NetIQ® AppManager® for Cisco® CallManager

Management Guide

February 2012

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 NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, please 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. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, 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, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introducing AppManager for Cisco CallManager

This chapter introduces AppManager for Cisco CallManager, providing an overview of the module, and describing how you can use AppManager to better monitor vital Cisco CallManager clusters and resources.

1.1 Features and Benefits

AppManager is designed to help you gain easy access to Cisco CallManager data, and to help you analyze and manage that data. The AppManager for CallManager solution minimizes the cost of maintaining a CallManager system, aids in capacity planning, and can prevent downtime.

With AppManager for Cisco CallManager, administrators charged with managing CallManager gain access to a new 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.

CallManager is designed to run on Windows systems, and uses Microsoft SQL and IIS servers and custom application services developed by Cisco Systems. AppManager can monitor and regulate all of the services and applications that are critical to CallManager performance:

- Cisco CallManager
- Cisco TFTP
- Cisco Messaging Interface
- Cisco IP Voice Media Streaming Application
- Cisco Database Layer Monitor
- Cisco SNMP Data Collector
- Cisco CTI Manager
- Cisco Extension Mobility Logout
- Cisco MOH Audio Translator
- Cisco RIS Data Collector
- Cisco Telephony Call Dispatcher
- DC Directory Server
- Microsoft SQL Server
- Microsoft IIS Server

AppManager for CallManager includes more than 150 Knowledge Scripts to create jobs that monitor the health, availability, and performance of key services, applications, and the operating system. These scripts allow you to monitor and manage any or all of these crucial CallManager services at a depth unparalleled by any other solution. Each Knowledge Script can be configured to send an alert, collect data for reporting, and perform automated problem management when an event occurs.

By continuously monitoring critical Cisco CallManager services, AppManager can keep you informed anytime something changes in your CallManager system. For example, you can configure a Knowledge Script to send an email to an administrator if the Cisco Telephony Call Dispatcher service goes down. In addition, you can configure another Knowledge Script to use the AppManager agent to restart the service.

AppManager for Cisco CallManager not only monitors CallManager services, but also collects data about their performance and availability and stores it in the AppManager repository, a SQL server database. The default repository name is QDB. You can set up Monitoring scripts to collect data and then run Report scripts to display the data in the Report Viewer of the Operator Web Console. You can also display the data in a graph in the Graph pane of the Operator Console or the Reports page of the Operator Web Console. In addition, you can use the data to create charts in the Chart Console and export the data to .csv files.

AppManager can also monitor the hardware platform on which CallManager runs, such as Compaq Insight Manager, to allow for extensive analysis of data collected from Cisco CallManager running on the Cisco Media Convergence Server (MCS) platform.

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

- Reduces the time you spend diagnosing and resolving CallManager issues
- Monitors and manages the entire Cisco CallManager system, including the CallManager application, SQL, IIS, TFTP, system resources, bandwidth usage, and call activity
- Provides the ability to view, manage, and report on CallManagers as a cluster
- Automates system management issues that could affect CallManager performance
- Pinpoints problems whether they originate at the hardware, operating system, or application level
- Supports the following versions of CallManager: 3.0, 3.1, 3.2, 3.3, 4.0, 4.1. 4.2, 4.3, 4.3(1)

1.2 Counting AppManager Licenses

Licensing of AppManager for Cisco CallManager is based on the number of registered hardware phones, which are monitored in the CallManager performance counter.

2 Installing AppManager for Cisco CallManager

This chapter provides installation instructions and describes system requirements for AppManager for Cisco CallManager.

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.

2.1 System Requirements

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page. Unless noted otherwise, this module supports all updates, hotfixes, and service packs for the releases listed below.

AppManager for Cisco CallManager has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, on all agent computers, and on all console computers	7.0, at minimum
Microsoft Windows operating system installed on the Cisco CallManager servers you want to monitor (agent computers)	One of the following ◆ Windows Server 2003 (supports CallManager 4.3(x) only) ◆ Windows 2000 Server, Advanced Server, or DataCenter Server ◆ Window NT 4.0 with Windows Management Instrumentation (WMI)
Cisco CallManager installed on the agent computers	3.x, 4.0(x), 4.1(x), 4.2(x), or 4.3(x)

If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

Only the following AppManager modules should be installed on a Cisco CallManager server:

- Cisco CallManager (`qccma4.dll`)
- CIM (`qcima4.dll`)
- Dell (`qdella4.dll`)
- IBM Netfinity (`qnfda4.dll`)
- NT (`qnta4.dll`)

- WTS (`qwtsa4.dll`)
- SQL (`qsqla4.dll`)

2.2 Installing the Module

The setup program automatically identifies and updates all relevant AppManager components on a computer. Therefore, run the setup program only once on any computer. The pre-installation check also runs automatically when you launch the setup program.

You can install the module in an AppManager version 7.x environment in one of the following ways:

- Run the module setup program, `AM70-CiscoCallMgr-7.x.x.0.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager.*
- Use Control Center to install the module on the remote computer where an agent is installed. For more information, see Section 2.4, "Deploying the Module with Control Center," on page 15.

NOTE: Control Center is designed to install modules on computers deployed in domains, not in workgroups, which is the Cisco-recommended deployment model for CallManager. To use Control Center with your CallManager workgroups, configure pass-through authentication. For more information, see Section 2.3, "Configuring Control Center for Workgroup Environments," on page 15.

To install the module:

1. Stop the Cisco Security Agent (CSA) service on each CallManager computer you want to monitor. From the Control Panel, double-click **Administrative Tools**, double-click **Services**, right-click the CSA service and select **Stop**.
2. Stop the Cisco IP Telephony Backup processes, `stiBack.exe` or `stiView.exe`, on each CallManager computer you want to monitor.
3. Run the module setup program on all AppManager repository (QDB) computers to install the Knowledge Scripts and reports.
   - Run the setup program on the primary repository computer first. Then run the setup program on all other repository computers.
   - For repositories running in active/active and active/passive clusters, run the setup program on the active node. Then, copy the following Registry key to the non-active node.

     `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0`
4. Install the module on the CallManager computer you want to monitor. Use one of the following methods:
   - Run the module setup program.
   - Use Control Center Console to deploy the installation package.
5. Run the module setup program on all Operator Console and Control Center computers to install the Help and console extensions.
6. Restart the CSA service and Backup processes on all agent computers where you installed the module.

7 Enable the generation of CMRs and CDRs. For more information, see Section 2.8, "Enabling Call Management & Call Detail Records," on page 20.

8 If you have not already discovered CallManager resources, run the Discovery_CiscoCallMgr Knowledge Script on all agent computers where you installed the module. For more information, see Section 2.6, "Discovering Cisco CallManager Resources," on page 16.

After the installation has completed, you can find a record of problems encountered in the `CiscoCallMgr_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<`*ServerName*`>` folder.

2.3 Configuring Control Center for Workgroup Environments

AppManager Control Center is designed to install modules on computers deployed in domains, not in workgroups, which is the Cisco-recommended deployment model for CallManager. To use Control Center in a workgroup environment, you need to configure *pass-through authentication*. Pass-through authentication allows the CallManager computer to recognize and allow access to Control Center functions.

To configure pass-through authentication:

1 On the Control Center computer on which you have installed the NetIQ AppManager Deployment Service, create a local account that has administrative privileges.

2 On the CallManager computer, create a local account with administrative privileges, using the same username and password that you assigned to the account you created in Step 1.

3 Use this username and password combination as your deployment credentials when you create your deployment rule in Control Center.

2.4 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.

2.4.1 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.

3 Configure an email 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.

2.4.2 Checking In the Installation Package

You must check in the installation package, `AM70-CiscoCallMgr-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 and navigate to the Administration pane.
2. In the Deployment folder, select **Packages**.
3. On the Tasks pane, click **Check in Packages**.
4. Navigate to the folder where you saved `AM70-CiscoCallMgr-7.x.x.0.xml` and select the file.
5. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.

2.5 Silently Installing the Module

To silently (without user intervention) install a module, create an initialization file (`.ini`) for this module that includes the required property names and values to use during the installation.

To create and use an initialization file for a silent installation:

1. Create a new text file and change the filename extension from `.txt` to `.ini`.
2. To specify the community string required to access hardware resources, include the following text in the `.ini` file:

   `MO_CommunityString=`*`string name`*

   where *string name* is the name of the community string, such as `public`.
3. Save and close the `.ini` file.
4. Run the following command from the folder in which you saved the module installer:

   `msiexec.exe /i "AM70-CiscoCallMgr-7.x.x.0.msi" /qn MO_CONFIGOUTINI="`*`full path to the initialization file`*`"`

   where *x.x* is the actual version number of the module installer.

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

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

The log file is created in the folder in which you saved the module installer.

2.6 Discovering Cisco CallManager Resources

Use the Discovery_CiscoCallMgr Knowledge Script to discover Cisco CallManager configuration and resources on the CallManager servers you want to monitor.

Unlike other Discovery scripts, which run once by default, Discovery_CiscoCallMgr runs weekly by default. By running the script periodically, you maintain up-to-date information about all of the CallManager registered devices in the repository. Click the **Schedule** tab to change the default run schedule.

Discovery_CiscoCallMgr retrieves the stiBack version number from the registry. If no backup has ever been run, the version number in the registry contains a "0" as its third number, for example: 3.1.0.39. However, if you were to look at **Help > About** for the stiView applet, you would not see the "0." To continue the example, you would see 3.1.39. Once you run a backup, the version number in the registry will match the version number in **Help > About**. Then, the next time CallManager discovery runs, AppManager will display the same version number as **Help > About**.

Set the parameters on the Values tab as needed:

Parameter	How to set it
Raise event if discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
SQL username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 15.

Parameter	How to set it
Create cluster server group?	Set to **y** to arrange in a cluster all CallManagers in a server group. The cluster is visible in the Master view only. The default is y. By arranging your CallManagers in a cluster, you can simplify your monitoring process by running Knowledge Scripts on a cluster to monitor every CallManager in the cluster. The Discovery_CiscoCallMgr Knowledge Script groups CallManagers according to Publisher. A cluster consists of a Publisher and one or more Subscriber CallManagers. Only the Subscribers perform call processing. The Publisher handles administrative activities such as configuration. The following combinations represent the most common clusters: ◆ **One Publisher and one Subscriber**. The Publisher server contains the TFTP server and any media resource applications. It also acts as the backup for the Subscriber. ◆ **One Publisher and three Subscribers**. The Publisher server contains the TFTP server and any media resource applications. Two of the Subscribers are primary CallManagers. The remaining Subscriber is the backup for the two primaries. ◆ **One Publisher, a TFTP server, and six Subscribers**. Either the Publisher or the TFTP server will contain the media resource applications. Four of the Subscribers are primary CallManagers. The remaining two are backups for the primaries. **NOTE**: For the Discovery script, the default action on the Actions tab is Action_AddComputerToServerGroup. When creating a server group, do *not* change this default selection.

2.7 Upgrading Knowledge Script Jobs

This release of AppManager for Cisco CallManager may contain updated Knowledge Scripts. 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.

2.7.1 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. In addition, the repository computer must have hotfix 72040 installed, or the most recent AppManager Repository hotfix. To download the hotfix, see the AppManager Suite Hotfixes Web page.

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.

2.7.2 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. Customized script parameters may have reverted to default parameters during the installation of the module. New parameters may need to be set appropriately for your environment or application.

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 both properties and the script.

For more information about propagating Knowledge Script changes, see the "Running Monitoring Jobs" chapter of the *Operator Console User Guide for AppManager*.

Propagating Changes to Ad Hoc Jobs

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.

To propagate changes to ad hoc Knowledge Script jobs:

1. In the Knowledge Script view, select the Knowledge Script for which you want to propagate changes.
2. Click **Properties Propagation** > **Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs:

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.

Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic (script) 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. For more information, see "Propagating Changes to Ad Hoc Jobs" on page 19.

To propagate Knowledge Script changes to Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script Group for which you want to propagate changes.
2. On the KS menu, select **Properties propagation** > **Ad Hoc Jobs**.
3. ***If you want to exclude a Knowledge Script member from properties propagation,*** deselect that member from the list in the Properties Propagation dialog box.

4 Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, including the schedule, actions, and Advanced properties.

5 Click **OK**. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

2.8 Enabling Call Management & Call Detail Records

Cisco CallManager produces two types of records: Call Detail Records (CDR) and Call Management Records (CMR). CDRs, also called data records, contain information about each call processed by a CallManager: call origination, call destination, and the data and time the call started, connected, and ended. CMRs, also called diagnostic records, contain information about the amount of data sent and received, jitter, latency, and lost packets.

CallManager does not collect CMR or CDR records automatically; you must enable it to do so. CDR records are stored in the Publisher. CMRs are generated only when CDRs are generated.

To enable CMR and CDR record collection:

1 In Cisco CallManager Administration, click **Service**.

2 Click **Service Parameters**.

3 Click **CallManager**.

4 *To enable the generation of CDR records*, set **CDREnabled** to **T**.

5 *To enable the generation of CMR records*, set **CallDiagnosticsEnabled** to **T**.

6 *To generate CDRs for calls that were not connected or were connected for less than one second*, set **CdrLogCallsWithZeroDurationFlag** to **T**. This setting is valid only if **CDREnabled** is set to **T**.

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 Cisco CallManager 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 CallManager.

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

3.1 Capacity Planning Reports

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 reports available from Analysis Center for Cisco CallManager data. For more information, see the Configuration Card details for each report.

Report Name	Description
Cisco CallManager Maximum Utilization Trend and Prediction	Displays the trend of the maximum utilization of CallManager ports and channels: the maximum number of ports or channels that were active on any device for each day over the specified range of existing data. Use the Metric context control to select the type of metric and resources to include in the trend report. You should set the **PredictionDays** property on the **Properties** tab 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.
Cisco CallManager Volume Trend and Prediction	Displays the trend of CallManager call volume: the total number of calls each day over the specified range of existing data. Use the Metric context control to select the type of calls to include in the trend report. You should set the **PredictionDays** property on the **Properties** tab 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.

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 Cisco CallManager data. For more information, see the Configuration Card details for each report.

Report Name	Description
Cisco Callmanager All Services Availability	Displays the availability of the various services that run on the CallManager server. In the Metric context, expand the **CallManager All Services Availability** metric to see a list of services, and then select one or more services for the report. Use the Group context to select computer groups or individual computers. The computers or groups are shown as rows in the report. The individual services are shown as columns in the report. Use the other context controls as data filters.
Cisco CallManager Call Completion	Displays attempted and completed calls for CallManagers for a specified time period. Use the Group context to select the groups, clusters, or individual CallManager servers for the report. By default, this report uses the **CallManager Calls Attempted** and **CallManager Calls Completed** data streams generated by the AppManager CiscoCallMgr_CallActivity Knowledge Script. In the report, a table shows the completion rate as a percentage, the number of attempted calls, and the number of completed calls. To create a graphical representation of the total calls and completed calls, use the Column Rules on the **Properties** tab to hide the Completion Rate column. To create a graphical representation of the completion rate, use the Column Rules to hide the Total Calls and Completed Calls columns, change **ViewMode** to **chart** or **both**, and set **AutoScale** under the AxisY property to **False**.
Cisco CallManager Performance Data	Examines CallManager 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 are shown as rows in the report. Use the Metric context to select the metrics that you want to include in the report; the metrics are shown as columns in the report. Use the other context controls as data filters. For example, use the Time context to control the time rate of the data. Use the Measures context to indicate whether to show the average, sum, or maximum of the data. For metrics such as memory or CPU utilization, selecting 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
Cisco CallManager Performance Data by Date and Time	Examines CallManager performance data by date and time. The date and time are shown as rows in the report. By default, this report shows the data by day. You can show data by hour or minute by using the Time context to change the **Interval** to **Hour** or **Minute**. Use the Group context to select the computers or computer groups that you want to include in the report. Computers or computer groups are show as columns in the report. If you are including several computers or computer groups, you may want to change **ChartType** 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 the metric shown in the report. For example, to create a report showing yesterday's average CallManager CPU usage for each hour, use the Metric context to select **CallManager Total CPU Usage**. Then use the Time context to select **Yesterday** in the **Date Range** field and **Hour** in the **Interval** field.
Cisco CallManager Performance Data by Hour	Examines CallManager 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 you want to include in the report; the computers or groups are shown as columns in the report. If you are including several computers or computer groups, you may want to change **ChartType** 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 the metric shown in the report. For example, to create a Busy Hour report for CallManager call volume, use the Metric context to select **CallManager Calls Attempted** and use the Measures context to select **Sum**.
Cisco CallManager 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 CallManager computer's total CPU usage (**CallManager Total CPU Usage**) to the CPU usage of the CallManager process (**CallManager Process CPU Usage**). Or, you can compare multiple instances of the same metric, such as the **Outbound Busy Attempts** of all of your MGCP PRI devices. Use the Metric context to select specific instances of the metric: expand the metric description and then select the instances you want to include. Use the Time context to set the **Time Range** and **Interval** (for instance **Last 28 Days** by **Day**). The interval you select determines the time aggregation. 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 the computers or groups to include in the report.
Cisco CallManager Performance Data Metrics by Hour	Examines metrics by hour of the day. For example, you can use this report to look at the average number of channels that are active on your MGCP PRI devices by hour of the day. This number provides an indication of the times of day during which the devices are most heavily utilized. Use the Metric context to select one or more metrics to include in the report. To select specific instances of a metric, expand the metric description and then select the instances you want to include in the report. Use the other context controls as data filters.

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 Cisco CallManager data. For more information, see the Configuration Card details for each report.

Report Name	Description
Cisco CallManager Call Completion Rate Pie Chart	Looks at the call-completion rate (completed calls vs. non-completed calls) for CallManagers for the time period that you specify. Use the Group context to select the groups, clusters, or individual CallManager servers that you want to include in the report. This report uses the **CallManager Calls Attempted** and **CallManager Calls Completed** data streams generated by the AppManager CiscoCallMgr_CallActivity Knowledge Script.
Cisco CallManager Service Availability	Shows the availability of the CallManager service running on CallManager servers. The availability of this service is critical for the CallManager to process calls. This report uses the Cisco CallManager instance of the **CallManager Service Availability** data stream generated by the AppManager CiscoCallMgr_CCM_HealthCheck Knowledge Script. This script uses a value of 1 to indicate availability and a value of 0 to indicate unavailability. By default, this report presents the availability of all CallManager servers. Use the Group context to show the availability of individual servers or groups. Servers or groups are shown as rows in the report. The columns of the report reflect the available and unavailable percentages — information can easily be graphed as a stacked column.
Cisco CallManager Service Levels Overview	Presents an overview of underlying reports that indicate key service level metrics. The member reports reflect the availability of the CallManager service running on CallManager servers and the completion rate of calls that are being processed. Click on the title of any member report to see the full view of that report. When deploying this report, remember to deploy each member report first.

4 CiscoCallMgr Knowledge Scripts

Cisco CallManager software provides enterprise telephony features and functions for packet-based network devices, including IP phones, media processing devices, voice over IP (VoIP) gateways, and multimedia applications. It offers an API that allows for additional data, voice, and video services such as unified messaging and multimedia video conferencing.

AppManager Knowledge Scripts help you monitor and regulate services that are critical to Cisco CallManager performance. 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**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AnalogOutboundBusy	Monitors the number of times during an interval that a call was attempted through an analog access when no ports were available.
AnalogPortsActive	Monitors active ports.
AnalogPortsOutOfService	Monitors out-of-service ports.
CallActivity	Monitors call activity on selected CallManagers.
CallFailures	Monitors Call Detail Records for calls that have an abnormal cause of termination.
CallQuality	Monitors the calls recorded in the Call Management Records for jitter, latency, lost data, and listening MOS.
CallsActive	Monitors active calls.
CallsAttemptedByPhone	Monitors calls attempted by an individual phone.
CallsInProgress	Monitors the number of calls in progress and the percentage of in-progress calls that are active.
CCM_CheckFirmware	Detects any device that is not using the default firmware load. Replaces the need to launch the Cisco CallManager Administration Web page in order to determine the same information.
CCM_CpuHigh	Monitors CPU usage for CallManager processes.
CCM_DeviceStatus	Monitors the status of up to 100 key phones within a cluster.
CCM_EventLog	Monitors event log entries from CallManager during the past *n* hours.
CCM_FXOPorts	Monitors active and in-service FXO ports for a CallManager.
CCM_FXSPorts	Monitors active and in-service FXS ports for a CallManager.
CCM_HealthCheck	Monitors the status of CallManager services.
CCM_HeartBeat	Monitors the CallManager heartbeat. A low heartbeat indicates the CallManager service was stopped and then restarted.

Knowledge Script	What It Does
CCM_MemByProcess	Monitors individual memory use for each specified process, and the total memory use for all specified processes.
CCM_MemoryHigh	Monitors memory usage and memory pool usage of specified CallManager processes.
CCM_MOHUnavailable	Monitors the number of times an attempt was made to allocate a Music On Hold resource when all MOH servers were active or when no MOH servers were registered.
CCM_PhoneCheck	Monitors your CallManager network for new and missing phones.
CCM_PhoneInventory	Takes an inventory of phones based on specified search criteria. You can choose to write the results to a file.
CCM_PRIChannels	Monitors active and in-service PRI channels for a CallManager.
CCM_Replication	Queries for failed actions in the history tables of the replication agents on the CallManager Publisher.
CCM_ResetDevice	Resets one or more devices in order for the devices to pick up new default firmware.
CCM_RestartService	Schedules a CallManager service to stop and then restart after a specified interval.
CCM_RoleStatus	Determines whether a CallManager's status is Primary or Backup. A Backup is defined as any CallManager with no registered phones (hardware or software).
CCM_SecureWebPageCheck	Monitors the ccmadmin and ccmuser Web pages for Cisco CallManager 4.1 and later.
CCM_SystemPerformance	Monitors call throttling, signals in queue, and severe and warning call-throttling states for a CallManager.
CCM_SystemUsage	Monitors average CPU and memory usage for all monitored CallManagers.
CCM_T1Channels	Monitors active and in-service T1-CAS channels for a CallManager.
CCM_WebPageCheck	Monitors up/down status and round-trip time for the ccmadmin and ccmuser Web pages. If you are monitoring CallManager 4.1 or later, use CCM_SecureWebPageCheck.
CDRQuery	Queries the CDR table on the CallManager Publisher.
CiscoBackupStatus	Monitors the status of the Cisco Backup Utility program (stiBack.exe) and the Cisco BARS program.
ConfBridgeActiveConf	Monitors active conferences for a Conference Bridge.
ConfBridgeActiveStreams	Monitors active streams for a Conference Bridge.
ConfBridgeAvailStreams	Monitors available streams for a Conference Bridge.
ConfBridgeConferences (page 100)	Monitors completed conferences for a Conference Bridge.
ConfBridgeStreams	Monitors streams on completed conferences for a Conference Bridge.
CTI_Manager	Monitors CTI Manager connections, open devices, open lines, and active CallManager links.

Knowledge Script	What It Does
DigitalOutboundBusy	Monitors the number of times during an interval that a call through a Digital Access was attempted when no ports were available.
DigitalPortsActive	Monitors active digital ports.
DigitalPortsOutOfService	Monitors out-of-service digital ports.
H323CallActivity	Monitors call activity on an H.323 device.
H323CallsAttempted	Monitors attempted calls for an H.323 device.
H323CallsInProgress	Monitors in-progress calls for an H.323 device.
IIS_CpuHigh	Monitors CPU usage for IIS application processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors CPU usage of the dllhost and MTX processes.
IIS_MemoryHigh	Monitors memory usage and memory pool usage of specified IIS applications.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors discovered Web sites and Web services uptime.
LineStatus	Monitors active calls for an individual line.
LocationBandwidth	Monitors the bandwidth statistics for a Location resource that has been defined in CallManager.
LocationOutOfBandwidth	Monitors the number of times calls through a Location failed due to lack of bandwidth.
LossOfHardwarePhones	Monitors registered hardware phones.
MGCP_FXO	Monitors call activity for MGCP FXO devices.
MGCP_FXS	Monitors call activity for MGCP FXS devices.
MGCP_Gateway_CCM30	Monitors station ports and voice channels for CallManager 3.0 MGCP gateway devices.
MGCP_Gateway_CCM31	Monitors station ports and voice channels for CallManager 3.1 (and higher) MGCP gateway devices.
MGCP_GatewayCheck	Monitors for new or missing MGCP gateways.
MGCP_PRI	Monitors call activity and data link availability for MGCP PRI devices.
MGCP_PRI_Channels	Monitors active and out-of-service channels for MGCP PRI devices.
MGCP_T1CAS	Monitors call activity and data link availability for MGCP T1-CAS devices.
MGCP_T1CAS_Channels	Monitors active and out-of-service channels for MGCP T1-CAS devices .
MLA_Logins	Scans the CallManager MLA log file for successful and failed logins during a specified interval.
MOHDevice	Monitors active and available resources for Music On Hold devices.
MOHServer	Monitors active and available streams for Music On Hold servers.

Knowledge Script	What It Does
MOHServer_LostConnections	Monitors lost connections for Music On Hold servers.
MTP_Device	Monitors active and available resources for a Media Termination Point device.
MTPActiveConnections	Monitors active connections for a Media Termination Point.
MTPActiveStreams	Monitors active streams for a Media Termination Point.
MTPAvailableStreams	Monitors available streams for a Media Termination Point.
MTPCompletedConnections	Monitors completed connections for a Media Termination Point.
MTPCompletedStreams	Monitors streams on completed connections for a Media Termination Point.
MTPsActive	Monitors active Media Termination Points.
MTPsAvailable	Monitors available Media Termination Points.
MTPsUnavailable	Monitors the number of times during an interval a Media Termination Point allocation was requested when none was available.
MulticastConfActive	Monitors active Multicast conferences.
MulticastConfAvailable	Monitors the number of new Multicast conferences that can be started.
MulticastConfCompleted	Monitors completed Multicast conferences.
MulticastConfPhones	Monitors active Multicast participants.
MulticastConfUnavailable	Monitors the number of times during an interval a Multicast conference was requested when none was available.
QRTEvent	Monitors the log files of the Quality Reporting Tool and starts a diagnostic action if a QRT request has been logged.
RegAnalogAccesses	Monitors registered analog accesses.
RegCtiPorts	Monitors CTI ports registered to the local CallManager.
RegDigitalAccesses	Monitors registered digital accesses.
RegHardwarePhones	Monitors registered hardware phones.
RegMGCPGateways	Monitors registered MGCP gateways.
RegOtherDevices	Monitors registered station devices using the SCCP protocol that are not hardware phones.
Report_CallActivity	Summarizes data relating to attempted and completed calls.
Report_CallQualityDailyAvg	Summarizes key call quality data: jitter, latency, and lost data.
Report_CallsByHour	Displays the number of active calls for all selected CallManagers.
Report_ClusterAvgValueByHr	Displays the average values by hour of the data stream(s) for all selected CallManager clusters.
Report_ClusterAvgValueByMin	Displays the average values by minute of the data stream(s) for the selected CallManager cluster.

Knowledge Script	What It Does
Report_ClusterGenCounter	For a selected CallManager cluster, displays the average, maximum, and minimum values of each data stream, and the actual data values of each data stream over time.
Report_ClusterSystemUsage	For a selected CallManager cluster, displays the average CPU and memory usage per CallManager.
Report_MGCPChannelUsage	Displays the number of total active and out-of-service voice channels for a particular MGCP PRI Group.
Report_MGCPDeviceUtil	Displays outbound busy attempts and completed calls for a particular MGCP device.
Report_MGCPGatewayUsage	Displays the number of active MGCP PRI Voice Channels for a particular gateway.
Report_ServicesAvailability	Summarizes the availability of the services most relevant to the selected CallManagers.
Report_SystemUsage	Displays the average CPU and memory usage for the selected CallManagers.
SQL_Accessibility	Monitors SQL Server and database accessibility.
SQL_BlockedProcesses	Monitors SQL processes that have been blocked for more than the specified period of time.
SQL_CPUUtil	Monitors CPU resources used by sqlservr and sqlagent processes.
SQL_DataGrowthRate	Monitors data growth and shrink rates for all SQL Server databases.
SQL_DataSpace	Monitors available data space and used data space in a SQL Server 7.0 database.
SQL_DBGrowthRate	Monitors database growth and shrink rates.
SQL_DbOption	Checks the database option.
SQL_DBSpace	Monitors available database space and used database space in a SQL Server 7.0 database.
SQL_Errorlog	Monitors the SQL Server error log.
SQL_LogGrowthRate	Monitors log growth and shrink rates for all SQL Server databases.
SQL_LogSpace	Monitors available log space and log data space in a SQL Server 7.0 database.
SQL_MemUtil	Monitors the percentage of memory used by `sqlservr` and `sqlagent` processes.
SQL_NearFileMaxSize	Monitors the size of all SQL Server database files.
SQL_NearMaxConnect	Monitors the percentage of used user connections.
SQL_NearMaxLocks	Monitors the lock usage of SQL Server.
SQL_NetError	Monitors SQL Server network packet errors.
SQL_RepTransactions	Monitors transactions in the transaction log of the publication database that are marked for replication but have not been replicated.
SQL_RepTranSec	Monitors transactions being replicated per second.

Knowledge Script	What It Does
SQL_RestartServer	Restarts a down SQL Server.
SQL_ServerDown	Monitors the up-and-down status of SQL Server.
SQL_ServerThroughput	Monitors the throughput of SQL Server by measuring the number of T-SQL batch requests executed per second and the number of physical page reads per second.
SQL_TopIOUsers	Monitors I/O read-and-write operations used by SQL Server users and their connections.
SQL_TopLockUsers	Monitors locks held by all SQL Server users and their connections.
SQL_TopMemoryUsers	Monitors the memory that can be allocated to all SQL Server users and their connections in 2-KB pages.
SQL_UserConnections	Monitors SQL Server user connections.
StreamAppIOCTLErr	Monitors the number of times in an interval an IOCTL error was detected.
StreamAppMissDDErr	Monitors the number of times in an interval a missing device driver error was detected.
TftpChangeNotify	Monitors handled TFTP change notifications.
TftpErrors	Monitors TFTP-related errors.
TftpHeartBeat	Monitors the Cisco TFTP heartbeat.
TftpRequests	Monitors handled TFTP requests.
TftpSegmentPctLost	Monitors lost TFTP segments.
TftpSegmentsSent	Monitors sent TFTP segments.
TraceArchive	Archives CallManager trace files to prevent losing files when tracing wraps.
TraceEvent	Scans CallManager trace files for entries that match a text string you specify.
Transcoder_Device	Monitors active and available resources for an individual transcoder device.
TranscoderResources	Monitors transcoder resources between the G.711, G.723, and G.729 codecs.
TranscoderUnavailable	Monitors the number of times during a specified period a transcoder resource was requested when none was available.
UnicastConfActive	Monitors active Unicast conferences.
UnicastConfAvailable	Monitors the number of new Unicast conferences that can be started.
UnicastConfBridge_Device	Monitors active and available resources for an individual software or hardware conference bridge device.
UnicastConfComplete	Monitors completed Unicast conferences.
UnicastConfParticipants	Monitors active Unicast participants.
UnicastConfUnavailable	Monitors the number of times in an interval a Unicast conference was requested when none was available.

Knowledge Script	What It Does
VerifyPasswords	Verifies the sa, Administrator, and Directory Manager passwords on a CallManager computer.
Recommended Knowledge Script Groups	Run all recommended Knowledge Scripts at one time.

4.1 AnalogOutboundBusy

Use this Knowledge Script to monitor the number of times a call was attempted through an analog access when no ports were available. This script raises an event if the number of outbound busy attempts exceeds the threshold. In addition, this script generates a data stream for outbound busy attempts.

4.1.1 Resource Object

CCM Analog Access object

4.1.2 Default Schedule

By default, this script runs every 30 minutes.

4.1.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of outbound busy attempts exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about outbound busy attempts for reports and graphs. The default is n.
Threshold - Maximum outbound busy attempts	Specify the maximum number of outbound busy attempts can occur before an event is raised. The default is 100 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of outbound busy attempts exceeds the threshold. The default is 25.

4.2 AnalogPortsActive

Use this Knowledge Script to monitor the number of active ports. This script raises an event if the number of active ports exceeds the threshold. In addition, this script generates a data stream for the number of active ports.

4.2.1 Resource Object

CCM Analog Access object

4.2.2 Default Schedule

By default, this script runs every 30 minutes.

4.2.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active ports exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active ports for reports and graphs. The default is n.
Threshold - Maximum active ports	Specify the maximum number of ports that can be active before an event is raised. The default is 20 ports.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active ports exceeds the threshold. The default is 25.

4.3 AnalogPortsOutOfService

Use this Knowledge Script to monitor the number of ports that are out of service. This script raises an event if the number of out-of-service ports exceeds the threshold. In addition, this script generates a data stream for out-of-service ports.

4.3.1 Resource Object

CCM Analog Access object

4.3.2 Default Schedule

By default, this script runs every 30 minutes.

4.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-service ports exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about out-of-service ports for reports and graphs. The default is n.
Threshold - Maximum out-of-service ports	Specify the maximum number of ports that can be out of service before an event is raised. The default is 2 ports.

Parameter	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-service ports exceeds the threshold. The default is 15.

4.4 CallActivity

Use this Knowledge Script to monitor call activity (attempted, completed, and incomplete) during a specified time range.

This script collects the data used by the Report_CallActivity Knowledge Script.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.4.1 Resource Object

CCM Call Processor

4.4.2 Default Schedule

By default, this script runs once each day.

4.4.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data about call activity for reports and graphs. The default is y.
Monitor completed calls?	Set to **y** to monitor completed calls. The default is y.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 500 calls.
Event severity when completed calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which completed calls exceed the threshold. Enter **0** if you do not want to raise an event. The default is 25.
Monitor attempted calls?	Set to **y** to monitor attempted calls, such as calls that received a busy signal or in instances when users leave the handset off the phone. The default is y.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 500 calls.
Event severity when attempted calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which attempted calls exceed the threshold. Enter **0** if you do not want to raise an event. The default is 25.
Monitor incomplete calls?	Set to **y** to monitor incomplete calls, such as calls that were attempted but did not complete or are not currently in progress. The default is y.

Parameter	How to Set It
Threshold - Maximum incomplete calls	Specify the maximum percentage of incomplete calls can occur before an event is raised. The default is 75%.
Event severity when incomplete calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of incomplete calls exceeds the threshold. Enter **0** if you do not want to raise an event. The default is 25.

4.5 CallFailures

Use this Knowledge Script to monitor the Call Detail Records (CDR) in the CallManager Publisher database for calls that ended with an abnormal cause code.

If a Subscriber loses its connection to a Publisher, it will store its CDR data locally until the connection is restored. If the connection is not restored within the collection interval, this script may not monitor some calls.

NOTE: CallManager does not collect CDR records by default. You must enable the collection of CDRs for each CallManager is a cluster. From the Cisco CallManager Administration Web page, navigate to **Service > Service Parameters > CallManager**. Set the **CdrEnabled** parameter to **T**.

4.5.1 Resource Object

CCM Publisher

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
Raise event if failed calls exceed the threshold?	Set to **y** to raise an event if the number of failed calls exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n. This parameter collects the total number of failed calls found during the time period you specify in the *Start time*, *Start date*, *Stop time*, and *Stop date* parameters. **NOTE**: Some third-party billing applications remove CDR records from the CallManager database. If records are removed before the CallFailures script has a chance to run, the script will not collect any data.

Parameter	How to Set It
CallManager database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Use Windows authentication?	Set to **y** to use Windows authentication to access the Publisher database. If you enable this parameter, the SQL user name is ignored. The `NetIQmc` service must be running with the proper authentication to access the database. The default is Yes.
Threshold - Maximum failed calls	Specify the maximum number of calls that can fail before an event is raised. The default is 0 calls. **NOTE**: You can trigger NetIQ Vivinet Diagnostics to diagnose the problem indicated by an event in which this threshold is exceeded. For more information, see Section 4.5.4, "Diagnosing VoIP Quality," on page 37.
Include call details?	Set to **y** to include call details in the event message. The default is y. If set to y, the event message includes details for up to 50 calls. The call details can include any or all of the following: ◆ Originator termination cause ◆ Destination termination cause ◆ Originating Party Device Name (if running on CallManager 3.1 or later) ◆ Originating Party Directory Number ◆ Originating Party Partition ◆ Originating Party CallManager Node ID ◆ Originating Party IP address ◆ Originating Party codec ◆ Destination Party Device Name (if running on CallManager 3.1 or later) ◆ Destination Party Directory Number ◆ Destination Party Partition ◆ Destination Party CallManager Node ID ◆ Destination Party IP address ◆ Destination Party codec ◆ Time the call was connected ◆ Time the call was disconnected ◆ Call duration

Parameter	How to Set It
Directory number to filter by	Provide a directory number by which to filter the calls that get monitored. The default is to monitor all calls. You can specify a group of directory numbers by using the % wildcard. For example, to monitor all the directory numbers that begin with 31, enter 31%. **NOTE**: This parameter returns results only if the directory number you enter is the originator's number. No results are returned if you enter the destination number.
Exclude these failure codes	Provide a comma-separated list of termination codes that are not to be considered failures. For more information, see Section 4.5.5, "Termination Codes," on page 37. **NOTE**: Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Minimum call duration	Specify the minimum number of seconds for which a call must be connected before the script checks whether the call has failed and includes it in the query. The default is 0 seconds.
Start date	Specify the date on which you want to start the query. This parameter is valid only when you select **Run Once** on the Schedule tab.
Start time	Specify the time at which you want to start the query. This parameter is valid only when you select **Run Once** on the Schedule tab.
Stop date	Specify the date on which you want to stop the query. This parameter is valid only when you select **Run Once** on the Schedule tab.
Stop time	Specify the time at which you want to stop the query. This parameter is valid only when you select **Run Once** on the Schedule tab.
Query timeout	Specify the maximum number of seconds it can take a query to run. The default is 10 seconds. **NOTE**: The script runs three queries in order to get data for each interval.
Monitoring offset	Because CallManager can have a delay when writing records to the database, a query may not return any call failures if the script is monitoring only the past few seconds. Use this parameter to have the script offset the monitoring period in order to capture those failures that occurred earlier. The default is 45 seconds. For example, if the delay for writing CDR data to the database is 10 minutes, enter 600 in this field. The script will then query for calls that ended 10 minutes ago, rather than for calls that ended at the current time.
Event severity when failed calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Event severity when no records found	Set the severity level for an event in which the query finds no records. This is not the same event as finding no failed calls; this means there were no CDR records in the database for the given query. Accept the default of **0** if you do not want to raise an event. **NOTE**: Set this parameter only to verify CDRs are actually being collected in a timely manner.

4.5.4 Diagnosing VoIP Quality

You can trigger NetIQ Vivinet Diagnostics to run a diagnosis of VoIP quality between two phones or two endpoints. A diagnosis is performed when one of the following Knowledge Scripts determines VoIP quality or call quality is poorer than a specified threshold:

- CallQuality. Vivinet Diagnostics can diagnose the problem when jitter, latency, and percentage of lost data exceed their thresholds.
- CallFailures. Vivinet Diagnostics can diagnose the problem when the number of failed calls exceeds its threshold.

The Action script runs by default only if Vivinet Diagnostics version 1.1 or later is installed on the computer on which the script is running.

For more information about Vivinet Diagnostics and VoIP quality diagnoses, see the *User Guide for Vivinet Diagnostics*

and the Help for the Action_DiagnoseVoIPQuality Knowledge Script.

To trigger Vivinet Diagnostics:

1. On the Actions tab, click **Properties**.
2. Enter values for all parameters. For more information about the parameter values, click **Help** on the Properties for Action_DiagnoseVoIPQuality dialog box.
3. Continue entering values on the other tabs of the Properties dialog box, or click **OK** to run the job.

4.5.5 Termination Codes

Termination Code	Description	Explanation
0	No error	No error.
1	Unallocated (unassigned) number	Indicates the called party cannot be reached because, although the called party number is in a valid format, it is not currently allocated (assigned).
2	No route to specified transit network (national use)	Indicates one of the following: ◆ The equipment sending this code has received a request to route the call through a particular transit network it does not recognize. The equipment does not recognize the transit network either because the transit network does not exist or because the transit network exists but does not serve the equipment that is sending the code. ◆ The prefix 0 is invalid for the entered number.
3	No route to destination	Indicates one of the following: ◆ The called party cannot be reached because the network through which the call has been routed does not service the desired destination. This cause is supported on a network-dependent basis. ◆ A 1 was dialed when not required. Redial without the 1.

Termination Code	Description	Explanation
4	Send special information tone	Indicates one of the following: ◆ The prefix 1 is not required for this number. ◆ The called party cannot be reached for reasons are of a long-term nature. The special information tone should be returned to the calling party.
5	Misdialed trunk prefix (national use)	Indicates the erroneous inclusion of a trunk prefix in the called party number.
6	Channel unacceptable	Indicates a called user cannot negotiate for a B-channel other than that specified in the SETUP message.
7	Call awarded and being delivered in an established channel	Indicates the user has been awarded the incoming call and Indicates the call is being connected to a channel (such as packet mode or X.25 virtual calls) already established to that user for similar calls.
8	Pre-emption	Indicates a call has been preempted.
9	Preemption - circuit reserved for reuse	Indicates a call has been preempted because the circuit is reserved for reuse.
16	Normal call clearing	Indicates normal call clearing has occurred.
17	User busy	Indicates the called party is unable to accept another call because the user busy condition has been encountered. Code 17 may be generated by the called user or by the network. In the case of user-determined user busy, it is noted the user equipment is compatible with the call.
18	No user responding	Indicates a called party does not respond to a call establishment message with either an alerting or connect indication within the allotted prescribed period of time (before timer T303 or T310 has expired).
19	No answer from user (user alerted)	Indicates the called user has provided an alerting indication, but not a connect indication within a prescribed period of time (before timer T301 has expired).
20	Subscriber absent	Indicates one of the following:· ◆ A mobile station has logged off. ◆ Radio contact is not obtained with a mobile station. ◆ A personal telecommunications user is temporarily not addressable at any user-network interface.
21	Call rejected	Indicates one of the following: ◆ The equipment sending this cause does not wish to accept the call, although it could have accepted the call because it is neither busy nor incompatible. ◆ May be generated by the network, indicated the call was cleared due to a supplementary service constraint.
22	Number changed	Indicates the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause, cause #1 shall be used.

Termination Code	Description	Explanation
26	Non-selected user clearing	Indicates the user has not been awarded the incoming call.
27	Destination out of order	Indicates the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" Indicates a signal message was unable to be delivered to the remote party, as in the following examples: ◆ Physical layer or data link layer failure at the remote party ◆ User equipment off-line
28	Invalid number format (address incomplete)	Indicates one of the following: ◆ The called party cannot be reached because the called party number is not in a valid format or is not complete. ◆ The user should be returned a Special Intercept Announcement.
29	Facility rejected	Indicates one of the following: ◆ The network cannot provide the requested facility. ◆ A user in a special business group, such as a Centrex, dialed an undefined code.
30	Response to STATUS ENQUIRY	Indicates one of the following: ◆ This cause is included in the Status Message when the reason for sending the Status Message was the previous receipt of a Status Enquiry message. ◆ A user from outside a basic business group, such as a Centrex, has violated an access restriction feature.
31	Normal, unspecified	Used to report a normal event only when no other cause in the normal class applies.
34	No circuit/channel available	Indicates no appropriate circuit or channel is available to handle the call.
38	Network out of order	Indicates the network is not functioning correctly and the condition is likely to last a relatively long time. Immediately re-attempting the call is not likely to be successful.
39	Permanent frame mode connection out of service	Indicates a permanent connection was terminated, probably due to equipment failure.
40	Permanent frame mode connection operational	Indicates a permanent connection is operational again. The connection was previously terminated, probably due to equipment failure.

Termination Code	Description	Explanation
41	Temporary failure	Indicates the network is not functioning correctly and the condition is not likely to last a long time. The user may wish to attempt another call almost immediately. May also indicate a data link layer malfunction locally or at the remote network interface, or a call was cleared due to protocol error(s) at the remote network interface.
42	Switching equipment congestion	Indicates the switching equipment generating this cause is experiencing a period of high traffic.
43	Access information discarded	Indicates the network is unable to deliver user information (such as user-to-user information, low-level compatibility, or sub-address) to the remote users as requested.
44	Requested circuit/ channel not available	Indicates the other side of the interface cannot provide the circuit or channel indicated by the requesting entity.
46	Precedence call blocked	Indicates the remote device that was called is busy.
47	Resource unavailable, unspecified	Indicates one of the following: ◆ No other cause in the resource unavailable class applies. ◆ The original destination is unavailable. Invoke redirection to a new destination.
49	Quality of Service not available	Indicates the network cannot provide the requested Quality of Service. May be a subscription problem.
50	Requested facility not subscribed	Indicates this facility is unavailable because the user has not subscribed to it.
53	Service operation violated	Indicates the user has violated the service operation.
54	Incoming calls barred	Indicates the user will not accept the call delivered in the SETUP message.
55	Incoming calls barred within CUG (Closed User Group)	Indicates the network does not allow the user to receiver calls.
57	Bearer capability not authorized	Indicates the user has requested a bearer capability that is implemented by the equipment that generated this cause, however the user is not authorized to use it. This common problem is caused by incorrect Telco provisioning of the line at the time of installation.
58	Bearer capability not presently available	Indicates the user has requested a bearer capability that is implemented by the equipment that generated this cause, however the bearer capability is unavailable at the present time. This problem may be due to a temporary network problem or a subscription problem.
62	Inconsistency in designated outgoing access information and subscriber class	Indicates an inconsistency in the designated outgoing access information and subscriber class.

Termination Code	Description	Explanation
63	Service or option not available, unspecified	Indicates a service or option is not available. Used only when no other cause in this class applies.
65	Bearer capability not implemented	Indicates the equipment sending this cause does not support the requested bearer capability.
66	Channel type not implemented	Indicates the called party has reached an unsupported channel type.
69	Requested facility not implemented	Indicates the network (or node) does not support the requested bearer capability and therefore cannot be accessed at this time.
70	Only restricted digital information bearer capability is available (national use)	Indicates the calling party has requested an unrestricted bearer service, however the equipment sending this cause only supports the restricted version of the requested bearer capability.
79	Service or option not implemented, unspecified	Indicates a service or option was not implemented. Used only when no other cause in this class applies.
81	Invalid call reference value	Indicates the equipment sending this cause has received a message with a call reference that is not currently in use on the user-network interface. This value applies only if the call reference values 1 or 2 octets long and is not the global call reference.
82	Identified channel does not exist	Indicates the equipment sending this cause has received a request to use a channel that is not active on the interface for a call.
83	A suspended call exists, but this call identity does not	Indicates a suspended call exists but the call's identity does not.
84	Call identity in use	Indicates a call identity is in use.
85	No call suspended.	Indicates no call is suspended.
86	Call having the requested call identity has been cleared	Indicates the call having the requested call identity has cleared.
87	User not member of CUG (Closed User Group)	Indicates the call was not completed, probably due to one of the following reasons: ◆ The dialed number is incorrect ◆ The user is not authorized to use (or has not subscribed to) the requested service ◆ User is using a service that the remote device is not authorized to use
88	Incompatible destination	Indicates the equipment sending this cause has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (such as data rate or DN subaddress), which cannot be accommodated. This call can be returned by a switch to a CPE when trying to route a call to an incompatible facility, or one without a data rate.

Termination Code	Description	Explanation
90	Destination number missing and DC not subscribed Nonexistent CUG (Closed User Group)	Indicates the call was not completed, probably due to one of the following reasons: ◆ The dialed number is incorrect ◆ The user is not authorized to use (or has not subscribed to) the requested service ◆ User is using a service that the remote device is not authorized to use
91	Invalid transit network selection (national use)	Indicates an invalid transit network selection has been requested.
95	Invalid message, unspecified	Indicates the entity sending this cause has received an invalid message. Used when no other cause in this class applies.
96	Mandatory information element is missing	Indicates the equipment sending this cause has received a message that is missing an information element that must be present in the message before the message can be processed.
97	Message type non-existent or not implemented	Indicates one of the following: ◆ The equipment sending this cause has received with a message type it does not recognize. Either the message is not defined, or it is defined and not implemented by the equipment sending this cause. ◆ A problem with the remote configuration or with the local D-channel.
98	Message is not compatible with the call state, or the message type is non-existent or not implemented	Indicates one of the following: ◆ Message received is not compatible with the call state ◆ Message type is non-existent or not implemented
99	An information element or parameter does not exist or is not implemented	Indicates the equipment sending this cause has received a message that includes information elements not recognized because either the information element identifier is not defined, or it is defined but not implemented by the equipment sending the cause. However, the information element is not required for the equipment sending the cause to process the message.
100	Invalid information element contents	Indicates the equipment sending this cause has received an information element it has implemented. However, one or more fields of the information elements are coded in such a way (such as truncated, invalid extension bit, invalid field values) that the information element has not been implemented by the equipment that is sending this cause.

Termination Code	Description	Explanation
101	The message is not compatible with the call state	Indicates one of the following: ◆ The equipment sending this cause has received a message the procedures indicate is not a permissible message to receive at this time. ◆ The switch sending this cause is clearing the call because a threshold has been exceeded for multiple protocol errors during an active call.
102	The call was terminated when a timer expired and a recovery routine was executed to recover from the error	Indicates a procedure has been initiated by the expiration of a timer in associated with error-handling procedures.
103	Parameter non-existent or not implemented - passed on (national use)	Indicates the equipment sending this cause has received a message that includes parameters not recognized because the parameters are defined but not implemented by the equipment sending the cause. The parameters were ignored. In addition, if the equipment sending this cause is an intermediate point, this cause Indicates the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates the equipment sending this cause has discarded a received message that includes a parameter that is not recognized.
111	Protocol error, unspecified	Reports a protocol error event only when no other cause in this class applies.This cause may be displayed if the user failed to dial a 9 or an 8 for an outside line. In addition, this cause may be returned in the event of certain types of restrictions as to number of calls.
126	Call split	A Cisco-specific code. Indicates a call was terminated during a transfer operation because it was split off and terminated (not part of the final transferred call). This code can help determine which calls were terminated as part of a transfer operation.
127	Internetworking, unspecified	Indicates an internetworking call (usually a call to SW56 service) has ended. May also be seen in the event of a non-specific rejection by a long distance carrier.

4.6 CallQuality

Use this Knowledge Script to monitor Call Management Records (CMRs) for information about the amount of data that is sent and received, and for information about jitter, latency, lost data, and listening MOS.

This script raises an event if a monitored value exceeds or falls below the threshold you set. In addition, this script generates data streams for average jitter, latency, lost data (%), and average and minimum listening MOS.

Cisco CallManager defines lost data, jitter, latency, and listening MOS as follows:

- *Lost data* equals the total number of real-time transport protocol (RTP) data packets that have been lost since the beginning of reception. This number is defined as the number of packets that were expected minus the number of packets that were 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. AppManager records any negative value as zero (0).
- *Jitter* is an estimate of the statistical variance of the RTP data packet interarrival time, measured in milliseconds and expressed as an unsigned integer. Interarrival jitter is the mean deviation (smoothed absolute value) of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
- *Latency* is an estimate of network latency, expressed in milliseconds. Latency is the average value of the difference between the NTP time stamp indicated by the senders of the RTCP messages and the NTP timestamp of the receivers, measured when the messages are received. In a CMR, the average is obtained by adding all of the estimates, then dividing by the number of RTCP messages that have been received.
- *Listening MOS* (Mean Opinion Score) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. In a CMR, the MOS is based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec. The term "listening" indicates the MOS value does not include "conversational" characteristics such as delay.

NOTE

- When a Subscriber loses its connection to the Publisher, it stores its CMR data locally until the connection is restored. If the connection is not restored within the collection interval, this script may not monitor some calls.
- When a Subscriber is flooded with calls, it throttles the number of calls that get returned to the Publisher at one time; some calls may not get monitored.
- The clocks on the Subscriber must be synchronized with those of the Publisher.
- CallManager writes CMRs only for Cisco IP phones and for gateways that use the MGCP (Media Gateway Control Protocol) to interface with CallManager.

4.6.1 Resource Object

CCM Publisher. Although you can run this script on the parent CallManager object, it will actually run only on the Publisher.

4.6.2 Default Schedule

By default, this script runs every five minutes.

4.6.3 Troubleshooting Hint

You can use this script as a troubleshooting tool for checking problems with an individual extension. Set the Schedule to "Run Once," set *Maximum acceptable jitter* to "**0**," set *Include call details* to "**Yes**," set *Call disconnect time range* to cover the time when the poor quality calls occurred, and set *Directory number to filter by* to the extension that has the problems. The details that are returned will include the IP address of the phone extension displayed as a link. If the phone supports it, click on this link to reveal some lower-level details about the phone.

4.6.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CallQuality job fails. The default is 5.
CallManager database user name	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Use Windows authentication?	Select **Yes** to use Windows authentication to access the Publisher database. If you enable this parameter, the SQL user name is ignored. The `NetIQmc` service must be running with the proper authentication to access the database. The default is Yes.

Parameter	How to Set It
Include call details?	Select **Yes** to include details for up to 50 calls in the Message tab of the Event Properties dialog box. The default is Yes. The call details can include any or all of the following: ◆ Originating Party Device Name (If running on CallManager 3.1)· ◆ Originating Party Directory Number ◆ Originating Party Partition ◆ Originating Party CallManager Node ID ◆ Time the call was completed ◆ Jitter ◆ Latency ◆ Lost Data Percentage ◆ Packets Sent ◆ Packets Received ◆ Packets Lost ◆ Originating Party IP address ◆ Originating Party codec ◆ Destination Party Device Name (If running on CallManager 3.1) ◆ Destination Party Directory Number ◆ Destination Party Partition ◆ Destination Party CallManager Node ID ◆ Destination Party IP address ◆ Destination Party codec ◆ Call Duration
Monitor Jitter, Latency, and Percent Lost Data	
Event Notification	
Raise event if jitter, latency, or percent lost data exceeds threshold?	Select **Yes** to raise an event if the jitter, latency, or percent lost data values exceed the thresholds you set. The default is Yes.
Threshold - Maximum acceptable jitter	Specify the maximum amount of jitter that must occur before an event is raised. The default is 60 milliseconds. **NOTE**: You can trigger Vivinet Diagnostics to diagnose the problem indicated by an event in which the jitter threshold is exceeded. For more information, see Section 4.5.4, “Diagnosing VoIP Quality,” on page 37.
Threshold - Maximum acceptable latency	Specify the maximum amount of latency that must occur before an event is raised. The default is 400 milliseconds. **NOTE**: You can trigger Vivinet Diagnostics to diagnose the problem indicated by an event in which the latency threshold is exceeded. For more information, see Section 4.5.4, “Diagnosing VoIP Quality,” on page 37.

Parameter	How to Set It
Threshold - Maximum acceptable percent lost data	Specify the maximum percentage of data that must be lost before an event is raised. The default is 1%. **NOTE**: You can trigger Vivinet Diagnostics to diagnose the problem indicated by an event in which the percentage lost data threshold is exceeded. For more information, see Section 4.5.4, “Diagnosing VoIP Quality,” on page 37.
Threshold - Minimum lost packets, if lost data threshold is exceeded	Set this threshold *only* if you set a threshold for *Maximum acceptable percent lost data*. Use this parameter on occasions when lost data does exceed the threshold you set, but you do not want to raise an event unless a specific number of packets has also been lost. The default is 0 packets. For example, you have set *Maximum acceptable percent lost data* to 10%, and you have set this parameter to 5 packets. If the amount of lost data is 15%, but the number of lost packets is only 2, no event is raised. An event is raised only if the percentage of lost data AND the number of lost packets exceed the thresholds you set.
Event severity if jitter, latency, or percent lost data exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which one or more of the jitter, latency, and lost data thresholds have been exceeded. The default is 15.
Data Collection	
Collect data for jitter, latency, and percent lost data?	Select **Yes** to collect data for reports and graphs. If enabled, data collection generates data streams for average jitter, latency, and percent lost data for the monitoring interval. **NOTE**: Some third-party billing applications remove CDR records from the CallManager database. If records are removed before the CallQuality script has a chance to run, the script will not collect any data.
Monitor Listening MOS	
Monitor Average Listening MOS	
Event Notification	
Raise event if average listening MOS for any call falls below threshold?	Select **Yes** to raise an event if the average listening MOS for any call falls below the threshold you set. The default is Yes.
Threshold - Average listening MOS	Specify the minimum value for average listening MOS that must occur for *any* call to prevent an event from being raised. The default is 3.60. Average listening MOS is defined as the running average of MOS scores (recorded at 8-second intervals) observed since the beginning of the call.
Event severity if average listening MOS for any call falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average listening MOS for any call falls below the threshold. The default is 15.
Data Collection	
Collect data for average listening MOS?	Select **Yes** to collect data for reports and graphs. If enabled, data collection generates a data stream for average listening MOS for the monitoring interval.

Parameter	How to Set It
Monitor Minimum Listening MOS	
Event Notification	
Raise event if minimum listening MOS for any call falls below threshold?	Select **Yes** to raise an event if the lowest listening MOS for any call falls below the threshold you set. The default is unselected.
Threshold - Minimum listening MOS	Specify the lowest listening MOS value that must occur for *any* call to prevent an event from being raised. The default is 3.60. Minimum listening MOS is defined as the worst of the MOS scores (recorded at 8-second intervals) observed since the beginning of the call.
Event severity if minimum listening MOS for any call falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the lowest listening MOS for any call falls below the threshold. The default is 15.
Data Collection	
Collect data for lowest listening MOS?	Select **Yes** to collect data for reports and graphs. If enabled, data collection generates a data stream for lowest listening MOS for the monitoring interval.
Query Filters	
Directory number to filter by	Specify a directory number to filter the calls that get monitored. The default is to monitor all calls. You can specify a group of directory numbers by using a '%' as a wildcard. For example, to monitor all the directory numbers that begin with 31, enter 31%. **NOTE**: This parameter returns results only if the directory number you enter is the originating number. No results are returned if you enter the destination number.
Minimum call duration filter	Use this parameter to filter out calls whose duration is less than the specified value. The default is 0 seconds.
No Records Found Notifications	
Event severity when no records found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no jitter, latency, or percent lost data records are found. Accept the default of **0** if you do not want to raise an event for this incident.
Event severity when no MOS records found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no MOS records are found. Accept the default of **0** if you do not want to raise an event for this incident.
Troubleshooting	
Select call disconnect time range	Select a **Specific** (fixed) or **Sliding** date/time range in which to search for call failures. The default is Specific.
Query timeout	Specify the maximum number of seconds it can take a query to run. The default is 10 seconds. **NOTE**: This script runs three queries in order to get data for each interval.

Parameter	How to Set It
Monitoring offset	Because CallManager can have a delay when writing records to the database, a query may not return any call failures if the script is monitoring only the past few seconds. You can choose to have the script offset the monitoring period in order to capture those failures that occurred earlier. The default is 45 seconds. For example, if the delay for writing CDR data to the database is 10 minutes, enter 600 in this field. The script will then query for calls that ended 10 minutes ago, rather than for calls that ended at the current time.

4.7 CallsActive

Use this Knowledge Script to monitor the number of active calls. This script raises an event if the number of active calls exceeds the threshold you set.

4.7.1 Resource Object

CCM Call Processor

4.7.2 Default Schedule

By default, this script runs once each day.

4.7.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active calls for reports and graphs. The default is n.
Threshold - Maximum active calls	Specify the maximum number of calls that can be active before an event is raised. The default is 500 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

4.8 CallsAttemptedByPhone

Use this Knowledge Script to monitor the number of calls attempted by an individual phone during an interval. This script raises an event if the number of attempted calls exceeds the threshold you set.

4.8.1 Resource Object

CCM Phone folder

4.8.2 Default Schedule

By default, this script runs every 30 minutes.

4.8.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about attempted calls for reports and graphs. The default is n.
Phones, separated by comma w/no space	Provide a comma-separated list of the names of the phones you want to monitor for attempted calls.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 100 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.9 CallsInProgress

Use this Knowledge Script to monitor the number of calls in progress and the percentage of in-progress calls that are active. A call is considered "in-progress" as soon as the receiver is lifted. A call is considered "active" once a connection is made.

This script raises an event if the number of in-progress calls exceeds the threshold or if the percentage of active in-progress calls falls below the threshold.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.9.1 Resource Object

CCM Call Processor

4.9.2 Default Schedule

By default, this script runs once each day.

4.9.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a monitored value exceeds or falls below the threshold you set. The default is y.

Parameter	How to Set It
Collect data for calls in progress?	Set to **y** to collect data about in-progress calls for reports and graphs. The default is n.
Threshold - Maximum calls in progress	Specify the maximum number of calls that can be in progress before an event is raised. The default is 100 calls.
Event severity when in-progress calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress calls exceeds the threshold. The default is 25.
Collect data for active calls?	Set to **y** to collect data about active in-progress calls for reports and graphs. The default is n.
Threshold - Minimum active calls	Specify the minimum percentage of calls that can be active before an event is raised. The default is 10%. **NOTE**: By seeing how many in-progress calls are active, you can determine whether any in-progress calls are simply stuck off-hook.
Event severity when active calls fall below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of active in-progress calls falls below the threshold. Accept the default of **0** if you do not want to raise an event.

4.10 CCM_CheckFirmware

Use this Knowledge Script to detect any device that has been configured with a non-default firmware load. This script returns the number of devices of each device type — the same information you would retrieve when accessing the Cisco CallManager Administration Web page.

This script does not determine which firmware load a device is running.

Only AppManager administrators should run this script.

4.10.1 Resource Object

CCM Publisher

4.10.2 Default Schedule

By default, this script runs once each day.

4.10.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Threshold - Maximum devices with non-default firmware load	Specify the maximum number of devices, from all selected device types, that can be configured for a non-default firmware load before an event is raised. The default is 0 devices.
Raise event when threshold is not exceeded?	Set to **y** to raise an event when the threshold is *not* exceeded. The default is y.

Parameter	How to Set It
Event severity when threshold is not exceeded	Set the event severity level to indicate the importance of an event in which the threshold is *not* exceeded. Enter **0** if you do not want to raise an event for this situation. The default is 25. For more information, see Section 4.10.4, “Event Messages for CCM_CheckFirmware,” on page 52.
Event severity when threshold is exceeded	Set the event severity level to indicate the importance of an event in which the threshold is exceeded. Enter **0** if you do not want to raise an event for this situation. The default is 15.
Check … types?	Set to n if you do not want to check any of the following types of devices. The default is y. ◆ Analog Access ◆ Analog Access WS-X6624 ◆ Cisco 12 S ◆ Cisco 12 SP ◆ Cisco 12 SP+ ◆ Cisco 30 SP+ ◆ Cisco 30 VIP ◆ Cisco IP Phone 7905 ◆ Cisco IP Phone 7910 ◆ Cisco IP Phone 7935 ◆ Cisco IP Phone 7940 ◆ Cisco IP Phone 7960 ◆ Cisco ATA 186 ◆ Cisco Conference Bridge WS-X6608 ◆ Digital Access WS-X6608 ◆ Digital Access+ ◆ Media Termination Point WS-X6608 ◆ VGC Gateway ◆ 14-Button Line Expansion Module

4.10.4 Event Messages for CCM_CheckFirmware

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

Devices using non-default firmware load exceed the threshold.

Explanation: The number of devices that are configured with a non-default firmware load is greater than the specified threshold. See the detailed event message for details of the devices not configured with a default firmware load.

Likely cause: Normal message when the threshold has been crossed.

Operator action: Notify your Cisco CallManager administrator that there are devices that are not configured for the default firmware load.

Internal error encountered.

Explanation: Errors were encountered while checking one or more of the selected devices. See the detailed event message for details about the error.

Likely cause: In most cases this message Indicates a COM interface was not available, either because the COM object has not been installed or is not registered.

Operator action: Verify the `dblx.dll` is installed and registered on the CallManager computer.

4.11 CCM_CpuHigh

Use this Knowledge Script to monitor the CPU resources that application processes are consuming. If application CPU utilization exceeds the thresholds you set, an event is raised. The script monitors CPU usage for each process individually and the total CPU usage for all processes. If a process is not found, the script assumes the process is not running, and reports zero as the CPU result.

4.11.1 Resource Object

CCM parent object

4.11.2 Default Schedule

By default, this script runs every 15 minutes.

4.11.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if any threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
Monitor the Cisco CallManager process?	Set to **y** to monitor the status of the Cisco CallManager process. The default is y.
Threshold - Maximum CPU for CallManager	Specify the maximum amount of CPU usage for the Cisco CallManager process that can occur before an event is raised. The default is 80%.
Monitor other Cisco processes?	Set to **y** to monitor the status of other Cisco processes. The default is n.
Threshold - Maximum CPU for other processes?	Specify the maximum amount CPU usage for other Cisco processes that can occur before an event is raised. The default is 20%.

4.12 CCM_DeviceStatus

Use this Knowledge Script to monitor the status of key devices within a cluster. The possible statuses are:

- **Registered**. This status indicates the device is available
- **Unregistered**. This status indicates a device that was previously registered with CallManager has become unregistered. This status may be generated as part of a normal unregistration event, or can be due to another reason such as loss of keepalives.
- **Rejected**. This status indicates CallManager has rejected the registration for the device. This script detects this status only if the device was at one time registered to the CallManager but a subsequent registration attempt was rejected.
- **Unknown**. This status indicates the device has not been registered to any CallManagers in the cluster for a long time, or the device was added to a CallManager but never registered, or the CallManager RIS service is not operational.

NOTE: Phones that are added while this script is running will not be monitored.

The first time you run this script, it builds a device list from the criteria you have selected. At each subsequent interval, the script checks the status of these devices. If the number or percentage of these devices that are registered does not meet the threshold you define, an event is raised. The device list is not rebuilt each time you run this script. Therefore, if you add a new device, delete a device, or change device details, the changes will *not* be picked up by this script unless you stop it and then restart it. If you delete a device, the status will change to "Unknown," but the device will remain in the list until you stop and restart the script.

If you enter multiple selection criteria and the selections find the same device or devices, there will be duplicate entries in the list of devices to be monitored. This is working as designed — if you select by directory numbers, and a device has more than one directory number, you will get duplicate entries for that device.

Different *Select By* choices will build different lists of devices to be monitored even if you select the same *Device Type*. For example, if you select *DeviceName*, the list will contain all of the directory numbers for each device with that device type. If you select *DirectoryNumber*, each row in the list will contain only a single directory number. If a device has multiple directory numbers, that device will be listed multiple times.

TIP: This script uses several COM modules. There is a one-time cost of about 7-10M of memory and CPU usage of around 30-40% the first time the script is run.

4.12.1 Prerequisite

This script relies on the CallManager RIS (Real-Time Information Server) function to be working properly. If this function is not working on all the CallManagers in a cluster, this script may not generate accurate results. Verify the Cisco Database Layer Monitor and the Cisco RIS Data Collector services are running on all the CallManagers in the clusters.

Cisco has documented the following for CallManager:

The Real-Time Information Server (RIS) collects, distributes, and maintains real-time Cisco CallManager information and provides an interface through which the Cisco RIS Data Collector service and the SNMP Agent retrieve that information. One RIS exists on each node that contains the

Cisco CallManager service. The Cisco RIS Data Collector service provides an interface for applications, such as Cisco CallManager Serviceability and the Cisco CallManager Administration, to retrieve information that is stored in all RIS nodes in the cluster.

- Cisco recommends the Cisco RIS Data Collector service reside on every server in the Cisco CallManager cluster.
- Cisco RIS Data Collector service requires the Cisco Database Layer Monitor service.

4.12.2 Examples of Using CCM_DeviceStatus

If you use centralized processing, you would benefit from using this script. You could monitor a group of devices at the remote site and then raise an event if a certain number of those devices were not registered.

In a second scenario, you could verify the phones in public places (such as conference rooms) have not been taken off the network. Many times, employees will use a public port for their laptops and forget to put the phone back online.

You can also use this script for troubleshooting. For example, you could retrieve the IP address of all the devices with a certain directory number.

4.12.3 Resource Object

CCM Publisher

4.12.4 Default Schedule

By default, this script runs every one minute.

4.12.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold not met?	Set to **y** to raise an event if the threshold is not met. The default is y. The detailed message for the event will contain the following information about each device that is not registered: ◆ Device Name ◆ Description ◆ Directory number(s) ◆ IP address (if available) ◆ Status ◆ CallManager node where device was registered (if available) ◆ Model ◆ Device Pool (if available) ◆ Calling Search Space (if available) For more information, see Section 4.12.2, “Examples of Using CCM_DeviceStatus,” on page 55.
Collect data?	Set to **y** to collect data for graphs and charts. The default is n. The data collected is the number of devices that are being monitored and the number of those devices that are registered.
Event severity when threshold is not met	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is not met. The default is 10.
Device to monitor	Select the type of devices to monitor. Valid values are: ◆ Phone (the default) ◆ MGCP_GatewayDevice ◆ CtiRoutePoint ◆ VoiceMailPort ◆ ConferenceBridge ◆ MusicOnHoldDevice ◆ MediaTerminationPoint
Select by	Choose the type of the selection criteria to be used to get the list of devices to monitor. Note that some criteria may not make sense for every device type. For example, you would not want to select by Directory Numbers if the Device Type is Conference Bridges. Valid values are: ◆ DeviceName (the default) ◆ DirectoryNumber ◆ Description ◆ DevicePool ◆ CallingSearchSpace

Parameter	How to Set It
Selection criteria	Enter the selection criteria for the devices to be monitored. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the devices with device names that begin with SEP, enter `SEP*`. The default is *, which Indicates you want to monitor all devices. You can enter multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*` The items must be the same type as the *Select By* parameter. So if *Select By* is **Device Name**, the items must be device names or patterns. If *Select By* is **Directory Number**, the items must be directory numbers or patterns. **NOTE**: If you enter a file path in *Full path to file with list of selection criteria*, ignore this parameter.
Full path to file with list of selection criteria	Enter the full path to a file on the agent computer containing a list of the selection criteria. The file should contain the selection criteria on one or more lines. Each line can have multiple items, separated by commas. For example: ◆ `SEP0009A*,SEP0009B*` ◆ `SEP999999994000,SEP999999994001` ◆ `SEP00044*` The items must be the same type as the *Select By* parameter. So if *Select By* is **Device Name**, the items must be device names or patterns. If *Select By* is **Directory Number**, the items must be directory numbers or patterns. **NOTE**: If you enter a file path, ignore the *Selection Criteria* parameter.
Maximum number of devices to monitor	Enter the maximum number of devices to be monitored. Only this number of devices will be monitored even if the selection criterion returns more than this number. Enter a number between 1 and 250. The default is 100 devices. **NOTE**: If the selection criterion does return more devices than the maximum number of devices to monitor, this script generates an event issued warning that this situation has occurred.

Parameter	How to Set It
Raise event with current status?	Enter **y** to generate an informational event containing the current status of the devices selected the first time this script runs. The default is y. The following details will be returned about each device: ◆ Device Name ◆ Description ◆ Directory number(s) ◆ IP address (if available) ◆ Status ◆ CallManager node where device is\was registered (if available) ◆ Model ◆ Special firmware load ◆ Device Pool (if available) ◆ Calling Search Space (if available) If you set this parameter to y, the first time the script is run an informational event will be generated containing the current status and details of all the monitored devices. The details of this informational event can be formatted in either XML or csv.
Format status event in XML?	Set to **y** to format the informational event containing the current status in XML. The default is y. If you use XML for the event, it will not be sent to any Actions that are defined for the script. If you want this information sent to an Action, set this parameter to n. The detailed message will then be formatted in .csv.
Threshold type	Select whether you want to monitor for a **Percentage** threshold or a **Number** threshold. The default is Percentage.
Threshold - Minimum % registered key devices	Specify the minimum percentage of devices that must have a status of "Registered" before an event is raised. The default is 75%.
Threshold - Minimum # registered key devices	Specify the minimum number of devices that must have a status of "Registered" before an event is raised. The default is 0 devices.
Event severity when key devices cross threshold and then return	Set the severity, from 1 to 40, of an event that is raised when the number or percent of key devices registered was previously below the threshold but now is within acceptable limits. Enter **0** if you do not want to raise an event. The default is 20.

4.12.6 Event Messages for CCM_DeviceStatus

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

Internal error encountered.

Explanation: An unrecoverable error was encountered. See the detailed event message for details about the error.

Likely cause: In most cases this message Indicates a COM interface was not available, either because the COM object has not been installed or is not registered.

Operator action: Verify the `dblx.dll` and `risx.dll` are installed and registered on the CallManager computer.

Initial device status.

Explanation: "y" was entered for the *Generate an event with the initial status* parameter. See the detailed event message for the status.

Likely Cause: See explanation.

Operator Action: No action is required.

 # key devices registered low.

Explanation: The number of devices you have selected to be monitored that have a status of "Registered" does not meet the threshold. See the detailed event message for a list of the devices that are not "Registered."

Likely Cause: If one or two devices are unavailable, it probably means someone has unplugged them from the network. If a large number of devices is unavailable, either there is a network problem or a failover may be in progress.

Operator Action: Verify the devices are plugged into the network and are operational. In the case of a large number of devices becoming unavailable, check to see whether a failover has occurred. In the case of a failover, the devices should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

% key devices registered low.

Explanation: The percentage of devices you have selected to be monitored that have a status of "Registered" does not meet the threshold. See the detailed event message for a list of the devices that are not registered.

Likely Causes: If one or two devices are unavailable, it probably means someone has unplugged them from the network. If a large number of devices are unavailable, either there is a network problem or a failover may be in progress.

Operator Action: Verify the devices are plugged into the network and are operational. In the case of a large number of devices becoming unavailable, check to see whether a failover has occurred. In the case of a failover, the devices should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

Syntax error: nothing selected.

Explanation: You must enter input into either the *Selection Criteria* or *File path containing selection criteria* parameter

Likely Cause: All selection parameters are empty.

Operator Action: Enter input into at least one of the selection parameters.

Unable to access device file.

Explanation: The file name entered could not be read. Either the path is inaccessible from the AppManager agent or the file does not exist.

Likely Cause: In most cases this message Indicates the file does not exist.

Operator Action: Verify the file exists and the path is accessible from the AppManager agent.

No devices to monitor.

Explanation: There were no devices found that match the selection criteria entered.

Likely Cause: See explanation.

Operator Action: Change the selection criteria.

Not all devices monitored.

Explanation: The number of devices found that match the selection criteria entered is greater than the maximum number of devices to be monitored. Only the maximum number of devices will be monitored.

Likely Cause: See explanation.

Operator Action: None, if the actual devices that are being monitored meet your objective. If not, change the selection criteria if possible so that a smaller list is returned from the selection.

Some devices not found.

Explanation: Multiple selection criteria were entered and one of the selection criteria did not find any devices.

Likely Cause: Most likely, the selection criteria are being read from a file, which contains one or more selection items or patterns that did not find a match. For example, if the file contains

```
SEP000ABD123,SEP000ABD124
SEP000ADD125,SEP000ABD126
```

and `SEP000ADD125` does not exist, you will get this warning message and only three devices will be monitored.

Operator Action: None, if the actual devices that are being monitored meet your objective. If not, change or remove the selection criterion that is not returning any devices.

4.13 CCM_EventLog

Use this Knowledge Script to monitor event log entries from Cisco CallManager during the past *n* hours. This script raises an event if the log contains the entries you identify.

4.13.1 Example of Using this Script

Cisco CallManager records events to the Windows Application Log under the source of the CallManager process that created the event. For example, a TFTP error is recorded under "Cisco Tftp." However, monitoring the Application Log is a time-consuming process, rendering the Application Log a diagnostic tool used only long after a problem occurs.

Using the CCM_EventLog Knowledge Script to periodically filter the Application Log, you can easily search for events that meet the criteria you specify, such as *Event Source=Cisco CallManager service name* or *Event Category=Error*. AppManager then raises an event with a description of the CallManager-related event.

Searching too many records can be CPU and memory intensive.

4.13.2 Resource Object

CCM parent object

4.13.3 Default Schedule

By default, this script runs every 10 minutes.

4.13.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to n, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Set to **y** to monitor for error events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is y.
Type: Warning	Set to **y** to monitor for warning events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is y.
Type: Information	Set to **y** to monitor for information events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is n.
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is n.

Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.·

- Separate include and exclude criteria with a colon (:). For example, `net:logon`.
- Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`.
- If you are specifying only include criteria, the colon is not necessary. For example, `SQL`.
- If you are specifying only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.

Parameter	How to Set It
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. For example: `NTDS KCC,NTDS General`
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the Events tab displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event. You may want to adjust the severity depending on the types of events for which you are checking. The default is 8.

4.14 CCM_FXOPorts

Use this Knowledge Script to monitor the number of active and in-service FXO (foreign exchange office) ports for this CallManager. This script raises an event if a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

4.14.1 Resource Object

CCM Call Processor

4.14.2 Default Schedule

By default, this script runs every 10 minutes.

4.14.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of a breached threshold. The default is 15.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that can be active before an event is generated. The default is 10 ports.
Threshold - Minimum in-service FXO ports	Specify the minimum number of FXO ports that can be in service before an event is generated. The default is 0 ports.

4.15 CCM_FXSPorts

Use this Knowledge Script to monitor the number of active and in-service FXS (foreign exchange station) ports for this CallManager. This script raises an event a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

4.15.1 Resource Object

CCM Call Processor

4.15.2 Default Schedule

By default, this script runs every 10 minutes.

4.15.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is n.

Parameter	How to Set It
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of a breached threshold. The default is 15.
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that can be active before an event is generated. The default is 10 ports.
Threshold - Minimum in-service FXS ports	Specify the minimum number of FXS ports that can be in service before an event is generated. The default is 0 ports.

4.16 CCM_HealthCheck

Use this Knowledge Script to monitor the status of Cisco CallManager services. This script automatically starts any down service when *Auto-start monitored services* is set to **y**.

This script collects the data used by the Report_ServicesAvailability Knowledge Script.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.16.1 Resource Object

CCM parent object

4.16.2 Default Schedule

By default, this script runs every one minute.

4.16.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to enable this script to collect data for reports and graphs. The default is y.
Auto-start monitored service(s)?	Set to **y** to automatically start any of the services you choose to monitor. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager successfully restarted it. The default is 25.

Parameter	How to Set It
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager has not been set to restart the service. The default is 18.
Event severity when service does not exist	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service does not exist. The default is 15.
Event severity when service is paused	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is in a paused state. The default is 20. Some services enter a paused state when the system is low on CPU or memory resources. Enter **0** when you do not want to raise an event for this situation.
Monitor Cisco CallManager service?	Set to **y** to monitor the status of Cisco CallManager. The default is y.
Monitor Cisco Database Layer Monitor service?	Set to **y** to monitor the status of Cisco Database Layer Monitor. The default is y.
Monitor Cisco TFTP service?	Set to **y** to monitor the status of Cisco TFTP. The default is y.
Monitor Cisco IP Voice Media Streaming App service?	Set to **y** to monitor the status of Cisco IP Voice Media Streaming App. The default is n.
Monitor Cisco Messaging Interface service?	Set to **y** to monitor the status of Cisco Messaging Interface. The default is n.
Monitor Cisco Telephony Call Dispatcher service?	Set to **y** to monitor the status of Cisco Telephony Call Dispatcher. The default is y.
Monitor DC Directory Server service?	Set to **y** to monitor the status of the DC Directory Server service. The default is y.
Monitor Cisco SNMP Data Collector service? (for CallManager 3.0 only services)	Set to **y** to monitor the status of Cisco SNMP Data Collector. The default is n.
Monitor Cisco CTI Manager service?	Set to **y** to monitor the status of Cisco CTI Manager (for CallManager 3.1 and later). The default is n.
Monitor Cisco Extension Mobility Logout service?	Set to **y** to monitor the status of Cisco Extension Mobility Logout (for CallManager 3.1 and later). The default is n.
Monitor Cisco MOH Audio Translator service?	Set to **y** to monitor the status of Cisco MOH Audio Translator (for CallManager 3.1 and later). The default is n.
Monitor Cisco RIS Data Collector service?	Set to **y** to monitor the status of Cisco RIS Data Collector (for CallManager 3.1 and later). The default is n.

4.17 CCM_HeartBeat

Use this Knowledge Script to monitor the CallManager heartbeat. This script raises an event if the heartbeat stops or falls below the specified threshold. A low heartbeat Indicates the CallManager service was stopped and then restarted.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, “Recommended Knowledge Script Groups,” on page 216.

4.17.1 Resource Object

CCM parent object

4.17.2 Default Schedule

By default, this script runs every one minute.

4.17.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if heartbeat stops or falls below the threshold?	Set to **y** to raise an event when the heartbeat stops or falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about the heartbeat for reports and graphs. The default is n.
Threshold - Minimum heartbeat	Specify the minimum heartbeat count that can be detected before an event is raised. The default is 500.
Event severity when heartbeat falls below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat fell below the threshold. The default is 20.
Event severity when heartbeat stops	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat stopped. The default is 10.

4.18 CCM_MemByProcess

Use this Knowledge Script to monitor working set memory use for individual CallManager processes, and the total working set memory use for all monitored CallManager processes. This script raises an event if working set memory use exceeds the threshold. If a process cannot be found, no events are generated.

4.18.1 Resource Object

CCM parent object

4.18.2 Default Schedule

By default, this script runs every five minutes.

4.18.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for memory use by all monitored processes?	Set to **y** to collect data for the total amount of memory being used by all the monitored processes. The default is y.
Threshold - Maximum memory use for all monitored processes	Specify the maximum amount of memory that can be used by all the monitored processes before an event is raised. The default is 512000 KB.
Event severity when total memory use exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory use for all monitored processes exceeds the threshold. Enter **0** if you do not want to raise an event. The default is 15.
Collect data for memory use by individual processes?	Set to **y** to collect data for the amount of memory being used by each monitored process.
Event severity when individual memory use exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory use for individual processes exceeds the threshold. Enter **0** if you do not want to raise an event. The default is 15.
Monitor the CallManager process?	Set to **y** to monitor memory usage of the Cisco CallManager process. The default is y.
Threshold - Maximum memory use for the CallManager process	Specify the maximum amount of memory that can be used by the Cisco CallManager process before an event is raised. The default is 200000 KB.
Monitor the DC Directory process?	Set to **y** to monitor memory usage of the DC Directory process. The default is y.
Threshold - Maximum memory use for the DC Directory process	Specify the maximum amount of memory that can be used by the DC Directory processes before an event is raised. The default is 100000 KB.
Monitor the CTI Manager process?	Set to **y** to monitor memory usage of the CTI Manager process. The default is y.
Threshold - Maximum memory use for the CTI Manager process	Specify the maximum amount of memory that can be used by the CTI Manager process before an event is raised. The default is 50000 KB.
Monitor the Cisco TFTP process?	Set to **y** to monitor memory usage of the Cisco TFTP process. The default is y.
Threshold - Maximum memory use for the Cisco TFTP process	Specify the maximum amount of memory that can be used by the Cisco TFTP process before an event is raised. The default is 50000 KB.
Monitor the Database Layer process?	Set to **y** to monitor memory usage of the Database Layer process (Aupair). The default is y.
Threshold - Maximum memory use for the Database Layer process	Specify the maximum amount of memory that can be used by the Database Layer process before an event is raised. The default is 50000 KB.
Monitor the Telephony Call Dispatcher process?	Set to **y** to monitor memory usage of the Telephony Call Dispatcher process. The default is y.

Parameter	How to Set It
Threshold - Maximum memory use for the Telephony Call Dispatcher process	Specify the maximum amount of memory that can be used by the Telephony Call Dispatcher process before an event is raised. The default is 50000 KB.
Monitor the CDR Insert process?	Set to **y** to monitor memory usage of the CDR Insert process. The default is n.
Threshold - Maximum memory use for the CDR Insert process	Specify the maximum amount of memory that can be used by the CDR Insert process before an event is raised. The default is 75000 KB.
Monitor the Messaging Interface process?	Set to **y** to monitor memory usage of the Messaging Interface process. The default is n.
Threshold - Maximum memory use for the Messaging Interface process	Specify the maximum amount of memory that can be used by the Messaging Interface process before an event is raised. The default is 50000 KB.
Monitor the Extension Mobility process?	Set to **y** to monitor memory usage of the Extension Mobility process. The default is n.
Threshold - Maximum memory use for the Extension Mobility process	Specify the maximum amount of memory that can be used by the Extension Mobility process before an event is raised. The default is 50000 KB.
Monitor the MOH Audio Translator process?	Set to **y** to monitor memory usage of the MOH (Music On Hold) Audio Translator process. The default is n.
Threshold - Maximum memory use for the MOH Audio Translator process	Specify the maximum amount of memory that can be used by the MOH Audio Translator process before an event is raised. The default is 50000 KB.
Monitor the RIS Data Collector process?	Set to **y** to monitor memory usage of the RIS (Real-Time Information Server) Data Collector process. The default is n.
Threshold - Maximum memory use for the RIS Data Collector process	Specify the maximum amount of memory that can be used by the RIS Data Collector process before an event is raised. The default is 50000 KB.
Monitor the IP Voice Streaming Media process?	Set to **y** to monitor memory usage of the IP Voice Streaming Media process. The default is n.
Threshold - Maximum memory use for the IP Voice Streaming Media process	Specify the maximum amount of memory that can be used by the IP Voice Streaming Media process before an event is raised. The default is 50000 KB.

4.19 CCM_MemoryHigh

Use this Knowledge Script to monitor the memory that application processes are consuming. This script checks the memory used by each process individually, and the total memory used by all processes. If a process is not found, the script assumes that the process is not running, and reports zero as the memory result.

4.19.1 Resource Object

CCM parent object

4.19.2 Default Schedule

By default, this script runs every five minutes.

4.19.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if one of the thresholds is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.
Monitor the Cisco CallManager process?	Set to **y** to monitor the Cisco CallManager process. The default is y.
Threshold - Maximum memory usage for CallManager process	Specify the maximum memory usage by the CallManager process that can occur before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for CallManager process	Specify the maximum memory pool usage by the CallManager process that can occur before an event is raised. The default is 5000 KB.
Monitor other Cisco processes?	Set to **y** to monitor other Cisco processes. The default is n.
Threshold - Maximum memory usage for other Cisco processes	Specify the maximum memory usage by other Cisco processes that can occur before an event is raised. The default is 25000 KB.
Threshold - Maximum memory pool use for other Cisco processes	Specify the maximum memory pool usage by other Cisco processes that can occur before an event is raised. The default is 5000 KB.

4.20 CCM_MOHUnavailable

Music on Hold (MOH) resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

Use this Knowledge Script to monitor the number of times that an attempt was made to allocate an MOH resource when either every available connection on all MOH servers was active, or when no MOH servers were registered.

4.20.1 Resource Object

CCM parent object

4.20.2 Default Schedule

By default, this script runs every 10 minutes.

4.20.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-resource instances exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about out-of-resource instances for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-resource instances exceeds the threshold. The default is 10.
Threshold - Maximum out-of-resource instances	Specify the maximum number of out-of-resource instances that can occur before an event is raised. The default is 0.

4.21 CCM_PhoneCheck

Use this Knowledge Script to monitor your CallManager for new and missing phones. With each iteration of the job, this script creates a list of the phones registered to the CallManager, and then compares the latest list information with the information from the previous list. You can determine the frequency with which this script runs from the Schedule tab.

NOTE

- This script does not return information about H.323 devices.
- The list is sorted by the Description, not the Device Name, of the phone that you configured in CallManager.

4.21.1 Resource Object

CCM Call Processor

4.21.2 Default Schedule

By default, this script runs every 15 minutes.

4.21.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Script Options	
Name for current phone list	Provide a name for the current list of new or missing phones. The default is `NQCurrentPhoneList`.

Parameter	How to Set It
Name for global phone list	Provide a name for the global list of new or missing phones. The default is `NQGlobalPhoneList`.
Monitor New and Missing Phones	
Event Notification	
Raise event if new phones are found?	Select **Yes** to raise an event if new phones are found since the last time you ran the script. The default is Yes.
Event severity when new phones are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which new phones are found. The default is 30.
Raise event if phones are missing?	Select **Yes** to raise an event if any phones are missing since the last time you ran the script. The default is Yes.
Event severity when phones are missing	Set the severity level, from 1 to 40, to indicate the importance of an event in which phones are missing. The default is 15.

4.22 CCM_PhoneInventory

Use this Knowledge Script to take an inventory of phones based on specified search criteria and to write the inventory results to a file. Unless you specify a UNC path, *\\servername\sharename\directoryname\filename*, the results file is written on the CallManager Publisher computer where the NetIQ agent is running.

4.22.1 Monitoring Phone Status

You can determine the status (registered or deregistered) of CallManager phones for active CallManager 4.x clusters and for CallManager 4.x clusters on which failover has occurred. Failover occurs when CallManager status changes from Primary to Backup.

For active CallManager clusters

In this scenario, use the phone deregistration support provided by the CiscoCM_4x_PhoneDeregistrations Knowledge Script from the AppManager for Cisco Unified CallManager module. By using this script, you can determine which phones have deregistered and maintain a history of phone deregistrations in the Cisco CM supplemental database.

AppManager for Cisco Unified CallManager provides limited support for monitoring phone deregistrations on CallManager 4.x clusters. For more information, see the *AppManager for Cisco Unified CallManager Management Guide*.

For CallManagers that have failed over

CallManagers that fail over contain only a list of phones that have registered since failover occurred. They do not provide a list of phones that deregistered as a result of failover. Use the CCM_PhoneInventory Knowledge Script to determine which phones have deregistered. Use the *Monitor for new/missing phone registrations?* parameter to monitor for phone registrations that are missing since the last time this script was run.

To determine whether failover has occurred, use the CCM_RoleStatus or LossOfHardwarePhones Knowledge Script.

4.22.2 Resource Object

CCM Publisher

4.22.3 Default Schedule

By default, this script runs once.

4.22.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Script Options	
Collect data?	Select **Yes** to collect data about the number of configured and registered phones for reports and graphs. The default is unselected.
CallManager database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Monitor for new/missing phone registrations?	Select **Yes** to monitor for phone registrations that are new or missing since the last time this script was run. The default is unselected.
Search Options	
Select by	Choose the type of the selection criteria that you want to use to create the list of phones. ◆ Name (the default) ◆ DirectoryNumber ◆ Description ◆ DevicePool ◆ CallingSearchSpace ◆ Partition ◆ Subnet. If you select this option, you must enter the subnet address in the *Selection criteria* parameter. Use the following syntax: `172.16.10.0/20`. ◆ SubnetFilepath. If you select this option, in the *Selection criteria* parameter, enter the UNC or full path to a file on the agent computer that contains a list of subnet specifications.

Parameter	How to Set It
Selection criteria	Provide the selection criteria for the phones to be listed. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the phones with device names that begin with SEP, enter `SEP*`. You can enter multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*` The items you enter must be of the same type as the *Select by* parameter. So if *Select by* is **Name**, the items you enter must be device names or patterns. If *Select by* is **Directory Number**, the items you enter must be directory numbers or patterns.
Result File Options	
Write details to result file?	Select **Yes** to write the details about each phone to the result file specified in the *Result file name* parameter. The default is Yes. The following details about each phone will be returned in a `.csv` file: ◆ Name ◆ Description ◆ Directory number ◆ Partition (if available) ◆ Model ◆ Device Pool (if available) ◆ Calling Search Space (if available) ◆ Location ◆ IP address (if available) ◆ CallManager node where device is\was registered (if available) ◆ Status ◆ Status Time
Result file name	Provide the full path or a UNC path to a location on the agent computer where the inventory `.csv` file should be written. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory.csv`
Write phone registration change details to a second result file?	Select **Yes** to write the details about new or missing registrations to the result file specified in the *Phone registration changes file name* parameter. The default is Yes.
Phone registration changes file name	Provide the full path or a UNC path to a location on the agent computer where the registration changes `.csv` file should be written. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventoryComparison.csv`

Parameter	How to Set It
List only phone with status of	Use this parameter to limit the phones listed in the results file to only those whose status is one of the following: ◆ Any (the default) ◆ Not Registered ◆ Registered ◆ Unregistered ◆ Rejected ◆ Unknown **NOTE**: Setting this parameter to a value of **Not Registered** will list those phones with a status of **Unregistered**, **Rejected**, and **Unknown**.
Order by	Select **Name** to display the contents of the results file in order by the phone name. The default is Name. Select **DirectoryNumber** to display the contents of the results file in order by directory numbers.
Threshold	
Threshold type	Select whether you want to monitor for **Percentage** or **Number** thresholds. The default is Percentage.
Threshold - Minimum % phones registered	Specify the minimum percentage of phones that must have a status of Registered before an event is raised. The default is 75%.
Threshold - Minimum # phones registered	Specify the minimum number of phones that must have a status of Registered before an event is raised. The default is 0 phones.
Events	
Raise event if threshold is exceeded?	Select **Yes** to raise an event when a threshold is exceeded. The default is Yes.
Raise informational event when inventory completes?	Select **Yes** to raise an informational event when the inventory has completed. The default is Yes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Event severity when failures occur	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a failure occurred, such as an inability to write to the file or access the database. The default is 15.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the results file returns no data. The default is 30.

4.22.5 Event Messages for CCM_PhoneInventory

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

PhoneInventory: x Configured and y Registered

Explanation: This message is returned when the inventory completes.

Likely causes: The script ran successfully.

Operator action: No action required.

 # registered phones is low

Explanation: The number of phones in the inventory that have a status of Registered does not meet the threshold.

Likely causes: If one or two phones are unavailable, it probably means that someone has unplugged them from the network. If many phones are unavailable, either there is a network problem or a failover may be in progress.

Operator action: Verify that the phones are plugged into the network and are operational. If many phones are unavailable, check to see whether a failover has occurred. If a failover has occurred, the phones should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

% registered phones is low

Explanation: The percentage of phones in the inventory that have a status of Registered does not meet the threshold.

Likely causes: If one or two phones are unavailable, it probably means that someone has unplugged them from the network. If many phones are unavailable, either there is a network problem or a failover may be in progress.

Operator action: Verify that the phones are plugged into the network and are operational. If many phones are unavailable, check to see whether a failover has occurred. If a failover has occurred, the phones should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

Syntax error: <reason>

Explanation: One or more parameters entered are invalid. See the detailed event message for details about the error.

Likely causes: An invalid parameter or combination of parameters were entered.

Operator action: Fix the invalid parameter and run the script again.

Unable to access result file.

Explanation: The file name entered could not be accessed.

Likely causes: The path is inaccessible from the NetIQ agent, *or* the NetIQ agent does not have the proper permissions to access the file, *or* the file is in use by another process.

Operator action: Verify that the file is not use by another process and the path is accessible from the NetIQ agent. If you are trying to write to a network share, you may need to change the netiqmc service to not run as the LocalSystem account. In most cases, this account does not have the necessary permissions to write to a network drive.

Error encountered getting password.

Explanation: A database user name was entered and errors were encountered while trying to retrieve the password for this user name from the NetIQ AppManager Security Manager.

Likely causes: In most cases, this message Indicates the user name has not been properly entered in AppManager Security Manager.

Operator action: Verify that the user name has been properly entered in AppManager Security Manager.

Incorrect managed object version.

Explanation: The NetIQ CallManager managed object (`qccma4.dll`) is not at the correct level to run this script.

Likely causes: The NetIQ agent on the CallManager server being monitored is not at the latest level.

Operator action: Upgrade the NetIQ agent to the latest level.

Database operation failed.

Explanation: An error was encountered executing a SQL query.

Likely causes: In most cases this message Indicates the NetIQ agent does not have the proper authority to execute the query. Another reason could be that the SQL query timed out because the SQL server was too busy. The detailed message should contain the reason that the SQL query failed.

Operator action: If a timeout occurred, try the query at a time when the SQL server is not so busy. If using a user name and password, verify that the user name has access to the CallManager configuration database. If using Windows authentication (blank user name), verify that the `netiqmc` process is running with the correct permissions to access the database.

Internal error encountered.

Explanation: An unrecoverable error was encountered. See the detailed event message for details about the error.

Likely causes: In most cases this message Indicates a COM interface was not available, either because the COM object has not been installed or is not registered.

Operator action: Verify that the NetIQ CallManager managed object (`qccma4.dll`) is installed and registered on the CallManager server.

4.23 CCM_PRIChannels

Use this Knowledge Script to monitor the number of active and in-service PRI (primary rate interface) channels for this CallManager. This script raises an event if a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

4.23.1 Resource Object

CCM Call Processor

4.23.2 Default Schedule

By default, this script runs every five minutes.

4.23.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about PRI channels for reports and graphs. The default is n.

Parameter	How to Set It
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is breached. The default is 15.
Threshold - Maximum active PRI channels	Specify the maximum number of PRI channels that can be active before an event is raised. The default is 10 channels.
Threshold - Minimum PRI spans in service	Specify the minimum number of PRI spans that can be in service before an event is raised. The default is 0 channels.

4.24 CCM_Replication

Use this Knowledge Script to query for failed actions in the distribution, snapshot, and logreader history tables of the replication agents on the CallManager Publisher.

Replication allows you to keep copies of the same data on multiple sites. The Publisher is the source of the replication. The Publisher defines an article for each table or other database object to be used as a replication source. One or more related articles from the same database are organized into a *publication*. A publication is a convenient way to group together related data that you want to replicate.

The Subscriber receives the replication data from the Publisher. The Subscriber defines a *subscription* to a particular publication. The subscription specifies when the Subscriber receives the publication from the Publisher, and maps the articles to tables and other database objects in the Subscriber.

Cisco CallManager uses two types of replication:

4.24.1 Snapshot Replication

Snapshot replication copies data or database objects exactly as they exist at the time of replication. Snapshot publications are typically defined to occur on a scheduled basis, however, the publication is sent to the Subscriber only if the latest publication reflects a difference from the previous publication. The Subscriber contains copies of the published articles, as they existed at the time of the last snapshot. Snapshot replication is typically used when the source data is relatively static, or when the Subscribers can be slightly out of date, or if the amount of data to replicate is small.

4.24.2 Transactional Replication

In a transactional replication, Subscribers are first synchronized with the Publisher (typically by using a snapshot), and then, as the publication data is modified, the transactions are captured and sent to the Subscribers. Transactional integrity is maintained across the Subscribers by having all modifications made at the Publisher and then replicated to the Subscribers. Transactional replication is typically used when data must be replicated as it is modified, you must preserve the transactions, and the Publishers and Subscribers are reliably and frequently connected through the network.

Database replication is accomplished through the use of several replication agents, processes that perform specific replication tasks. CallManager uses three replication agents: snapshot agent, log reader agent, and distribution agent.

To begin transactional replication, the Subscriber needs an initial snapshot of the entire database. The *snapshot agent* on the Publisher collects the information for database snapshots. The snapshot agents takes a snapshot only if a Subscriber becomes out of sync with the Publisher, or if the subscription was re-initialized. If the Subscriber does not need a snapshot, the snapshot agent does nothing when it runs on its schedule.

The *log reader agent* is responsible for moving any changes made to the Publisher database to the distribution database. For each Subscriber, a *distribution agent* is responsible for taking information from the distribution database and moving it to the appropriate Subscriber.

NOTE: This script assumes that the distribution database on the CallManager Publisher has not been renamed to something other than "distribution," which is the name assigned when CallManager installed the database.

4.24.3 Resource Object

CCM Publisher

4.24.4 Default Schedule

By default, this script runs every hour.

4.24.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
On first run, hours to go back	Specify the number of hours of previous replication agent history to check the first time you run this script. For instance, if you enter 24, the first time you run this script it will check actions made by the agents in the last 24 hours. On subsequent runs, it will check only agent actions that have occurred during the interval. The default is 1 hour. **NOTE**: Using a high "hours to go back" time may cause this script to be CPU-intensive on its first run, depending on the number of database entries being retrieved from the server.
Distribution database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum failed actions by any agent	Specify the maximum number of failed actions that can have occurred during the interval for any of the agents. If the number of failed actions is greater than the threshold that you set, an event is raised. The default is 0.

Parameter	How to Set It
Raise informational event with agent history?	Set to **y** to raise an informational event containing the last 10 actions that occurred during the interval for each replication agent. The default is y.
Raise informational event if snapshot generated?	Set to **y** to raise an informational event if, during the interval, the snapshot agent on the CallManager Publisher has generated any replication snapshots. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold has been exceeded. The default is 5.
Event severity for informational messages	Set the severity level, from 1 to 40, to indicate the importance of an informational event message. The default is 30.
Event format	Select the format in which you want to receive the informational event: CSV, XML, or both. If you select **Both**, the CSV (comma separated value) event is collapsed under the XML event. To access the CSV event, turn off **Collapse duplicate events into a single event** on the Advanced tab before running this script. **Notes** ◆ Events formatted in XML are not forwarded to an Action script (if you selected to initiate an Action script if this script generates an event). If you select **Both**, two events are generated: one in CSV format, which is forwarded to an Action script, and one in XML format. ◆ Error messages are formatted in plain text — this parameter does not apply to error messages.

4.24.6 Event Messages for CCM_Replication

Following are common event messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

 # failed replications actions high.

Explanation: The number of failed actions in one or more of the replication agent history tables exceeded the threshold.

Likely cause: One or more replication actions have failed.

Operator action: Check the detailed message, which will contain a list of the last 25 failed actions, as well as the name of the replication agent that has the failures. Forward the information to your database administrator.

Replication history.

Explanation: This is an informational message containing the last 25 actions for all the replication agents. See the detailed event message for the data.

Likely cause: This is a normal event message when *Generate informational event with agent history?* is set to "y."

Operator action: No action is required.

Replication snapshot(s) generated.

Explanation: This is an informational message created when a replication snapshot has been generated on the CallManager Publisher during the interval. See the detailed event message for information about the snapshot.

Likely cause: This is a normal event message when *Generate informational event if a replication snapshot was generated?* is set to "y."

Operator action: No action is required.

Error encountered getting password.

Explanation: A database user name was entered and errors were encountered while trying to retrieve the password for this user name from the AppManager Security Manager.

Likely cause: In most cases, this message Indicates the user name was not properly entered in the AppManager Security Manager.

Operator action: Verify that the user name has been properly entered in the AppManager Security Manager.

Incorrect managed object version.

Explanation: The AppManager CallManager managed object (`qccma4.dll`) is not at the correct level to run this script.

Likely cause: The AppManager agent on the CallManager server being monitored is not version 6.0.

Operator action: Upgrade the AppManager agent to Version 6.0 or later.

No CallManager replication agents found.

Explanation: No CallManager replication agents (snapshot, log reader, or distribution) were found when querying the distribution database on the Publisher.

Likely cause: In most cases, this message occurs when the distribution database has been renamed to something other than "distribution."

Operator action: Verify that the distribution database has not been renamed.

Database operation failed.

Explanation: An error was encountered while executing a SQL query.

Likely cause: In most cases, this message Indicates the AppManager agent does not have the proper authority to execute the query. The detailed message should contain the reason for the failure of the SQL query.

Operator action: If using a user name and password, verify that the user name has access to the distribution database. If using Windows authentication (blank user name), verify that the netiqmc process is running with the correct permissions to access the distribution database.

Internal error encountered.

Explanation: An unrecoverable error was encountered. See the detailed event message for details about the error.

Likely cause: In most cases, this message Indicates a COM interface was not available, because either the COM object is not installed or is not registered.

Operator action: Verify that the AppManager CallManager managed object (`qccma4.dll`) is installed and registered on the CallManager server.

4.25 CCM_ResetDevice

Use this Knowledge Script to reset one or more devices in order for the devices to pick up new default firmware. For example, if a new firmware load is placed on the TFTP servers, all devices using this firmware need to be reset.

To avoid resetting all the devices during peak times, schedule this script to run when the system is not busy.

This script initiates only the Reset or Restart command. It does *not* check on the success or failure of the command.

If a device is not registered with Cisco CallManager, you cannot reset or restart it. Resetting a gateway/trunk drops any in-progress calls that are using the gateway/trunk. Restarting a gateway tries to preserve the in-progress calls that are using the gateway. Other devices wait until calls are complete before restarting or resetting. Resetting or restarting an H.323 device does not physically reset or restart the device, but only re-initializes the configuration loaded by Cisco CallManager.

NOTE: Only an AppManager administrator should run this script.

4.25.1 Resource Object

CCM Publisher

4.25.2 Default Schedule

By default, this script runs once.

4.25.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Select reset type	Select the type of reset that you want to initiate: **Reset** or **Restart**. This parameter is valid only for the Directory Number, Device Name, and Device Description patterns. The reset type is *always* Reset for the Device Type and Device Pool parameters. A Restart resets the device without shutting it down. A Reset shuts down the device and then restarts it. The default is Reset.
Directory Number pattern	Specify the directory number pattern of the devices that you want to reset. You can specify a group of directory numbers by using the % wildcard. For example, to reset all the devices with directory numbers that begin with "31," enter `31%`. The reset/restart is performed only if the pattern results in 100 or fewer devices being selected.
Device Name pattern	Specify the device name pattern of the devices that you want to reset. You can specify a group of device names by using the % wildcard. For example, to reset all the devices with device names that begin with "SEP," enter `SEP%`. The reset/restart is performed only if the pattern results in 100 or fewer devices being selected.

Parameter	How to Set It
Device Description pattern	Specify the device description pattern of the devices that you want to reset. You can specify a group of device descriptions by using the % wildcard. For example, to reset all the devices with device descriptions that begin with "Auto," enter `Auto%`. The reset/restart is performed only if the pattern results in 100 or fewer devices being selected.
Select device type	Select the type of the device that you want to reset. All devices of that type will be reset. The default is None. Valid device types are indicated as follows: ◆ AllPhones, which resets devices of the following types: Cisco 12 S, Cisco 12 SP, Cisco 12 SP+, Cisco 30 SP+, Cisco 30 VIP, Cisco IP Phone 7905, Cisco IP Phone 7910, Cisco IP Phone 7935, Cisco IP Phone 7940, Cisco IP Phone 7960, Cisco ATA 186, Cisco VGC Phone, Cisco VGC Virtual Phone, and H.323 Phone. ◆ All79xxPhones, which resets devices of the following types: Cisco IP Phone 7905, Cisco IP Phone 7910, Cisco IP Phone 7935, Cisco IP Phone 7940, and Cisco IP Phone 7960. ◆ Analog Access ◆ Analog Access WS-X6624 ◆ Cisco 12 S, 12 SP, and 12 SP+ ◆ Cisco 30 SP+ and 30 VIP ◆ Cisco IP Phone 7905, 7910, 7935, 7940, and 7960 ◆ Cisco ATA 186 ◆ Cisco VGC Phone and VGC Virtual Phone ◆ Conference Bridge and Conference Bridge WS-X6608 ◆ Digital Access, Digital Access WS-X6608, and Digital Access+ ◆ H.323 Phone ◆ Load Simulator ◆ MTP and MTP WS-X6608 ◆ MGCP Station and MGCP Trunk ◆ VGC Gateway ◆ 14-Button Line Expansion Module
Device pool name	Specify the name of the device pool that you want to reset. All devices in the pool will be reset.
Event severity when reset succeeds	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which the reset succeeds. The default is 25. For more information, see Section 4.25.4, “Event Messages for CCM_ResetDevice,” on page 83.
Event severity when warnings occur	Set the severity level of the event, from 1 to 40, to indicate the importance of the event in which warnings occurred. The default is 15.
Event severity when errors occur	Set the severity level of the event, from 1 to 40, to indicate the importance of the event in which errors occurred. The default is 5.

4.25.4 Event Messages for CCM_ResetDevice

Following are three common event messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

Reset issued successfully.

Explanation: The reset command was issued successfully for all selected devices. See the detailed event message for the number of devices for which the reset was issued.

Likely cause: Normal message.

Operator action: None.

Reset issued with warnings.

Explanation: Warnings were encountered while issuing the reset command for one or more of the selected devices. See the detailed event message for more information.

Likely causes: In most cases, this message Indicates one or more of the selections resulted in no devices being found to reset. Another likely cause is that too many devices were selected for reset.

Operator action: No action is required if there are no devices associated with the command. If too many devices were selected, then, if possible, use the device type or device pool parameter.

Reset issued with errors.

Explanation: Errors were encountered while issuing the reset command for one or more of the selected devices. See the detailed event message for details about the error.

Likely cause: In most cases, this message Indicates a COM interface was not available, either because the COM object has not been installed or because the COM object is not registered.

Operator action: Verify that the `dblx.dll` is installed and registered on the CallManager computer.

4.26 CCM_RestartService

Use this Knowledge Script to schedule a CallManager service to stop and then restart after a specified interval. This script raises an event when stop fails or succeeds, when restart fails or succeeds, and when the status of a service is unavailable. In addition, this script generates data streams for service availability.

4.26.1 Resource Object

CCM Service folder

4.26.2 Default Schedule

By default, this script runs every hour.

4.26.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data about CallManager services for graphs and reports. The default is n.
Wait N seconds before restarting	Set the number of seconds that you want to wait before restarting a stopped CallManager service. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop failed. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart failed. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the service is unavailable. The default is 15.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop succeeds. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart succeeds. The default is 25.
Event severity when service is paused	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is paused. The default is 20. Some services enter a paused state when the system is low on CPU or memory resources. Enter **0** when you do not want to raise an event for this situation.
Restart Cisco CallManager service?	Set to **y** to restart Cisco CallManager. The default is y.
Restart Cisco Database Layer Monitor service?	Set to **y** to restart Cisco Database Layer Monitor. The default is y.
Restart Cisco IP Voice Media Streaming App service?	Set to **y** to restart Cisco IP Voice Media Streaming App. The default is n.
Restart Cisco Messaging Interface service?	Set to **y** to restart Cisco Messaging Interface. The default is n.
Restart Cisco SNMP Data Collector service?	Set to **y** to restart Cisco SNMP Data Collector. The default is n.
Restart Cisco Telephony Call Dispatcher service?	Set to **y** to restart Cisco Telephony Call Dispatcher. The default is n.
Restart Cisco TFTP service?	Set to **y** to restart Cisco TFTP. The default is n.
Restart Cisco SNMP Data Collector service? (For CallManager 3.0 only)	Set to **y** to restart Cisco SNMP Data Collector service. The default is n.
Restart Cisco CTI Manager service? (for CallManager 3.1 only)	Set to **y** to restart Cisco CTI Manager. The default is n.
Restart Cisco Extension Mobility Logout service? (for CallManager 3.1 only)	Set to **y** to restart Cisco Extension Mobility Logout. The default is n.

Parameter	How to Set It
Restart Cisco MOH Audio Translator service? (for CallManager 3.1 only)	Set to **y** to restart Cisco MOH Audio Translator. The default is n.
Restart Cisco RIS Data Collector service?	Set to **y** to restart Cisco RIS Data Collector. The default is n.

4.27 CCM_RoleStatus

Use this Knowledge Script to determine whether a CallManager's status is Primary or Backup. You can choose to raise an event for status transitions. A Backup is defined as any CallManager with no registered hardware or software phones.

In the event of a failover from a Primary CallManager to a Backup CallManager, you can set the **Actions** tab of this script to run Action_RunDiscoveryCiscoCallMgr. The Action script will discover CallManager resources on the backup device and, if you have configured a monitoring policy to do so, any jobs that are running on the Primary device will be transferred to the Backup CallManager.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

You can also use this script to monitor phone status. For more information, see CCM_PhoneInventory.

4.27.1 Resource Object

CCM Call Processor

4.27.2 Default Schedule

By default, this script runs every five minutes.

4.27.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when Backup changes to Primary?	Set to **y** to raise an event when the CallManager status changes from Backup to Primary. The default is y.
Event severity when Backup changes to Primary	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the status changes from Backup to Primary. The default is 15.
Raise event when Primary changes to Backup?	Set to **y** to raise an event when the CallManager status changes from Primary to Backup. The default is y.
Event severity when Primary changes to Backup	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the status changes from Primary to Backup. The default is 15.
Collect data?	Set to **y** to collect data for reports and graphs. A Primary returns a value of 100; a Backup returns a value of 0. The default is n.

4.28 CCM_SecureWebPageCheck

Use this Knowledge Script to monitor accessibility to the `ccmadmin` and `ccmuser` secure Web pages, and raise an event if the Web pages cannot be accessed. This script can collect data about the availability of the Web pages and round-trip connection time. If a URL is not reachable, the detail message records the reason, such as the format of the request was invalid or the server name was not found. If the Web pages cannot be accessed, you can arrange for this script to restart the IIS server and sites that are down.

NOTE: This script is supported for Cisco CallManager version 4.1 or later. If you are running an earlier version, use CCM_WebPageCheck.

4.28.1 Resource Objects

CCM IIS Server

CCM IIS W3 SRV

CCM IIS Web Inst

4.28.2 Default Schedule

By default, this script runs every 30 minutes.

4.28.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Web page is inaccessible?	Set to **y** to raise an event if the Web page cannot be accessed. The default is y.
Collect data for up/down URL?	Set to **y** to collect data about the up and down status of the URL. If set to y, the script returns a value of 100 if the connection is up and a value of 0 if the connection is down. The default is y.
Collect data for round-trip time?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the round-trip connection time (in milliseconds). The default is n.
Monitor ccmadmin?	Set to **y** to monitor the ccmadmin Web page. The default is y.
Monitor ccmuser?	Set to **y** to monitor the ccmuser Web page. The default is y.
Username for ccmadmin	Enter the user name to use when logging on to ccmadmin. If a user name is not required, you can leave this field blank. For more information about the user name, see Section 4.28.4, "CCMAdmin User Name and Password Configuration," on page 87.

Parameter	How to Set It
Treat Access Denied errors as "Up"?	When no password or user name is specified for ccmadmin, the URL check for ccmadmin will produce an "access denied" error. However, because the script determines whether the Web page is available, you may want the user name/password prompt to appear (to avoid exposing the admin password). Therefore, if a user name/password is specified (i.e., the user name and password are *not* blank), set this parameter to n. If no user name/password is specified (i.e., if the user name or password is blank), set this parameter to y. The default is y.
Number of times to retry after a fail	Specify the number of times to retry the connection. The default is 3 times.
Amount of time to wait between retries	Specify the number of seconds to wait for a connection before timing out and returning an error. The default is 0 seconds.
Event severity when Web page is inaccessible	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Monitor IIS server and site(s)?	Set to **y** to monitor the IIS server and associated sites. The default is y.
Auto-start monitored server and site(s)?	Set to **y** to automatically restart down IIS servers and sites. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has been set not to restart the service. The default is 18.

4.28.4 CCMAdmin User Name and Password Configuration

If you require a user name and password for access to your `ccmadmin` Web page, configure that information into AppManager Security Manager. Then, when you run CCM_SecureWebPageCheck or CCM_WebPageCheck, the script will have authority to access the Web page.

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

Field	Description
Label	CCMADMIN
Sub-label	User name required for accessing the ccmadmin Web page
Value 1	Password required for accessing the ccmadmin Web page
Extended application support	Encrypts the user name and password in Security Manager. Do not leave this option unselected.

4.29 CCM_SystemPerformance

Use this Knowledge Script to monitor Cisco CallManager for call throttling, signals in queue, and severe and warning call-throttling states. Call throttling allows administrators to define CallManager performance parameters to limit the number of incoming calls from phones, IOS gateways, MGCP gateways, and MGCP PRI gateways. The CallManager code red and code yellow call-throttling states map to AppManager severe and warning level states, respectively.

NOTE: This script is supported only for CallManager versions 3.3(4) and later.

4.29.1 Resource Object

CCM parent object

4.29.2 Default Schedule

By default, this script runs every five minutes.

4.29.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor Call Throttling	
Event Notification	
Raised event if threshold is exceeded?	Select **Yes** to raise an event if either or both of the call throttling thresholds are exceeded. The default is Yes.
Threshold - Maximum rejected calls	Specify the maximum number of calls that can be rejected due to call throttling before an event is raised. The default is 10 calls.
Threshold - Maximum throttled skinny devices	Specify the maximum number of skinny devices that can be throttled before an event is raised. The default is 10 devices.
Event severity when rejected calls exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of rejected calls exceeds the threshold that you set. The default is 5.
Event severity when throttled skinny devices exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of throttled skinny devices exceeds the threshold that you set. The default is 5.
Raise event if severe call-throttling state entered?	Select **Yes** to raise an event if call throttling enters a severe (Code Red) state. The default is Yes.
Event severity when severe state entered	Set the severity level, from 1 to 40, to reflect the importance of an event in which call throttling has entered a severe state. The default is 5.
Raise event if warning call-throttling state entered?	Select **Yes** to raise an event if call throttling enters a warning (Code Yellow) state. The default is unselected.

Parameter	How to Set It
Event severity when warning state entered	Set the severity level, from 1 to 40, to reflect the importance of an event in which call throttling has entered a warning state. The default is 15.
Data Collection	
Collect data for call throttling?	Select **Yes** to collect data about calls rejected due to call throttling and about throttled skinny devices. The default is unselected.
Monitor Signals in Queue	
Event Notification	
Raise event if threshold is exceeded?	Select **Yes** to raise an event if either or both of the signal thresholds are exceeded. The default is Yes.
Threshold - Maximum high-priority signals in queue	Specify the maximum number of high-priority signals that can be in queue before an event is raised. The default is 500.
Threshold - Maximum normal-priority signals in queue	Specify the maximum number of normal-priority signals that can be in queue before an event is raised. The default is 1000.
Event severity when high-priority signals exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of high-priority signals in queue exceeds the threshold that you set. The default is 5.
Event severity when normal-priority signals exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of normal-priority signals in queue exceeds the threshold that you set. The default is 5.
Data Collection	
Collect data for signals in queue?	Select **Yes** to collect data about high and normal priority queue signals. The default is unselected.

4.30 CCM_SystemUsage

Use this Knowledge Script to monitor CPU and physical memory usage for the Cisco CallManager process, and total CPU and physical memory usage for the CallManager. If any threshold is exceeded, an event is raised. This script collects data about percentage of CPU and physical memory used by CallManager and percentage of CPU and physical memory used by the entire device. When monitoring a device without the CallManager process (such as a standalone Publisher) only the percentage of CPU and physical memory used by the device are collected. To make the most of the data collected by this script, run Report_SystemUsage.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, “Recommended Knowledge Script Groups,” on page 216.

TIP: On the Advanced tab, set the *Raise event if event condition occurs* parameter to **3** times within **3** job iterations to prevent the raising of events during peak usage.

4.30.1 Resource Object

CCM parent object

4.30.2 Default Schedule

By default, this script runs every five minutes.

4.30.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about CPU and memory usage or reports and graphs. The default is y.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40,to indicate the importance of an event in which a threshold is exceeded. The default is 10.
Threshold - Maximum CallManager CPU usage	Specify the maximum percentage of CallManager CPU resources that can be used before an event is raised. The default is 65%.
Threshold - Maximum total CPU usage	Specify the maximum percentage of system CPU resources that can be used before an event is raised. The default is 80%.
Threshold - Maximum CallManager memory usage	Specify the maximum amount of CallManager memory resources that can be used before an event is raised. The default is 65%.
Threshold - Maximum total memory usage	Specify the maximum percentage of system memory resources that can be used before an event is raised. The default is 80%.

4.31 CCM_T1Channels

Use this Knowledge Script to monitor the number of active and in-service T1-CAS (channel associated signaling) channels for this CallManager. This script raises an event if a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

4.31.1 Resource Object

CCM Call Processor

4.31.2 Default Schedule

By default, this script runs every five minutes.

4.31.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data about T1-CAS channels for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Threshold - Maximum active T1-CAS channels	Specify the maximum number of T1-CAS channels that can be active before an event is raised. The default is 10 channels.
Threshold - Minimum T1-CAS spans in service	Specify the minimum number of T1-CAS spans that can be in service before an event is raised. The default is 0 channels.

4.32 CCM_WebPageCheck

Use this Knowledge Script to monitor accessibility to the `ccmadmin` and `ccmuser` Web pages and raise an event if the Web pages cannot be accessed. This script can collect data about the availability of the Web pages and round-trip connection time. If a URL is not reachable, the detail message records the reason (for example, because the format of the request was invalid or the server name was not found). If the Web pages cannot be accessed, you can arrange for this script to restart the IIS server and sites that are down.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, “Recommended Knowledge Script Groups,” on page 216.

NOTE: This script is not supported for Cisco CallManager versions 4.1 and later. If you are running 4.1 or later, use CCM_SecureWebPageCheck.

4.32.1 Resource Objects

CCM IIS Server

CCM IIS W3SRV

CCM IIS WebInst

4.32.2 Default Schedule

By default, this script runs every 30 minutes.

4.32.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Web page is inaccessible?	Set to **y** to raise an event if either Web page is inaccessible. The default is y.
Collect data for up/down URL?	Set to **y** to collect data about the up and down status of the URL. If set to y, the script returns a value of 100 if the connection is up and a value of 0 if the connection is down. The default is y.
Collect data for round-trip time?	Set to **y** to collect information about the round-trip connection time (in seconds). The default is n.
Monitor ccmadmin?	Set to **y** to monitor ccmadmin. The default is y.
Monitor ccmuser?	Set to **y** to monitor ccmuser. The default is y.
Username for ccmadmin	Enter the user name to use when logging on to ccmadmin. If a user name is not required, you can leave this field blank. For more information about the user name, see Section 4.28.4, “CCMAdmin User Name and Password Configuration,” on page 87. **NOTE**: If you installed Cisco CallManager MLA (multi-level administration), this script will only verify that the ccmadmin Web page is present. It will not log in. Therefore, if you have MLA, there is no need to enter the user name.
Treat Access Denied errors as "Up"?	When no password or user name is specified for ccmadmin, the URL check for ccmadmin will produce an "access denied" error. However, because the script determines whether the Web page is available, you may want the user name/password prompt to appear, to avoid exposing the admin password. Therefore, if the user name and password are not blank, set this parameter to n. If the user name or password is blank, set this parameter to y. The default is y.
Number of times to retry after a fail	Specify the number of times to retry the connection. The default is 3 times.
Amount of time to wait between retries	Specify the number of seconds to wait for a connection before timing out and returning an error. The default is 0 seconds.
Event severity when Web page is inaccessible	Set the event severity level, from 1 to 40,to indicate the importance of an event in which a Web page is inaccessible. The default is 8.
Monitor IIS server and site(s)?	Set to **y** to monitor the IIS server and associated sites. The default is y.
Auto-start monitored server and site(s)?	Set to **y** to automatically restart down IIS servers and sites. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.

Parameter	How to Set It
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has not been set to restart the service. The default is 18.

4.33 CDRQuery

Use this Knowledge Script to query the CDR (Call Detail Records) table on the CallManager Publisher. The purpose of this script is twofold:

- Monitoring. In monitoring mode, this script checks the CDR tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in the CDR table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- Diagnostic. In diagnostic mode, this script runs once, and checks the CDR tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. To run this script in diagnostic mode, select Run once on the Schedule tab.

4.33.1 Resource Object

CCM Publisher

4.33.2 Default Schedule

By default, this script runs once.

4.33.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Options	
CDR database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.

Parameter	How to Set It
Select event format	Select the format in which you want to receive the informational event: CSV, XML, or Both. The default is XML. ◆ Select **CSV** (comma-separated value) to format an event message that can be forwarded to an Action script that is triggered by the event (if you have selected to initiate an Action script when an event is raised). ◆ Select **XML** to format an event message that is not forwarded to an Action script. ◆ Select **Both** to generate two event messages: one in CSV format, which is forwarded to an Action script, and one in XML format. If you select **Both**, the CSV event is collapsed under the XML event; it is not displayed in the Operator Console. To access the CSV event, turn off "Collapse duplicate events into a single event" on the Advanced tab before running this script. **NOTE**: Error messages are formatted in plain text — this parameter does not apply to error messages.

Parameter	How to Set It
Columns to return	Select the columns that you want returned from the query: All, Basic, or Minimal. The default is Basic. Choose All to return all columns in the CDR table. Different versions of CallManager contain different columns in the CDR tables; you should check your CallManager documentation to see which columns you have. Choose Basic to return the following columns: ◆ origDeviceName ◆ origIpAddr ◆ callingPartyNumber ◆ origMediaCap_payloadCapability ◆ destDeviceName ◆ destIpAddr ◆ originalCalledPartyNumber ◆ finalCalledPartyNumber ◆ destMediaCap_payloadCapability ◆ dateTimeOrigination ◆ dateTimeConnect ◆ dateTimeDisconnect ◆ duration ◆ originalCalledPartyNumberPartition ◆ callingPartyNumberPartition ◆ finalCalledPartyNumberPartition ◆ origCause_value ◆ destCause_value Choose Minimal to return the following columns: ◆ origDeviceName ◆ origIpAddr ◆ callingPartyNumber ◆ destDeviceName ◆ destIpAddr ◆ originalCalledPartyNumber ◆ finalCalledPartyNumber ◆ dataTimeConnect ◆ dataTimeDisconnect ◆ duration
Collect data?	Set to **y** to collect data for graphs and charts. This script collects one data stream for the number of records found. The default is n.
Threshold	

Parameter	How to Set It
Threshold - Maximum matching records	Specify how many records must match the specified query before an event is raised. The default is 0, which means that an event is raised if at least one record matches the query.
Query Filters	
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of **0** if you do not want to filter for minimum call duration.
Maximum duration	Set this parameter to filter out records whose call duration is less than or equal to the specified value. Accept the default of **0** if you do not want to filter for maximum call duration.
Calling directory number	Set this parameter to the number of the calling directory that you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any calling directory number.
Directory number connector	Set this parameter ONLY if you specify both a *Calling directory number* and a *Called directory number*. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Called directory number	Set this parameter to the number of the called directory that you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any called directory number.
Originating device name	Set this parameter to query for those calls whose originating device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any originating device name.
Device name connector	Set this parameter ONLY if you specify both an *Originating device name* and a *Destination device name*. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Destination device name	Set this parameter to query for those calls whose destination device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any destination device name.
Events	
Raise event if threshold is exceeded?	Set to **y** to raise an event if the matching records threshold is exceeded. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.
Event severity when no records are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the script finds no records in the CDR. Accept the default of **0** if you do not want to raise an event for this situation.
Custom event message	Provide a custom message for the event, such as "Calls to 911" or "Calls exceeding 30 minutes." The default message is "# of records exceeded the threshold."
Diagnostics	
Select call disconnect time range	Select a Specific or Sliding date/time range for which the query should search for data. The default time range is fixed at 24 hours. Note This parameter is valid only when you select Run once on the Schedule tab.

4.34 CiscoBackupStatus

Use this Knowledge Script to monitor the Cisco IP Telephony Applications Backup Utility (`stiBack.exe`) program or the Cisco BARS (Backup and Restore System) program. This script verifies that the corresponding backup service is running and restarts the service if you choose. It reads the backup log to check the status of the previous backup. This script raises an event if the previous backup failed and can raise an event for successful backups.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.34.1 Resource Object

CCM Backup Utility

4.34.2 Default Schedule

By default, this script runs every two hours.

4.34.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start backup service?	Select **Yes** to automatically restart stiBack.exe or BARS if it is down. The default is Yes.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the service is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the service was down but AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "No"	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the service is down and that AppManager has been set to not restart it. The default is 18.
Event Notification	
Raise event if backup succeeds?	This script always raises an event when it determines that the backup has failed. In addition, you can set this parameter to **Yes** to raise an event when the script determines that the backup has succeeded. The default is Yes.
Event severity when backup succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which backup succeeds. The default is 25.
Event severity when backup fails	Set the event severity level, from 1 to 40, to reflect the importance an event in which backup fails. The default is 5.
Ignore DC Directory service errors?	Select **Yes** to ignore errors related to the DC Directory service, such as failures to restore, stop, and restart. The default is unselected.

4.35 ConfBridgeActiveConf

Use this Knowledge Script to monitor the number of active conferences for a Conference Bridge. If the number of active conferences exceeds the threshold, an event is raised.

4.35.1 Resource Object

CCM Conference Bridge object

4.35.2 Default Schedule

By default, this script runs every 30 minutes.

4.35.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active conferences for graphs and reports. The default is n.
Threshold - Maximum active conferences	Specify the maximum number of conferences that can be active before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.36 ConfBridgeActiveStreams

Use this Knowledge Script to monitor the number of active streams for a Conference Bridge. This script raises an event if the number of active streams exceeds the threshold.

4.36.1 Resource Object

CCM Conference Bridge object

4.36.2 Default Schedule

By default, this script runs every 30 minutes.

4.36.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active streams for graphs and reports. The default is n.
Threshold - Maximum active streams	Specify the maximum number of streams that can be active before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.37 ConfBridgeAvailStreams

Use this Knowledge Script to monitor the number of available streams for a Conference Bridge. This script raises an event if the number of available streams falls below the threshold.

4.37.1 Resource Object

CCM Conference Bridge object

4.37.2 Default Schedule

By default, this script runs every 30 minutes.

4.37.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available streams falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available streams for graphs and reports. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to “backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Threshold - Minimum available streams	Specify the minimum number of streams that can be available before an event is raised. The default is 20.
Event severity when threshold is not met	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is not met. The default is 25.

4.38 ConfBridgeConferences

Use this Knowledge Script to monitor the number of conferences completed during an interval. This script raises an event if the number of completed conferences exceeds the threshold.

4.38.1 Resource Object

CCM Conference Bridge object

4.38.2 Default Schedule

By default, this script runs every 30 minutes.

4.38.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about completed conferences for graphs and reports. The default is n.
Threshold - Maximum completed conferences	Specify the maximum number of conferences that can be completed before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.39 ConfBridgeStreams

Use this Knowledge Script to monitor the number of streams on conferences that were completed during an interval. This script raises an event if the number of streams exceeds the threshold.

4.39.1 Resource Object

CCM Conference Bridge object

4.39.2 Default Schedule

By default, this script runs every 30 minutes.

4.39.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about conference bridge streams for graphs and reports. The default is n.
Threshold - Maximum streams	Set the threshold for the number of streams. If the number exceeds this amount, an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.40 CTI_Manager

Use this Knowledge Script to monitor the number of CTI (Computer Telephony Interface) manager connections, open devices, open lines, and active CallManager links. This script raises an event if a value exceeds or falls below a threshold you set.

4.40.1 Resource Object

CCM CTI object

4.40.2 Default Schedule

By default, this script runs every 10 minutes.

4.40.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about connections, devices, lines, and links for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.

Parameter	How to Set It
Threshold - Maximum active CallManager links	Specify the maximum number of CallManager links that can be active before an event is raised. Enter -1 to ignore this parameter. The default is 10.
Threshold - Minimum active CallManager links	Specify the minimum number of CallManager links that can be active before an event is raised. Enter -1 to ignore this parameter. The default is 0.
Threshold - Maximum CTI connections	Specify the maximum number of CTI connections that can occur before an event is raised. Enter -1 to ignore this parameter. The default is 100.
Threshold - Minimum CTI connections	Specify the minimum number of CTI connections that can occur before an event is raised. Accept the default of -1 to ignore this parameter.
Threshold - Maximum open CTI devices	Specify the maximum number of CTI devices that can be open before an event is raised. Enter -1 to ignore this parameter. The default is 100.
Threshold - Minimum open CTI devices	Specify the minimum number of CTI devices that can be open before an event is raised. Accept the default of -1 to ignore this parameter.
Threshold - Maximum open CTI lines	Specify the maximum number of CTI lines that can be open before an event is raised. Enter -1 to ignore this parameter. The default is 100.
Threshold - Minimum open CTI lines	Specify the minimum number of CTI lines that can be open before an event is raised. Accept the default of -1 to ignore this parameter.

4.41 DigitalOutboundBusy

Use this Knowledge Script to monitor the number of times during an interval that a call through this digital access was attempted when no ports were available. This script raises an event if the number of outbound busy attempts exceeds the threshold.

4.41.1 Resource Object

CCM Digital Access object

4.41.2 Default Schedule

By default, this script runs every 30 minutes.

4.41.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about outbound busy attempts for graphs and reports. The default is n.

Parameter	How to Set It
Threshold - Maximum outbound busy attempts	Specify the maximum number of outbound busy attempts that can occur before an event is raised. The default is 100.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the template is exceeded. The default is 25.

4.42 DigitalPortsActive

Use this Knowledge Script to monitor the number of active digital ports. This script raises an event if the number of active digital ports exceeds the threshold.

4.42.1 Resource Object

CCM Digital Access object

4.42.2 Default Schedule

By default, this script runs every 30 minutes.

4.42.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active ports for graphs and reports. The default is n.
Threshold - Maximum active ports	Specify the maximum number of ports that can be active before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

4.43 DigitalPortsOutOfService

Use this Knowledge Script to monitor the number of digital ports that are out of service. This script raises an event if the number of out-of-service digital ports exceeds the threshold.

4.43.1 Resource Object

CCM Digital Access object

4.43.2 Default Schedule

By default, this script runs every 30 minutes.

4.43.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about out-of-service ports for graphs and reports. The default is n.
Threshold - Maximum active ports	Specify the maximum number of ports that can be active before an event is raised. The default is 2.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active ports exceeds the threshold. The default is 15.

4.44 H323CallActivity

Use this Knowledge Script to monitor completed calls, attempted calls, and incomplete calls on H.323 devices for CallManager 4.2. This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Attempted calls per device
- Attempted calls for all devices
- Incomplete calls (%) per device
- Incomplete calls (%) for all devices

TIP: Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

4.44.1 Resource Object

CCM H.323 Device object

4.44.2 Default Schedule

By default, this script runs every five minutes.

4.44.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	

Parameter	How to Set It
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the H323CallActivity job fails. The default is 5.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if attempted calls exceed threshold?	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 0 attempts.
Event severity when attempted calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold. The default is 15.
Raise event if percentage of incomplete calls exceeds threshold?	Select **Yes** to raise an event if the percentage of incomplete calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of incomplete calls	Specify the maximum percentage of incomplete calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of incomplete calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of incomplete calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of attempted calls per monitored device. The default is unselected.
Collect data for percentage of incomplete calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of incomplete calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the **Objects** tab. Leave this field blank to accept the default group name: `H323_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if attempted calls exceed threshold?	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 0 attempts.
Event severity when attempted calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold. The default is 15.
Raise event if percentage of incomplete calls exceeds threshold?	Select **Yes** to raise an event if the percentage of incomplete calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of incomplete calls	Specify the maximum percentage of incomplete calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of incomplete calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of incomplete calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of attempted calls per group. The default is unselected.
Collect data for percentage of incomplete calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of incomplete calls per group. The default is unselected.

4.45 H323CallsAttempted

Use this Knowledge Script to monitor the number of calls attempted by an H.323 device during an interval. This script raises an event if a threshold is exceeded.

4.45.1 Resource Object

CCM H.323 Device object

4.45.2 Default Schedule

By default, this script runs every 30 minutes.

4.45.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about attempted H.323 calls for graphs and reports. The default is n.
Threshold - Maximum attempted calls	Specify the maximum number of H.323 calls that can be attempted before an event is raised. The default is 100.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.46 H323CallsInProgress

Use this Knowledge Script to monitor the number of calls in progress for an H.323 device. This script raises an event if a threshold is exceeded.

4.46.1 Resource Object

CCM H.323 Device object

4.46.2 Default Schedule

By default, this script runs every 30 minutes.

4.46.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about in-progress H.323 calls for graphs and reports. The default is n.
Threshold - Maximum in-progress calls	Specify the maximum number of calls that can be in progress before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.47 IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if CPU usage exceeds the threshold that you set.

4.47.1 Resource Object

CCM IIS Server

4.47.2 Default Schedule

By default, this script runs every five minutes.

4.47.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data for CPU usage?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Process names	Specify the name of the application processes you want to monitor. The default is `inetinfo`. Separate multiple entries with commas. For example: `inetinfo,dllhost` **NOTE**: Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.

4.48 IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. If any server or Web site is not running, an event is raised. In addition, you can choose to automatically restart the IIS server or Web site. If the blocked I/O queue length is longer than the specified threshold, an event is raised.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

4.48.1 Resource Objects

CCM IIS server

CCM IIS FTP server

CCM IIS W3SRV

CCM IIS WebInst

4.48.2 Default Schedule

By default, this script runs every five minutes.

4.48.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart down servers. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has been set not to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of blocked requests exceeds the threshold. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum number of I/O requests that can be in queue before an event is raised. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

4.49 IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. If one or both processes exceed the CPU usage threshold you set, an event is raised. You can set this script to automatically stop a process that exceeds the CPU usage threshold.

4.49.1 Resource Object

CCM IIS server

4.49.2 Default Schedule

By default, this script runs every three minutes.

4.49.3 Setting Parameters Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event if an attempt to stop a process is successful or unsuccessful. The default is y.
Kill CPU-intensive processes?	Set to **y** to automatically stop any process that exceeds the threshold. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU usage allowed by the dllhost and mtx processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager has successfully stopped the process. The default is 20.

4.50 IIS_MemoryHigh

Use this Knowledge Script to detect whether an IIS application process has exceeded the memory usage threshold you set. This script monitors the number of bytes of memory being used by the specified process. This script raises an event if an application process exceeds the memory usage threshold you set.

4.50.1 Resource Object

CCM IIS server

4.50.2 Default Schedule

By default, this script runs every five minutes.

4.50.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.

Parameter	How to Set It
Process names	Specify the name of the application process you want to monitor. The default is `inetinfo`. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost` **NOTE**: Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

4.51 IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server either successfully restarts or fails to restart.

4.51.1 Resource Object

CCM IIS server

4.51.2 Default Schedule

By default, this script runs once.

4.51.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is five seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default if 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.

Parameter	How to Set It
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

4.52 IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if the amount of time the sites and services are running is less than the threshold you set.

NOTE: This script supports IIS versions 5 and later.

4.52.1 Resource Objects

IIS Web server and FTP server

4.52.2 Default Schedule

By default, this script runs every one hour.

4.52.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event in uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about service uptime for reports and graphs. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of uptime that is required for Web/FTP sites and services to prevent an event from being raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

4.53 LineStatus

Use this Knowledge Script to monitor the status (number of active calls) of an individual phone line. This script raises an event if the number of calls exceeds the threshold.

4.53.1 Resource Objects

CCM Lines folder

4.53.2 Default Schedule

By default, this script runs every 30 minutes.

4.53.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about line status for graphs and reports. The default is n.
Phone lines	Enter a comma-separated list of phone names to which you want to test communication.
Threshold - Maximum calls	Specify the most calls a phone line can have before an event is raised. The default is 1 call.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.54 LocationBandwidth

Use this Knowledge Script to monitor bandwidth statistics for a Location resource, if that resource has been defined in CallManager.

The Locations feature in Cisco CallManager provides call admission control for centralized call processing systems. Call admission control enables you to control the audio quality of calls over a wide area (IP WAN) link by limiting the number of calls allowed on the link at the same time. A centralized system uses a single Cisco CallManager cluster to control all of the locations.

In a centralized call processing system, the Cisco CallManager cluster resides at the main location along with other devices such as phones and gateways. Remote locations, such as branch offices of your company, house additional phones and other devices, but do not contain any call processing capability. The remote locations connect to the main location and to each other by means of IP WAN links.

Calls between devices at the same location do not need call admission control because those devices reside on the same LAN, which has unlimited available bandwidth. However, calls between devices at different locations must travel over an IP WAN link, which has limited available bandwidth. The Locations feature lets you specify the maximum amount of bandwidth available for calls to and from each location, thereby limiting the number of active calls and preventing oversubscription of the bandwidth on the IP WAN links.

For bandwidth calculations, CallManager assumes that each call consumes the following amount of bandwidth:

- G.711 calls use 80 kbps
- G.723 calls use 24 kbps
- G.729 calls use 24 kbps

- GSM calls use 29 kbps
- Wideband calls use 272 kbps

4.54.1 Resource Objects

CCM Location object

4.54.2 Default Schedule

By default, this script runs every 10 minutes.

4.54.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about bandwidth for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Threshold - Minimum available bandwidth	Specify the minimum amount of bandwidth that can be available before an event is raised. The default is 500 kbps.
Threshold - Maximum bandwidth in use	Specify the maximum amount of bandwidth that can be in use before an event is raised. The default is 75%.

4.55 LocationOutOfBandwidth

Use this Knowledge Script to monitor the number of times that calls through a particular Location failed due to lack of bandwidth. This script raises an event if the number of failures exceeds the threshold that you set. In addition, this script generates a data stream for the number of bandwidth failures.

4.55.1 Resource Object

CCM Location object

4.55.2 Default Schedule

By default, this script runs every 10 minutes.

4.55.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LocationOutOfBandwidth job fails. The default is 5.
Monitor Out of Bandwidth Failures	
Event Notification	
Raise event if bandwidth failures exceed threshold?	Select **Yes** to raise an event if the number of calls that fail due to lack of bandwidth exceeds the threshold that you set. The default is 3 calls
Event severity when bandwidth failures exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of bandwidth failures exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for bandwidth failures?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that failed due to lack of bandwidth.

4.56 LossOfHardwarePhones

Use this Knowledge Script to monitor the number of registered hardware phones. This script raises an event if the number of lost phones exceeds a specified number or percentage during the monitored interval.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

You can also use this script to help you monitor phone status. For more information, see CCM_PhoneInventory.

4.56.1 Comparing Results of LossOfHardwarePhones and CCM_PhoneInventory

You can use the LossOfHardwarePhones script to launch an Action script that, in turn, launches the CCM_PhoneInventory script. By doing so, you can improve upon the results you get from LossOfHardwarePhones.

For example, say LossOfHardwarePhones indicates you have lost five phones since the last time it ran. But you configured the script to launch Action_RunPhoneInventory when the lost-phone event was raised, so CCM_PhoneInventory further refined the results. Based on criteria you selected, CCM_PhoneInventory identified the five phones by Directory Number, or Device Pool, or Subnet, or several other filtering options.

For several reasons, however, it is possible your results were inconsistent between LossOfHardwarePhones and CCM_PhoneInventory. Although you cannot fix the consistency problem, you can understand why it occurred:

- The scripts obtain phone data from two different sources. LossOfHardwarePhones uses the Performance Monitor counters on the Subscriber; CCM_PhoneInventory makes an API call to query phone information from the Publisher.
- The Subscriber and the Publisher can be out of sync because of the difference between timing windows or a lack of connectivity between the two devices. The information that is available from the two devices can change between the time LossOfHardwarePhones checks the counters and CCM_PhoneInventory makes its API call.
- Even if the Subscriber and the Publisher are in sync, differences in filtering can produce inconsistent results. The data from LossOfHardwarePhones is unfiltered — it includes everything; the data from CCM_PhoneInventory can be filtered by subnet, Directory Number, or several other filtering options.

4.56.2 Resource Object

CCM Subscriber

4.56.3 Default Schedule

By default, this script runs every five minutes.

4.56.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor Loss of Hardware Phones	
Event Notification	
Raise event if threshold is exceeded?	Select **Yes** to raise an event if a threshold is crossed. The default is Yes.
Threshold type	Select whether you want to set a threshold for the **Number** of lost phones or a **Percent** of hardware phones. The default is Percent.
Threshold - Maximum # lost hardware phones	Specify the maximum number of hardware phones that can be lost before an event is raised. The default is 24.
Threshold - Maximum % lost hardware phones	Specify the maximum percentage of hardware phones that can be lost before an event is raised. The default is 10%.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 10.
Data Collection	
Collect data for lost hardware phones?	Select **Yes** to collect data about lost phones for graphs and reports. The default is unselected.

4.57 MGCP_FXO

Use this Knowledge Script to monitor completed calls, outbound busy attempts, and blocked calls for Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

TIP: Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

4.57.1 Resource Object

CCM MGCP FXO object

4.57.2 Default Schedule

By default, this script runs every 10 minutes.

4.57.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_FXO job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `FXO_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

4.58 MGCP_FXS

Use this Knowledge Script to monitor completed calls, outbound busy attempts, and blocked calls for Media Gateway Control Protocol (MGCP) Foreign Exchange Station (FXS) devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

TIP: Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

4.58.1 Resource Object

CCM MGCP FXS object

4.58.2 Default Schedule

By default, this script runs every 10 minutes.

4.58.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_FXS job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `FXS_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.

Parameter	How to Set It
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

4.59 MGCP_Gateway_CCM30

Use this Knowledge Script to monitor the station ports and voice channels for Media Gateway Control Protocol (MGCP) devices in CallManager 3.0. This script raises an event if a threshold is exceeded.

4.59.1 Resource Object

CCM MGCP Gateway object

4.59.2 Default Schedule

By default, this script runs every 10 minutes.

4.59.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about station ports and voice channels for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Monitor station ports?	Set to **y** to monitor station ports. The default is y.
Threshold - Maximum active station ports	Specify the maximum number of station ports that can be active before an event is raised. The default is 10 ports.
Monitor voice channels?	Set to **y** to monitor voice channels. The default is n.
Threshold - Maximum active voice channels	Specify the maximum number of voice channels that can be active before an event is raised. The default is 10 channels.

4.60 MGCP_Gateway_CCM31

Use this Knowledge Script to monitor the number of active MGCP Gateway station ports or voice channels for Media Gateway Control Protocol (MGCP) devices in CallManager 3.1 and later.

This script collects the data used by the Report_MGCPGatewayUsage Knowledge Script.

4.60.1 Resource Object

CCM MGCP Gateway object

4.60.2 Default Schedule

By default, this script runs every 10 minutes.

4.60.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about station ports and voice channels for reports and graphs. The default is n.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Monitor FXO ports?	Set to **y** to monitor FXO (foreign exchange office) ports. The default is n.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that can be active before an event is raised. The default is 10 ports.
Threshold - Minimum FXO ports in service	Specify the minimum number of FXO ports that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.
Monitor FXS ports?	Set to **y** to monitor FXS (foreign exchange station) ports. The default is n.
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that can be active before an event is raised. The default is 10 ports.
Threshold - Minimum FXS ports in service	Specify the minimum number of FXS ports that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.
Monitor PRI voice channels?	Set to **y** to monitor PRI (primary rate interface) channels. The default is y.
Threshold - Maximum active PRI voice channels	Specify the maximum number of PRI voice channels that can be active before an event is raised. The default is 10 channels.
Threshold - Minimum PRI channels in service	Specify the minimum number of PRI voice channels that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.

Parameter	How to Set It
Monitor T1_CAS voice channels?	Set to **y** to monitor T1-CAS (channel associated signaling) channels. The default is n.
Threshold - Maximum active T1-CAS voice channels	Specify the maximum number of T1 CAS voice channels that can be active before an event is raised The default is 10 channels.
Threshold - Minimum T1-CAS channels in service	Specify the minimum number of T1-CAS voice channels that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.

4.61 MGCP_GatewayCheck

Use this Knowledge Script to monitor your CallManager for new and missing MGCP gateways. With each iteration of the job, this script creates a list of the MGCP gateways that are registered to the CallManager, and then compares the latest list information with the information from the previous list.

The list created by this script is sorted by the description of the MGCP gateway that you entered into CallManager.

4.61.1 Resource Object

CCM MGCP Gateway folder

4.61.2 Default Schedule

By default, this script runs every 15 minutes.

4.61.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if new or missing gateways are found?	Set to **y** to raise an event if new MGCP gateways are found or if any gateway is missing within an interval that you specify. The default is y.
File name for saving list	Provide a name for the list of new or missing MGCP gateways. The default is `NQMGCPList`.
Raise event for the initial list?	Set to **y** to raise an event for the first time that this script creates a list. The default is n.
Event severity when MGCP gateways are missing	Set the severity level, from 1 to 40, to reflect the importance of an event in which MGCP gateways are missing. The default is 15.
Event severity when new MGCP gateways are found	Set the severity level, from 1 to 40, to reflect the importance of an event in which new MGCP gateways are found. Enter **0** if you do not want to raise an event. The default is 30.

4.62 MGCP_PRI

Use this Knowledge Script to monitor completed calls, outbound busy attempts, blocked calls, and data link availability for Media Gateway Control Protocol (MGCP) Primary Rate Interface (PRI) devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

TIP: Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

4.62.1 Resource Object

CCM MGCP PRI object

4.62.2 Default Schedule

By default, this script runs every 10 minutes.

4.62.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_PRI job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Raise event if data link out of service?	Select **Yes** to raise an event if the PRI data link is out of service. The default is Yes.
Event severity when data link out of service	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PRI data link is out of service. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `PRI_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.

Parameter	How to Set It
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

4.63 MGCP_PRI_Channels

Use this Knowledge Script to monitor an individual MGCP PRI device for active and out-of-service channels. In addition, you can run this script to monitor the number of active channels for a group of MGCP PRI devices. To monitor a group, run the script on the MGCP PRI Devices folder in the TreeView pane (instead of running it on an individual PRI device) and then use the Objects tab to select the PRI devices that you want to include in the group.

The first time you run this script, you can raise an informational event whose event message will contain the current status of all the channels being monitored. The possible statuses are listed below:

- 0 (unknown) - Indicates this channel is not defined. For example, channels 25-31 on T1-PRI devices are not defined. These channels are used by E1-PRI devices.
- 1 (out of service) - Indicates this channel is not available for use.
- 2 (idle) - Indicates this channel has no active call and is ready for use.
- 3 (busy) - Indicates an active call on this channel.
- 4 (reserved) - Indicates this channel has been reserved for use as a D-Channel or as a Synch-Channel for E1.

The detailed event messages and detailed data stream messages will contain the number of channels that are active or out-of-service.

The detailed event message and detailed data stream messages for a group of devices will contain the number of active channels for each device in the group.

This script collects the data used by the Report_MGCPChannelUsage Knowledge Script.

NOTE: If you use this script to monitor a group of devices, NetIQ Corporation recommends that you make a copy of the script and then rename it to something more specific to your needs, such as "Headquarter_Gateway_Activity" or "PSTN_Gateway_Actvity."

4.63.1 Resource Object

CCM MGCP PRI object

4.63.2 Default Schedule

By default, this script runs every five minutes.

4.63.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y. This script can collect data streams for the number of active channels and, optionally, the number of out-of-service channels.
Monitor these channels	Provide a range or a comma-separated list of the channel numbers that you want to monitor. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31. The default is 1-23.
Exclude these channels	Provide a range or a comma-separated list of the channel numbers that you want to exclude from monitoring. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31.
Threshold - Maximum active channels for any device	Specify the maximum number of monitored channels that can be active (status = 3) before an event is raised. The default is 20.
Event severity when active channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active channels exceeds the threshold. The default is 15.
Monitor out-of-service channels?	Set to **y** to monitor out-of-service channels. The default is y.
Threshold - Maximum out-of-service channels	Specify the maximum number of monitored channels that can be out-of-service (status = 1) for an individual device. If the number of out-of-service channels exceeds this amount, an event is raised. The default is 0 channels.

Parameter	How to Set It
Event severity when out-of-service channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-service channels exceeds the threshold. The default is 5.
Collect data for out-of-service channels?	Set to **y** to collect data about the number of out-of-service channels for reports and graphs. The default is n.
Raise event with current status?	Set to **y** to create an event that indicates the current status of the channels. The default is n.
Additional event information	Enter any additional message text that you want to append to the Detailed Event Message for any events that are raised. You can enter up to 128 characters.
Monitor totals for a group of devices	Set to **y** to monitor all the devices in the group for which you are running this script. The default is y.
Name this group of PRI devices	If you are monitoring a group of PRI devices, enter a name for the group. This name will be displayed on events and charts. If no name is entered, this script generates a default name based on the current time.
Threshold - Maximum active channels for group of devices	Specify the maximum number of monitored channels that can be active (status = 3) for all devices in the group. If the number of active channels exceeds this amount, an event is raised. The default is 1250 channels.
Event severity when active channels for group exceed the threshold	Set the severity level, from 1 to 40, to indicate that the number of active channels for the entire group of PRI devices being monitored has exceeded the threshold. The default is 15.

4.64 MGCP_T1CAS

Use this Knowledge Script to monitor completed calls, outbound busy attempts, blocked calls, and data link availability for Media Gateway Control Protocol (MGCP) T1-CAS devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

TIP: Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

4.64.1 Resource Object

CCM MGCP T1-CAS object

4.64.2 Default Schedule

By default, this script runs every 10 minutes.

4.64.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_T1CAS job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Raise event if data link out of service?	Select **Yes** to raise an event if the T1-CAS data link is out of service. The default is Yes.

Parameter	How to Set It
Event severity when data link out of service	Set the severity level, from 1 to 40, to indicate the importance of an event in which the T1-CAS data link is out of service. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `T1CAS_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.

Parameter	How to Set It
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

4.65 MGCP_T1CAS_Channels

Use this Knowledge Script to monitor an individual MGCP T1-CAS device for active and out-of-service channels. In addition, you can run this script to monitor the number of active channels for a group of MGCP T1-CAS devices. To monitor a group, run the script on the MGCP T1-CAS Devices folder, instead of running it on an individual T1-CAS device. Then use the Objects tab to select the specific T1-CAS devices you want to include in the group.

The first time you run this script, you can choose to raise an informational event whose event message will contain the current status of all the channels being monitored. The possible statuses are listed below:

- 0 (unknown) - Indicates this channel is not defined.
- 1 (out of service) - Indicates this channel is not available for use.
- 2 (idle) - Indicates this channel has no active call and is ready for use.
- 3 (busy) - Indicates an active call on this channel.
- 4 (reserved) - Indicates this channel has been reserved for use as a D-Channel or as a Synch-Channel for E1.

This script collects the data used by the Report_MGCPChannelUsage Knowledge Script.

The detailed event messages and detailed data stream messages will contain the number of channels that are active or out-of-service.

The detailed event message and detailed data stream messages for a group of devices will contain the number of active channels for each device in the group.

NOTE: If you use this script to monitor a group of devices, NetIQ Corporation recommends making a copy of the script and renaming it to something more specific to your needs, such as "Headquarter_Gateway_Activity" or "PSTN_Gateway_Actvity."

4.65.1 Resource Object

CCM MGCP T1-CAS object

4.65.2 Default Schedule

By default, this script runs every five minutes.

4.65.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs.The default is y. This script can collect data streams for the number of active channels and, optionally, the number of out-of-service channels.
Monitor these channels	Specify a range or a comma-separated list of the channel numbers that you want to monitor. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31. The default is 1-23.
Exclude these channels	Specify a range or a comma-separated list of the channel numbers that you want to exclude from monitoring. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31.
Threshold - Maximum active channels for any device	Specify the maximum number of monitored channels that can be active (status = 3) before an event is raised. The default is 20 channels.
Event severity when active channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Monitor out-of-service channels?	Set to **y** to monitor out-of-service channels. The default is y.
Threshold - Maximum out-of-service channels	Specify the maximum number of monitored channels that can be out-of-service (status = 1) for an individual device before an event is raised. The default is 0.
Event severity when out-of-service channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which out-of-service channels exceed the threshold. The default is 5.
Collect data for out-of-service channels?	Set to **y** to collect data about the number of out-of-service channels for reports and graphs. The default is n.
Raise event with current status?	Set to **y** to raise an event that indicates the current status of the channels. The default is n.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor totals for a group of devices?	Set to **y** to monitor all the devices in the group for which you are running this script. The default is y.
Name this group of T1CAS devices	If you are monitoring a group of T1CAS devices, enter a name for the group. This name will be displayed on events and charts. If no name is entered, this script generates a default name based on the current time.
Threshold - Maximum active channels for all devices in group	Specify the maximum number of monitored channels that can be active (status = 3) for all devices in the group. If the number of active channels exceeds this amount, an event is raised. The default is 1250 channels.

Parameter	How to Set It
Event severity when active channels for group exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the group's active channels exceed the threshold. The default is 15.

4.66 MLA_Logins

Use this Knowledge Script to scan CallManager MLA (multi-level administration) log files for successful and failed logins. In addition to information about successful and failed logins, the log files contain the user name, group name, date, and time of the login session.

Multi-level administration allows users with full access to configure different levels of administration access for CallManager administrators. Users with full access configure functional groups, user groups, and access privileges for user groups. In general, full-access users configure the access of other users to Cisco CallManager Administration.

The first time you run this script, you can check for the number of logins during the past n hours. Subsequent runs will check for the number of logins within the specified interval.

4.66.1 Resource Object

CCM MLA object

4.66.2 Default Schedule

By default, this script runs every one hour.

4.66.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about successful and failed logins for reports and graphs. The default is n.
Log file directory	Enter the directory path to the log file. The default is `c:\ciscoWebs\MLA\logs`
On first run, scan for logins in the past N hours	Enter the number of hours of log file entries through which the script will search for trace files. For instance, if you enter 15, the script will search through the last 15 hours of log file entries. The default is 1 hour. Setting this parameter to a high value may result in high CPU usage.
Threshold - Maximum failed logins	Specify the maximum number of logins that can fail before an event is raised. The default is 3 logins.

Parameter	How to Set It
Threshold - Maximum successful logins	Set the threshold for the number of logons that have succeeded during the specified interval. If the number of successful logons exceeds this amount, an event is raised. The default is 3 logins.
Event severity when failed logins exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed logins exceeds the threshold. The default is 5.
Event severity when successful logins exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of successful logins exceeds the threshold. The default is 25.

4.67 MOHDevice

Use this Knowledge Script to monitor the number of active and available resources for Music on Hold (MOH) devices.

MOH resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

4.67.1 Resource Object

CCM MOH device object

4.67.2 Default Schedule

By default, this script runs every five minutes.

4.67.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a value exceeds or falls below a threshold. The default is y.
Collect data?	Set to **y** to collect data about MOH resources for reports and graphs. The default is n.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of an event in which a value exceeded or fell below a threshold. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.

Parameter	How to Set It
Threshold - Maximum active Multicast connections	Specify the maximum number of Multicast connections that can be active before an event is raised. The default is 25 connections.
Threshold - Maximum active Unicast connections	Specify the maximum number of Unicast connections that can be active before an event is raised. The default is 250 connections.
Threshold - Minimum available Multicast connections	Specify the minimum number of Multicast connections that must be available to prevent an event from being raised. The default is five connections.
Threshold - Minimum available Unicast connections	Specify the minimum number of Unicast connections that must be available to prevent an event from being raised. The default is 50 connections.

4.68 MOHServer

Use this Knowledge Script to monitor active and available streams for Music on Hold (MOH) servers.

MOH resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

4.68.1 Resource Object

CCM MOH server

4.68.2 Default Schedule

By default, this script runs every five minutes.

4.68.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a value exceeds or falls below a threshold. The default is y.
Collect data?	Set to **y** to collect data about MOH devices for reports and graphs. The default is n.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of an event in which a value exceeded or fell below a threshold. The default is 15.
Threshold - Maximum active audio sources	Specify the maximum number of audio sources for the MOH server that can be active before an event is raised. The default is 25 sources.
Threshold - Maximum active Music On Hold streams	Specify the maximum number of MOH streams that can be active before an event is raised. The default is 200 streams.

Parameter	How to Set It
Threshold - Minimum available Music On Hold streams	Specify the minimum number of MOH streams that must be available to prevent an event from being raised. The default is 50 streams.

4.69 MOHServer_LostConnections

Use this Knowledge Script to monitor the number of times that a Music on Hold (MOH) server lost connection with a CallManager.

MOH resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

4.69.1 Resource Object

CCM MOH server

4.69.2 Default Schedule

By default, this script runs every five minutes.

4.69.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if lost connections exceed the threshold?	Set to **y** to raise an event if the number of lost connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about lost connections for reports and graphs. The default is n.
Event severity when lost connections exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Threshold - Maximum lost connections	Specify the maximum number of lost connections that can occur before an event is raised. The default is 0 connections.

4.70 MTP_Device

Use this Knowledge Script to monitor the number of active and available resources for an individual MTP (media termination point) device. This script also monitors whether the MTP device ran out of resources at any time during the specified interval.

4.70.1 Resource Object

CCM MTP device object

4.70.2 Default Schedule

By default, this script runs every 15 minutes.

4.70.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a value exceeds or falls below a threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is n. This script collects the number of active MTP resources.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a value exceeded or fell below a threshold. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a CallManager in backup mode.
Threshold - Maximum active resources	Specify the maximum number of MTP resources that can be active before an event is raised. The default is 20 resources.
Threshold - Minimum available resources	Specify the minimum number of MTP resources that must be available to prevent an event from being raised. The default is 0 resources.
Event severity when MTP device was out of resources	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MTP device ran out of resources at least once during the interval. Set to 0 to ignore an out-of-resource event. The default is 25. **NOTE**: The event message for the out-of-resources event contains the number of times that the device ran out of resources.

4.71 MTPActiveConnections

Use this Knowledge Script to monitor the number of active connections for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.71.1 Resource Object

CCM Media Termination Point object

4.71.2 Default Schedule

By default, this script runs every 30 minutes.

4.71.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active connections for reports and graphs. The default is n.
Threshold - Maximum active connections	Specify the maximum number of connections that can be active before an event is raised. The default is 20 connections.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active connections exceeds the threshold. The default is 25.

4.72 MTPActiveStreams

Use this Knowledge Script to monitor the number of active streams for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.72.1 Resource Object

CCM Media Termination Point object

4.72.2 Default Schedule

By default, this script runs every 30 minutes.

4.72.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active streams for reports and graphs. The default is n.
Threshold - Maximum active streams	Specify the maximum number of streams that can be active before an event is raised. The default is 20 streams.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

4.73 MTPAvailableStreams

Use this Knowledge Script to monitor the number of available streams for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.73.1 Resource Object

CCM Media Termination Point object

4.73.2 Default Schedule

By default, this script runs every 30 minutes.

4.73.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available streams falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available streams for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum available streams	Specify the minimum number of streams that must be available to prevent an event from being raised. The default is 20.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available streams falls below the threshold. The default is 25.

4.74 MTPCompletedConnections

Use this Knowledge Script to monitor the number of connections completed during an interval for a Media Termination Point (MTP). If the number of completed connections exceeds the threshold, an event is raised. An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.74.1 Resource Object

CCM Media Termination Point object

4.74.2 Default Schedule

By default, this script runs every 30 minutes.

4.74.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of completed connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed connections for reports and graphs. The default is n.
Threshold - Maximum completed connections	Specify the maximum number of connections that can be completed before an event is raised. The default is 20 connections.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed connections exceeds the threshold. The default is 25.

4.75 MTPCompletedStreams

Use this Knowledge Script to monitor the number of streams on connections completed during an interval for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.75.1 Resource Object

CCM Media Termination Point object

4.75.2 Default Schedule

By default, this script runs every 30 minutes.

4.75.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of completed streams exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed streams for reports and graphs. The default is n.
Threshold - Maximum completed streams	Specify the maximum number of streams that can be completed before an event is raised. The default is 20 streams.

Parameter	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed streams exceeds the threshold. The default is 25.

4.76 MTPsActive

Use this Knowledge Script to monitor the number of active Media Termination Points (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.76.1 Resource Object

CCM Call Processor

4.76.2 Default Schedule

By default, this script runs every five minutes.

4.76.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active MTPs exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active MTPs for reports and graphs. The default is n.
Threshold - Maximum active Media Termination Points	Specify the maximum number of MTPS that can be active before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MTPs exceeds the threshold. The default is 25.

4.77 MTPsAvailable

Use this Knowledge Script to monitor the number of Media Termination Points (MTP) available for use. An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.77.1 Resource Object

CCM Call Processor

4.77.2 Default Schedule

By default, this script runs every five minutes.

4.77.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available MTPs falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available MTPs for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum available Media Termination Points	Specify the minimum number of MTPs that must be available to prevent an event from being raised. The default is 3.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available MTPs falls below the threshold. The default is 15.

4.78 MTPsUnavailable

Use this Knowledge Script to monitor the number of times during an interval that a Media Termination Point (MTP) allocation was requested when none was available. An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

4.78.1 Resource Object

CCM Call Processor

4.78.2 Default Schedule

By default, this script runs every five minutes.

4.78.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-resource instances exceeds the threshold. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data about resource unavailability for reports and graphs. The default is n.
Threshold - Maximum out-of-resource instances	Specify the maximum number of times that MTP resources can be unavailable before an event is raised. The default is 0.
Event severity if threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-resource instances exceeds the threshold. The default is 5.

4.79 MulticastConfActive

Use this Knowledge Script to monitor the number of active Multicast conferences. This script raises an event if the number of active conferences exceeds the threshold.

NOTE: This script supports only Cisco CallManager version 3.0.

4.79.1 Resource Object

CCM Call Processor

4.79.2 Default Schedule

By default, this script runs every five minutes.

4.79.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active Multicast conferences exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active conferences for reports and graphs. The default is n.
Threshold - Maximum active Multicast conferences	Specify the maximum number of Multicast conferences that can be active before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active Multicast conferences exceeds the threshold. The default is 25.

4.80 MulticastConfAvailable

Use this Knowledge Script to monitor the number of new Multicast conferences that can be started. This script raises an event if the number of available conferences is less than the threshold.

NOTE: This script supports only Cisco CallManager version 3.0.

4.80.1 Resource Object

CCM Call Processor

4.80.2 Default Schedule

By default, this script runs every five minutes.

4.80.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available Multicast conferences falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available conferences for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum available Multicast conferences	Specify the minimum number of Multicast conferences that must be available to prevent an event from being raised raised. The default is 3 conferences.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available Multicast conferences falls below the threshold. The default is 15.

4.81 MulticastConfCompleted

Use this Knowledge Script to monitor the number of Multicast conferences completed during an interval. This script raises an event if the number of completed conferences exceeds the threshold.

NOTE: This script supports only Cisco CallManager version 3.0.

4.81.1 Resource Object

CCM Call Processor

4.81.2 Default Schedule

By default, this script runs every 30 minutes.

4.81.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of completed Multicast conferences exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed conferences for reports and graphs. The default is n.
Threshold - Maximum completed Multicast conferences	Specify the maximum number of Multicast conferences that can be completed before an event is raised. The default is 50 conferences.
Event severity if threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed Multicast conferences exceeds the threshold. The default is 25.

4.82 MulticastConfPhones

Use this Knowledge Script to monitor the number of active Multicast participants. This script raises an event if the number of participants exceeds the threshold.

NOTE: This script supports only Cisco CallManager version 3.0.

4.82.1 Resource Object

CCM Call Processor

4.82.2 Default Schedule

By default, this script runs every five minutes.

4.82.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active Multicast participants exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about Multicast participants for reports and graphs. The default is n.
Threshold - Maximum active Multicast participants	Specify the maximum number of Multicast participants that can be active before an event is raised. The default is 100 participants.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active Multicast participants exceeds the threshold. The default is 25.

4.83 MulticastConfUnavailable

Use this Knowledge Script to monitor the number of times during an interval that a Multicast conference was requested when none was available. This script raises an event if the threshold is exceeded.

NOTE: This script supports only Cisco CallManager version 3.0.

4.83.1 Resource Object

CCM Call Processor

4.83.2 Default Schedule

By default, this script runs every five minutes.

4.83.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-resource instances exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about unavailable resources for reports and graphs.The default is n.
Threshold - Maximum out-of-resource instances	Specify the maximum number of out-of-resource instances that can occur before an event is raised. The default is 0 instances.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-resource instances exceeds the threshold. The default is 5.

4.84 QRTEvent

Use this Knowledge Script to monitor the log files of the Quality Reporting Tool (QRT). This script will start a diagnostic action and raise an event if a QRT request has been logged.

4.84.1 Resource Object

CCM parent object

4.84.2 Default Schedule

By default, this script runs every minute.

4.84.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Script Options	
QRT log file directory	Provide the file path to the QRT log file. The default is `C:\Program Files\Cisco\QRT`.
Maximum number of entries per event message	Specify the maximum number of entries that can be placed into a single event message. If more entries are found, a new event is raised. The default is five entries.
On first run, scan files modified in the last N minutes	Specify the number of minutes of previous activity through which the script will search the log file. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 30 minutes.
Monitor Quality Reporting Tool Log Entries	
Event Notification	
Raise event if new QRT log entry is found?	Select **Yes** to raise an event if a new QRT log entry is found. The default is Yes.
Event severity when new QRT log entry is found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a new log entry is found. The default is 5.
Data Collection	
Collect data for QRT log entries?	Select **Yes** to collect data about QRT log entries for reports and graphs. The default is unselected.

4.85 RegAnalogAccesses

Use this Knowledge Script to monitor the number of registered analog accesses. This script raises an event if the number of registered accesses exceeds the threshold.

4.85.1 Resource Object

CCM Call Processor

4.85.2 Default Schedule

By default, this script runs every 30 minutes.

4.85.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of registered analog accesses exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered analog accesses for reports and graphs. The default is n.
Threshold - Maximum registered analog accesses	Specify the maximum number of analog accesses that can be registered before an event is raised. The default is 50 accesses.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered analog accesses exceeds the threshold. The default is 25.

4.86 RegCtiPorts

Use this Knowledge Script to monitor the number of CTI (Computer Telephony Interface) ports registered to the local CallManager.

A CTI port is a virtual device that can have one or more virtual lines. Software-based CallManager applications, such as SoftPhone, AutoAttendant, and IP Interactive Voice Response (IVR), can be configured to use CTI ports. You use the same CallManager Administration area to configure CTI ports that you use to configure phones. Because these virtual devices use up resources on the CallManager, you can use this script to monitor how many CTI ports are registered and to raise an event if this number exceeds a threshold you set.

This script queries the CallManager database for CTI ports.

4.86.1 Resource Object

CCM parent object

4.86.2 Default Schedule

By default, this script runs every 30 minutes.

4.86.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if registered CTI ports exceed the threshold?	Set to **y** to raise an event if the number of registered CTI ports exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered CTI ports for reports and graphs. The default is n.

Parameter	How to Set It
SQL username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you have changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum registered CTI ports	Specify the maximum number of ports that can be registered before an event is raised. The default is 200 ports.
Event severity when registered CTI ports exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of registered CTI ports exceeds the threshold. The default is 25.

4.87 RegDigitalAccesses

Use this Knowledge Script to monitor the number of registered digital accesses. This script raises an event if the number of registered accesses exceeds the threshold.

NOTE: This script supports only Cisco CallManager version 3.0.

4.87.1 Resource Object

CCM Call Processor

4.87.2 Default Schedule

By default, this script runs every 30 minutes.

4.87.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of registered digital accesses exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered digital accesses for reports and graphs. The default is n.
Threshold - Maximum registered digital accesses	Specify the maximum number of digital accesses that can be registered before an event is raised. The default is 50 accesses.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered digital accesses exceeds the threshold. The default is 25.

4.88 RegHardwarePhones

Use this Knowledge Script to monitor the number of registered hardware phones. This script raises an event if the number of registered hardware phones exceeds the threshold.

4.88.1 Resource Object

CCM Call Processor

4.88.2 Default Schedule

By default, this script runs every 30 minutes.

4.88.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if registered hardware phones exceed the threshold?	Set to **y** to raise an event if the number of registered hardware phones exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered hardware phones for reports and graphs. The default is n.
Threshold - Maximum registered hardware phones	Specify the maximum number of hardware phones that can be registered before an event is raised. The default is 1000 phones.
Event severity when registered hardware phones exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered hardware phones exceeds the threshold. The default is 25.

4.89 RegMGCPGateways

Use this Knowledge Script to monitor the number of registered MGCP gateways. This script raises an event if the number of registered gateways falls below the threshold.

4.89.1 Resource Object

CCM Call Processor

4.89.2 Default Schedule

By default, this script runs every 30 minutes.

4.89.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of registered MGCP gateways falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered MGCP gateways for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum registered MGCP gateways	Specify the minimum number of MGCP gateways that must be registered to prevent an event from being raised. The default is 0 gateways.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered MGCP gateways falls below the threshold. The default is 25.

4.90 RegOtherDevices

Use this Knowledge Script to monitor the number of registered station devices using the SCCP protocol (Skinny Protocol) that are not hardware phones, such as Cisco IP SoftPhones, Cisco uOne ports and Cisco Unity voice ports.

4.90.1 Resource Object

CCM Call Processor

4.90.2 Default Schedule

By default, this script runs every 30 minutes.

4.90.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of registered “other” devices exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered “other” devices for reports and graphs.
Threshold - Maximum registered “other” devices	Specify the maximum number of “other” devices that can be registered before an event is raised. The default is 50 devices. I

Parameter	How to Set It
Event severity if threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered “other” devices exceeds the threshold. The default is 25.

4.91 Report_CallActivity

Use this Knowledge Script to summarize the call activity for a selected time range for all CallManagers in a CallManager view. This report displays the data collected by the CallActivity script.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, “Recommended Knowledge Script Groups,” on page 216.

4.91.1 Resource Object

Report agent

4.91.2 Default Schedule

By default, this script runs once.

4.91.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report by view, computer, or data group. The default is View.
Select Knowledge Script	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Total by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.

Parameter	How to Set It
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
All data on a single chart?	Set to **y** to create a chart that displays all of the collected data. If you accept the default of **n**, the data is spread over several charts based on the following: ◆ If you chose **Hour** in the "Total by" parameter, each chart will display a maximum of 48 data points. ◆ If you chose **Day** in the "Total by" parameter, each chart will display a maximum of 14 data points.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoCallMgrCallActivity.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Call Activity.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.92 Report_CallQualityDailyAvg

Use this Knowledge Script to display information about key call quality factors: jitter, latency, and lost data. This script uses the data collected by the CallQuality script.

CallQualityDailyAvg summarizes by hour, and weights by the total number of calls for each measured interval. For example, if you select two days of data, the chart represents the weighted average of all calls in a given hour for both days.

When running this script, take into consideration the following factors:

- The CallQuality script monitors only the jitter, latency, and lost data as seen from the originator of the call.
- The CallQuality script pulls its data from the actual Cisco CallManager database. It is possible that when the Monitoring script reads information from the database, CallManager may not have completed all updates to the database.
- There is no overall call-quality metric.

NOTE: If you want to report on call quality as seen by the recipient of the call, include real-time call quality data, or display an overall call quality metric, NetIQ Corporation recommends that you license the AppManager for VoIP Quality module, which provides more robust call-quality reporting.

4.92.1 Resource Object

Report agent

4.92.2 Default Schedule

By default, this script runs once.

4.92.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select CallManager Publisher	Select the CallManager Publisher on which you ran the Knowledge Script that you selected in the previous parameter.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Threshold - Jitter	Specify the jitter threshold to display on the jitter charts in the report. The default is 0 milliseconds.
Threshold - Latency	Specify the latency threshold to display on the latency charts in the report. The default is 0 milliseconds.
Threshold - Percent lost data	Specify the lost data threshold to display on the charts in the report. The default is 0%.
Report Settings	
Include charts?	Set to **y** to include a chart in the report. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.

Parameter	How to Set It
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CCMCallQualityDailyAvg.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Call Quality Daily Average.
Select chart style	Select chart properties in the Chart Settings dialog box. The default style is Bar.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.93 Report_CallsByHour

Use this Knowledge Script to summarize the active calls for all selected CallManagers in a selected time period.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.93.1 Resource Object

Report agent

4.93.2 Default Schedule

By default, this script runs once.

4.93.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer(s)	Select the computers that you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.

Parameter	How to Set It
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart in the report. The default is y.
Include tables?	Set to **y** to include a table of information in the report. The default is y.
Select chart properties	Select a chart type. The default style is Bar.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CCMCallsByHour.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Calls By Hour.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.94 Report_ClusterAvgValueByHr

Use this Knowledge Script to display the average values by hour of the data streams for a CallManager cluster that were collected by a Knowledge Script within a specified time range.

4.94.1 Resource Object

Report agent

4.94.2 Default Schedule

By default, this script runs once.

4.94.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select data wizard	Select the data for your report by view, computer, or data group.
Select the style	Select the style for the first page of the report: ◆ By computer provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) ◆ By data stream provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers ◆ By computer and data stream provides links to pages showing a single data stream collected from a computer ◆ By Knowledge Script provides links to pages showing all data streams collected by a script (each page shows all data streams collected from all computers on which the script has run) ◆ All data streams on one page generates a report with all data on a single page
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregation interval	Select the time period by which the data in your report is aggregated. The default is 1 hour.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.
Select output folder	Set parameters for the output folder. The default folder name is ClusterAvgValueByHr.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster Average By Hour.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.95 Report_ClusterAvgValueByMin

Use this Knowledge Script to display the average values by minute of the data streams collected for a CallManager cluster by a Knowledge Script within a specified time range.

4.95.1 Resource Object

Report agent

4.95.2 Default Schedule

By default, this script runs once.

4.95.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report by view, computer, or data group.

Parameter	How to Set It
Select the style	Select the style for the first page of the report: ◆ By computer provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) ◆ By data stream provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers ◆ By computer and data stream provides links to pages showing a single data stream collected from a computer ◆ By Knowledge Script provides links to pages showing all data streams collected by a script (each page shows all data streams collected from all computers on which the script has run) ◆ All data streams on one page generates a report with all data on a single page
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregation interval	Select the time period by which the data in your report is aggregated. The default is 1 hour.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.
Select output folder	Set parameters for the output folder. The default folder name is ClusterAvgValueByMin.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster Average By Minute.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	

Parameter	How to Set It
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.96 Report_ClusterGenCounter

Use this Knowledge Script to display a chart showing the average, maximum, and minimum values of each CallManager cluster data stream and the actual data values of each data stream over time.

4.96.1 Resource Object

Report agent

4.96.2 Default Schedule

By default, this script runs once.

4.96.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report, either by view, computer, or data group.
Select the style	Select the style for the first page of the report: ◆ By computer provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) ◆ By data stream provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers ◆ By computer and data stream provides links to pages showing a single data stream collected from a computer ◆ By Knowledge Script provides links to pages showing all data streams collected by a script (each page shows all data streams collected from all computers on which the script has run) ◆ All data streams on one page generates a report with all data on a single page

Parameter	How to Set It
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Maximum number of points per chart	Specify the maximum number of data points to include in the chart. The default is 200 points.
Select average, minimum, or maximum	Select the type of value you want to represent in your report. The default is AVG.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.
Select output folder	Set parameters for the output folder. The default folder name is ClusterGenCounter.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster General Counter.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.97 Report_ClusterSystemUsage

Use this Knowledge Script to display the average CPU and memory usage per CallManager cluster within a specified time frame.

4.97.1 Resource Object

Report agent

4.97.2 Default Schedule

By default, this script runs once.

4.97.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select cluster	Select a view and CallManager cluster for your report.
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data.
Charts	
Include CPU usage chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include physical memory chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
Chart threshold - CPU usage	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Chart threshold - Physical memory	Specify the physical memory threshold (in KB) to display on the charts in the report. The default is 0 KB.
Select chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Select chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is ClusterSystemUsage.

Parameter	How to Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.98 Report_MGCPChannelUsage

Use this Knowledge Script to display the average and maximum active channels for a particular MGCP PRI or T1-CAS Group within a specified time range. This report uses the data collected by the MGCP_PRI_Channels and MGCP_T1CAS_Channels scripts.

4.98.1 Resource Object

Report agent

4.98.2 Default Schedule

By default, this script runs once.

4.98.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select device type	Select whether to report on PRI or T1-CAS devices.

Parameter	How to Set It
Select Knowledge Script(s)	Select the scripts that collected the data you want to include in the report.
Select device groups	Select the MGCP PRI or T1-CAS Groups that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart of data stream values in the report. The default is y.
Include tables?	Set to **y** to include a table of data stream values in the report. The default is y.
Select chart style for average values	Define the graphic properties of the charts in your report. The default style is Line.
Chart title	Provide a name for the chart in your report. The default title is Cisco CallManager MGCP Device Group Channel Usage.
All data on a single chart?	Set to **y** to display all data points on a single chart. The default is n. If you set to n, up to 24 data points are displayed on a single chart when aggregating by hour and up to 14 data points are displayed when aggregating by day.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallManager MGCPDeviceGroupChannelUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager MGCP Device Group Channel Usage.
Add time stamp to title	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.

Parameter	How to Set It
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.99 Report_MGCPDeviceUtil

Use this Knowledge Script to display average outbound busy attempts and calls completed for a particular MGCP PRI, T1-CAS, FXO, or FXS device within a specified time range. This report uses the data collected by the following scripts:

- MGCP_PRI
- MGCP_T1CAS
- MGCP_FXO
- MGCP_FXS

4.99.1 Resource Object

Report agent

4.99.2 Default Schedule

By default, this script runs once.

4.99.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select device type	Select whether to report on PRI, T1-CAS, FXO, or FXS devices.
Select Knowledge Script	Select the scripts that collected the data you want to include in the report.
Select device(s)	Select the PRI, T1-CAS, FXO, or FXS devices that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.

Parameter	How to Set It
Chart Settings	
Chart threshold - Completed calls	Specify the completed calls threshold value to display on the charts in the report. The default is 0.
Chart threshold - Outbound busy attempts	Specify the outbound busy attempts threshold value to display on the charts in the report. The default is 0.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart of data stream values in the report. The default is y.
Include tables?	Set to **y** to include a table of data stream values in the report. The default is y.
Select chart style	Define the graphic properties of the charts in your report. The default style is Line.
Chart title	Provide a name for the chart in your report. The default title is Cisco CallManager MGCP Device Utilization.
All data on a single chart?	Set to **y** to display all data points on a single chart. The default is n. If you set to n, up to 24 data points are displayed on a single chart when aggregating by hour and up to 14 data points are displayed when aggregating by day.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallManager MGCPDeviceUtil.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager MGCP Device Utilization.
Add time stamp to title	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.100 Report_MGCPGatewayUsage

Use this Knowledge Script to display the average number of active MGCP PRI and T1-CAS Voice Channels for a particular gateway within a specified time range. This report uses the data collected by the MGCP_Gateway_CCM31 script.

4.100.1 Resource Object

Report agent

4.100.2 Default Schedule

By default, this script runs once.

4.100.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select Knowledge Script(s)	Select the scripts that collected the data you want to include in the report.
Select gateway(s)	Select the name of the MGCP gateways that you want to include in the report. You can include nor more than 10 gateways in a single report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart of data stream values in the report. The default is y.
Include tables?	Set to **y** to include a table of data stream values in the report. The default is y.
Select chart style	Define the graphic properties of the charts in your report. The default style is Line.
Chart title	Provide a name for the chart in your report. The default title is Cisco CallManager MGCP Gateway Usage.

Parameter	How to Set It
All data on a single chart?	Set to **y** to display all data points on a single chart. The default is n. If you set to n, up to 24 data points are displayed on a single chart when aggregating by hour and up to 14 data points are displayed when aggregating by day.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallManager MGCPGatewayUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager MGCP Gateway Usage.
Add time stamp to title	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.101 Report_ServicesAvailability

Use this Knowledge Script to summarize the availability (throughout the day) of the services most relevant to CallManager, for all CallManagers in a CallManager view. This report displays the data collected by the CCM_HealthCheck script.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, “Recommended Knowledge Script Groups,” on page 216.

4.101.1 Resource Object

Report agent

4.101.2 Default Schedule

By default, this script runs once.

4.101.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report, either by view, computer, or data group. The default is View.
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoCallMgrServicesAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Services Availability.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.102 Report_SystemUsage

Use this Knowledge Script to display the processes that are using the most CPU and memory for a selected CallManager. The report can contain a table for top CPU usage, which will be displayed as a percentage averaged over the time interval, and another for top memory usage, which will be displayed in KB averaged over the time interval.

This script displays the data collected by the CCM_SystemUsage Knowledge Script.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.102.1 Resource Object

Report agent

4.102.2 Default Schedule

By default, this script runs once.

4.102.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Charts	
Include CPU usage chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include memory usage chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
Chart threshold - CPU usage	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Chart threshold - Memory usage	Specify the physical memory threshold (in KB) to display on the charts in the report. The default is 0 KB.
Select chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Select chart color scheme	Select a color scheme template. The default is NetIQ1.

Parameter	How to Set It
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallMgrSystemUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

4.103 SQL_Accessibility

Use this Knowledge Script to monitor SQL Server and database accessibility. This script raises an event if a SQL Server or a specified database is not accessible.

4.103.1 Resource Object

CCM SQL Server

4.103.2 Default Schedule

By default, this script runs every one hour.

4.103.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default is n. If set to y, this script returns 100 if all specified databases are accessible, 50 if some of the specified databases are accessible and some are not, or 0 if none of the specified databases is accessible.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Database name	Provide a comma-separated list of the database names you want to monitor. For example, enter `master,pubs,tempdb`. If you leave this field blank, the script checks access to all databases. The default name is master.
Timeout	Specify a timeout period in seconds. The timeout period is the number of seconds to wait for a response before retrying or determining the database is inaccessible. The default is 0 seconds. **NOTE**: This script continues waiting until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Therefore, limit your use of this parameter or keep the timeout period at a minimum for regular monitoring jobs. When you run this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow a longer timeout period.
Number of retries	Specify the number of times to try connecting to the database before determining the database is inaccessible. The default is 0. **NOTE**: This script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, limit your use of this parameter or keep retry attempts at a minimum for regular monitoring jobs. When you run this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow more retry attempts.
Event severity when SQL Server or database is inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server or the database is inaccessible. The default is 5.

4.104 SQL_BlockedProcesses

Use this Knowledge Script to monitor the number of SQL processes that are blocked (queued) for longer than the period of time that you define. When the number of blocked processes is greater than the threshold, an event is raised.

4.104.1 Resource Object

CCM SQL Server

4.104.2 Default Schedule

By default, this script runs every one minute.

4.104.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if blocked processes exceed the threshold?	Set to **y** to raise an event if the number of blocked (queued) processes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about blocked processes for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Blocked for duration	Specify the length of time that a process can be queued before it is considered a blocked process. The default is 500 milliseconds.
Threshold - Maximum blocked processes	Specify the maximum number of processes that can be blocked before an event is raised. The default is 5.
Number of blocked processes to display	Specify the number of processes to display in the Graph pane of the Operator Console. The default is 20.
Event severity when blocked processes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

4.105 SQL_CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr` and `sqlagent` processes. If the SQL Server processes exceed the threshold you set, an event is raised.

4.105.1 Resource Object

CCM SQL Server

4.105.2 Default Schedule

By default, this script runs every 15 minutes.

4.105.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.
Monitor the SQL Server process?	Set to **y** to monitor SQL Server. The default is y.
Threshold - Maximum CPU usage for SQL Server process	Specify the maximum amount of CPU resources that can be consumed by the SQL process before an event is raised. The default is 10%.
Monitor the SQL Agent process?	Set to y to monitor SQL Agent. The default is y.
Threshold - Maximum CPU usage for SQL Agent process	Specify the maximum amount of CPU resources that can be consumed by the SQL Agent process before an event is raised. The default is 10%.

4.106 SQL_DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the data space utilization from the current interval from the data space utilization from the last interval. If these rates exceed the thresholds you set, an event is raised.

4.106.1 Resource Objects

CCM SQL Database folder

CCM SQL Database object

4.106.2 Default Schedule

By default, this script runs every one hour.

4.106.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval?	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Databases object, not when it runs on an individual database.

Parameter	How to Set It
Exclude these objects	Provide a comma-separated list of the names of objects you want to exclude. For example, enter `master,model,mdb`. **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about growth and shrink rates for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **NOTE**: If you are monitoring SQL Server 7, you need to use a sysadmin role account. Only members of the `sysadmin` role can get file statistics on SQL Server 7.0.
Threshold - Maximum growth rate	Specify the maximum percentage of data growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of data shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

4.107 SQL_DataSpace

Use this Knowledge Script to monitor the data space available and the percentage of data space being used for each database. This script raises an event if the available data space is lower or the percentage of data space used is higher than the threshold for any database.

You can set this script to discover new databases dynamically each time it runs. Discovering databases dynamically allows you to monitor data space for databases that have been added since running the SQL Discovery script and prevents you from attempting to monitor databases that have been dropped since discovery.

This script uses the `sysadmin` role account for SQL 7.0.

4.107.1 Resource Objects

CCM SQL Database folder

CCM SQL Database object

4.107.2 Default Schedule

By default, this script runs every one hour.

4.107.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval?	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Databases object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you want to exclude. For example: master,model,mdb **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to y to collect data about available and used data space for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **NOTE**: If you are monitoring SQL Server 7, you need to use a `sysadmin` role account. Only members of the sysadmin role can get file statistics on SQL Server 7.0.
Threshold - Minimum available space	Specify the minimum amount of disk space that must be available to prevent an event from being raised. The default is 0 MB. Enter **0** to ignore this threshold.
Threshold - Maximum used space	Specify the maximum percentage of data space that can be used before an event is raised. The default is 90%.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 5.

4.108 SQL_DBGrowthRate

Use this Knowledge Script to monitor database growth and shrink rates. Growth and shrink rates are calculated by taking the difference between the database space utilization from the current interval and the database space utilization from the last interval. If these rates exceed the thresholds you set, an event is raised.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.108.1 Resource Objects

CCM SQL Database folder

CCM SQL Database object

4.108.2 Default Schedule

By default, this script runs every one hour.

4.108.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Database object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about database growth and shrink rates for reports and graphs. The default is y.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **NOTE**: If you are monitoring SQL Server 7, you need to use a sysadmin role account. Only members of the sysadmin role can get file statistics on SQL Server 7.0.

Parameter	How to Set It
Update usage?	Set to **y** to have SQL Server recalculate the space usage. The default is n.
Threshold - Maximum growth rate	Specify the maximum percentage of database growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of database shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

4.109 SQL_DbOption

Use this Knowledge Script to verify how SQL Server database options are set. You can select which options to check and whether to raise an event when an option is set (On) or not set (Off).

4.109.1 Resource Object

CCM SQL Database object

4.109.2 Default Schedule

By default, this script runs every one hour.

4.109.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when option is on?	Set to **y** to raise an event when the specified options are set. The default is y.
Raise event when option is off?	Set to **y** to raise an event when the specified options are not set. The default is n.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns 100 if all of the specified options are on, 50 if some options are on, and 0 if no options are on. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Check all options?	Set to **y** to check all database options. The default is y.

Parameter	How to Set It
Check ANSI null default option?	Set to **y** to check whether this option is on. When set, this database option controls whether database columns are null by default. The default is n.
Check ANSI nulls option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, all comparisons to a null value evaluate to unknown. The default is n.
Check ANSI warnings option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether errors or warnings are issued when conditions such as "divide by zero" occur. The default is n.
Check auto_close option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, the database is shutdown cleanly and its resources are freed after the last user exits. The default is n.
Check auto_create statistics option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, statistics are automatically created on columns used in a predicate. The default is n.
Check auto_update_statistics option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, existing statistics are automatically updated when the statistics become out-of-date. The default is n.
Check auto_shrink option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, the database files are candidates for automatic periodic shrinking. The default is n.
Check concat null yields null option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, if either operand in a concatenation operation is null, the result is null. The default is n.
Check cursor close on commit option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, any cursors that are open when a transaction is committed or rolled back are closed. The default is n.
Check dbo use only option?	Set to **y** to check whether this option is on. This database option specifies that only the database owner can access the database. The default is n.
Check default to local cursor option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether cursor declarations default to local. The default is n.
Check merge publish option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether the database can be published for a merge replication. The default is n.
Check no chkpt on recovery option?	Set to **y** to check whether this option is on. When this database option is off, a checkpoint record is added to the database after a recovery/ restart operation. The default is n. This option is applicable only for SQL Server 6.x.
Check offline option?	Set to **y** to check whether the database is configured for offline operation. The default is n.

Parameter	How to Set It
Check published option?	Set to **y** to check whether the database is configured for publishing (replication). The default is n.
Check quoted identifier option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether double quotation mark characters can be used to surround delimited identifiers. The default is n.
Check read only option?	Set to **y** to check whether this option is on. When set, this database option specifies that database records are read-only; data cannot be modified. The default is n.
Check recursive triggers option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option enables the recursive firing of raises. The default is n.
Check select into/bulkcopy option?	Set to **y** to check whether this option is on. When set, this database option allows unlogged database transactions. The default is n.
Check single user option?	Set to **y** to check whether this option is on. When set, this database option specifies that only one user can access the database at a time. The default is n.
Check subscribed option?	Set to **y** to check whether the database is configured as a subscriber database. The default is n.
Check torn page detection option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether SQL Server detects incomplete pages. The default is n.
Check trunc. log on chkpt option?	Set to **y** to check whether this option is on. This database option controls whether the transaction log is truncated when the Checkpoint process runs. The default is n.
Event severity when option is on or off	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored option is on or off. The default is 5.

4.110 SQL_DBSpace

Use this Knowledge Script to monitor available database space and the percentage of database space being used for each database. Database space includes both data space and log space. If the available database space exceeds the maximum threshold or falls below the minimum threshold you set, an event is raised.

You can set this script to discover new databases dynamically each time it runs. Discovering databases dynamically allows you to monitor database space for databases that have been added since running the Discovery_SQL Knowledge Script and prevents you from attempting to monitor databases that have been dropped since discovery.

NOTE: Although this script discovers databases each time it runs, the new databases are not reflected in the TreeView pane.

This script uses the `sysadmin` role account for SQL 7.0.

4.110.1 Resource Objects

CCM SQL Database folder

CCM SQL Database object

4.110.2 Default Schedule

By default, this script runs every one hour.

4.110.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Database object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about available and used database space for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Update usage?	Set to **y** to have SQL Server recalculate the space usage. The default is n.
Threshold - Minimum available database space	Specify the minimum amount of disk space that must be available for the database (including data space and log space) to prevent an event from being raised. The default is 0 MB.
Threshold - Maximum used database space	Enter the maximum percentage of database space that can be used before an event is raised. The default is 90%.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 5.

4.111 SQL_Errorlog

Use this Knowledge Script to monitor the SQL Server error logs (`Errorlog`, `Errorlog.*` in `\MSSQL\LOG`). In the first interval, this script sets a starting point for future scanning. It does not scan the existing entries in the logs, and therefore it does not return any results on the first scan. As it continues to run at the interval specified in the Schedule tab, this script scans the logs for any new entries created since the last time it checked. This script raises an event if the number of entries that match the Find criteria exceeds the threshold you set.

NOTE: In general, the detail message for the script contains details about the occurrences found. If the message is larger than 32KB, the data is saved in a file on the managed computer (`<NetIQ_Home>\log`, for example, `C:\NetIQ\bin\log`) and the detail message contains the truncated data. If you generate these log files, you should periodically remove the files when you are done with them.

4.111.1 Resource Object

CCM SQL Server

4.111.2 Default Schedule

By default, this script runs every one hour.

4.111.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about log entries for reports and graphs. The default is n.
Case sensitive?	Set to **y** to match upper and lower case letters when checking for a match to the search string. The default is n.
Literal match?	Set to **y** if you only want to register a match when there is an exact match to the search string. If set to n, the log text containing any of the words in Find will be matched. For example, if you set this parameter to **y** and enter "foo bar" as the Find string, only lines containing "foo bar" are considered a match. If you set this parameter to n with the same string, any lines that contain "foo," "bar," or "foo bar" are considered a match. The default is n.
Find log text	Specify all or part of the text string you want to find. Separate multiple entries with a space. The default is deadlock.
Threshold - Maximum log text matches	Specify the maximum number of matching entries that can be found before an event is raised. If you accept the default of **0**, the first instance exceeds the threshold and raises an event.

Parameter	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.

4.112 SQL_LogGrowthRate

Use this Knowledge Script to monitor log growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the log space utilization from the current interval from the log space utilization from the last interval. This script raises an event if these rates exceed the thresholds you set.

4.112.1 Resource Objects

CCM SQL Database folder

CCM SQL Database object

4.112.2 Default Schedule

By default, this script runs every one hour.

4.112.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Database object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if the growth or shrink rate exceeds its threshold. The default is y.
Collect data?	Set to **y** to collect data about growth and shrink rates for reports and graphs. The default is n.

Parameter	How to Set It
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **NOTE**: If you are monitoring SQL Server 7, you need to use a sysadmin role account. Only members of the sysadmin role can get file statistics on SQL Server 7.0.
Threshold - Maximum growth rate	Specify the maximum percentage of log growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of log shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

4.113 SQL_LogSpace

Use this Knowledge Script to monitor a database's available log space and log space usage. If the available log space is lower or the percentage of log space used is higher than the threshold you set, an event is raised.

You can set this script to discover new databases dynamically each time it runs.

NOTE: Although this script discovers databases each time it runs, the new databases are not reflected in the TreeView pane.

This script uses the `sysadmin` role account for SQL 7.0.

4.113.1 Resource Objects

CCM SQL Database folder

CCM SQL Database object

4.113.2 Default Schedule

By default, this script runs every one hour.

4.113.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about used and available log space for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Minimum available log space	Specify the minimum amount of log space that must be available to prevent an event from being raised. The default is 0 MB.
Threshold - Maximum used log space	Specify the maximum percentage of log space that can be used before an event is raised. The default is 90%.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 5.

4.114 SQL_MemUtil

Use this Knowledge Script to monitor the amount of memory that is used by SQL Server processes: `sqlservr` and `sqlagent`.

If using SQL Server 7.0 or 2000, you can use this script to monitor total server memory usage, number of free buffers, and memory usage.

If the amount of memory used by SQL Server exceeds the threshold you set, an event is raised.

4.114.1 Resource Object

CCM SQL Server

4.114.2 Default Schedule

By default, this script runs every 10 minutes.

4.114.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.
Threshold - Maximum process memory usage	Specify the maximum amount of memory that can be consumed by SQL Server before an event is raised. The default is 50000000 bytes.
Threshold - Maximum number of free buffers	Specify the maximum number of free buffers that can be in use before an event is raised. The default is 50 buffers.
Threshold - Maximum SQL Server memory usage	Specify the maximum amount of memory that can be in use by SQL Server and all related processes before an event is raised. The default is 30000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

4.115 SQL_NearFileMaxSize

Use this Knowledge Script to monitor the size of all SQL Server database files. This script enables you to set a threshold for when a file is reaching its maximum size. If any database file size exceeds the threshold you set, an event is raised.

You can set this script to discover new databases dynamically each time it runs.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, “Recommended Knowledge Script Groups,” on page 216.

NOTE: Although this script discovers databases each time it runs, the new databases are not reflected in the TreeView pane.

4.115.1 Resource Objects

CCM SQL DB File folder

CCM SQL DB File object

4.115.2 Default Schedule

By default, this script runs every 24 hours.

4.115.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a file's size exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about file size for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum file size	Specify the maximum size a database file can attain before an event is raised. The default is 500 MB.
Threshold - Maximum file size utilization	Specify the maximum percentage that a file can use of its maximum allowed size before an event is raised. The default is 90%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

4.116 SQL_NearMaxConnect

Use this Knowledge Script to monitor the open connection usage of SQL Server. This script compares the current number of connections being used to the maximum number of connections configured for the server. This script raises an event if the used percentage (current connections/maximum connections) exceeds the threshold you set.

4.116.1 Resource Object

CCM SQL Server

4.116.2 Default Schedule

By default, this script runs every one hour.

4.116.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if used connections exceed the threshold?	Set to **y** to raise an event if the percentage of used connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about connection usage for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum used connections	Specify the maximum percentage of connections that can be in use before an event is raised. The default is 95%.
Event severity when used connections exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of used connections exceeds the threshold. The default is 5.

4.117 SQL_NearMaxLocks

Use this Knowledge Script to monitor the lock usage of SQL Server. This script compares the current number of locks being used to the maximum number of locks configured for the server. This script raises an event if the used percentage (current locks/maximum locks) exceeds the threshold you set.

4.117.1 Resource Object

CCM SQL Server

4.117.2 Default Schedule

By default, this script runs every one hour.

4.117.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if lock usage exceeds the threshold?	Set to **y** to raise an event if the percentage of used locks exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about lock usage for reports and graphs. The default is n.

Parameter	How to Set It
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum lock usage	Enter the maximum percentage of locks that can be in use before an event is raised. The default is 95%.
Event severity when lock usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which lock usage exceeds the threshold. The default is 5.

4.118 SQL_NetError

Use this Knowledge Script to monitor SQL Server network errors. This script compares the number of packet errors that occurred between the current and previous monitoring interval. This script raises an event if the number of errors exceeds the threshold you set.

4.118.1 Resource Object

CCM SQL Server

4.118.2 Default Schedule

By default, this script runs every 10 minutes.

4.118.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if network errors exceed the threshold?	Set to **y** to raise an event if network errors exceed the threshold. The default is y.
Collect data?	Set to **y** to collect data about network errors for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum network errors	Specify the maximum number of network errors allowed before an event is raised. The default is 0 errors.

Parameter	How to Set It
Event severity when network errors exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of network errors exceeds the threshold. The default is 5.

4.119 SQL_RepTransactions

Use this Knowledge Script to monitor the number of transactions in the transaction log of the publication database that are marked for replication but have not yet been replicated. This script raises an event if the number of transactions exceeds the threshold you set.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.119.1 Resource Object

CCM SQL Server

4.119.2 Default Schedule

By default, this script runs every one hour.

4.119.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if pending transactions exceed the threshold?	Set to **y** to raise an event if the number of transactions awaiting replication exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about pending transactions for reports and graphs. The default is n.
Threshold - Maximum pending transactions	Specify the maximum number of transactions that can be awaiting replication before an event is raised. The default is 1000 transactions.
Event severity when pending transactions exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of transactions awaiting replication exceeds the threshold. The default is 5.

4.120 SQL_RepTranSec

Use this Knowledge Script to monitor the number of transactions being replicated per second. This script raises an event if the number of transactions exceeds the threshold you set.

4.120.1 Resource Object

CCM SQL Server

4.120.2 Default Schedule

By default, this script runs every one hour.

4.120.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if replicated transactions exceed the threshold?	Set to **y** to raise an event if the number of transactions replicated per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about replicated transactions for reports and graphs. The default is n.
Threshold - Maximum transactions replicated per second	Specify the maximum number of transactions that can be replicated per second before an event is raised. The default is 1000 transactions.
Event severity when replicated transactions exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of transactions replicated per second exceeds the threshold. The default is 5.

4.121 SQL_RestartServer

Use this Knowledge Script to restart SQL Server. This script raises an event if the server either successfully restarts or fails to restart.

To restart the SQL services, this script will also stop dependent CallManager services, such as Cisco Database Layer Monitor. These services will be automatically restarted.

4.121.1 Resource Object

CCM SQL Server

4.121.2 Default Schedule

By default, this script runs once.

4.121.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is five seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.

Parameter	How to Set It
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of event in which AppManager cannot restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

4.122 SQL_ServerDown

Use this Knowledge Script to monitor the up/down status of SQL Server. If SQL Server is down, the script reports an event and, optionally, attempts to re-start SQL Server.

4.122.1 Resource Object

CCM SQL Server

4.122.2 Default Schedule

By default, this script runs every one hour.

4.122.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start SQL Server?	Set to **y** to automatically restart SQL Server if it is down. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot start SQL Server. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully starts SQL Server. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server is down and auto-start is set to n. The default is 18.

4.123 SQL_ServerThroughput

Use this Knowledge Script to monitor SQL Server throughput by measuring the number of T-SQL batch requests executed per second and the number of physical page reads per second. This script raises an event if either threshold is exceeded.

4.123.1 Resource Object

CCM SQL Server

4.123.2 Default Schedule

By default, this script runs every five minutes.

4.123.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about throughput for reports and graphs. The default is n.
Threshold - Maximum batch requests per second	Specify the maximum number of batch request transactions allowed per second before an event is raised. The default is 120 requests.
Threshold - Maximum page reads per second	Specify the maximum number of page reads allowed per second before an event is raised. The default is 100 page reads.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

4.124 SQL_TopIOUsers

Use this Knowledge Script to monitor the number of I/O read and write operations used by SQL Server users and their connections. This script raises an event if the number of operations exceeds the threshold. You can specify the number of top user connections to display in the detail event and data message.

The detail message includes user name, most recent SQL statements executed, spid, and the number of operations used by each user.

4.124.1 Resource Object

CCM SQL Server

4.124.2 Default Schedule

By default, this script runs every 30 minutes.

4.124.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if I/O operations exceed the threshold?	Set to **y** to raise an event if the number if I/O read and writer operations exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about I/O operations for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Display T-SQL?	Set to **y** to display the executing T-SQL in the detail message. The default is y. **NOTE**: The executing SQL statements are included in the detail message only when you use the sa login account.
Exclude these applications	Provide a comma-separated list of the names of applications you do not want to monitor. The default is SQLEXEC.
Number of top user connections to display	Specify the number of top user connections you want displayed in the detail message (event or data). Enter **0** if you want all user connections displayed. The default is 5 connections.
Threshold - Maximum I/O operations	Specify the maximum number of I/O operations allowed before an event is raised. The default is 9999999 operations. **NOTE**: This number represents the cumulative operations for a user connection.
Event severity when I/O operations exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of I/O operations exceeds the threshold. The default is 5.

4.125 SQL_TopLockUsers

Use this Knowledge Script to monitor the total number of locks held by all SQL Server users and their connections. This script raises an event if the number of user locks held exceeds threshold you set.

4.125.1 Resource Object

CCM SQL Server

4.125.2 Default Schedule

By default, this script runs every 30 minutes.

4.125.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if held user locks exceeds the threshold?	Set to **y** to raise an event if the number of held user locks exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about held locks for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Display T-SQL?	Set to **y** to display the executing T-SQL in the detail message. The default is y. **NOTE**: The executing SQL statements are included in the detail message only when you use the sa login account.
Exclude these applications	Provide a comma-separated list of the names of applications you do not want to monitor. The default is SQLEXEC.
Threshold - Maximum held user locks	Specify the maximum number of user locks that can be held before an event is raised. The default is 1000 locks.
Number of top user connections to display	Specify the number of top user connections you want displayed in the detail message (event or data). Enter **0** if you want all user connections displayed. The default is five connections.
Event severity when held user locks exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of held user locks exceeds the threshold. The default is 5.

4.126 SQL_TopMemoryUsers

Use this Knowledge Script to monitor the memory that can be allocated to all SQL Server users and their connections in 2KB pages. This script raises an event if the total number of allocated pages exceeds the threshold you set.

4.126.1 Resource Object

CCM SQL Server

4.126.2 Default Schedule

By default, this script runs every 30 minutes.

4.126.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if allocated memory pages exceed the threshold?	Set to **y** to raise an event if the number of allocated memory pages exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about allocated memory pages for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Display T-SQL?	Set to **y** to display the executing T-SQL in the detail message. The default is y. **NOTE**: The executing SQL statements are included in the detail message only when you use the sa login account.
Exclude these applications	Provide a comma-separated list of the names of applications you do not want to monitor. The default is SQLEXEC.
Threshold - Maximum allocated memory pages	Specify the maximum number of 2-KB memory pages that can be allocated before an event is raised. The default is 15000 pages.
Number of top user connections to display	Specify the number of top user connections you want displayed in the detail message (event or data). Enter **0** if you want all user connections displayed. The default is five connections.
Event severity when allocated memory pages exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of allocated memory pages exceeds the threshold. The default is 5.

4.127 SQL_UserConnections

Use this Knowledge Script to monitor the total number of SQL Server user connections. This script raises an event if the total number of SQL Server user connections exceeds the threshold you set.

4.127.1 Resource Object

CCM SQL Server

4.127.2 Default Schedule

By default, this script runs every 30 minutes.

4.127.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if user connections exceed the threshold?	Set to **y** to raise an event if the number of SQL Server user connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about SQL Server user connections for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum user connections	Specify the maximum number of user connections allowed before an event is raised. The default is 100 connections.
Number of user connections to display	Specify the number of user connections you want displayed in the detail message (event or data). Enter **0** to display all user connections. The default is 20 connections.
Event severity when user connections exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user connections exceeds the threshold. The default is 5.

4.128 StreamAppIOCTLErr

Use this Knowledge Script to monitor the number of times during an interval that an IOCTL (input/output control) error was detected. This script raises an event if the number of IOCTL errors exceeds the threshold.

4.128.1 Resource Object

CCM VoIP Application object

4.128.2 Default Schedule

By default, this script runs every five minutes.

4.128.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of detected errors exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about IOCTL errors for graphs and reports. The default is n.
Threshold - Maximum IOCTL errors	Specify the maximum number of IOCTL errors that can be detected before an event is raised. The default is 0.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of IOCTL errors exceeds the threshold. The default is 5.

4.129 StreamAppMissDDErr

Use this Knowledge Script to monitor the number of times during an interval that a missing device driver (DD) error was detected. This script raises an event if the number of missing driver errors exceeds the threshold.

4.129.1 Resource Object

CCM VoIP Application object

4.129.2 Default Schedule

By default, this script runs every five minutes.

4.129.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of errors exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about missing device driver errors for graphs and reports. The default is n.
Threshold - Maximum missing device driver errors	Specify the maximum number of missing device driver errors that can be detected before an event is raised. The default is 0.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of errors exceeds the threshold. The default is 5.

4.130 TftpChangeNotify

Use this Knowledge Script to monitor the number of TFTP change notifications handled during an interval. This script raises an event if the number of change notifications exceeds the threshold.

4.130.1 Resource Object

CCM TFTP object

4.130.2 Default Schedule

By default, this script runs every 30 minutes.

4.130.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of change notifications exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about TFTP change notifications for graphs and reports. The default is n.
Threshold - Maximum TFTP change notifications	Specify the maximum number of TFTP change notifications that can be handled before an event is raised. The default is 10.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of TFTP change notifications exceeds the threshold. The default is 25.

4.131 TftpErrors

Use this Knowledge Script to monitor the number of TFTP-related errors occurring during an interval. This script raise an event if a threshold is exceeded.

4.131.1 Resource Object

CCM TFTP object

4.131.2 Default Schedule

By default, this script runs every 30 minutes.

4.131.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if any threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about TFTP-related errors for graphs and reports. The default is n.
Threshold - Maximum aborted requests	Specify the maximum number of aborted requests that can occur before an event is raised. The default is 0 requests.
Threshold - Maximum NOT FOUND errors	Specify the maximum number of NOT FOUND errors that can occur before an event is raised. The default is 0. A NOT FOUND error is returned when a device requests a configuration file or firmware load, but the requested file does not exist in the TFTPPath of the TFTP server. Each time this error is returned, the TFTP server updates its NOT FOUND counter in perfmon. This script checks the NOT FOUND counter and raises an event if the number of NOT FOUND errors that occurred during the interval exceeds the threshold.
Threshold - Maximum overflow errors	Specify the maximum number of overflow errors that can occur before an event is raised. The default is 0. Overflow occurs when the TFTP service rejects some TFTP requests because it has reached the maximum number of allowable client connections. Note Overflow also occurs when the TFTP service is rebuilding configuration files; the TFTP service denies all requests while rebuilding files. If you don't want to generate an for requests that were denied during file rebuilding, you may want to click on the Advance tab and set this script to generate an event only if the overflow threshold is exceeded twice within two job iterations or three times within three job iterations. If events are generated more than three times in a row, you may have an overflow problem that requires your attention.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 25.

4.132 TftpHeartBeat

Use this Knowledge Script to monitor the Cisco TFTP heartbeat. This script raises an event if the heartbeat stops or is too low. In addition, this script generates a data stream for TFTP heartbeat data.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, “Recommended Knowledge Script Groups,” on page 216.

4.132.1 Resource Object

CCM TFTP object

4.132.2 Default Schedule

By default, this script runs every five minutes.

4.132.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if heartbeat stops or falls below the threshold?	Set to **y** to raise an event if the heartbeat stops or falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about the TFTP heartbeat for graphs and reports. The default is n.
Threshold - Minimum heartbeat	Specify the minimum heartbeat count that must occur to prevent an event from being raised. The default is 500.
Event severity when heartbeat falls below the threshold	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the heartbeat falls below the threshold. The default is 20.
Event severity when heartbeat stops	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the heartbeat stops. The default is 10.

4.133 TftpRequests

Use this Knowledge Script to monitor the number of TFTP requests handled during an interval. This number includes local requests that were successfully handled by the server, "NotFound" requests, and requests that were aborted or rejected by the TFTP server.

This script is a member of a Recommended Knowledge Script Group. For more information, see Section 4.148, "Recommended Knowledge Script Groups," on page 216.

4.133.1 Resource Object

CCM TFTP object

4.133.2 Default Schedule

By default, this script runs every 30 minutes.

4.133.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of TFTP requests exceeds the threshold. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data about TFTP requests for graphs and reports. The default is n.
Threshold - Maximum TFTP requests	Specify the maximum number of TFTP requests that can be handled before an event is raised. The default is 100 requests.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of TFTP requests exceeds the threshold. The default is 25.

4.134 TftpSegmentPctLost

Use this Knowledge Script to monitor the percentage of TFTP segments lost during an interval. This script raises an event if the percentage of lost segments exceeds the threshold.

4.134.1 Resource Object

CCM TFTP object

4.134.2 Default Schedule

By default, this script runs every five minutes.

4.134.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the percentage of lost TFTP segments exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about lost TFTP segments for graphs and reports. The default is n.
Threshold - Maximum lost segments	Specify the maximum percentage of lost segments that can occur before an event is raised. The default is 1%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of lost TFTP segments exceeds the threshold. The default is 15.

4.135 TftpSegmentsSent

Use this Knowledge Script to monitor the number of TFTP segments sent during an interval. This script raises an event if the number of sent segments exceeds the threshold.

4.135.1 Resource Object

CCM TFTP object

4.135.2 Default Schedule

By default, this script runs every 30 minutes.

4.135.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of sent segments exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about sent TFTP segments for graphs and reports. The default is n.
Threshold - Maximum sent TFTP segments	Specify the maximum number of TFTP segments that can be sent before an event is raised. The default is 100000 segments.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sent TFTP segments exceeds the threshold. The default is 25.

4.136 TraceArchive

Use this Knowledge Script to archive CallManager trace files to avoid losing files when tracing wraps.

This script archives files based on the "last modified time" of each file, rather than the individual trace date or time stamp within each file.

NOTE: This script may be CPU-intensive based on the number of trace files the CallManager has collected. NetIQ Corporation recommends using this script for debugging purposes only — it may affect call processing.

4.136.1 Resource Object

CCM parent object

4.136.2 Default Schedule

By default, this script runs every 30 minutes.

4.136.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Trace file directory	Provide the file path to the trace file. The default is `c:\program files\cisco\trace\ccm`.

Parameter	How to Set It
Destination directory	Provide the file path of the archive file. The default is `c:\tracearchive`.
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search for trace files. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 30 minutes. **NOTE**: Ensure that the time you set is smaller than the amount of time that it takes CallManager to wrap or begin overwriting files. CallManager's iteration time varies based on the trace output format, the debug tracing level, the maximum number of files, the maximum lines per file, and the maximum minutes per file specified within the CallManager Serviceability tool. The larger the call volume, the faster CallManager will fill the trace files.

4.137 TraceEvent

Use this Knowledge Script to scan CallManager trace files for entries that match a text string that you specify. This script raises an event when matching entries are found.

NOTE: This script may be CPU-intensive based on the number of trace files the CallManager has collected. NetIQ Corporation recommends using this script for debugging purposes only — it may affect call processing.

4.137.1 Resource Object

CCM parent object

4.137.2 Default Schedule

By default, this script runs every 30 minutes.

4.137.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if matching entries are found?	Set to **y** to raise an event if the trace files contain entries that match your text string. The default is y.
Collect data?	Set to **y** to collect data about trace file entries for reports and graphs. The default is n.
Trace file directory	Specify the file path to the trace file. The default is `c:\program files\cisco\trace\ccm`.
Search for this text	Specify the text string that you want to find in the trace files. The default is `error|warning|failed|unexpected`.

Parameter	How to Set It
On first run, scan files modified in the last N minutes	Set this parameter to determine how many minutes to go back and check for modified files the first time you run this script. Subsequent searches begin where the previous one finished. For instance, if you enter 15, the script will check for files modified within the past 15 minutes. The default is 30 minutes.
Event severity when matching entries are found	Set the event severity level, from 1 to 40,to indicate the importance of the event. The default is 25.
Maximum entries per event message	Specify the maximum number of entries that can be placed into a single event message. If more entries are found, a new event is generated. The default is 100 entries.

4.138 Transcoder_Device

Use this Knowledge Script to monitor the number of active and available resources for an individual transcoder device. This script also monitors whether the transcoder device ran out of resources at any time during the specified interval.

4.138.1 Resource Object

CCM Transcoder Device object

4.138.2 Default Schedule

By default, this script runs daily every 15 minutes.

4.138.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The event message for an out-of-resource event contains the number of times that the device ran out of resources. The default is y.
Collect data?	Set to **y** to collect data about active and available resources for reports and graphs. The default is n.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not registered.

Parameter	How to Set It
Threshold - Maximum active resources	Specify the maximum number of transcoder resources that can be active (in use) before an event is raised. The default is 20 resources.
Threshold - Minimum available resources	Specify the minimum number of transcoder resources that must be available to prevent an event from being raised. The default is 0 resources.
Event severity when transcoder device was out of resources	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the transcoder device ran out of resources at least once during the interval. Set to 0 to ignore an out-of-resource event. The default is 25.

4.139 TranscoderResources

A transcoder is a device that takes the output stream of one codec and transcodes (converts) it from one compression type to another compression type. In CallManager, the transcoders convert between the G.711, G.723, and G.729 codecs.

Cisco CallManager invokes a transcoder on behalf of endpoint devices when the two devices are using different codecs. When inserted into a call, the transcoder converts the data streams between the different codecs, enabling communication between them.

Use this Knowledge Script to monitor the transcoder performance counters:

- **TranscoderResourcesActive**. The total number of transcoders that are in use on all transcoder devices registered with this CallManager. A transcoder in use is one transcoder resource that has been allocated for use in a call.
- **TranscoderResourcesAvailable**. The total number of transcoders that are not in use and are available for allocation on all transcoder devices registered with this CallManager.

4.139.1 Resource Object

CCM Call Processor

4.139.2 Default Schedule

By default, this script runs every five minutes.

4.139.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about transcoder resources for reports and graphs. The default is n.

Parameter	How to Set It
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 15.
Threshold - Maximum active transcoder resources	Specify the maximum number of transcoder resources that can be active before an event is raised. The default is 10 resources.
Threshold - Minimum available transcoder resources	Specify the minimum number of transcoder resources that must be available to prevent an event from being raised. The default is 2 resources.

4.140 TranscoderUnavailable

A transcoder is a device that takes the output stream of one codec and transcodes (converts) it from one compression type to another compression type. In CallManager, the transcoders convert between the G.711, G.723, and G.729 codecs.

Cisco CallManager invokes a transcoder on behalf of endpoint devices when the two devices are using different codecs. When inserted into a call, the transcoder converts the data streams between the different codecs, enabling communication between them.

Use this Knowledge Script to monitor the number of times that CallManager attempted to allocate a transcoder resource from one of the transcoder devices registered to this CallManager when none was available, either because all were in use or none was registered.

4.140.1 Resource Object

CCM Call Processor

4.140.2 Default Schedule

By default, this script runs every five minutes.

4.140.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if transcoder resources are unavailable?	Set to **y** to raise an event. if transcoder resources are unavailable. The default is y.
Collect data?	Set to **y** to collect data about unavailable transcoder resources for reports and graphs. The default is n.

Parameter	How to Set It
Event severity when transcoder resources are unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unavailable resource instances exceeds the threshold. The default is 10.
Threshold - Maximum unavailable resource instances	Specify the maximum number of times that transcoder resources can be unavailable before an event is raised. The default is 0 resources.

4.141 UnicastConfActive

Use this Knowledge Script to monitor the number of active Unicast software and hardware conferences. This script raises an event if the number of active conferences exceeds the threshold.

4.141.1 Resource Object

CCM Call Processor

4.141.2 Default Schedule

By default, this script runs every five minutes.

4.141.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a the number of active hardware or software conferences exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active conferences for graphs and reports. The default is n.
Monitor active Unicast software conferences?	Set to **y** to monitor the number of active Unicast software conferences. The default is y
Threshold - Maximum active Unicast software conferences	Specify the maximum number of software conferences that can be active before an event is raised. The default is 50 conferences.
Monitor active Unicast hardware conferences?	Set to **y** to monitor the number of active Unicast hardware conferences. The default is y.
Threshold - Maximum active hardware conferences	Specify the maximum number of hardware conferences that can be active before an event is raised. The default is 50 conferences.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active hardware or software conferences exceeds the threshold. The default is 25.

4.142 UnicastConfAvailable

Use this Knowledge Script to monitor the number of new Unicast conferences that can be started. This script raises an event if the number of available hardware or software conferences falls below the threshold.

4.142.1 Resource Object

CCM Call Processor

4.142.2 Default Schedule

By default, this script runs every five minutes.

4.142.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available hardware or software conferences falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available conferences for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Monitor available Unicast software conferences?	Set to **y** to monitor the number of available Unicast software conferences. The default is y.
Threshold - Minimum available software conferences	Specify the minimum number of software conferences that must be available to prevent an event from being raised. The default is 3 conferences.
Monitor available Unicast hardware conferences?	Set to **y** to monitor the number of available Unicast hardware conferences. The default is y.
Threshold - Minimum available hardware conferences	Specify the minimum number of hardware conferences that must be available to prevent an event from being raised. The default is 3 conferences.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available hardware or software conferences falls below the threshold. The default is 15.

4.143 UnicastConfBridge_Device

Use this Knowledge Script to monitor the number of active and available resources for an individual Unicast software or hardware conference bridge device. This script also detects whether the Unicast device ran out of resources at any time during the specified interval.

4.143.1 Resource Objects

CCM Unicast Software Conference Bridge object

CCM Unicast Hardware Conference Bridge object

4.143.2 Default Schedule

By default, this script runs every 15 minutes.

4.143.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about active and available resources for graphs and reports. The default is n.
Event severity when resource threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a resource threshold is exceeded or not met. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not handling calls.
Threshold - Maximum active hardware resources	Specify the maximum number of conference bridge hardware resources that can be active (in use) before an event is raised. The default is 8 resources.
Threshold - Maximum active software resources	Specify the maximum number of conference bridge software resources that can be active (in use) before an event is raised. The default is 36 resources.
Threshold - Minimum available resources	Specify the minimum number of software and hardware resources that must be available to prevent an event from being raised. The default is 0 resources.
Monitor for active participants?	Set to n if you do not want to monitor or collect data for the number of active conference participants. The default is y.
Threshold - Maximum active participants	Specify the maximum number of participants that can be active before an event is raised. The default is 10.
Event severity when active participants exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active participants exceeds the threshold. Set to 0 to ignore an active participant event. The default is 25.
Monitor for completed conferences?	Set to **n** if you do not want to monitor or collect data for the number of conferences completed during the interval. The default is y.

Parameter	How to Set It
Threshold - Maximum completed conferences	Specify the maximum number of conferences that can have been completed since the last time this script ran. If the number of completed conferences exceeds this amount, an event is raised. The default is 20 conference. A conference is started when the first call is connected to the bridge. The conference is completed when the last call is disconnected from the bridge.
Event severity when completed conferences exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed conferences exceeds the threshold. Set to 0 to ignore a completed conference event. The default is 25.
Event severity when conference bridge device is out of resources	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the conference bridge device ran out of resources at least once during the interval. Set to 0 to ignore an out-of-resource event. The default is 25.

4.144 UnicastConfComplete

Use this Knowledge Script to monitor the number of Unicast conferences completed during an interval. This script raises an event if the number of completed hardware or software conferences exceeds the threshold.

The event message for the out-of-resources event contains the number of times that the device ran out of resources. Short messages, detailed event messages, and data stream headers will specify whether the device was a hardware or software conference bridge device.

4.144.1 Resource Object

CCM Call Processor

4.144.2 Default Schedule

By default, this script runs every five minutes.

4.144.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if completed conferences exceed the threshold?	Set to **y** to raise an event if the number of completed hardware and software conferences exceed the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed conferences for graphs and reports. The default is n.
Monitor completed Unicast software conferences?	Set to **y** to monitor the number of completed Unicast software conferences. The default is y.

Parameter	How to Set It
Threshold - Maximum completed software conferences	Specify the maximum number of software conferences that can be completed before an event is raised. The default is 50 conferences.
Monitor completed Unicast hardware conferences?	Set to **y** to monitor the number of completed Unicast hardware conferences. The default is y.
Threshold - Maximum completed hardware conferences	Set the threshold for the most hardware conferences that can be completed before an event is raised. The default is 50 conferences.
Event severity when completed conferences exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed hardware and software conferences exceed the threshold. The default is 25.

4.145 UnicastConfParticipants

Use this Knowledge Script to monitor the number of active Unicast participants. This script raises an event if the number of active software or hardware participants exceeds a threshold.

4.145.1 Resource Object

CCM Call Processor

4.145.2 Default Schedule

By default, this script runs every five minutes.

4.145.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if active participants exceed threshold?	Set to **y** to raise an event if the number of active software or hardware participants exceed a threshold. The default is y.
Collect data?	Set to **y** to collect data about active participants for graphs and reports. The default is n.
Monitor active Unicast software participants?	Set to **y** to monitor the number of active Unicast software participants. The default is y.
Threshold - Maximum active software participants	Specify the maximum number of software participants that can be active before an event is raised. The default is 100 participants.
Monitor active Unicast hardware participants?	Set to **y** to monitor the number of active Unicast hardware participants. The default is y.
Threshold - Maximum active hardware participants	Specify the maximum number of hardware participants that can be active before an event is raised. The default is 100 participants.
Event severity when active participants exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software or hardware participants exceeds a threshold. The default is 25.

4.146 UnicastConfUnavailable

Use this Knowledge Script to monitor the number of times during an interval that a Unicast conference resource was requested when none was available. This script raises an event if the number exceeds the threshold.

4.146.1 Resource Object

CCM Call Processor

4.146.2 Default Schedule

By default, this script runs every five minutes.

4.146.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of unavailable resource instances exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about unavailable resources for graphs and reports. The default is n.
Monitor Unicast software conference unavailable resource instances?	Set to **y** to monitor the number of times that a Unicast software conference resource was unavailable. The default is y.
Threshold - Maximum software unavailable resource instances	Specify the maximum number of times that a software conference resource can be unavailable before an event is raised. The default is 0.
Monitor Unicast hardware conference unavailable resource instances?	Set to **y** to monitor the number of times that a Unicast hardware conference resource was unavailable. The default is y.
Threshold - Maximum hardware unavailable resource instances	Specify the maximum number of times that a hardware conference resource can be unavailable before an event is raised. The default is 0.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unavailable resource instances exceeds the threshold. The default is 5.

4.147 VerifyPasswords

Use this Knowledge Script to verify the sa, Administrator, and Directory Manager passwords on a CallManager computer. Cisco CallManager requires these passwords to be the same for all computers in a cluster. You can run this script daily to monitor whether any password has changed. This script raises an event if a password cannot be verified.

Reasons other than an invalid password can prevent this script from verifying the password, such as services being down or connection failures.

4.147.1 Resource Object

CCM parent object

4.147.2 Default Schedule

By default, this script runs every 24 hours.

4.147.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if any verification fails or if all verifications succeed?	Set to **y** to raise an event if any password verification fails or if all verifications succeed. The default is y.
Event severity when any verification fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which any password verification attempt fails. The default is 15.
Event severity when all verifications succeed	Set the severity level, from 1 to 40, to indicate the importance of an event in which all password verification attempts succeed. Accept the default of **0** if you do not want to raise an event for this scenario.
Windows username	Provide the name of the Windows user whose password you want to verify. Leave this parameter blank to skip Windows verification. The default is Administrator.
Windows password	Provide the Windows password that you want to verify.
Domain name	Specify the domain name of the Windows user whose password you want to verify. Leave this parameter blank to use the name of the computer on which the script will be running. This parameter is optional if you are verifying a Windows password.
SQL username	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. Leave this parameter blank to skip SQL verification. The default is sa.
SQL password	SPecify the SQL password that you want to verify.
SQL Server name	Specify the name of the server where the user is to be verified. Leave this parameter blank to use the name of the computer on which the script will be running. This parameter is optional if you are verifying a SQL password.
SQL database name	Specify the name of the database for which the SQL password is to be verified. The default is master.

Parameter	How to Set It
DC Directory username	SPecify the name of the DC Directory (LDAP) user whose password you want to verify. Leave this parameter blank to skip DC Directory verification. The default is Directory Manager.
DC Directory password	SPecify the DC Directory password that you want to verify.

4.148 Recommended Knowledge Script Groups

The several CiscoCallMgr Knowledge Scripts are members of recommended Knowledge Script Groups (KSG). The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the KSG on a CallManager resource.

NetIQ Corporation does not recommend you run large numbers of jobs all at the same time on one CallManager system. Running a large numbers of jobs that are collecting data and running at frequent intervals may impact the performance of the CallManager server. The Knowledge Scripts in the KSGs are optimized to run continually on CallManager systems with minimal performance impact.

The KSGs provide a "best practices" usage of AppManager for monitoring your CallManager environment. You can use these KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoCallMgr tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoCallMgr tab are not affected.

When deployed as part of a KSG, a script's default script parameter settings may differ from when the script is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the KSGs and want to restore it to its original form, you can reinstall the AppManager for Cisco CallManager module on the repository computer or check in the appropriate script from the AppManager\qdb\kp\CiscoCallMgr\RECOMMENDED directory.

4.148.1 Monitoring Scripts

You can find these scripts in a the **CiscoCallMgr** group on the RECOMMENDED tab of the Knowledge Script pane, or individually on the CiscoCallMgr tab.

- CallActivity
- CallsInProgress
- LossOfHardwarePhones
- CCM_HealthCheck
- CCM_HeartBeat
- CCM_RoleStatus
- CCM_SystemUsage

- CCM_WebPageCheck
- CiscoBackupStatus
- SQL_DBGrowthRate
- SQL_NearFileMaxSize
- SQL_RepTransactions
- TftpHeartBeat
- TftpRequests

4.148.2 Report Scripts

You can find these scripts in a the **CiscoCallMgr_Reports** group on the RECOMMENDED tab of the Knowledge Script pane, or individually on the CiscoCallMgr tab.

- Report_CallActivity
- Report_CallsByHour
- Report_ServicesAvailability
- Report_SystemUsage