, and lost packets. This script also monitors R-factor for CS1000 versions 4.0 and later.
SS_H323Stats	Monitors Signaling Server H.323 trunk statistics: incoming voice and fax calls, and outgoing voice and fax calls.
SS_Registration	Monitors registration failures and attempts on the Signaling Server.
SS_SIPStats	Monitors Signaling Server SIP trunk statistics: incoming voice and fax calls, and outgoing voice and fax calls. **NOTE:** This script supports CS1000 versions 4.0 and later.
VGMC_CallQuality	Monitors channel statistics of the VGMC, Media Gateway Controller, and MC32S: audio setups, voice time, average and maximum jitter, maximum average latency, and lost packets.

4.1 Alarms

Use this Knowledge Script to monitor CS1000 alarms. Call Servers, Signaling Servers, Media Gateways, MGCs, ECMs, NRSs, VGMCs and SIPL send alarms to the proxy agent computer using SNMP traps.

When setting parameters for this script, you will be asked to provide a list of alarm identifiers (system messages) to include or exclude from monitoring. System messages are discussed in the CS1000 *Software Input/Output System Message* publication (Avaya publication number 553-3001-411). Their format consists of a multi-letter code followed by a multi-digit alarm number, such as AUD000 or SRPT194.

Running this Knowledge Script job consumes approximately 20 MB of memory, per instance, on the proxy agent computer.

This script can launch an Action Knowledge Script that triggers NetIQ Vivinet Diagnostics to diagnose the problem when QoS alarms are raised. For more information, see the Help for the Action_DiagnoseNortelIPT Knowledge Script.

4.1.1 Prerequisites

- Install the Windows SNMP service. If you installed the service *before* you installed the AppManager for CS1000 module, then you do not need to do anything else. If you installed the service *after* you installed the module, then stop and restart the proxy agent computer before using this script.
- Configure CS1000 devices to send SNMP traps to the proxy agent computer. For more information, see Section 4.1.6, “Identifying the SNMP Trap Receiver,” on page 51.
- The AppManager for Avaya CS1000 module is incompatible with the Avaya Telephony Manager application, which competes with the module for UDP port 162. AppManager will not receive SNMP traps if Telephony Manager is installed.
- The AppManager for Avaya CS1000 module is incompatible with NetIQ SNMP Trap Receiver (Trap Receiver), which competes with the module for UDP port 162. AppManager will not receive SNMP traps if Trap Receiver is installed.

4.1.2 Resource Objects

NortelCS Call Server

NortelCS Signaling Server

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

NortelCS Network Routing Server

NortelCS Enterprise Common Manager

NortelCS SIP Line

NOTE: In most circumstances, the Alarms Knowledge Script raises events for alarms (traps) received from the CS1000 component on which you run the job. The component ID property of each trap identifies the source of the trap. For example, a component ID of “CS” identifies the Call Server. The component ID also determines which resource object an event is raised against.

For environments in which a co-resident server hosts multiple applications, the component ID may not correctly identify the source of a trap. When the component ID incorrectly identifies the source of a trap, events are raised against the incorrect resource object.

For example, if a co-resident server hosts the Call Server, the Signaling Server, and the Network Routing Server (NRS), the component ID may indicate a trap was received from the NRS. In addition, the event will be raised against the NRS object. However, experience may tell you that the trap actually came from the Signaling Server.

To ensure events are raised for all traps received from all components on a co-resident server, run the Alarms Knowledge Script on the co-resident server parent object so that all component child objects are monitored. If you run the Alarms job on only the Signaling Server, for example, AppManager will not raise an event for the Signaling Server trap that is incorrectly identified as an NRS trap.

4.1.3 Default Schedule

By default, this script runs on an asynchronous schedule.

4.1.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Notes for the “critical to monitor” and QoS alarm categories: ◆ If you “Include” selected alarm identifiers in a category, AppManager raises events for those alarm identifiers plus the identifiers that are, by default, included in the category. ◆ If you “Include only” selected alarm identifiers in a category, AppManager raises events *only* for those identifiers. *AppManager will not raise events for the other identifiers included in the category*. ◆ If you “Exclude” selected alarm identifiers from a category, AppManager raises events for all alarm identifiers included in the category *except* those you specifically excluded. ◆ If you accept the default settings in the *Alarm identifiers* parameters, “Exclude” and blank, AppManager raises events for all identifiers in the category, because you excluded nothing from the category.	
Monitor “critical to monitor” alarms?	Select **Yes** to monitor alarms in the “critical to monitor” category. The default is Yes.

Parameter	How to Set It
Include or exclude alarms?	Select whether you want to **Include**, **Include only**, or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include** to *add* the listed identifiers to the "critical to monitor" category. ◆ Select **Include only** to include *only* the listed identifiers in the "critical to monitor" category. ◆ Select **Exclude** to exclude the listed identifiers from the "critical to monitor" category. This is the default option. By default, the "critical to monitor" category includes all alarms designated as "critical to monitor" in the CS1000 *Software Input/Output System Messages* publication (Avaya publication number 553-3001-411).
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the "critical to monitor" category. The default is an empty list.
Monitor QoS alarms?	Select **Yes** to monitor the proxy agent computer for alarms in the QoS category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include**, **Include only**, or **Exclude** the alarm identifiers you specify in the *Alarm identifiers* parameter. ◆ Select **Include** to *add* the listed identifiers to the QoS category. ◆ Select **Include only** to include *only* the listed identifiers in the QoS category. ◆ Select **Exclude** to exclude the listed identifiers from the QoS category. This is the default option. By default, the QoS category includes the following alarms for CS1000 versions 4.0 and later: ITG1028, ITG2028, ITG3028, ITG4028, ITG4043, ITG4044, QOS0012, QOS0013, QOS0014, QOS0015, QOS0017, QOS0018, QOS0019, QOS0020, QOS0022, QOS0024, QOS0026, QOS0028, QOS0030, QOS0032, QOS0034, QOS0036, QOS0038, QOS0039, QOS0040, QOS0041, QOS0042, QOS0043
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the "QoS" category. The default is an empty list.
Phone filter	
Include or exclude phones?	You can use IP addresses to further filter the results of the QoS alarm monitoring. Select whether you want to **Include only** or **Exclude** the IP addresses you specify in *Phone IP addresses* or *Phone IP address ranges*. AppManager will monitor — or exclude — QoS alarms related to the calling and called phones that belong to the IP addresses. ◆ Select **Include only** to monitor QoS alarms *only* the listed phone IP addresses. ◆ Select **Exclude** to exclude listed phone IP addresses from QoS alarm monitoring. This is the default option
Phone IP addresses	Provide a comma-separated list of the IP addresses of the phones you want to monitor for QoS alarms. For example: `10.14.2.21,10.14.3.100,10.14.1.50`

Parameter	How to Set It
Phone IP address ranges	Type a comma-separated list of IP address ranges for the phones you want to monitor for QoS alarms. For example: `10.14.2.21-10.14.3.100,10.14.1.10-10.14.1.50`
Launch Diagnostics when the following alarm is received ...	
Warning packet loss QOS0022?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0022 alarm is raised. The default is unselected.
Warning latency QOS0024?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0024 alarm is raised. The default is unselected.
Warning jitter QOS0026?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0026 alarm is raised. The default is unselected.
Warning R-factor QOS0028?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0028 alarm is raised. The default is Yes.
Unacceptable packet loss QOS0030?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0030 alarm is raised. The default is unselected.
Unacceptable latency QOS0032?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0032 alarm is raised. The default is unselected.
Unacceptable jitter QOS0034?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0034 alarm is raised. The default is unselected.
Note for the following alarm categories: AppManager raises an event **only** for those alarm identifiers you specifically include, or it raises an event for all alarm identifiers **except** those you specifically exclude. If you accept the default of an empty list in the *Alarm identifiers* parameters, AppManager raises events for **all** alarm identifiers.	
Monitor critical alarms?	Select **Yes** to monitor alarms in the critical category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include only** to include *only* the listed identifiers in the critical category. ◆ Select **Exclude** to exclude the listed identifiers from the critical category. This is the default value. By default, the critical category includes all alarms with critical severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the critical category. The default is an empty list.
Monitor major alarms?	Select **Yes** to monitor alarms in the major category. The default is unselected.

Parameter	How to Set It
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include only** to include *only* the listed identifiers in the major category. ◆ Select **Exclude** to exclude the listed identifiers from the major category. This is the default option. By default, the major category includes all alarms with major severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the major category. The default is an empty list.
Monitor minor alarms?	Select **Yes** to monitor alarms in the minor category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include only** to include *only* the listed identifiers in the minor category. ◆ Select **Exclude** to exclude the listed identifiers from the minor category. This is the default option. By default, the minor category includes all alarms with minor severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the minor category. The default is an empty list.
Monitor warning alarms?	Select **Yes** to monitor alarms in the warning category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include only** to include *only* the listed identifiers in the warning category. ◆ Select **Exclude** to exclude the listed identifiers from the warning category. This is the default option. By default, the warning category includes all alarms with warning severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the warning category. The default is an empty list.
Monitor info alarms?	Select **Yes** to monitor alarms in the informational category. The default is unselected.

Parameter	How to Set It
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include only** to include *only* the listed identifiers in the informational category. ◆ Select **Exclude** to exclude the listed identifiers from the informational category. This is the default option. By default, the informational category includes all alarms with informational severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the informational category. The default is an empty list.
Monitor cleared alarms?	Select **Yes** to monitor alarms in the cleared category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include only** to include *only* the listed identifiers in the cleared category. ◆ Select **Exclude** to exclude the listed identifiers from the cleared category. This is the default option. By default, the cleared category includes all alarms with cleared severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the cleared category. The default is an empty list.
Monitor indeterminate alarms?	Select **Yes** to monitor alarms in the indeterminate category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. ◆ Select **Include only** to include *only* the listed identifiers in the indeterminate category. ◆ Select **Exclude** to exclude the listed identifiers from the indeterminate category. By default, the indeterminate category includes all alarms with indeterminate severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the indeterminate category. The default is an empty list.
Event Severities	
Severity - Critical alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a critical alarm is detected. The default is 10.
Severity - Major alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a major alarm is detected. The default is 15.
Severity - Minor alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a minor alarm is detected. The default is 20.

Parameter	How to Set It
Severity - Warning alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a warning alarm is detected. The default is 25.
Severity - Info alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which an informational alarm is detected. The default is 30.
Severity - Cleared alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a cleared alarm is detected. The default is 30.
Severity - Indeterminate alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which an indeterminate alarm is detected. The default is 30.

4.1.5 Understanding an Alarms Event Message

The message on the Message tab of an event raised by the Alarms script provides not only a brief description of the event, but also recommends any corrective action you can take. AppManager retrieves the recommended actions from a database provided by Avaya.

In the following example, the Alarms script raised an event for the ITS2008 alarm on a Signaling Server:

```
NTP index: ITS2008
Nortel CS device:SIG_SERV
Alarm: Terminal connection status: 10.40.101.112 lost
```

The Message tab for this event provided the following “Help” and “Recommended Action” for the alarm:

```
Help for ITS2008:
Terminal connection status: <terminalIP><ok/lost>.

Recommended action for ITS2008:
1. Alarm may indicate random occurrence that is not service impacting; note
occurrence time and date for further follow-up. If any service-impacting problems
occur at the same time, further analysis is required immediately.
2. If alarm persists, log into device and capture maintenance report log (if possible) and
send
the text to Nortel support staff via email. Follow any steps described above for
the specific alarm.
```

Occasionally, more than one Help is available for an alarm. In this case, all Helps are shown first:

```
NTP index: XMI0002
Extra diagnostic information: 18 MGATE
Help for XMI0002 XFIL 1:
Main fiber interface (MFI) local is operational.

Help for XMI0002 XFIR 2:
Expansion fiber interface (EFI) remote is operational in first expansion cabinet.

Help for XMI0002 XFIR 3:
Expansion fiber interface (EFI) remote is operational in second expansion cabinet.

Help for XMI0002 I s c:
Card polling re-established.
```

Any Recommended Actions will follow the Helps. It is possible, though, for no Recommended Actions to be available.

The Event tab in an Alarms event message provides a one-line *Message* that briefly describes the problem detailed on the Message tab. For CS1000 version 5.x and 6.0 alarms, the message can look something like this example:

```
Critical alarm IOD0040: Raleigh CS1K:RTP:CS [10.42.1.11]
```

The format of this message is defined as follows:

```
<severity>alarm<index>: <navigation system name>:<navigation site
name>:<component> [<component IP address>]
```

The navigation system name and navigation site name are taken from the SNMP Configuration information you set in Element Manager.

4.1.6 Identifying the SNMP Trap Receiver

Configure CS1000 to send SNMP traps to the CS1000 proxy agent computer. The configuration procedures are different for CS1000 versions 4.0 and later.

- "Configuring the Trap Receiver in Version 6.0 and Later" on page 51
- "Configuring the Trap Receiver in Version 5.x" on page 52
- "Configuring the Trap Receiver in Version 4.50" on page 52
- "Configuring the Trap Receiver in Version 4.0" on page 52

Configuring the Trap Receiver in Version 6.0 and Later

Use Unified Communications Manager or Element Manager to configure the trap receiver. To use Element Manager to configure the trap receiver, see "Configuring the Trap Receiver in Version 5.x" on page 52.

To configure the trap receiver using Unified Communications Manager:

1. Navigate to **Network**, click **CS1000 Services**, and then click **SNMP Profiles**.
2. Click **SNMP Profile**.
3. Select the SNMP profile you want to use.

   Or, to create a new profile, click **Add** and specify a new name for an **Alarm** type of profile.
4. In the **Trap Destination IP address** field, provide the IP address of the proxy agent computer to which the Avaya devices should sent SNMP traps.
5. Click **Save**.
6. Click **SNMP Distribution**, and then select all Avaya devices that should send SNMP traps to the proxy agent computer.
7. Click **Assign**.
8. In the **Alarm Profile** field, select the SNMP profile name from Step 3.

Configuring the Trap Receiver in Version 5.x

Use Element Manager to configure the trap receiver.

To configure the trap receiver:

1. Navigate to **System**, click **Alarms**, and then click **SNMP**.
2. In the **Trap Destination IP address** field, provide the IP address of the proxy agent computer to which you want to send Call Server traps.

Configuring the Trap Receiver in Version 4.50

Use Element Manager to configure the trap receiver.

To configure the trap receiver:

1. Navigate to **System** and click **SNMP**.
   - In the **SNMP trap destination address** field, type the IP address of the proxy agent computer to which you want to send Call Server traps.
2. Navigate to **IP Telephony > Nodes > Configuration**.
   - Select the node ID for which you want to enable SNMP traps.
   - Click **Edit** and then select **SNMP** on the Edit page.
   - Click **Add** to create a new **IP address** field, and then enter the IP address of the proxy agent computer to which you want to send SNMP traps. Repeat for each IP address you want to add.
   - Select **Enable SNMP traps**.
   - Click **Save and Transfer**.
3. Repeat the items in Step 2 for each additional node ID you want to configure.

Configuring the Trap Receiver in Version 4.0

Use Element Manager to configure the trap receiver.

To configure the trap receiver:

1. Navigate to **Configuration**, click **IP Telephony**, and then click **SNMP Configuration**.
   - In the **SNMP trap destination address** field, type the IP address of the proxy agent computer to which you want to send Call Server traps.
2. Navigate to **Configuration**, click **IP Telephony**, and then click **Node Summary**.
   - Select the node ID for which you want to enable SNMP traps.
   - Click **Edit** and then click **SNMP**.
   - Click **Add** to create new **IP address** and **Subnet mask** fields, and then type the IP address and subnet mask of the proxy agent computer to which you want to send SNMP traps. Repeat for each IP address and subnet mask you want to add.
   - Select **Enable SNMP traps**.
   - Click **Save and Transfer**.
3. Repeat the items in Step 2 for each additional node ID you want to configure.

4.2 BMZ_CallQuality

Run this Knowledge Script to monitor blocked calls, peak bandwidth, and call quality metrics for Bandwidth Management Zones (BMZs) for intrazone and interzone traffic. AppManager retrieves call quality statistics from the Zone Traffic MIB on the Signaling Server. For CS1000 version 6.0 and later, AppManager retrieves statistics from the Zone Traffic MIB on the Call Server.

You can use BMZs to prioritize or restrict the amount of bandwidth that can be consumed by voice traffic.

This script raises an event if zone statistics are unavailable, if the percentage of calls blocked and the percentage of peak bandwidth exceed the thresholds you set, and if call quality metrics exceed the thresholds you set in Element Manager more than *n* times in one hour. In addition, this script generates data streams for the call quality metrics you choose to monitor.

AppManager supports BMZ monitoring for CS1000 versions 4.50 and later.

4.2.1 Prerequisites

- For Signaling Server version 4.50, install Avaya patch `MPLR21714`. The patch requires configuration of the Call Server. Obtain the patch and its Readme from your Avaya support and maintenance provider.
- Configure BMZ QoS threshold levels in CS1000 Element Manager. For more information, see Section 4.2.6, “Setting Bandwidth Management Zone Thresholds,” on page 57.
- For CS1000 versions 4.50 and 5.x, create user account **snmpqosq**. For more information, see Section 4.2.7, “Enabling Access to the Signaling Server QoS MIB for CS1000 version 5.x,” on page 58.
- For CS1000 versions 4.50 and 5.x, ensure no user or application is logged into the Call Server when the Signaling Server attempts to retrieve zone statistics from the Call Server. The Signaling Server uses a special login to issue Overlay commands that allow it to retrieve zone statistics. The Signaling Server cannot retrieve statistics from a Call Server that is in use at the time of retrieval.

4.2.2 Understanding BMZ Call Data

The BMZ_CallQuality script monitors QoS and other IP statistics.

The Terminal Proxy Server in the Signaling Server extracts QoS statistics from the IP phones in an active call by periodically polling the phones during the length of the call. A Quality Detail Record (QDR) is created at the end of a call. A QDR is created for each segment of a call that is modified, perhaps by being transferred, conferenced, put on hold, or muted.

The QDR summarizes the overall **call quality** as good, warning, or unacceptable. Once created, the QDR is forwarded to the Call Server to be aggregated into interzone and intrazone statistics.

In addition to a summary of overall call quality, the QDR also contains QoS statistics that are collected for the duration of the call with respect to the incoming media stream: **latency**, **jitter**, **packet loss, and Listening R-factor**.

Peak bandwidth is the highest bandwidth reported in a call. Peak bandwidth and **average bandwidth** are expressed as percentages of the bandwidths configured for the zone.

The QDR contains QoS statistics *only* for Phase 2 phones.

The QDR categorizes each QoS statistic as good, warning, or unacceptable. The thresholds for these categories are user-configurable. The BMZ_CallQuality script raises events if a QoS statistic exceeds or falls below a threshold you set.

4.2.3 Resource Objects

Bandwidth Management Zone objects

For CS1000 versions 4.50 and 5.x, BMZ objects are children of the Signaling Server object. Run this script on only one Signaling Server per Call Server. All zones for your CS1000 deployment are displayed under every Signaling Server object. Limit your monitoring to one Signaling Server per Call Server to prevent this script from gathering duplicate data and generating duplicate data streams.

For CS1000 version 6.0 and later, BMZ objects are children of the Call Server.

You can run this script on a top-level object, and then use the Objects tab to select the specific BMZ objects you want to monitor.

4.2.4 Default Schedule

By default, this script runs at ten minutes past the hour. Do not change this schedule. The Zone Traffic MIB is updated on the hour. By retrieving call quality metrics at ten minutes past the hour, you receive most recent data. Because the MIB is updated only once each hour, you do not need to run this script more than once an hour.

4.2.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if zone statistics are inaccessible?	Select **Yes** to raise an event if BMZ statistics are inaccessible. The default is Yes. BMZ statistics are inaccessible if the Zone Traffic MIB from which they are retrieved does not respond to SNMP queries before the end of the interval specified in the *Timeout* parameter.
Timeout	Specify the length of time AppManager should attempt to access the Zone Traffic MIB before raising an event indicating zone statistics are inaccessible. The default is 300 seconds, which is equal to 300 attempts. **NOTE:** For CS1000 versions 4.50 and 5.x, AppManager cannot access the MIB if a user or application is logged into the Call Server, and will retry the attempt once each second during the timeout interval.
Event severity when zone statistics are inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which BMZ statistics cannot be retrieved. The default is 15.
Select traffic type	Select the type of call traffic you want to monitor: ◆ **Interzone**: calls made between zones ◆ **Intrazone**: calls made within a zone ◆ **Interzone and intrazone**: calls made between and within zones. This is the default selection.
Interzone	

Parameter	How to Set It
Event Notification	
Raise event if % of calls blocked exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked interzone calls exceeds the threshold you set. The default is Yes. AppManager calculates the percentage of calls blocked as: $\frac{callsBlocked}{callsMade+callsBlocked}$
Event severity when % of calls blocked exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of blocked interzone calls exceeds the threshold you set. The default is 15.
Raise event if peak bandwidth exceeds threshold?	Select **Yes** to raise an event if the percentage of interzone peak bandwidth exceeds the threshold you set. The default is Yes.
Event severity when peak bandwidth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of interzone peak bandwidth exceeds the threshold you set. The default is 15.
Raise event if call quality exceeds threshold?	Select **Yes** to raise an event if interzone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is Yes.
Event severity when call quality exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which interzone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is 15.
Monitoring	
Threshold - Maximum % of calls blocked	Specify the highest percentage of calls that can be blocked in one hour in interzone traffic before an event is raised. The default is 15%.
Threshold - Maximum peak bandwidth	Specify the highest percentage of peak bandwidth utilization that can occur in one hour in interzone traffic before an event is raised. The default is 90%.
Call Quality	
Threshold - Maximum occurrences of listen R-factor warnings	Specify the maximum number of times in one hour the listen R-factor value can fall below the warning threshold in interzone traffic before an event is raised. The default is 0. You set the R-factor threshold in Element Manager.
Threshold - Maximum occurrences of unacceptable lost packets	Specify the maximum number of times in one hour the unacceptable lost packets threshold can be exceeded in interzone traffic before an event is raised. The default is 0. You set the lost packets threshold in Element Manager.
Threshold - Maximum occurrences of unacceptable jitter	Specify the maximum number of times in one hour the unacceptable jitter threshold can be exceeded in interzone traffic before an event is raised. The default is 0. You set the jitter threshold in Element Manager. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.

Parameter	How to Set It
Threshold - Maximum occurrences of unacceptable latency	Specify the maximum number of times in one hour the unacceptable latency threshold can be exceeded in interzone traffic before an event is raised. The default is 0. You set the latency threshold in Element Manager. Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.
Intrazone	
Event Notification	
Raise event if % of calls blocked exceeds threshold?	Select **Yes** to raise an event if the percentage of intrazone calls blocked exceeds the threshold you set. The default is Yes. AppManager calculates the percentage of calls blocked as: $\frac{callsBlocked}{callsMade+callsBlocked}$
Event severity when % of calls blocked exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of intrazone calls blocked exceeds the threshold you set. The default is 15.
Raise event if peak bandwidth exceeds threshold?	Select **Yes** to raise an event if the percentage of intrazone peak bandwidth exceeds the threshold you set. The default is Yes.
Event severity when peak bandwidth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of intrazone peak bandwidth exceeds the threshold you set. The default is 15.
Raise event if call quality exceeds threshold?	Select **Yes** to raise an event if intrazone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is Yes.
Event severity when call quality exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which intrazone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is 15.
Monitoring	
Threshold - Maximum % of calls blocked	Specify the highest percentage of calls that can be blocked in one hour in intrazone traffic before an event is raised. The default is 15%.
Threshold - Maximum peak bandwidth	Specify the highest percentage of peak bandwidth utilization that can occur in one hour in intrazone traffic before an event is raised. The default is 90%.
Call Quality	
Threshold - Maximum occurrences of listen R-factor warnings	Specify the maximum number of times in one hour the listen R-factor value can fall below the warning threshold in intrazone traffic before an event is raised. The default is 0. You set the R-factor threshold in Element Manager.

Parameter	How to Set It
Threshold - Maximum occurrences of unacceptable lost packets	Specify the maximum number of times in one hour the unacceptable lost packets threshold can be exceeded in intrazone traffic before an event is raised. The default is 0. You set the lost packets threshold in Element Manager.
Threshold - Maximum occurrences of unacceptable jitter	Specify the maximum number of times in one hour the unacceptable jitter threshold can be exceeded in intrazone traffic before an event is raised. The default is 0. You set the jitter threshold in Element Manager. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.
Threshold - Maximum occurrences of unacceptable latency	Specify the maximum number of times in one hour the unacceptable latency threshold can be exceeded in intrazone traffic before an event is raised. The default is 0. You set the latency threshold in Element Manager. Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.
Collect data?	Select **Yes** to collect data for reports and graphs. The default is unselected. This script generates the following data streams, depending on the type of traffic you choose to monitor: ◆ Total number of sampling intervals ◆ Total intrazone/interzone calls ◆ Total intrazone/interzone calls blocked ◆ Average bandwidth percentage of intrazone/interzone traffic ◆ Peak bandwidth percentage of intrazone/interzone traffic ◆ Number of instances of unacceptable latency in intrazone/interzone traffic ◆ Number of instances of unacceptable packet loss in intrazone/interzone traffic ◆ Number of instances of unacceptable jitter in intrazone/interzone traffic ◆ Number of instances of listen R-factor warnings in intrazone/interzone traffic

4.2.6 Setting Bandwidth Management Zone Thresholds

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

To configure BMZ QoS thresholds:

1 Navigate to **Configuration**, click **IP Telephony**, and then click **Quality Of Service Thresholds**.

or

In version 5.x, navigate to **System**, click **IP Network**, and then click **QoS Thresholds**.

2. Set the **Warning** and **Unacceptable** thresholds appropriate for your 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**.
4. Use Element Manager or Overlay 43 to perform a Call Server data dump.

4.2.7 Enabling Access to the Signaling Server QoS MIB for CS1000 version 5.x

Enable SNMP access to the QoS MIB (`QoS-MIB.mib`) on the Signaling Server. A dedicated Limited Access Password (LAPW) user account named `snmpqosq` provides this access. Create the user account in Overlay 117.

The QoS MIB is also known as the zone traffic report MIB.

For more information about creating the user account, see the “MIBs” chapter of the document titled *Communication Server 1000 Fault Management — SNMP* (document

NN43001-719, version 01.03).

4.3 CallCapacity

Use this Knowledge Script to retrieve the calculated call capacity utilization (CCU) value from the Host Resource MIB on a Call Server. This script raises an event if CCU exceeds the threshold you set. In addition, this script generates a data stream for CCU.

Rated call capacity (RCC) is a function of idle time and the number of call attempts in an hour for a Call Server. It represents the maximum level at which a Call Server’s CPU can operate and still maintain a high grade of service. RCC assumes the highest call traffic peak during a busy hour is 30% higher than the average traffic level. CCU is an indicator of the call traffic load on the Call Server and is calculated as follows:

$$CCU = 100[\frac{CallAttempts}{RCC}]$$

The CallCapacity script retrieves the result of this calculation from the Host Resource MIB.

4.3.1 Prerequisites

- CS1000 Call Server, version 4.50 or 5.0. The CallCapacity script **does not support** other versions of the Call Server. Avaya removed the call capacity metric beginning with version 5.5 of the Call Server.
- AppManager for Network Device, build 6.2.24.0, at minimum

4.3.2 Resource Object

NortelCS Call Server

4.3.3 Default Schedule

By default, this script runs every five minutes.

4.3.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if call capacity utilization exceeds threshold?	Select **Yes** to raise an event if call capacity utilization exceeds the threshold you set. The default is Yes.
Event severity when call capacity utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which call capacity utilization exceeds the threshold. The default is 10.
Monitoring	
Threshold - Maximum call capacity utilization	Specify the highest percentage of call capacity utilization that must be reached before an event is raised. The default is 80%.
Collect data?	Select **Yes** to collect data for charts, reports, and graphs. When enabled, data collection returns the percentage of call capacity utilization for the Call Server. The default is unselected. **NOTE:** The CCU value is not available from the Call Server until 24 hours after a system restart. During that 24-hour window, only negative values are returned until the correct value is available. Therefore, the data stream for the CallCapacity script will be “0” until the correct CCU value has been calculated.

4.4 GetOMReport

Use this Knowledge Script to retrieve the latest Operational Measurement (OM) report from the Signaling Server, the VGMC, the MGC, and the MC32S. This script also retrieves the previous OM Report, if one is available.

Run GetOMReport on the Signaling Server resource object before running the following scripts:

- SS_CallQuality
- SS_H323Stats
- SS_Registration
- SS_SIPStats

Run GetOMReport on the VGMC, MGC, and MC32S resource objects before running the VGMC_CallQuality Knowledge Script.

4.4.1 Prerequisites

- The GetOMReport Knowledge Script automatically uses FTP to retrieve the OM Report from the Signaling Server, the VGMC, the MGC, and MC32S. Configure special FTP requirements in AppManager Security Manager. For more information, see Section 4.4.5, “Configuring FTP Server Parameters,” on page 61.
- The script hangs in Running state unless you configured all required SNMP community strings, PDT passwords, and SL1 Level 1 logins and passwords, and ensured you cannot ping the TLAN interface of the CS1000 device.

4.4.2 Resource Objects

NortelCS Signaling Server

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

4.4.3 Default Schedule

By default, this script runs once every hour, at five minutes past the hour. Do not change the default. Devices collect data for the OM Report at the top of each hour. You receive the most recent data if you retrieve the OM Report at five minutes past the hour.

By default, the call quality-related NortelCS Knowledge Scripts run once every hour, at ten minutes past the hour. Under most circumstances, you do not need to change the default schedule. Devices collect data for the Operational Measurement (OM) report at the top of each hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour. And you have to run GetOMReport before you can run the CallQuality scripts.

You probably run multiple instances of each script in order to collect the data you need. Running several virtually identical jobs at the same time could put a heavy strain on CPU usage.

If you want to run multiple instances of any NortelCS script, you should offset the schedules just a bit, one or two minutes, so you are not running all of the jobs at the same time.

Keep in mind the following:

- OM Reports are retrieved by the GetOMReport Knowledge Script
- OM Reports are collected hourly, at five minutes past the hour (by default)
- OM Reports are requested from Signaling Servers, VGMCs, MC32Ss, and MGCs by using SNMP, but are transferred by using FTP
- OM Reports generally grow to as large as 200K
- Multiple FTP sessions can interfere with SNMP requests for other OM Reports, thereby making the OM Reports unavailable

To alleviate FTP contention or to reduce bandwidth requirements, consider creating multiple GetOMReport jobs. Stagger the times by using the Schedule tab to change the **Starting at** time in the Frequency panel.

NOTE: Do not set the **Starting at** time for later than 12:58:00. You do not want to miss the creation of the OM Report, which happens on the hour.

4.4.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if NortelCS_GetOMReport fails?	Select **Yes** to raise an event when this Knowledge Script fails to retrieve the latest OM Report. The default is Yes.
Event severity if NortelCS_GetOMReport fails	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the GetOMReport job fails. The default is 15.
FTP timeout	Specify the number of seconds to allow for the transfer of the OM Report before the job times out. The default is 60 seconds.

4.4.5 Configuring FTP Server Parameters

The AppManager for Avaya CS1000 module uses a built-in FTP (File Transfer Protocol) server to transfer Operational Measurement (OM) reports. If your FTP requirements do not fall within the category of “special” as defined below, you can use the built-in FTP server as-is. You do not need to complete the procedures in this topic.

If you have special FTP requirements, use the procedures in this topic to configure FTP parameters in AppManager Security Manager *before* you run the GetOMReport Knowledge Script.

If you do not have special FTP requirements, **do not** complete the following procedures. “Special” FTP requirements are defined as one or both of the following:

- You want to use IIS as the FTP server.
- Your proxy agent computer has two or more network interface cards (NICs).

Configuration for Using Two or More NICs

Whether you use the built-in FTP server or the IIS FTP server, configure AppManager Security Manager when your proxy agent computer has two or more NICs (network interface cards). Configure Security Manager in the following instances:

- You have a preference as to which NIC is used in the FTP process
- One NIC has access to the ELAN and the others do not

NOTE

- If one NIC has access to the ELAN and another has access to the TLAN, ensure the binding order is such that the NIC connected to the ELAN is listed first.
- If you use NetIQ Vivinet Diagnostics to diagnose VoIP quality problems in your CS1000 environment, the proxy agent computer *must* also have TLAN connectivity.

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

Field	Description
Label	`NortelCS_FTP_IPAddress`
Sub-label	◆ *For a single CS1000 device*, type the IP address of the Signaling Server, VGMC, MC32S, or MGC. ◆ *For all CS1000 devices*, type `default`. All devices will FTP OM Reports to the FTP server listening on the IP address you specify in the **Value 1** field.
Value 1	IP address of the FTP server that resides on the proxy agent computer. By identifying this IP address, you tell incoming connections which IP address to use when the computer has more than one NIC. This IP address should have access to the ELAN

Configuration for Using IIS as the FTP Server

To use IIS as the FTP server, configure the root directory, the login username, and the login password into AppManager Security Manager.

- "Configuring the Root Directory" on page 62
- "Configuring the Login Username and Password" on page 63

Configuring the Root Directory

Identify the IIS FTP root directory path in AppManager Security Manager. Ensure the FTP path is write enabled.

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

Field	Description
Label	`NortelCS_FTP_Path`
Sub-label	◆ *For a single CS1000 device*, type the IP address of the Signaling Server, VGMC, MC32S, or MGC. ◆ *For all CS1000 devices*, type `default`. All devices will FTO the OM Reports to the FTP server directory path you specify in the **Value 1** and **Value 2** fields.
Value 1	Root directory of the FTP server. The FTP server root directory, called "local path" in IIS, must be write enabled.
Value 2	File directory path, relative to the root directory, of the folder where OM Report files are to be saved. If this value is not specified, the OM Report files are saved in the root directory path. **NOTE:** Virtual directory paths for IIS FTP are not supported.

Configuring the Login Username and Password

In AppManager Security Manager, configure the login username and password required for accessing the IIS FTP server.

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

Field	Description
Label	`NortelCS_FTP_Login`
Sub-label	◆ *For a single CS1000 device*, type the IP address of the Signaling Server, VGMC, MC32S, or MGC. ◆ *For all CS1000 devices*, type `default`.
Value 1	Login user name required for accessing the IIS FTP server. The user name should have access to the file directory, or root directory if the file directory is not specified.
Value 2	Login password associated with the user name you entered in the **Value 1** field
Extended application support	Encrypts the password in Security Manager. You must select this option.

4.5 HealthCheck

Use this Knowledge Script to monitor the state of the Call Server, Signaling Server, Media Gateway Controller (MGC), Voice Gateway Media Card (VGMC), MC32S (a 32-channel VGMC), Enterprise Common Manager (ECM), Network Routing Server (NRS), and SIP Gateway (SIPL). This script raises an event if a device is not responsive or is in an abnormal state. In addition, this script generates data streams for device availability or state.

4.5.1 Resource Objects

NortelCS Call Server

NortelCS Signaling Server

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

NortelCS Network Routing Server

NortelCS Enterprise Common Manager

NortelCS SIPL

4.5.2 Default Schedule

By default, this script runs every five minutes.

4.5.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if health check fails?	Select **Yes** to raise an event when the selected device is unresponsive or in an abnormal state. The default is Yes.
Event severity if health check failed	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the selected device is unresponsive or in an abnormal state. The default is 15.
Collect data?	Select **Yes** to collect availability data for reports and graphs. 100 indicates the device is available. 0 indicates the device is in any state that is not normal, or there is no response to SNMP. The default is unselected.

4.5.4 Understanding Event Messages

The following are two common error messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

<Device> unresponsive to SNMP:<IP address>

Explanation: The Call Server, MGC, Signaling Server, VGMC, MC32S, ECM, NRS, or SIPL is not responding to SNMP.

Likely cause: Normal message when item is unresponsive.

Operator action: Restart the device.

<Device> in abnormal state:IP address>

Explanation: The Call Server, MGC, Signaling Server, VGMC, MC32S, ECM, or NRS is not running in the proper state.

Likely cause: Normal message when state is abnormal.

Operator action: Change the state of the device.

4.6 PhoneInventory

Use this Knowledge Script to create an inventory of IP phones based on data in the Call Server Entity MIB. The inventory is in `.CSV` format. This script raises an event if no IP phones are found.

4.6.1 Prerequisite

For CS1000 versions 4.0 and later, populate the Entity MIB with IP phone information. For more information, see Section 4.6.5, “Configuring the Call Server to Count IP Phones,” on page 65.

4.6.2 Resource Object

NortelCS Call Server

4.6.3 Default Schedule

By default, this script runs once.

4.6.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if NortelCS_PhoneInventory succeeds?	Select **Yes** to raise an event if the PhoneInventory job succeeds in creating an inventory. The default is Yes.
Event severity if NortelCS_PhoneInventory succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job succeeds in creating an inventory. The default is 30.
Raise event if NortelCS_PhoneInventory fails?	Select **Yes** to raise an event if the PhoneInventory job fails for any reason. The default is Yes.
Event severity if NortelCS_PhoneInventory fails	Set the severity level, between 1 and 40, to indicate the importance of an event in which the PhoneInventory job fails. The default is 15.
Raise event if no IP phones are found?	Select **Yes** to raise an event if no IP phones are found in the Entity MIB. The default is Yes.
Event severity if no IP phones are found	Set the severity level, between 1 and 40, to indicate the importance of an event in which the Entity MIB contains no IP phones. The default is 15.
Report directory's pathname	Specify the full local or UNC path to the root of the directory in which you want to save the phone inventory report, which will be titled `NortelCS_PhoneInventory_<IP address of Call Server>.csv`. Ensure the `NetIQmc` service (NetIQ AppManager Client Resource Monitor) is configured to run as a user that has access to the UNC path. The default setting of "local system" does not have access to the UNC path. Without access to the path, AppManager cannot save the inventory to the output folder. Leave this field blank to save the inventory report to the default location: `c:\Program Files\NetIQ\temp`

4.6.5 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. However, for this process to work, you must issue two or three commands in Overlay 117:

- Tell the Call Server to generate the inventory report once every midnight
- Tell the Call Server to include the IP telephones from the inventory report in the Entity MIB
- Optional: Tell the Call Server to generate the inventory report immediately

NOTE: Do not issue the following commands if you are using CS1000 version 3.0. The following instructions apply only for versions 4.0 and later.

Issue the commands *before* running Discovery_NortelCS. If you run discovery before issuing the commands, AppManager raises an event indicating phone counting was unsuccessful because AppManager expects to find at least one phone.

Issue the following commands in Overlay 117:

```
INV MIDNIGHT SETS
INV ENTITY SETS ON
```

These two commands generate an inventory report at midnight and add the phones from the inventory report to the Entity MIB. Once the phones are added to the MIB, rerun Discovery_NortelCS.

If you do 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: 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.

4.7 SS_CallQuality

Use this Knowledge Script to monitor call quality statistics on the Avaya Signaling Server: audio setups, voice time, average and maximum jitter, latency, lost packets, listening R-factor, and Mean Opinion Score (MOS). This script raises an event if a statistic exceeds the threshold you set. In addition, this script generates the following data streams:

- **Total number of audio setups**, which is the number of call legs established in a call. A simple call may have only one audio setup, but a conference call or a call on hold can have multiple audio setups.
- **Average and maximum percentage of lost data packets**, calculated based on the number of expected packets and the number of packets actually received. The number of packets received includes those that were late or duplicates. Packets that arrive late are not counted as lost. The presence of duplicate packets can result in a negative value for lost data.
- **Average and minimum listening MOS on the phones** (CS1000 versions 4.0 and later only). The Listening MOS value represents the overall quality of a call from the listener's perspective. The MOS is a number between 1 and 5. A MOS of 5 is excellent. A MOS of 1 is unacceptably bad. The MOS calculation considers measured items plus jitter buffer size. AppManager uses a modified version of the ITU (International Telecommunications Union) G.107 standard E-model equation to calculate the MOS. This algorithm is used to evaluate the quality of a transmission by factoring in the "mouth to ear" characteristics of a speech path.
- **Average and minimum listening R-factor on the phones** (CS1000 versions 4.0 and later only). The E-model equation that calculates MOS also calculates R-factor. R-factors range from 100 (excellent) to 0 (poor), and are a direct measure of call quality or transmission quality with respect to codec type and quality factors such as packet loss and delay. A Listening R-factor score represents call or transmission quality from a listener's perspective.
- **Total voice time**, in seconds, for all calls of a particular set type during the reporting period.

- **Average and maximum jitter for each selected phone model**. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.
- **Average and maximum latency for each selected phone model**. Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.

For more information, see Section 4.7.6, “Understanding How Data Streams are Calculated,” on page 69.

4.7.1 Tip for Using This Script

You can use the SS_CallQuality script to retrieve data about every CS1000 phone type in your environment. However, data streams are based on *all* selected phone types, not *each* selected phone type. So if you run SS_CallQuality and choose to monitor all phones types, you will not be able to tell which phone type is responsible for a high percentage of lost packets, for example.

To ensure the SS_CallQuality script provides values for individual phone types, run the script once for each phone type. For instance, run SS_CallQuality once to monitor the i2004 model phones. Then run it again to monitor i2050 model phones.

Note that phone model names changed with CS1000 versions 4.50, 5.0, and 6.0. The phone models you monitor on a 4.50 Signaling Server may not exist on a 5.0 Signaling Server.

4.7.2 Prerequisite

Run GetOMReport before running this script.

4.7.3 Resource Object

NortelCS Signaling Server

4.7.4 Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not getting the latest data.

4.7.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if audio setups exceed threshold?	Select **Yes** to raise an event if the number of audio setups exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Event severity if audio setups exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of audio setups exceeds the threshold you set. The default is 15.
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time exceeds the threshold you set. The default is 15.
Raise event if call quality threshold crossed?	Select **Yes** to raise an event if any of the call quality statistics exceeds or fails to meet the threshold you set. The default is Yes.
Event severity if call quality threshold crossed	Set the severity level, between 1 and 40, to indicate the importance of an event raised when any of the call quality statistics (MOS, R-factor, lost packets, maximum jitter, or maximum latency) exceeds or fails to meet) the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum audio setups	Specify the highest number of audio setups that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Call Quality	
Score	Select whether you want to set a threshold for **R-factor** or **MOS**.
Threshold - Minimum listen R-factor	Specify the minimum R-factor score can that occur before an event is raised. The default is 70.
Threshold - Minimum listen MOS	Specify the minimum Mean Opinion Score (MOS) that can occur before an event is raised. The default is 3.6.
Threshold - Maximum lost packets	Specify the highest percentage of packets that can be lost before an event is raised. The default is 1%.
Threshold - Maximum jitter	Specify the highest amount of jitter that can occur before an event is raised. The default is 60 milliseconds.
Threshold - Maximum latency	Specify the highest amount of latency that can occur before an event is raised. The default is 400 milliseconds.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns several data streams based on the thresholds you set. The default is unselected.

Parameter	How to Set It
Phone model selection	Type a regular expression that defines which phone models you want to monitor. For example, type `2007` to monitor only the 2007 phone model. Type `.*2004` to monitor any phone model name that contains 2004, such as 3Pi2004, i2004, 2004, and 2004P2. Type `i200[124]` to monitor phone models i2001, i2002, and i2004. Leave this parameter blank to monitor all phone models. The default is blank.

4.7.6 Understanding How Data Streams are Calculated

This topic applies to call metrics monitored by the following Knowledge Scripts:

- SS_CallQuality
- SS_H323Stats
- SS_Registration
- SS_SIPStats
- VGMC_CallQuality

AppManager retrieves CS1000 call metrics (audio setups, voice time, jitter, latency, R-factor, MOS, registration, and lost packets) from the Operational Measurement (OM) Reports created each hour on the Signaling Server, VGMC, MC32S, and MGC.

OM Reports provide call data per phone *model*, not per phone. For example, the OM Report identifies the average jitter for all of the i2004 model phones, but does not identify the jitter value for each phone of that model. In addition, the OM Report collects average and maximum values for jitter and latency, but only a single value for R-factor, voice time, registration, and audio setups.

Therefore, when you run a data collection script, it is important to understand that the resulting data streams are based on groups of phone types and are limited by the type of raw data available in the OM Report. The following table illustrates how each data stream is calculated:

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Total number of audio setups	Total number of audio setups for each phone model	AppManager finds the total number of audio setups from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of audio setups for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Average jitter	Average amount of jitter for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and average jitter. For example, you choose to monitor three phone types. The average amount of jitter for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which AJ = average jitter and VT = voice time: $\frac{(AJ_a \times VT_a)+(AJ_b \times VT_b)+(AJ_c \times VT_c)}{VT_a+VT_b+VT_c}$ In the formula, the products of average jitter and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average jitter is 2.222.
Maximum jitter	Maximum amount of jitter for each phone model	AppManager finds the highest amount of maximum jitter from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The maximum amount of jitter for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The maximum of these three values is 3 ms, which is the value represented by the data stream.
Average latency	Average amount of latency for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and average latency. For example, you choose to monitor three phone types. The average amount of latency for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which AL = average latency and VT = voice time: $\frac{(AL_a \times VT_a)+(AL_b \times VT_b)+(AL_c \times VT_c)}{VT_a+VT_b+VT_c}$ In the equation, the products of average latency and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average latency is 2.222.
Maximum latency	Maximum amount of latency for each phone model	AppManager finds the highest amount of maximum latency from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The maximum amount of latency for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The maximum of these three values is 3 ms, which is the value represented by the data stream.

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Average percentage of lost packets	Total percentage of lost packets for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and lost packets. For example, you choose to monitor three phone types. The percentage of lost packets for type A is 1%, for type B is 2%, and for type C is 3%. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which LP = lost packets and VT = voice time: $\frac{(LP_a \times VT_a)+(LP_b \times VT_b)+(LP_c \times VT_c)}{VT_a+VT_b+VT_c}$ In the equation, the products of lost packets and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average percentage of lost packets is 2.222.
Maximum percentage of lost packets	Maximum percentage of lost packets for each phone model	AppManager finds the highest percentage of lost packets from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total percentage of lost packets for type A is 3, for type B is 6, and for type C is 9. The highest of these three values is 9, which is the value represented by the data stream.
Average listen MOS	N/A	AppManager converts the average R-factor value into MOS using a conversion formula provided by the ITU (International Telecommunications Union).
Minimum listen MOS	N/A	AppManager converts the minimum R-factor value into MOS using a conversion formula provided by the ITU (International Telecommunications Union).

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Average listen R-factor	An R-factor value for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and R-factor. For example, you choose to monitor three phone types. The R-factor value for type A is 99, for type B is 97 and for type C is 95. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which RF = R-factor and VT = voice time: $\frac{(RF_a \times VT_a)+(RF_b \times VT_b)+(RF_c \times VT_c)}{VT_a+VT_b+VT_c}$ In the equation, the products of R-factor and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average listen R-factor is 96.56.
Minimum listen R-factor	An R-factor value for each phone model	AppManager finds the lowest R-factor value from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The R-factor value for type A is 99, for type B is 97 and for type C is 95. The lowest of these three values is 95, which is the value represented by the data stream.
Total registration attempts	A registration value for each phone model	AppManager finds the total number of registration attempts from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of registration attempts for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.
Total registration failures	A registration value for each phone model	AppManager finds the total number of registration failures from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of registration failures for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.
Total unregistration attempts	An unregistration value for each phone model	AppManager finds the total number of unregistration attempts from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of unregistration attempts for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Total voice time	Total amount of voice time for each phone model. This value includes the voice time for both phase 1 and phase 2 phones.	AppManager finds the total amount of voice time from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total amount of voice time for type A is 20 seconds, for type B is 25, and for type C is 30. The total amount of these three values is 75, which is the value represented by the data stream.

4.8 SS_H323Stats

Use this Knowledge Script to monitor H.323 virtual trunk statistics for the Avaya Signaling Server: incoming voice and fax calls, and outgoing voice and fax calls. This script raises an event if a statistic exceeds the threshold you set. In addition, this script generates the following data streams:

- **Maximum amount of voice time** on the H.323 virtual trunk for all calls of a particular set type during the reporting period.
- **Number of incoming attempted and completed voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming voice calls.
- **Number of outgoing attempted and completed voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing voice calls.
- **Number of incoming attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming FAX calls.
- **Number of outgoing attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing FAX calls.

For more information, see Section 4.7.6, “Understanding How Data Streams are Calculated,” on page 69.

4.8.1 Prerequisite

Run GetOMReport before running this script.

4.8.2 Resource Object

NortelCS Signaling Server

4.8.3 Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not receiving the latest data.

4.8.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time is greater than the threshold you set. The default is 15.
Raise event if incomplete incoming voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete incoming fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming fax calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing fax calls exceeds the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete incoming voice calls	Specify the largest number of incomplete incoming voice calls that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.

Parameter	How to Set It
Threshold - Maximum incomplete outgoing voice calls	Specify the largest number of incomplete outgoing voice calls that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete incoming fax calls	Specify the largest number of incomplete incoming fax calls that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete outgoing fax calls	Specify the largest number of incomplete outgoing fax calls that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.

4.9 SS_Registration

Use this Knowledge Script to monitor registration attempts and failures on the Avaya Signaling Server. This script raises an event if the number of registration failures or attempts exceeds the threshold you set. In addition, this script generates the following data streams:

- Total number of registration attempts
- Total number of registration failures
- Total number of unregistration attempts

For more information, see Section 4.7.6, “Understanding How Data Streams are Calculated,” on page 69.

4.9.1 Tip for Using This Script

You can to use the SS_Registration script to retrieve data about every CS1000 phone type in your environment. However, data streams are based on *all* selected phone types, not *each* selected phone type. So if you run SS_Registration and choose to monitor all phones types, you will not be able to tell which phone type is responsible for a high number of registration failures, for example.

The only way you can ensure the SS_Registration script provides values for individual phone types is to run the script once for each phone type. For instance, run SS_Registration once to monitor the i2004 model phones. Then run it again to monitor i2050 model phones.

Note that phone model names changed with CS1000 version 4.50, 5.0, and 6.0. The phone models you monitor on a 4.50 Signaling Server may not exist on a 5.0 Signaling Server.

4.9.2 Prerequisite

Run GetOMReport before running this script.

4.9.3 Resource Object

NortelCS Signaling Server

4.9.4 Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not getting the latest data.

4.9.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if registration attempts exceed threshold?	Select **Yes** to raise an event if the number of registration attempts exceeds the threshold you set. The default is unselected.
Event severity if registration attempts exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of registration attempts exceeds the threshold you set. The default is 15.
Raise event if registration failures exceed threshold?	Select **Yes** to raise an event if the number of registration failures exceeds the threshold you set. The default is Yes.
Event severity if registration failures exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of registration failures exceeds the threshold you set. The default is 15.
Raise event if unregistration attempts exceed maximum?	Select **Yes** to raise an event if the number of unregistration attempts exceeds the threshold you set. The default is unselected.
Event severity if unregistration attempts exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of unregistration attempts exceeds the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum registration attempts	Specify the largest number of registration attempts that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum registration failures	Specify the largest number of registration failures that can occur before an event is raised. The default is 0.
Threshold - Maximum unregistration attempts	Specify the largest number of unregistration attempts that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.

Parameter	How to Set It
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.
Phone model selection	Type a regular expression that defines which phone models you want to monitor. For example: ◆ Type `2007` to monitor only the 2007 phone model. ◆ Type `.*2004` to monitor any phone model name that contains 2004, such as 3Pi2004, i2004, 2004, and 2004P2. ◆ Type `i200[124]` to monitor phone models i2001, i2002, and i2004. Leave this parameter blank to monitor all phone models. The default is blank.

4.10 SS_SIPStats

Use this Knowledge Script to monitor SIP virtual trunk statistics for the Avaya Signaling Server: incoming voice and fax calls, and outgoing voice and fax calls. This script raises an event if a statistic exceeds the threshold you set.

- **Maximum amount of voice time** on the SIP virtual trunk for all calls of a particular set type during the reporting period.
- **Number of incoming attempted and completed voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming voice calls.
- **Number of outgoing attempted and completed outgoing voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing voice calls.
- **Number of incoming attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming FAX calls.
- **Number of outgoing attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing FAX calls.

For more information, see Section 4.7.6, “Understanding How Data Streams are Calculated,” on page 69.

This script supports CS1000 version 4.0 and later.

4.10.1 Prerequisite

Run GetOMReport before running this script.

4.10.2 Resource Object

NortelCS Signaling Server

4.10.3 Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not getting the latest data.

4.10.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time exceeds the threshold you set. The default is 15.
Raise event if incomplete incoming voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete incoming fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming fax calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing fax calls exceeds the threshold you set. The default is 15.
Monitoring	

Parameter	How to Set It
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete incoming voice calls	Specify the largest number of incomplete incoming voice calls that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete outgoing voice calls	Specify the largest number of incomplete outgoing voice calls that can occur before an event is raised. The default is 0.
Threshold - Maximum incomplete incoming fax calls	Specify the largest number of incomplete incoming fax calls that can occur before an event is raised. The default is 0.
Threshold - Maximum incomplete outgoing fax calls	Specify the largest number of incomplete outgoing fax calls that can occur before an event is raised. The default is 0.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.

4.11 VGMC_CallQuality

Use this Knowledge Script to monitor channel statistics for the Avaya Voice Gateway Media Card (VGMC), Media Gateway Controller (MGC), and MC32S: audio setup, voice time, jitter, lost packets, and channel latency. This script raises an event if a statistic exceeds the threshold you set. In addition, this script generates the following data streams:

- **Total number of audio setups**, which is the number of call legs established in a call. A simple call may have only one audio setup, but a conference call or a call on hold can have multiple audio setups.
- **Total amount of voice time** for all calls of a particular set type during the reporting period.
- **Average and maximum jitter**. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.
- **Average percentage of lost packets**, calculated based on the number of expected packets and the number of packets actually received. The number of packets received includes those that were late or duplicates. Packets that arrive late are not counted as lost. The presence of duplicate packets could result in a negative lost data amount.
- **Average channel latency** (not available from VGMCs). Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.

For more information, see Section 4.7.6, “Understanding How Data Streams are Calculated,” on page 69.

4.11.1 Prerequisite

Run GetOMReport before running this script.

4.11.2 Resource Objects

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

4.11.3 Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not retrieving the latest data.

4.11.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if audio setups exceed threshold?	Select **Yes** to raise an event if the number of audio setups exceeds the threshold you set. The default is unselected.
Event severity if audio setups exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of audio setups exceeds the threshold you set. The default is 15.
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time exceeds the threshold you set. The default is 15.
Raise event if call quality exceeds threshold?	Select **Yes** to raise an event if any of the call quality statistics exceeds the threshold you set. The default is Yes.
Event severity if call quality exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the call quality statistics (maximum lost packets or maximum jitter) exceed the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum audio setups	Specify the highest number of audio setups that can occur before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **NOTE:** The default value has no significance and is not a recommended threshold value.
Call Quality	

Parameter	How to Set It
Threshold - Maximum lost packets	Specify the highest average percentage of packets that can be lost before an event is raised. The default is 1%.
Threshold - Maximum jitter	Specify the highest amount of jitter that can occur before an event is raised. The default is 60 milliseconds.
Threshold - Maximum average latency	Specify the highest amount of average channel latency that can occur before an event is raised. The default is 60 milliseconds.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.