Management Guide

NetIQ® AppManager® for Cisco Unified Communications Manager

December 2019

Legal Notice

Contents

About this Book and the Library

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

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

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

User Guide for AppManager Control Center

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

Administrator Guide for AppManager

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

Upgrade and Migration Guide for AppManager

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

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

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

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

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 Introducing AppManager for Cisco Unified Communications Manager

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

Cisco Unified Communications Manager, once known as Unified CallManager, is the call-processing component of a Cisco Unified Communications system. It is a scalable, distributable, and highly available call-processing solution for enterprises.

1.1 Features and Benefits

The following are a few of the features and benefits of monitoring Cisco Unified Communications Manager with AppManager:

- Monitors cluster resources without interruption across failovers
- Discovers Unified Communications Manager clusters with a single discovery
- Offers cluster-aware Knowledge Scripts that collect data for all Unified Communications Managers in a cluster:
  - Call activity for MGCP, skinny, H.323, and SIP devices
  - Port usage for FXO, FXS, PRI, and T1
  - Bandwidth availability
  - Configuration and inventory data for phones, firmware, and devices
  - Registered devices
  - Active and available conference bridges for Multicast and Unicast
  - Active and available Media Termination Points
  - Active and available transcoders
  - TFTP requests, errors, and heartbeat
- Offers other Knowledge Scripts that collect data about Unified Communications Manager, Music-on-Hold, and TFTP servers:
  - Call activity for MGCP, skinny, H.323, and SIP devices
  - Server health
  - Memory, CPU, and system usage
  - System performance
- Provides comprehensive reporting with Analysis Center
- Supports appliance-based Unified Communications Manager systems. For more information about supported versions, see Section 2.1, “System Requirements,” on page 13.

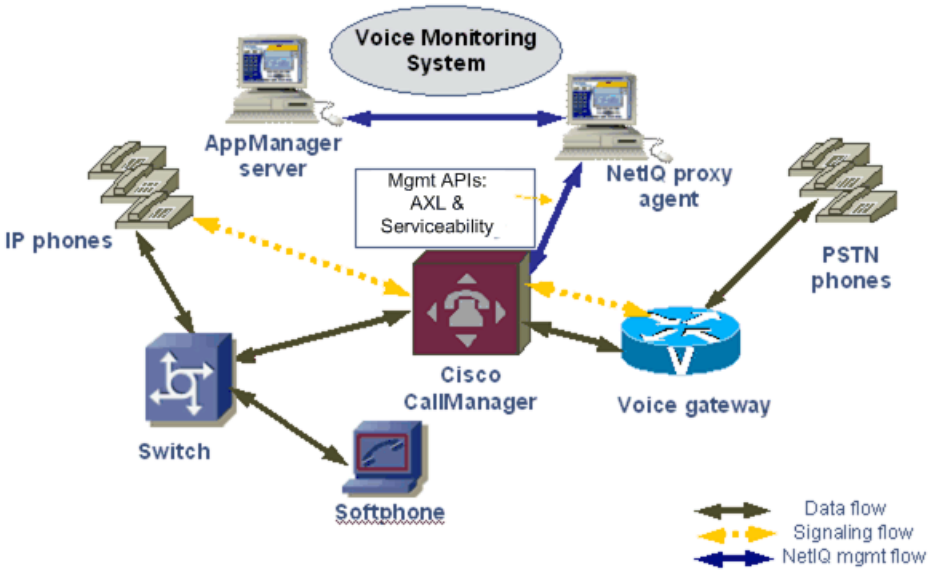
NOTE: AppManager supports Windows-based CallManagers with the AppManager for Cisco CallManager (CiscoCallMgr) module.

- Provides limited support for monitoring deregistered phones on Communications Manager 4.x clusters
- Checks for SNMP traps forwarded from NetIQ SNMP Trap Receiver

1.2 Proxy Architecture

The AppManager for Cisco Unified Communications Manager module does not need to be installed on every device you want to monitor. With this *proxy* architecture, you install the module on a proxy agent computer. When you run a Knowledge Script job, the module runs on the proxy agent computer and sends messages to and from Cisco Unified Communications Manager.

The following diagram shows the relationship between Cisco Unified Communications Manager devices, the AppManager server, and the proxy agent computer. In this configuration, management information is provided by the Cisco Serviceability and AXL APIs. Information from call detail records is transferred by secure FTP.



1.3 Counting AppManager Licenses

AppManager for Cisco Unified Communications Manager consumes one AppManager license for every registered hardware phone and softphone. The number of registered phones is monitored in the Unified Communications Manager performance counter.

2 Installing AppManager for Cisco Unified Communications Manager

This chapter provides installation instructions and describes system requirements for AppManager for Cisco Unified Communications Manager.

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 Unified Communications Manager has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computer, on all proxy agent computers, and on all console computers	9.1, 9.2, 9.5, or later Support for Windows Server 2008 R2 on AppManager 7.x requires AppManager Windows Agent hotfix 71704 or later. For more information, see the AppManager Suite Hotfixes page.
Microsoft operating system installed on all proxy agent computers	One of the following: ◆ Windows Server 2016 ◆ Windows Server 2012 ◆ Windows Server 2012 R2 ◆ Windows 8 (32-bit and 64-bit) ◆ Windows Server 2008, R2 only **NOTE:** Because of an error in Microsoft WinHTTP libraries in Windows 2008, this module does not support Windows 2008 installations prior to the R2 release. ◆ Windows 7 (32-bit and 64-bit)
AppManager for Microsoft Windows module installed on repository, agent, and console computers	Latest agent version of 9.x. For more information, see the AppManager Module Upgrades & Trials page.

Software/Hardware	Version
Microsoft SQL Server installed on the proxy agent computer	All listed versions enable you to create and use the Cisco CM supplemental database. ◆ SQL Server 2016 SP1 Express edition ◆ SQL Server 2016 ◆ SQL server 2014 ◆ SQL server 2012 ◆ SQL Server 2008 R2
Cisco Unified Communications Manager on the computers you want to monitor	12.5, 11.5, 10.5, 10.0, 9.1, 9.0, 8.6, 8.5, 8.0, 7.1(2), 7.0, 6.1, 6.0, 5.1, or 5.0
Microsoft .NET Framework	4.0 or above.
Microsoft SQL Server Native Client 11.0 **(for TLS 1.2 support)**	11.3.6538.0 or later **NOTE:** The SQL Server Native client can be installed from this Microsoft download link.

NOTE: If you want TLS 1.2 support and are running AppManager 9.1 or 9.2, then you are required to perform some additional steps. To know about the steps, see the article.

2.2 Scalability Considerations

Any given Unified Communications Manager device should have only one computer designated as its proxy agent.

In addition, only one computer should act as proxy agent for no more than ten Unified Communications Manager clusters of ten servers per cluster. This number is only a recommendation and can vary based on the capabilities of your proxy agent computer.

The CiscoCM module provides a GeneralCounters Knowledge Script that allows you to monitor an arbitrary performance counter. The scalability of this Knowledge Script is primarily determined by the number of counter instances collected in a single session on the AXL interface. When the instance match results in more than 100 instances, the counter collection uses multiple sessions, which can slow down performance due the Cisco-imposed limit of 50 AXL messages per second.

You may be able to improve the performance of this Knowledge Script, in your environment, by increasing the number of counter instances per message to a value greater than 100.

To change the size of the counter instances per message:

1. On the management server computer, open the Registry Editor.
   a. For 64-bit navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\AppManager\4.0\NetIQmc\Config`
   b. For 32-bit navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0\NetIQmc\Config`
2. In the right pane, double-click **CiscoCM_AXL_MaxCounterDefault**.
3. In the Edit DWORD Value dialog, change the value in the **Value data** field.

NOTE: If this value is not present, it defaults to the current value of 100.

4. Restart any jobs that need to be changed to the new counter collection defaults. The new defaults will not take effect until the job restarts.

2.3 Installing the Module

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

Access the `AM70-CiscoCM-7.x.x.0.msi` module installer from the `AM70_CiscoCM_7.x.x.0.exe` self-extracting installation package on the AppManager Module Upgrades & Trials page.

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

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

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

You can install the module manually, or you can use Control Center to deploy the module to a remote computer where an agent is installed. For more information, see Section 2.4, “Deploying the Module with Control Center,” on page 16. However, if you use Control Center to deploy the module, Control Center only installs the *agent* components of the module. The module installer installs the QDB and console components as well as the agent components on the agent computer.

To install the module manually:

1. Double-click the module installer `.msi` file.
2. Accept the license agreement.
3. Review the results of the pre-installation check. You can expect one of the following three scenarios:
   - **No AppManager agent is present:** In this scenario, the pre-installation check fails, and the installer does not install agent components.
   - **An AppManager agent is present, but some other prerequisite fails:** In this scenario, the default is to not install agent components because of one or more missing prerequisites. However, you can override the default by selecting **Install agent component locally**. A missing application server for this particular module often causes this scenario. For example, installing the AppManager for Microsoft SharePoint module requires the presence of a Microsoft SharePoint server on the selected computer.
   - **All prerequisites are met:** In this scenario, the installer installs the agent components.

4 To install the Knowledge Scripts into the QDB:

   4a Select **Install Knowledge Scripts** to install the repository components, including the Knowledge Scripts, object types, and SQL stored procedures.

   4b Specify the SQL Server name of the server hosting the QDB, as well as the case-sensitive QDB name.

5 Run the module installer for each QDB attached to Control Center.

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

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

8 Configure AXL passwords in AppManager Security Manager. For more information, see Section 2.6, “Configuring AXL Passwords in Security Manager,” on page 18.

9 To use the SNMPTrap_Async Knowledge Script, configure SNMP permissions in AppManager Security Manager. For more information, see Section 4.50.6, “Configuring SNMP Permissions in Security Manager,” on page 157.

10 Enable the collection of Call Management Records and Call Detail Records. For more information, see Section 2.7, “Collecting Call Management and Call Detail Records,” on page 19.

11 (Conditional) If you have not discovered Cisco Unified Communications Manager resources, run the Discovery_CiscoCM Knowledge Script on all proxy agent computers where you installed the module. For more information, see Section 2.8, “Discovering Unified Communications Manager Resources,” on page 19.

TIP: To ensure the discovery of NetIQ SNMP Trap Receiver, stop and delete existing Discovery jobs before creating new jobs. For more information, see Section 4.50.5, “Working with NetIQ SNMP Trap Receiver,” on page 154.

---

12 Configure the proxy agent computer as an FTP server. For more information, see Section 2.9, “Configuring the Proxy Agent Computer as an FTP Server,” on page 22.

13 Configure the proxy agent computer as a billing server. For more information, see Section 2.10, “Configuring the Proxy Agent Computer as a Billing Server,” on page 24.

14 (Conditional) If you have not created the CiscoCM supplemental database, run the SetupSupplementalDB Knowledge Script.

15 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.15, “Upgrading Knowledge Script Jobs,” on page 29.

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

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. For more information, see Section 2.4.2, “Checking In the Installation Package,” on page 17.

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

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

5 Approve the deployment task.

6 View the results.

2.4.2 Checking In the Installation Package

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

To check in a module installation package:

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

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

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

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

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

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

7 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.15, “Upgrading Knowledge Script Jobs,” on page 29.

2.5 Silently Installing the Module

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

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

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

To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.15, “Upgrading Knowledge Script Jobs,” on page 29.

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

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

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

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

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

Windows authentication:

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

SQL authentication:

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

2.6 Configuring AXL Passwords in Security Manager

AVVID XML Layer (AXL), a Cisco application programming interface, enables Unified Communications Manager to access the HTTP server. Configure the AXL password in AppManager Security Manager *before* running the Discovery_CiscoCM Knowledge Script. Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`CiscoCM_AXL`
Sub-label	Indicates whether the AXL information will be used for a single Communications Manager or for all Communications Managers. ◆ For a single Communications Manager, provide the name of the Communications Manager server. ◆ For all Communications Managers, type `default`.
Value 1	AXL user ID that has the authority to use the AXL API. In most cases, the Communications Manager Administrator user has this authority.
Value 2	AXL password that has the authority to use the AXL API. In most cases, the Communications Manager Administrator user has this authority.
Value 3	Use this field *only* if you used Cisco Unified Communications Manager Administration to change the number of the HTTPS port the proxy agent computer uses to connect to the Communications Manager server. Type the new secure port number. Leave this field blank to use the default port number, 8443.
Extended application support	Required field. Encrypts the AXL password in Security Manager.

2.7 Collecting Call Management and Call Detail Records

Cisco Communications Manager produces two types of records, Call Detail Records (CDRs) and Call Management Records (CMRs). CDRs, also called data records, contain information about each call processed by Communications Manager: call origination, call destination, as well as the date 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.

Communications Manager does not collect CMR or CDR records automatically. You must manually enable collection. CDR records are stored in the Publisher. CMRs are generated only when CDRs are generated.

To collect CDRs and CMRs:

1. Navigate to the Cisco Unified Communications Manager Administration Web page.
2. On the **System** menu, click **Service Parameters**.
3. In the **Server** field, select the IP address of the Publisher.
4. In the **Service** field, select **Cisco Communications Manager**.
5. In the System group, set the parameter value for **CDR Enabled Flag** to **True**.
6. In the Clusterwide Parameters group, set the parameter value for **Call Diagnostics Enabled** to **Enabled Only When CDR Enabled Flag is True**.

2.8 Discovering Unified Communications Manager Resources

Use the Discovery_CiscoCM Knowledge Script to discover resource and configuration information for Cisco Unified Communications Manager clusters. The Cisco AXL Web service, the Tomcat service, and the SOAP API services must be active on all servers in the cluster. Only one computer can act as proxy agent for any given Unified Communications Manager cluster. Therefore, run Discovery_CiscoCM on only one Windows server at a time.

NOTE

- Configure the AXL password in AppManager Security Manager before discovering Unified Communications Manager devices and configuration. For more information, see Section 2.6, “Configuring AXL Passwords in Security Manager,” on page 18.
- To prevent AppManager from using the `CCMAdmin` account to access Unified Communications Manager data, create a new user in a new user group and then configure that information in AppManager Security Manager. For more information, see Section 2.11, “Enabling Access to the Unified Communications Manager Server,” on page 25.

By default, this script runs once a week.

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

Set the parameters on the Values tab as needed:

Parameter	How to Set It
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 Discovery_CiscoCM job fails. The default is 5.

Full path to file with list of primary CallManager servers	Specify the full path to a file on the proxy agent computer that contains a list of the DNS hostnames or the IP addresses of the primary servers you want to monitor. List the names on one or more lines in the file, and separate multiple names in one line with a comma. For example,
	
	`primarycluster1,primarycluster2,primarycluster4`
	
	If you specify the names on multiple lines, ensure that each line contains only one entry. For example:
	
	`primarycluster1`
	`primarycluster2`
	`primarycluster4`
	
	Important
	
	◆ After running the Discovery_CiscoCM job, note the name of the discovered cluster in the TreeView, which will look similar to the following example:
	`Proxy agent computer`
	`CiscoCM:`**`CCM80-01`**`-Cluster`
	
	◆ Even if you use IP addresses in this parameter, the text in bold, the *TreeView cluster name*, might look like a hostname. You will use the TreeView cluster name for the following tasks:
	
	◆ Configuring the Proxy Agent Computer as an FTP Server
	
	◆ Configuring the Proxy Agent Computer as a Billing Server
	
	◆ SetupSupplementalDB

Parameter	How to Set It

Comma-separated list of primary CallManager servers	If you do not have a file that contains a list of server names or addresses, you can use this parameter to type the DNS hostnames or the IP addresses of the primary servers in the clusters that you want to monitor. Separate multiple names with a comma. For example:
	
	`primarycluster1,primarycluster2,primarycluster4`
	
	Important
	
	◆ After running the Discovery_CiscoCM job, note the name of the discovered cluster in the TreeView, which will look similar to the following example:
	`Proxy agent computer`
	`CiscoCM:`**`CCM80-01`**`-Cluster`
	
	◆ Even if you use IP addresses in this parameter, the text in bold, the *TreeView cluster name*, might look like a hostname. You will use the TreeView cluster name for the following tasks:
	◆ Configuring the Proxy Agent Computer as an FTP Server
	◆ Configuring the Proxy Agent Computer as a Billing Server
	◆ SetupSupplementalDB

Comma-separated list of CallManager IP address pairs in a single NAT cluster	MSPs (Managed Service Providers) frequently maintain distributed customer networks in which NAT (Network Address Translation) is used to translate the IP address ranges that are monitored from a single NOC (Network Operations Center). The use of NAT prevents AppManager from recognizing the actual IP addresses of the servers in the remote cluster. If your AppManager agent is located on a server in the NOC, but the monitored devices are located in a cluster in the remote customer network, you must provide a list of the IP addresses of the remote monitored devices.
	
	Use this parameter to enable AppManager to recognize the IP addresses of the servers for a single remote Communications Manager cluster.
	
	Type a list of IP address pairs for the Communications Manager servers in a remote cluster. Use commas to separate the addresses. A pair consists of a server's NAT (external) IP address and its IP address inside the cluster. The first address pair in the list must be that of the Communications Manager Publisher (also call the Primary Communications Manager), followed by address pairs for the Subscribers inside the remote cluster. Use the following format:
	
	`publisherexternaladdress,publisherinternaladdress,subscriberexternaladdress1,subscriberinternaladdress1,subscriberexternaladdress2,subscriberinternaladdress2`
	
	In the following example, the 10.41* addresses are externally visible and the 172.16* addresses are visible only to the Communications Manager servers:
	
	`10.41.1.10,172.16.1.10,10.41.1.11,172.16.1.11,...`

Raise event if discovery succeeds?	Select **Yes** to raise an event when discovery succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.

Parameter	How to Set It
Raise event if discovery succeeds with warnings	Select **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery succeeds with warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discover generates warning messages. The default is 15.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.
Discovery Details	
Display FQDN in TreeView for discovered servers?	Select **Yes** to display CiscoCM servers in the TreeView using fully qualified domain names (FQDNs) instead of the host name after you run discovery. Selecting this option does not affect the name of the top-level CiscoCM cluster object. The default is unselected.
Discover Trap Receiver?	Select **Yes** to discover NetIQ SNMP Trap Receiver. The default is Yes. For more information, see Section 4.50.5, “Working with NetIQ SNMP Trap Receiver,” on page 154.
Trap Receiver IP address	Specify the IP address of the computer on which Trap Receiver is installed. The default is `localhost`.
Trap Receiver TCP port	Specify the TCP port number through which Trap Receiver will communicate with AppManager. The default is port 2735.

2.9 Configuring the Proxy Agent Computer as an FTP Server

The Unified Communications Manager server must be able to perform an FTP `PUT` command on the proxy agent computer. Therefore, configure the proxy agent computer as an FTP server and enable write access. The configuration procedure for Windows Server 2008 R2 is different from the procedure for the other supported operating systems.

The Microsoft FTP Service is not secure. If you want secure FTP (sFTP), use a service from a different vendor. If you use sFTP, provide your secure user name and password when configuring the proxy agent computer as a billing server. For more information, see Section 2.10, “Configuring the Proxy Agent Computer as a Billing Server,” on page 24.

2.9.1 Configuring the FTP Server for Other Supported Operating Systems

Use the following procedure for all supported operating systems except Windows Server 2008 R2.

To configure the proxy agent computer as an FTP server:

1. Navigate to the Control Panel, double-click **Add or Remove Programs**, and then click **Add/ Remove Windows Components**.
2. Select **Internet Information Services (IIS)** and then click **Details**.

3 Select **File Transfer Protocol (FTP) Service** and then click **OK**.

4 In the default FTP folder, `c:\inetpub\ftproot`, create a sub-folder with the same name as the TreeView cluster created after you ran Discovery_CiscoCM. For example, if discovery creates a TreeView cluster named `CiscoCM:CCM80-01-Cluster`, then create the following sub-folder: `c:\inetpub\ftproot\CCM80-01`.

2.9.2 Configuring the FTP Server for Windows Server 2008 R2

Use the following procedure to configure the FTP server for a proxy agent computer running Windows Server 2008 R2, which uses a version of FTP that provides different configuration options.

You can use the default publishing FTP folder, `c:\inetpub\wwwroot`, or you create a new FTP site that uses `c:\inetpub\ftproot` as the publishing FTP folder.

Using the Default Publishing FTP Folder

To configure a Windows Server 2008 R2 proxy agent computer as an FTP server:

1 Ensure you installed Application Server with IIS and FTP enabled.

2 Navigate to the Control Panel, double-click **Administrative Services**, and then double-click **Internet Information Services Manager**.

3 In the Connections pane, right-click the default Web site and select **Add FTP Publishing**.

4 In the Binding and SSL Settings dialog box, select the following options:

- **Start FTP site automatically**
- **No SSL**

5 Click **Next**.

6 In the Authentication and Authorization Information dialog box, select the following options:

- **Anonymous** authentication
- Allow access to **All users**
- **Write** permissions

7 Click **Finish**.

8 Restart the Microsoft FTP service.

9 In the publishing FTP folder, create a sub-folder with the same name as the TreeView cluster created after you ran Discovery_CiscoCM. For example, if discovery creates a TreeView cluster named `CiscoCM:CCM80-01-Cluster`, then create the following sub-folder: `c:\inetpub\wwwroot\CCM80-01`.

Creating a New Publishing FTP Folder

To configure a Windows Server 2008 R2 proxy agent computer as an FTP server:

1 Ensure you installed Application Server with IIS and FTP enabled.

2 Navigate to the Control Panel, double-click **Administrative Services**, and then double-click **Internet Information Services Manager**.

3 In the Connections pane, right-click **Sites** and select **Add FTP Site**.

4 In the Site Information dialog box, provide an **FTP Site name** and browse to the physical path of the new folder: `c:\inetpub\ftproot`.

5 In the Binding and SSL Settings dialog box, select the following options:
   - **Start FTP site automatically**
   - **No SSL**
6 Click **Next**.
7 In the Authentication and Authorization Information dialog box, select the following options:
   - **Anonymous** authentication
   - Allow access to **All users**
   - **Write** permissions
8 Click **Finish**.
9 Restart the Microsoft FTP service.
10 In the publishing FTP folder, create a sub-folder with the same name as the TreeView cluster created after you ran Discovery_CiscoCM. For example, if discovery creates a TreeView cluster named `CiscoCM:CCM80-01-Cluster`, then create the following sub-folder: `c:\inetpub\ftproot\CCM80-01`.

2.9.3 Enabling Write Access

Write access allows the Unified Communications Manager server to perform an FTP `put` command on the proxy agent computer.

To enable write access:

1 On the proxy agent computer, navigate to the Control Panel, double-click **Administrative Tools**, and then double-click **Internet Information Services**.
2 In the left pane, expand **[***computer name***](local computer)** and then expand **FTP Sites**.
3 Right-click **Default FTP Site** and select **Properties**.
4 On the Home Directory tab, select **Write** in the FTP Site Directory panel.

2.10 Configuring the Proxy Agent Computer as a Billing Server

To allow the Unified Communications Manager server to send Call Detail Records (CDRs) to the proxy agent computer, configure the Unified Communications Manager server to recognize the proxy agent computer as a billing application server.

If you do not configure the billing application server, AppManager for Cisco Unified Communications Manager cannot perform the functions described in Section 4.47.1, “Understanding the CiscoCM Supplemental Database,” on page 145.

Use the Cisco Unified Communications Manager Administration Web site to configure the proxy agent computer as a billing server.

TIP: If the proxy agent computer does not receive CDRs after you complete the following procedure, ensure the FTP server is working. Verifying FTP functionality usually eliminates most problems. If the FTP server is working as expected, then verify network connectivity. Firewalls can prevent the Unified Communications Manager server from sending CDRs to the proxy agent computer.

To configure the billing server:

1. Navigate to the Administration Web site of your primary Unified Communications Manager server.
2. In the **Navigation** field, select **Cisco Unified CallManager Serviceability** and then click **Go**.
3. In the Serviceability window, click **CDR Management** on the Tools menu.
4. In the CDR Management window, click **Add new** and complete the following fields:

Field	Description
Host Name/IP Address	DNS hostname or IP address of the proxy agent computer, which must be configured as an FTP or sFTP server. For more information, see Section 2.9, "Configuring the Proxy Agent Computer as an FTP Server," on page 22.
User Name	User name required to access the proxy agent computer. If you use sFTP, provide the user name you used when configuring the sFTP server.
Password	Password required to access the proxy agent computer. If you use sFTP, provide the password you used when configuring the sFTP server.
Protocol	Indicates whether to use **FTP** or **sFTP** to push CDRs to the proxy agent computer.

Directory Path	Location to which CDRs are pushed on the proxy agent computer. Do not type a full path. Instead, type a relative path based on the FTP publishing folder on the proxy agent computer, which is, by default, `c:\inetpub\ftproot`.
	
	The path must include the TreeView cluster name and a trailing backslash (\).
	
	For example, if the TreeView cluster name is "CiscoCM:CCM80-01-Cluster," then type `CCM80-01\`.
	
	Files will be written to the following folder on the proxy agent computer:
	
	`c:\inetpub\ftproot\CCM80-01`
	
	NOTE: A folder with the same name as the host name must exist on the FTP server, such as:
	
	`c:\inetpub\ftproot\<host name>`
	
	Use the same TreeView cluster name you use in the SetupSupplementalDB Knowledge Script parameters.
	
	Important If you are running Unified Communications Manager 5.x, use forward slashes (/), not backslashes (\), in your file path. In version 5.x, backslashes cause a corruption of the Cisco database. Backslashes are acceptable in later versions of Communications Manager.

2.11 Enabling Access to the Unified Communications Manager Server

By default, AppManager uses the `CCMAdmin` account to access Unified Communications Manager data. If you do not want to use the `CCMAdmin` account, you can set up a new user in a new user group and then configure that group with read-only permission for AppManager. After configuring the new user group, configure the new information in AppManager Security Manager and then run Discovery_CiscoCM on the primary Unified Communications Manager server.

2.11.1 Configuring a New User

To allow AppManager to access Unified Communications Manager data, create a new user and assign the user to a new user group.

To configure a new user:

1. Navigate to the Administration Web site of your primary Unified Communications Manager server.
2. In the **Username** and **Password** fields, type your user name and password, and then click **Submit**.
3. From the Cisco Unified Communications Manager Administration Web page, select **Application User** from the User Management menu, and then click **Add New**.
4. In the **User ID** field, type `netiq`.
5. In the **Password** and **Confirm Password** fields, type a password for the new user and then click **Save**.
6. On the Cisco Unified Communications Manager Administration Web page, select **User Group** from the User Management menu, and then click **Find**.
7. In the Search Results panel, click the **Copy** icon in the Standard CCM Read Only row.
8. In the Explorer User Prompt dialog box, type `NetIQ CCM Read Only` and then click **OK**.
9. Click **Add Application Users to Group** and then click **Find**.
10. Select **netiq** and then click **Add Selected**.
11. On the Cisco Unified Communications Manager Administration Web page, select **User Group** from the User Management menu.
12. In the NetIQ CCM Read Only row, click the **Roles** icon.
13. Click **Assign Role to Group** and then click **Find**.
14. Select **Standard AXL API Access** and then click **Add Selected**.
15. On the Cisco Unified Communications Manager Administration Web page, confirm the NetIQ CCM Read Only group is assigned to the following roles:
    - Standard CCM Admin Users
    - Standard CCMADMIN Read Only
    - Standard SERVICEABILITY Read Only
    - Standard AXL API Access

2.11.2 Adding the New User in Security Manager

After you create a new user in a new user group, add the new user name and password in AppManager Security Manager. Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`CiscoCM_AXL`
Sub-label	Computer name of the primary Unified Communications Manager server for which you created the new user and user group in Section 2.11.1, “Configuring a New User,” on page 26.

Field	Description
Value 1	`netiq`
Value 2	Password you created for the new user in Section 2.11.1, “Configuring a New User,” on page 26.
Extended application support	Required field to encrypt the new password in Security Manager.

2.11.3 Running Discovery_CiscoCM

After you create a new user and configure the new user in Security Manager, run the Discovery_CiscoCM Knowledge Script on the proxy agent computer. For more information about the discovery process, see Section 2.8, “Discovering Unified Communications Manager Resources,” on page 19.

In the *Comma-separated list of primary Communications Manager servers* parameter, provide the host name of the primary server for which you created the new user and user group in Section 2.11.1, “Configuring a New User,” on page 26.

2.12 Verifying Your Installed Module

To verify installation on many computers, run the ReportAM_CompVersion Knowledge Script. Ensure you discover a report-enabled agent before running this script. For more information, see the Help for the script.

To verify installation on one or only a few computers, use the Operator Console.

To verify your installed module with the Operator Console:

1. In the TreeView pane, select the computer for which you want to verify your installed module.
2. From the TreeView menu, select **Properties**. On the System tab, the System information pane displays the version numbers for all modules installed on the computer.
3. Verify that the version number from the *AppManager for Cisco Unified Communications Manager Readme* matches the version number shown in the System information pane.

2.13 Understanding Cluster Details in the Operator Console

After you discover a Unified Communications Manager cluster, the Details tab of the Operator Console displays information about the cluster in seven columns. To review the information, click the cluster name in the TreeView pane and then click the Details tab.

Column Name	Description
Name	Name AppManager has assigned to the cluster, based on the primary node name with a suffix of “`-Cluster`.”
Cluster ID	Cluster ID parameter from the Communications Manager configuration for the cluster.
Cluster Support	5.x for clusters 5.x and higher, depending on the cluster that was discovered.

Column Name	Description
Cisco Node Licenses	Value to the left of the colon (:) - Number of licensed Cisco Unified Communications Manager servers in a cluster at the time of discovery. Value to the right of the colon (:) - Number of licensed Cisco Unified Communications Manager nodes at the time of discovery.
Cisco Phone Licenses	Value to the left of the colon (:) - Number of licensed phone units in a cluster at the time of discovery. A phone might require more than one unit, depending on the phone type. For example, a Cisco 7970 phone requires five license units. Value to the right of the colon (:) - Number of authorized phone units in a cluster at the time of discovery.
NetIQ License Count	The number of registered hardware phones.
NetIQ MO Version	The build number of the most recently installed version of the managed object for AppManager for Cisco Unified Communications Manager.

In this example, the two columns identify a cluster that has a two configured servers, a 13-node license, enough phones to equal 1252 phone units, and a 21,000-phone license.

NOTE: You can use the LicenseUsage Knowledge Script to monitor available and used license units on a Cisco Unified Communications Manager cluster.

2.14 Monitoring Cluster Up/Down Status

AppManager provides a simple way to determine whether the computers in a cluster are up or down: the General_PingMachine Knowledge Script. Located on the **General** tab, which is available in the Master and NT views of the Operator Console, the General_PingMachine Knowledge Script checks the availability of computers that respond to ICMP Echo requests.

In the *List of computers to check* parameter, type a comma-separated list of the computers for which you want to check availability. You can also use the *Full path to file with list of computers* parameter to specify the location of a file that contains a list of the computers you want to check. For more information, see the Help for the General_PingMachine Knowledge Script.

2.15 Upgrading Knowledge Script Jobs

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

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

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

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

2.15.1 Running AMAdmin_UpgradeJobs

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

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

2.15.2 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. New parameters may need to be set appropriately for your environment or application.

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

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

2.15.3 Propagating Changes to Ad Hoc Jobs or Knowledge Script Groups

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

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

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

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

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

2.16 Uninstalling the Module

You can use the **Add or Remove Programs** or **Programs and Features** option from the Control Panel to uninstall this module.

The uninstallation process does not remove the Cisco Unified Applications Manager supplemental database, nor does it remove items from the QDB, including the Knowledge Scripts. To remove the database, use SQL Server Enterprise Manager or `osql.exe`. You must manually remove Knowledge Scripts.

3 Reporting with NetIQ Analysis Center

This chapter highlights the steps you should take to create several recommended reports using NetIQ Analysis Center and the data collected by several scripts in the Recommended Knowledge Script Group (KSG) for AppManager for Cisco Unified Communications Manager. This chapter assumes you have installed and are familiar with NetIQ Analysis Center 2.7. For more information, see the *User Guide for Analysis Center.*

Analysis Center imports raw data from multiple AppManager repositories, transforms that data into useful information about your computing infrastructure, and publishes that information in graphical and tabular reports.

In your Unified Communications Manager environment, you must monitor certain metrics to ensure the health of your system and its resources. By analyzing the metrics created by the activity in your environment, you can track performance, uncover trends, and make forecasts you can use for capacity planning and IT support.

In the following topics are instructions for creating recommended Unified Communications Manager reports in the following categories: Service Levels, Performance, and Capacity Planning.

TIP: When working in the Metric context of the Analysis Center Console, remember to deselect all applications except **CiscoCM** in the **Applications** drop list. By filtering for CiscoCM, you reduce the number of metrics displayed in the Metric context.

3.1 Service Levels Report

The reporting capability of Analysis Center enables organizations to demonstrate the value of IT and how well IT is aligned with business objectives. To these ends, create a Service Levels management report to reflect server availability.

The Service Levels report should summarize the availability of the Cisco Communications Manager Service running on Communications Manager servers. The availability of this service is vital to Unified Communications Manager's ability to process calls. This report will tell you whether your Communications Manager service is maintaining the percentage of availability promised in your Service Level Agreements.

The HealthCheck Knowledge Script gathers data about Communications Manager service availability. Before you create the report, ensure the HealthCheck script has been running with the *Collect data for service availability?* parameter set to **Yes**. When enabled, data collection returns a value of 1 to indicate availability and a value of 0 to indicate unavailability.

In Analysis Center, base your Service Levels report on the **Service availability_CiscoCallManager** metric, which is one of the data streams generated by the HealthCheck script if you chose to collect data. Use the **Metric By Machine** report template, located in the Templates > AppManager > By Metric folder in the Analysis Center Navigation pane.

3.2 Performance Reports

The performance side of your organization might not be the flashiest aspect, but it is probably one of the most vital in terms of VoIP functionality. Performance reports provide the details behind the Service Levels reports — the day-to-day activity in your Unified Communications Manager environment. Creating Performance reports helps you isolate servers that are experiencing problems such as excessive call volume or CPU usage.

The Performance reports should summarize call activity and system usage, and therefore depend upon the data gathered by two Knowledge Scripts: CCM_CallActivity and SystemUsage.

3.2.1 Call Activity Report

The CCM_CallActivity Knowledge Script monitors all call activity for a Communications Manager server. By default, this script generates seven types of data streams, which are represented in the Analysis Center Metric context as the following metrics:

- Active calls (Calls)
- Attempted calls (Calls)
- Attempted system calls (Calls)
- Calls in progress (Calls)
- Completed calls (Calls)
- Completed video calls (Calls)
- Incomplete calls (%)

Base your call activity report on one or more of these metrics. Use the **Performance Data Filtered by KS Over Time** report, located in the Performance folder of the Analysis Center Navigation pane.

To summarize call activity for all of your Communications Manager clusters, use the Group context to select the cluster group name instead of the individual Communications Manager computer. Cluster group names are visible only in the Master view.

You can create a *busy hour*

report by selecting **Attempted calls** in the Metric context, and selecting **Sum** in the Measures context. If you include several Communications Managers in one report, change the **ChartType** on the **Properties** tab from **Column** to **Line**, which is more suited to displaying data from multiple sources.

You can create a *call completion rate* report to compare completed calls and incomplete calls by selecting **Incomplete calls** and **Completed calls** metrics in the Metric context.

3.2.2 System Usage Report

The SystemUsage Knowledge Script monitors CPU, memory, and disk usage for a Communications Manager server. By default, this script generates nine types of data streams, which are represented in the Analysis Center Metric context as the following metrics:

- Active partition usage (%)
- Common partition usage (%)
- CPU usage (%)
- Physical memory usage (%)

- Swap partition usage (%)
- Swap space usage (%)
- Total processes (Processes)
- Total threads (Threads)
- Virtual memory usage (%)

You can base your System Usage report on the **Performance Data Filtered by KS Over Time** report, located in the Performance folder of the Analysis Center Navigation pane. Use this report to examine Unified Communications Manager system usage by date and time, which 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 clusters you want to include in the report. Computers and clusters are shown as columns in the report.

If you are including several computers or clusters, you might want to change the **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 Communications Manager CPU usage for each hour, use the Metric context to select **CPU usage**. Then use the Time context to select **Yesterday** in the **Date Range** field and **Hour** in the **Interval** field.

3.3 Trend and Prediction Report

Trend and Prediction reports should answer such questions as "How busy is this device?" or "Is this device being used at all?" They should provide data you can use to plan upgrades or reorganizations of the devices and resources in your Unified Communications Manager environment.

The Trend and Prediction report should summarize MGCP resource usage, and therefore depends upon the data gathered by the CCM_MGCPResources Knowledge Script. By summarizing data about MGCP resource usage, you will be able to determine whether your current configuration meets usage demands.

The MGCPResources script monitors active and in-service MGCP gateway resource usage for a Communications Manager server. By default, this script generates 10 types of data streams, which are represented in the Analysis Center Metric context as the following metrics:

- Active BRI channels (Channels)
- Active FXO ports (Ports)
- Active FXS ports (Ports)
- Active PRI channels (Channels)
- Active T1CAS channels (Channels)
- BRI spans in service (Channels)
- FXO ports in service (Channels)
- FXS ports in service (Ports)
- PRI spans in service (Spans)
- T1CAS spans in service (Spans)

You can base your Trend and Prediction report on the **Performance Data Trend and Prediction** report, located in the Trend and Prediction folder in the Analysis Center Navigation pane. Use this report to show the trend of the maximum utilization of Unified Communications Manager 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 to select one or more of the metrics noted above. 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.

4 CiscoCM Knowledge Scripts

AppManager for Cisco Unified Communications Manager provides the following Knowledge Scripts for monitoring a Unified Communications Manager environment.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, select any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
4x_PhoneDeregistrations	Monitors phone deregistrations on a Communications Manager 4.x cluster and maintains a history of deregistrations in the CiscoCM supplemental database.
4x_RetrieveConfigData	Retrieves Communications Manager 4.x configuration data and stores it the CiscoCM supplemental database.
4x_SetupSupplementalDB	Creates a CiscoCM supplemental database in which to store Communications Manager 4.x configuration and phone deregistration information.
AnalogAccess_GatewayUsage	Monitors resource usage for analog access gateways.
Annunciator_Device	Monitors resource usage for annunciator devices.
AttendantConsole	Monitors activity for the Attendant Console application.
CCM_CallActivity	Monitors call activity on a Communications Manager server.
CCM_MediaResources	Monitors media resources for a Communications Manager.
CCM_MGCPResources	Monitors active MGCP gateway resource usage for a Communications Manager.
CCM_RegisteredResources	Monitors changes in the number of resources registered to a Communications Manager server.
CCM_ResourceAvailability	Monitors the number of times Communications Manager requests a resource that is unavailable.
CCM_SystemPerformance	Monitors call throttling and signal processing queues for a Communications Manager.
CDR_CallFailures	Monitors call detail records retrieved from Communications Manager for calls that ended with an abnormal termination code.
CDR_CallQuality	Monitors call detail records and call management records retrieved from Communications Manager for jitter, latency, lost data, and MOS.
CDR_Query	Queries call detail records retrieved from Communications Manager and stored in the CiscoCM supplemental database.
CDR_RetrieveCallRecords	Retrieves call detail records from Communications Manager and places them in the CiscoCM supplemental database.
CDR_RetrieveConfigData	Retrieves Communications Manager configuration data and stores it the CiscoCM supplemental database.

Knowledge Script	What It Does
CFB_Hardware_Device	Monitors the resource usage of registered hardware conference bridge devices.
CFB_Software_Device	Monitors the resource usage of registered software conference bridge devices.
CFB_Video_Device	Monitors the resource usage of registered video conference bridge devices.
CTIManager	Monitors the usage of the Communications Manager CTI Manager.
ExtensionMobility	Monitors activity for the Extension Mobility application.
GatekeeperActivity	Monitors the activity on a gatekeeper.
GeneralCounter	Monitors a user-specified Performance Monitor counter.
H323_Gateway_CallActivity	Monitors call activity for H323 gateway devices.
H323_Trunk_CallActivity	Monitors call activity for H323 trunk devices.
HealthCheck	Monitors the operational status of active services on Communications Manager servers.
HuntAndRouteList	Monitors hunt lists and route lists for availability and call activity.
LicenseUsage	Monitors authorized, used, remaining, and the percentage of used licenses on a Cisco Unified Communications Manager cluster.
Locations	Monitors Cisco locations for voice and video bandwidth availability and usage.
LocationsList	Monitors all combinations of location bandwidth counters, including inter-location pairs.
MediaStreamingApp	Monitors the resources handled by the Media Streaming Application.
MGCP_FXO_CallActivity	Monitors completed calls, blocked calls, outbound busy attempts, and port status on MGCP FXO devices.
MGCP_FXS_CallActivity	Monitors completed calls, blocked calls, outbound busy attempts, and port status on MGCP FXS devices.
MGCP_GatewayUsage	Monitors active and in-service ports, active channels, and in-service spans for MGCP gateways.
MGCP_PRI_CallActivity	Monitors completed calls, outbound busy attempts, active calls, blocked calls, and data link availability for MGCP PRI devices.
MGCP_PRI_ChannelHealth	Monitors the status of channels for MGCP PRI devices.
MGCP_T1CAS_CallActivity	Monitors completed calls, outbound busy attempts, active calls, and blocked calls for MGCP T1CAS devices.
MGCP_T1CAS_ChannelHealth	Monitors the status of channels for an MGCP T1CAS device.
MOH_Device	Monitors the resource usage for a registered Music-on-Hold device.
MTP_Device	Monitors the resource usage for a registered Media Termination Point device.
PhoneDeregistrations	Monitors phone deregistrations for a Communications Manager and retains deregistration history in the CiscoCM supplemental database.

Knowledge Script	What It Does
PhoneInventory	Creates an inventory of the phones configured in a Communications Manager cluster.
Report_PhoneDeregAudit	Creates a history of phone deregistrations and reregistrations.
Report_PhoneDeregWatchList	Creates a list of phones that frequently deregister.
RoleStatus	Monitors status changes for primary and backup Communications Managers in a Communications Manager group.
SetupSupplementalDB	Creates a CiscoCM supplemental database in which to store Communications Manager call detail records.
SIP_Trunk_CallActivity	Monitors call activity for SIP trunk devices.
SNMPTrap_AddMIB	Add management information bases for monitoring by the SNMPTrap_AddMIB Knowledge Script.
SNMPTrap_Async	Checks for incoming SNMP traps forwarded from NetIQ SNMP Trap Receiver.
SystemUpTime	Monitors the number of hours Communications Manager has been operational since its last reboot.
SystemUsage	Monitors CPU, memory, and disk usage for a Communications Manager server.
TFTPActivity	Monitors activity on the Cisco TFTP server.
Transcoder_Device	Monitors the resources used by registered transcoder devices.
WebDialer	Monitors activity for the Cisco Web Dialer application.
WebPageCheck	Monitors the availability of and round-trip time to the ccmadmin and ccmuser Web pages.
Recommended Knowledge Script Group	Performs essential monitoring of your Cisco Unified Communications Manager environment.

4.1 4x_PhoneDeregistrations

Use this Knowledge Script to monitor phone deregistrations on a Communications Manager 4.x cluster and to maintain a history of deregistrations in the CiscoCM supplemental database. This script raises an event if the number or percentage of lost phones exceeds the threshold you set. You determine how long a phone must be deregistered before it is considered “lost.” In addition, you determine whether to group events by cluster, device pool, location, or partition.

For more information, see Appendix A, “Monitoring Deregistration for Communications”.

4.1.1 Prerequisites

Run the 4x_SetupSupplementalDB Knowledge Script to create the CiscoCM supplemental database. Then, run the 4x_RetrieveConfigData Knowledge Script to retrieve Communications Manager 4.x configuration information.

4.1.2 Resource Object

CiscoCM_Cluster4xMgmt

4.1.3 Default Schedule

By default, this script runs every five minutes.

4.1.4 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 the failure of the 4x_PhoneDeregistration job. The default is 5.
Event Notification	
Raise event if lost phones in group exceed threshold?	Select **Yes** to raise an event if the number or percentage of lost phones in a group exceeds the threshold you set. The default is Yes. Use *Select event grouping* to select how to group the lost phones. Use *Maximum time phone deregistered before counted as lost* to determine how long a phone must be deregistered before it is considered lost.
Select event grouping	Select whether to group lost phones by **Cluster**, **Device Pool**, **Location**, or **Partition**. AppManager raises an event based on whether the number of lost phones in *each* group exceeds the threshold you set. For example, you set *Maximum number of lost phones in the group* to 5, you set *Select event grouping* to Device Pool, and you have three device pools. If AppManager detects six lost phones in the first pool, two in the second, and seven in the third, it will raise two events: one for the six lost phones in the first pool and another for the seven lost phones in the third pool. Because you set the threshold to “5,” no event is raised for the lost phones in the second pool. The default is Cluster.
Maximum time phone deregistered before counted as lost	Specify the number of minutes that must elapse before a deregistered phone can be considered a “lost” phone. The default is 0 minutes. Accept the default if you want *all* deregistered phones to be considered lost.
Type of threshold	Select whether you want to raise events based on the **Number** or **Percent** of lost phones. The default is Number.
Threshold - Maximum number of lost phones	Use this parameter if you selected **Number** in *Type of threshold*. Specify the maximum number of phones that can be lost before an event is raised. The default is 0.

Parameter	How to Set It
Threshold - Maximum percent of lost phones	Use this parameter if you selected **Percent** in *Type of threshold*. Specify the maximum percentage of phones that can be lost before an event is raised. The default is 0.
Event severity when lost phones exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number or percentage of lost phones in a group exceeds the threshold you set. The default is 15.
Include lost phone details in event message	Select **Yes** to include details of the lost phones in the event message. Phone details can include device name, device IP address, directory number, description, name of device pool, time of deregistration, and the Communications Manager from which the phone was deregistered. The default is Yes.
Maximum number of detail rows to include in event detail	Specify the maximum number of detail rows to include in an event message. Each row contains details for one phone. Rows are sorted in order by most recently lost phone. Specify “0” to include all rows. The default is 20. This parameter is applicable only if you selected **Yes** for *Include lost phone details in event message*.

4.2 4x_RetrieveConfigData

Use this Knowledge Script to retrieve Communications Manager configuration data from the Communications Manager 4.x Publisher and store it in the CiscoCM supplemental database.

For more information, see Monitoring Deregistration for Communications Manager 4.x Clusters.

4.2.1 Prerequisite

Run the 4x_SetupSupplementalDB Knowledge Script to create the CiscoCM supplemental database.

4.2.2 Resource Object

CiscoCM_Cluster4xMgmt

4.2.3 Default Schedule

By default, this script runs once a day, at 3 A.M, so as to perform its possibly CPU-intensive function at a time when the Communications Manager is least busy.

However, because the 4x_PhoneDeregistrations script uses the configuration data this script retrieves, you might want to set this script to “Run Once” so the configuration data is retrieved immediately. Once the “Run Once” job is complete, you can then run this script using the default schedule of once daily.

4.2.4 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 the failure of the 4x_RetrieveConfigData job. The default is 5.
Raise event if configuration retrieval succeeds?	Select **Yes** to raise an event if Communications Manager 4.x configuration data is successfully retrieved from the CiscoCM supplemental database. The default is unselected.
Event severity when configuration retrieval succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which configuration data is successfully retrieved from the CiscoCM supplemental database. The default is 25.

4.3 4x_SetupSupplementalDB

Use this Knowledge Script to create a CiscoCM supplemental database in which to store Communications Manager 4.x phone deregistration information.

For more information, see Appendix A, “Monitoring Deregistration for Communications Manager 4.x Clusters.”

4.3.1 Resource Object

CiscoCM_Cluster4xMgmt

4.3.2 Default Schedule

By default, this script runs once.

4.3.3 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 the failure of the 4x_SetupSupplementalDB job. The default is 5.
Raise event if database setup succeeds?	Select **Yes** to raise an event if the CiscoCM supplemental database is successfully created on the proxy agent computer. The default is unselected.

Parameter	How to Set It
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CiscoCM supplemental database is successfully created. The default is 25.
Phone Deregistration Parameters	
Number of days to keep phone deregistration audit entries	Specify the number of days' worth of phone deregistration audit entries you want to keep in the CiscoCM supplemental database. Any data older than what you specify is discarded. The default is 180 days.
Is your CallManager configured to use secure Web access (HTTPS)?	Select **Yes** if you use secure HTTP (HTTPS) to access your Communications Manager. AppManager uses this information to build the Communications Manager URL that is displayed in event message details. The default is unselected.
SQL Server Information	
Local SQL Server Instance name	Specify the name of the local SQL Server instance (on the proxy agent computer) in which you want to create the new CiscoCM supplemental database. Leave this parameter blank to accept the default name.

4.4 AnalogAccess_GatewayUsage

Use this Knowledge Script to monitor active ports, out-of-service ports, and outbound busy attempts for analog access gateways. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active ports, out-of-service ports, and outbound busy attempts.

4.4.1 Resource Object

CiscoCM_AnalogAccessObj

4.4.2 Default Schedule

By default, this script runs every 15 minutes.

4.4.3 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 the failure of the AnalogAccess_GatewayUsage job. The default is 5.
Monitor Active Ports	
Event Notification	
Raise event if active ports exceed threshold?	Select **Yes** to raise an event if the number of active ports exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
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 active ports exceed threshold	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 15.
Data Collection	
Collect data for active ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports that are active at each script iteration. The default is unselected.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of times that the gateway received a busy signal exceeds the threshold you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of times the gateway can attempt a connection that receives a busy signal before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event 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.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of gateway connection attempts that received a busy signal during the monitoring period. The default is unselected.
Monitor Out of Service Ports	
Event Notification	
Raise event if out of service ports exceed threshold?	Select **Yes** to raise an event if the number of ports that were out of service exceeds the threshold you set. The default is Yes.
Threshold - Maximum out of service ports	Specify the maximum number of ports that must be out of service before an event is raised. The default is 0 ports.
Event severity when out of service ports exceed threshold	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.
Data Collection	
Collect data for out of service ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports that are out of service at each script iteration. The default is unselected.

4.5 Annunciator_Device

Use this Knowledge Script to monitor the annunciator resource usage for a Communications Manager. An annunciator enables Communications Manager to play recorded announcements and tones to Cisco IP phones, gateways, and other configurable devices.

This script raises an event if the number of times annunciator resources were unavailable exceeds the threshold, or if the percentage of resource usage exceeds the threshold. In addition, this script generates data streams for the number of active resources, the number of available resources, the number of times resources were unavailable, and the percentage of resource usage.

4.5.1 Resource Object

CiscoCM_AnnunciatorObj

4.5.2 Default Schedule

By default, this script runs every 15 minutes.

4.5.3 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 the failure of the Annunciator_Device job. The default is 5.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of annunciator resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the highest percentage of annunciator resource usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which annunciator resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of annunciator resource usage at each script iteration. The default is unselected.
Monitor Active Resources	
Data Collection	

Parameter	How to Set It
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator resources that are active at each script iteration. The default is unselected.
Monitor Available Resources	
Data Collection	
Collect data for available resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator resources that are available at each script iteration. The default is unselected.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times that annunciator resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times annunciator resources must be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times annunciator resources were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times annunciator resources were unavailable during the monitoring period. The default is unselected.

4.6 AttendantConsole

Use this Knowledge Script to monitor handled and in-progress requests for the Attendant Console application. Attendant Console allows you to set up Cisco IP phones to use speed-dial buttons and quick directory access, look up phone numbers, monitor line status, and redirect calls.

This script raises an event if the number of redirected calls and online clients exceed the threshold you set. In addition, this script generates data streams for the number of redirected calls, the number of total calls, the number of online clients, the number of registered clients, and the line connection state.

NOTE: Cisco Systems no longer supports the Cisco Unified Communications Manager Attendant Console. As a result, the CiscoCM_AttendantConsole Knowledge Script will not work on Cisco Unified Communications Manager 8.0 or later.

4.6.1 Resource Object

CiscoCM_AttendConsole

4.6.2 Default Schedule

By default, this script runs every 15 minutes.

4.6.3 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 the failure of the AttendantConsole job. The default is 5.
Monitor Redirected Calls	
Event Notification	
Raise event if redirected calls exceed threshold?	Select **Yes** to raise an event if the number of redirected calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum redirected calls	Specify the maximum number of calls that must be redirected before an event is raised. The default is 50 calls.
Event severity when redirected calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of redirected calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for redirected calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were redirected during the monitoring period.
Monitor Total Calls	
Data Collection	
Collect data for total calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of calls handled by Attendant Console during the monitoring period.
Monitor Online Clients	
Event Notification	
Raise event if online clients exceed threshold?	Select **Yes** to raise an event if the number of online clients exceeds the threshold you set. The default is Yes.
Threshold - Maximum online clients	Specify the maximum number of clients that must be online before an event is raised. The default is 100 clients.
Event severity when online clients exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of online clients exceeds the threshold. The default is 15.
Data Collection	
Collect data for online clients?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of clients that are online at each script iteration.
Monitor Registered Clients	

Parameter	How to Set It
Data Collection	
Collect data for registered clients?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of clients that are registered at each script iteration.
Monitor Connection State	
Data Collection	
Collect data for connection state?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the line connection state for the Cisco Telephony Call Dispatcher (TCD) at each script iteration. Attendant Console uses TCD for login services, line state, and directory services. You can choose from the following line connection states: ◆ 0 - Not registered or not receiving line link state information from Communications Manager ◆ 1 - Registered and receiving line link state information from Communications Manager ◆ 10 - TCD is logged in, but has not registered or received line link state information from Communications Manager ◆ 11 - TCD is logged in, has registered, and is receiving line link state information from Communications Manager

4.7 CCM_CallActivity

Use this Knowledge Script to monitor call activity on a Communications Manager server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Attempted calls
- Completed calls
- Active calls
- In-progress calls
- Incomplete calls (%)
- Attempted system calls
- Completed video calls

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.7.1 Resource Object

CiscoCM_CMServer

4.7.2 Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.7.3 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 the failure of the CCM_CallActivity job. The default is 5.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that are active at each script iteration. The default is Yes. A call is considered “active” once a connection is made.
Monitor Attempted Calls	
Event Notification	
Raise event if attempted calls exceed threshold?	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the maximum number of calls that must be attempted before an event is raised. The default is 0 calls.
Event severity when attempted calls exceed threshold	Set the event 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 25.
Data Collection	
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were attempted during the monitoring period. The default is Yes.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were completed during the monitoring period. The default is Yes.
Monitor Calls in Progress	
Event Notification	

Parameter	How to Set It
Raise event if calls in progress exceed threshold?	Select **Yes** to raise an event if the number of in-progress calls exceeds the threshold you set. The default is Yes. A call is considered “in-progress” as soon as the receiver is lifted.
Threshold - Maximum calls in progress	Specify the maximum number of calls that must be in progress before an event is raised. The default is 100 calls.
Event severity when calls in progress exceed 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.
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration. The default is Yes.
Monitor Incomplete Calls	
Event Notification	
Raise event if incomplete calls exceeds threshold?	Select **Yes** to raise an event if the percentage of incomplete calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum incomplete calls	Specify the highest percentage of incomplete calls that must be detected before an event is raised. The default is 0%.
Event severity when incomplete calls exceed threshold	Set the event 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 25.
Data Collection	
Collect data for incomplete calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of incomplete calls during the monitoring period. The default is Yes.
Monitor Attempted System Calls	
Event Notification	
Raise event if attempted system calls exceed threshold?	Select **Yes** to raise an event if the number of attempted system calls exceeds the threshold you set. The default is Yes. System calls are signals sent to phones to turn on/off the Message Waiting indicator. A system call is sent to illuminate the indicator when a message is left, and another one is sent to turn off the indicator when the user listens to that message.
Threshold - Maximum attempted system calls	Specify the highest number of system calls that must be attempted before an event is raised. The default is 0 calls.
Event severity when attempted system calls calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of attempted system calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for attempted system calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of system calls attempted during the monitoring period. The default is unselected.
Monitor Completed Video Calls	

Parameter	How to Set It
Data Collection	
Collect data for completed video calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video calls that were completed during the monitoring period. The default is unselected.

4.8 CCM_MediaResources

Use this Knowledge Script to monitor Communications Manager media resources:

- Annunciators
- Conference bridges
- Music-on-Hold (MOH)
- Media Termination Points (MTP)
- Transcoders

This script raises an event if a threshold is exceeded. In addition, this script generates percentage and active data streams for annunciator resource usage, conference bridge resource usage (hardware, software, and video), MTP resource usage, MOH (unicast and multicast) resource usage, and transcoder resource usage.

4.8.1 Resource Object

CiscoCM_CallProcessor

4.8.2 Default Schedule

By default, this script runs every 15 minutes.

4.8.3 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 the failure of the CCM_MediaResources job. The default is 5.
Monitor Annunciator Resource Usage	
Event Notification	
Raise event if annunciator resource usage exceeds threshold?	Select **Yes** to raise an event if annunciator resource usage exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum annunciator resource usage	Specify the maximum percentage of annunciator resource usage that must be detected before an event is raised. The default is 90%.
Event severity when annunciator resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which annunciator resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for annunciator resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of annunciator resource usage at each script iteration. The default is unselected.
Monitor Hardware Conference Bridge Resource Usage	
Event Notification	
Raise event if hardware conference bridge resource usage exceeds threshold?	Select **Yes** to raise an event if hardware conference bridge resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum hardware conference bridge resource usage	Specify the maximum percentage of hardware conference bridge resource usage that must be detected before an event is raised. The default is 90%.
Event severity when hardware conference bridge resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which hardware conference bridge resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for hardware conference bridge resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of hardware conference bridge resource usage at each script iteration. The default is unselected.
Monitor Software Conference Bridge Resource Usage	
Event Notification	
Raise event if software conference bridge resource usage exceeds threshold?	Select **Yes** to raise an event if software conference bridge resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum software conference bridge resource usage	Specify the maximum percentage of software conference bridge resource usage that must be detected before an event is raised. The default is 90%.
Event severity when software conference bridge resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which software conference bridge resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for software conference bridge resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of software conference bridge resource usage at each script iteration. The default is unselected.
Monitor Video Conference Bridge Resource Usage	

Parameter	How to Set It
Event Notification	
Raise event if video conference bridge resource usage exceeds threshold?	Select **Yes** to raise an event if video conference bridge resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum video conference bridge resource usage	Specify the maximum percentage of video conference bridge resource usage that must be detected before an event is raised. The default is 90%.
Event severity when video conference bridge resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which video conference bridge resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for video conference bridge resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of video conference bridge resource usage at each script iteration. The default is unselected.
Monitor Media Termination Point Resource Usage	
Event Notification	
Raise event if Media Termination Point resource usage exceeds threshold?	Select **Yes** to raise an event if MTP resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum Media Termination Point resource usage	Specify the maximum percentage of MTP resource usage that must be detected before an event is raised. The default is 90%.
Event severity when Media Termination Point resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MTP resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for Media Termination Point resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MTP resource usage at each script iteration. The default is unselected.
Monitor Music-on-Hold Multicast Resource Usage	
Event Notification	
Raise event if Music-on-Hold multicast resource usage exceeds threshold?	Select **Yes** to raise an event if MOH multicast resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum Music-on-Hold multicast resource usage	Specify the maximum percentage of MOH multicast resource usage that must be detected before an event is raised. The default is 90%.
Event severity when Music-on-Hold multicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MOH multicast resource usage exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for Music-on-Hold multicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MOH multicast resource usage at each script iteration. The default is unselected.
Monitor Music-on-Hold Unicast Resource Usage	
Event Notification	
Raise event if Music-on-Hold unicast resource usage exceeds threshold?	Select **Yes** to raise an event if MOH unicast resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum Music-on-Hold unicast resource usage	Specify the maximum percentage of MOH unicast resource usage that must be detected before an event is raised. The default is 90%.
Event severity when Music-on-Hold unicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MOH unicast resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for Music-on-Hold unicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MOH unicast resource usage at each script iteration. The default is unselected.
Monitor Transcoder Resource Usage	
Event Notification	
Raise event if transcoder resource usage exceeds threshold?	Select **Yes** to raise an event if transcoder resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum transcoder resource usage	Specify the maximum percentage of transcoder resource usage that must be detected before an event is raised. The default is 90%.
Event severity when transcoder resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which transcoder usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for transcoder resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of transcoder resource usage at each script iteration. The default is unselected.
Monitor Active Annunciator Resources	
Data Collection	
Collect data for active annunciator resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator resources that are active at each script iteration. The default is unselected.
Monitor Active Hardware Conference Resources	
Data Collection	
Collect data for active hardware conference resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conference resources that are active at each script iteration. The default is unselected.

Parameter	How to Set It
Monitor Active Software Conference Resources	
Data Collection	
Collect data for active software conference resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conference resources that are active at each script iteration. The default is unselected.
Monitor Active Video Conference Resources	
Data Collection	
Collect data for active video conference resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conference resources that are active at each script iteration. The default is unselected.
Monitor Active Media Termination Point Resources	
Data Collection	
Collect data for active Media Termination Point resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MTP resources that are active at each script iteration. The default is unselected.
Monitor Active Music-on-Hold Multicast Resources	
Data Collection	
Collect data for active Music-on-Hold multicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH multicast resources that are active at each script iteration. The default is unselected.
Monitor Active Music-on-Hold Unicast Resources	
Data Collection	
Collect data for active Music-on-Hold unicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH unicast resources that are active at each script iteration. The default is unselected.
Monitor Active Transcoder Resources	
Data Collection	
Collect data for active transcoder resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of transcoder resources that are active at each script iteration. The default is unselected.

4.9 CCM_MGCPResources

Use this Knowledge Script to monitor active and in-service MGCP gateway resource usage for a Communications Manager:

- BRI (basic rate interface) channels and spans
- FXO (foreign exchange office) ports
- FXS (foreign exchange station) ports
- PRI (primary rate interface) channels and spans
- T1CAS (channel associated signaling) channels and spans

An *active* resource is currently handling a call. An *in-service* resource is available to handle a call.

This script raises an event if any threshold is exceeded. In addition, this script generates data streams for active and in-service ports/channels/spans for any monitored resources.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.9.1 Resource Object

CiscoCM_CallProcessor

4.9.2 Default Schedule

By default, this script runs every ten minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.9.3 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 the failure of the CCM_MGCPResources job. The default is 5.
Monitor Active BRI Channels	
Event Notification	
Raise event if active BRI channels exceed threshold?	Select **Yes** to raise an event if the number of active BRI channels exceeds the threshold you set. The default is Yes.
Threshold - Maximum active BRI channels	Specify the maximum number of BRI channels that must be active before an event is raised. The default is 100 channels.
Event severity when active BRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active BRI channels exceeds the threshold. The default is 15.
Data Collection	
Collect data for active BRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of BRI channels that are active at each script iteration. The default is unselected.
Monitor BRI Spans in Service	
Data Collection	

Parameter	How to Set It
Collect data for BRI spans in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of BRI spans that are in service at each script iteration. The default is Yes.
Monitor Active FXO Ports	
Event Notification	
Raise event if active FXO ports exceed threshold?	Select **Yes** to raise an event if the number of active FXO ports exceeds the threshold you set. The default is Yes.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that must be active before an event is raised. The default is 25 ports.
Event severity when active FXO ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXO ports exceeds the threshold. The default is 15.
Data Collection	
Collect data for active FXO ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXO ports that are active at each script iteration. The default is unselected.
Monitor FXO Ports in Service	
Data Collection	
Collect data for FXO ports in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXO ports that are in service at each script iteration. The default is Yes.
Monitor Active FXS Ports	
Event Notification	
Raise event if active FXS ports exceed threshold?	Select **Yes** to raise an event if the number of active FXS ports exceeds the threshold you set. The default is Yes.
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that must be active before an event is raised. The default is 25 ports.
Event severity when active FXS ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXS ports exceeds the threshold. The default is 15.
Data Collection	
Collect data for active FXS ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXS ports that are active at each script iteration. The default is unselected.
Monitor FXS Ports in Service	
Data Collection	
Collect data for FXS ports in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXS ports that are in service at each script iteration. The default is Yes.
Monitor Active PRI Channels	
Event Notification	

Parameter	How to Set It
Raise event if active PRI channels exceed threshold?	Select **Yes** to raise an event if the number of active PRI channels exceeds the threshold you set. The default is Yes.
Threshold - Maximum active PRI channels	Specify the maximum number of PRI channels that must be active before an event is raised. The default is 100 channels.
Event severity when active PRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active PRI channels exceeds the threshold. The default is 15.
Data Collection	
Collect data for active PRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of PRI channels that are active at each script iteration. The default is unselected.
Monitor PRI Spans in Service	
Data Collection	
Collect data for PRI spans in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of PRI spans that are in service at each script iteration. The default is Yes.
Monitor Active T1CAS Channels	
Event Notification	
Raise event if active T1CAS channels exceed threshold?	Select **Yes** to raise an event if the number of active T1CAS channels exceeds the threshold you set. The default is Yes.
Threshold - Maximum active T1CAS channels	Specify the maximum number of T1CAS channels that must be active before an event is raised. The default is 100 channels.
Event severity when active T1CAS channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active T1CAS channels exceeds the threshold. The default is 15.
Data Collection	
Collect data for active T1CAS channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of T1CAS channels that are active at each script iteration. The default is unselected.
Monitor T1CAS Spans in Service	
Data Collection	
Collect data for T1CAS spans in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of T1CAS spans that are in service at each script iteration. The default is Yes.

4.10 CCM_RegisteredResources

Use this Knowledge Script to monitor changes in the number of resources (phones, gateways, and station devices) registered to a Communications Manager server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the percentage of increase or decrease in registered resources, as well as data streams for the number of registered resources related to those percentages of increases or decreases.

If the number of registered resources increases from zero to a larger number, this script reports the increase as 100% multiplied by the number of new registered resources. For example, if the previous number of registered gateways is zero, and the latest iteration of this script finds seven new registered gateways, then the script reports the increase in registered gateways as 700%. For more information about phone resources, see PhoneInventory.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.10.1 Resource Object

CiscoCM_CMServer

4.10.2 Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.10.3 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 the failure of the CCM_RegisteredResources job. The default is 5.
Monitor Registered Hardware Phones	
Data Collection	
Collect data for registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number hardware phones that are registered at each script iteration. The default is unselected.
Monitor Increase in Registered Hardware Phones	
Event Notification	

Parameter	How to Set It
Raise event if increase in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the increase in registered hardware phones exceeds the threshold you set. The default is unselected.
Threshold - Maximum increase in registered hardware phones	Specify the maximum increase in the number of registered hardware phones that can occur before an event is raised. The default is 1 phone.
Event severity when increase in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of new registered hardware phones exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in hardware phones during the monitoring period. The default is unselected.
Monitor Percentage Increase in Registered Hardware Phones	
Event Notification	
Raise event if percentage increase in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the percentage increase in registered hardware phones exceeds the threshold you set. The default is Yes.
Threshold - Maximum percentage increase in registered hardware phones	Specify the maximum decrease in registered hardware phones that can occur before an event is raised. The default is 10%.
Event severity when percentage increase in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered hardware phones exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in hardware phones during the monitoring period. The default is unselected.
Monitor Decrease in Registered Hardware Phones	
Event Notification	
Raise event if decrease in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the decrease in registered hardware phones exceeds the threshold you set. The default is unselected.
Threshold - Maximum decrease in registered hardware phones	Specify the maximum decrease in the number of registered hardware phones that can occur before an event is raised. The default is 1 phone.
Event severity when decrease in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the decrease in number of registered hardware phones exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for decrease in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the decreasing number of registered hardware phones during the monitoring period. The default is unselected.
Monitor Percentage Decrease in Registered Hardware Phones	
Event Notification	
Raise event if percentage decrease in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the percentage decrease in registered hardware phones exceeds the threshold you set. The default is Yes.
Threshold - Maximum percentage decrease in registered hardware phones	Specify the maximum percentage decrease in registered hardware phones that can occur before an event is raised. The default is 10%.
Event severity when percentage decrease in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered hardware phones exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for percentage decrease in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in hardware phones during the monitoring period. The default is unselected.
Monitor Registered MGCP Gateways	
Data Collection	
Collect data for registered MGCP gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MGCP gateways registered at each script iteration. The default is unselected.
Monitor Increase in Registered MGCP Gateways	
Event Notification	
Raise event if increase in registered MGCP gateways exceeds threshold?	Select **Yes** to raise an event if the increase in registered MGCP gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered MGCP gateways	Specify the maximum increase in registered MGCP gateways that can occur before an event is raised. The default is 10%.
Event severity when increase in registered MGCP gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered MGCP gateways exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered MGCP gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered MGCP gateways during the monitoring period. The default is unselected.

Parameter	How to Set It
Monitor Decrease in Registered MGCP Gateways	
Event Notification	
Raise event if decrease in registered MGCP gateways exceeds threshold?	Select **Yes** to raise an event if the decrease in registered MGCP gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered MGCP gateways	Specify the maximum decrease in registered MGCP gateways that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered MGCP gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered MGCP gateways exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered MGCP gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered MGCP gateways during the monitoring period. The default is unselected.
Monitor Registered Analog Access Gateways	
Data Collection	
Collect data for registered Analog Access gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Analog Access gateways registered at each script iteration. The default is unselected.
Monitor Increase in Registered Analog Access Gateways	
Event Notification	
Raise event if increase in registered Analog Access gateways exceeds threshold?	Select **Yes** to raise an event if the increase in registered Analog Access gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered Analog Access gateways	Specify the maximum increase in registered Analog Access gateways that can occur before an event is raised. The default is 10%.
Event severity when increase in registered Analog Access gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered Analog Access gateways exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered Analog Access gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the increase in registered Analog Access gateways during the monitoring period. The default is unselected.
Monitor Decrease in Registered Analog Access Gateways	
Event Notification	

Parameter	How to Set It
Raise event if decrease in registered Analog Access gateways exceeds threshold?	Select **Yes** to raise an event if the decrease in registered Analog Access gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered Analog Access gateways	Specify the maximum decrease in registered Analog Access gateways that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered Analog Access gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered Analog Access gateways exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered Analog Access gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered Analog Access gateways during the monitoring period. The default is unselected.
Monitor Registered Other Station Devices	
Data Collection	
Collect data for registered other station devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of other station devices registered at each script iteration. The default is unselected.
Monitor Increase in Registered Other Station Devices	
Event Notification	
Raise event if increase in registered other station devices exceeds threshold?	Select **Yes** to raise an event if the increase in registered other station devices exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered other station devices	Specify the maximum increase in registered other station devices that can occur before an event is raised. The default is 10%.
Event severity when increase in registered other station devices exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered other station devices exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered other station devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered other station devices during the monitoring period. The default is unselected.
Monitor Decrease in Registered Other Station Devices	
Event Notification	
Raise event if decrease in registered other station devices exceeds threshold?	Select **Yes** to raise an event if the decrease in registered other station devices exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum decrease in registered other station devices	Specify the maximum decrease in registered other station devices that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered other station devices exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered other station devices exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered other station devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered other station devices during the monitoring period. The default is unselected.

4.11 CCM_ResourceAvailability

Use this Knowledge Script to monitor the number of times Communications Manager requests a resource that is unavailable. This script monitors the following resources:

- Annunciators
- Hardware, software, and video conference bridges
- Locations
- Media Termination Points (MTPs)
- Music-on-Hold (MOH)
- Transcoders

This script raises an event if an availability threshold is exceeded. In addition, this script generates data streams for instances of unavailability for each monitored resource.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.11.1 Resource Object

CiscoCM_CallProcessor

4.11.2 Default Schedule

By default, this script runs every 15 minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.11.3 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 the failure of the CCM_ResourceAvailability job. The default is 5.
Monitor Unavailable Annunciator Resources	
Event Notification	
Raise event if number of times annunciator resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times annunciator resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times annunciator resources were unavailable	Specify the maximum number of times an annunciator resource can be unavailable before an event is raised. The default is 0 times
Event severity when number of times annunciator resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times an annunciator resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times annunciator resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times annunciator resources were unavailable during the monitoring period. The default is unselected.
Monitor Unavailable Hardware Conference Bridge Resources	
Event Notification	
Raise event if number of times hardware conference bridge resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times hardware conference bridge resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times hardware conference bridge resources ere unavailable	Specify the maximum number of times a hardware conference bridge resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times hardware conference bridge resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a hardware conference bridge resource was unavailable exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for number of times hardware conference bridge resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times hardware conference bridge resources were unavailable during the monitoring period. The default is unselected.
Monitor Unavailable Software Conference Bridge Resources	
Event Notification	
Raise event if number of times software conference bridge resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times software conference bridge resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times software conference bridge resources were unavailable	Specify the maximum number of times a software conference bridge resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times software conference bridge resource were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a software conference bridge resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times software conference bridge resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times software conference bridge resources were unavailable during the monitoring period. The default is unselected.
Monitor Unavailable Video Conference Bridge Resources	
Event Notification	
Raise event if number of times video conference bridge resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times video conference bridge resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times video conference bridge resources were unavailable	Specify the maximum number of times a video conference bridge resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times video conference bridge resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a video conference bridge resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for number of times video conference bridge resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times video conference bridge resources were unavailable during the monitoring period. The default is unselected.
Monitor Unavailable Location Resources	
Event Notification	
Raise event if number of times location resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number times location resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times location resources were unavailable	Specify the maximum number of times a location resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times location resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a location resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times location resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times location resources were unavailable during the monitoring period. The default is unselected.
Monitor Unavailable Media Termination Point Resources	
Event Notification	
Raise event if number of times Media Termination Point resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MTP resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times Media Termination Point resources were unavailable	Specify the maximum number of times an MTP resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times Media Termination Point resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times an MTP resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times Media Termination Point resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MTP resources were unavailable during the monitoring period. The default is unselected.
Monitor Unavailable Music-on-Hold Resources	
Event Notification	

Parameter	How to Set It
Raise event if number of times Music-on-Hold resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MOH resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times Music-on-Hold resources were unavailable	Specify the maximum number of times an MOH resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times Music-on-Hold resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times an MOH resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times Music-on-Hold resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MOH resources were unavailable during the monitoring period. The default is unselected.
Monitor Unavailable Transcoder Resources	
Event Notification	
Raise event if number of times transcoder resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times transcoder resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times transcoder resources were unavailable	Specify the maximum number of times a transcoder resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times transcoder resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a transcoder resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times transcoder resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times transcoder resources were unavailable during the monitoring period. The default is unselected.

4.12 CCM_SystemPerformance

Use this Knowledge Script to monitor call throttling and signal processing queues for a Communications Manager. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Low, normal, and high priority signals that are processed and in queue
- Calls rejected due to throttling
- Throttled SCCP (Skinny Client Control Protocol) devices

- Number of times the Communications Manager went into a throttling state
- Average amount of expected delay

Throttling refers to an internal process within Communications Manager that prevents it from being inundated with heavy call traffic.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.12.1 Resource Object

CiscoCM_CallProcessor

4.12.2 Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.12.3 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 the failure of the CCM_SystemPerformance job. The default is 5.
Event Notification	
Raise event if call throttling warning (Code Yellow) state entered?	Select **Yes** to raise an event if Communications Manager enters a Code Yellow call throttling warning state. The default is Yes.
Event severity when call throttling warning (Code Yellow) state entered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Communications Manager enters a Code Yellow call throttling state. The default is 10.
Raise event if severe (Code Red) call throttling state entered?	Select **Yes** to raise an event if Communications Manager enters a severe (Code Red) call throttling state. The default is Yes.
Event severity when severe (Code Red) call-throttling state entered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Communications Manager enters a severe (Code Red) call-throttling state. The default is 5.
Monitor High Priority Signals in Queue	
Event Notification	

Parameter	How to Set It
Raise event if high priority signals in queue exceed threshold?	Select **Yes** to raise an event if the number of high-priority signals in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum high priority signals in queue	Specify the maximum number of high-priority signals that must be in queue before an event is raised. The default is 500 signals.
Event severity when high priority signals in queue exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of high-priority signals in queue exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for high priority signals in queue?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of high-priority signals in queue at each script iteration. The default is unselected.
Monitor High Priority Signals Processed	
Data Collection	
Collect data for high priority signals processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of high-priority signals that were recently processed at each script iteration. The default is unselected.
Monitor Normal Priority Signals in Queue	
Event Notification	
Raise event if normal priority signals in queue exceed threshold?	Select **Yes** to raise an event if the number of normal priority signals in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum normal priority signals in queue	Specify the maximum number of normal-priority signals that must be in queue before an event is raised. The default is 1000 signals.
Event severity when normal priority signals in queue exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of normal-priority signals in queue exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for normal priority signals?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of normal-priority signals in queue at each script iteration. The default is unselected.
Monitor Normal Priority Signals Processed	
Data Collection	
Collect data for normal priority signals processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of normal-priority signals that were recently processed at each script iteration. The default is unselected.
Monitor Low Priority Signals in Queue	
Event Notification	
Raise event if low priority signals in queue exceed threshold?	Select **Yes** to raise an event if the number of low-priority signals in queue exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum low priority signals in queue	Specify the maximum number of low-priority signals that must be in queue before an event is raised. The default is 1000 signals.
Event severity when low priority signals in queue exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of low-priority signals in queue exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for low priority signals in queue?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of low-priority signals in queue at each script iteration. The default is unselected.
Monitor Low Priority Signals Processed	
Data Collection	
Collect data for low priority signals processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of low-priority signals that were recently processed at each script iteration.The default is unselected.
Monitor Rejected Calls	
Event Notification	
Raise event if rejected calls exceed threshold?	Select **Yes** to raise an event if the number of rejected calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum rejected calls	Specify the maximum number of calls that must be rejected before an event is raised. The default is 10 calls.
Event severity when rejected calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of rejected calls exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for rejected calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls rejected during the monitoring period. The default is unselected.
Monitor Throttled SCCP Devices	
Event Notification	
Raise event if throttled SCCP devices exceed threshold?	Select **Yes** to raise an event if the number of throttled SCCP devices exceeds the threshold you set. The default is Yes.
Threshold - Maximum throttled SCCP devices	Specify the maximum number of SCCP devices that must be throttled before an event is raised. The default is 10 devices.
Event severity when throttled SCCP devices exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of throttled SCCP devices exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for throttled SCCP devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of SCCP devices throttled during the monitoring period. The default is unselected.
Monitor Call-Throttling	

Parameter	How to Set It
Event Notification	
Raise event if number of times in call-throttling mode exceeds threshold?	Select **Yes** to raise an event if the number of times Communications Manager entered a call-throttling state exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times in call-throttling mode	Specify the maximum number of times Communications Manager must enter a call-throttling state before an event is raised. The default is 0 times.
Event severity when number of times in call-throttling mode exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times Communications Manager entered a call-throttling state exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times in call-throttling mode?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times Communications Manager entered a call-throttling state during the monitoring period. The default is unselected.
Monitor Average Expected Delay	
Event Notification	
Raise event if average expected delay exceeds threshold?	Select **Yes** to raise an event if the average amount of time it takes Communications Manager to handle incoming messages exceeds the threshold. The default is Yes.
Threshold - Maximum average expected delay	Specify the maximum amount of average delay Communications Manager can expect before an event is raised. The default is 2 seconds.
Event severity when average expected delay exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average amount of expected delay exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for average expected delay?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average amount of expected delay. The default is unselected.

4.13 CDR_CallFailures

Use this Knowledge Script to monitor call detail records (CDRs) retrieved from the primary Communications Manager for calls that ended with an abnormal termination code.

This script raises an event if the number of failed calls exceeds the threshold you set. In addition, this script generates a data stream for the number of failed calls.

This script provides the following features:

- **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.
- **Troubleshooting**. In troubleshooting 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 troubleshooting mode, select **Run once** on the Schedule tab.

- **Diagnosing**. In diagnostic mode, this script works in conjunction with NetIQ Vivinet Diagnostics to diagnose VoIP quality problems detected monitoring. If the *Maximum number of failed calls* threshold is exceeded, then, by default, this script launches Action_DiagnoseVoIPQuality, a Knowledge Script that in turn launches Vivinet Diagnostics to generate a diagnosis of the problem.

  To turn off diagnostic mode, click the Actions tab, select **Action_DiagnoseVoIPQuality**, and click **Delete**. Turning diagnostic mode off or on does not affect the events raised by this script.

4.13.1 Prerequisites

- Run the SetupSupplementalDB Knowledge Script to create the CiscoCM supplemental database that will house the call detail records.
- Run the CDR_RetrieveCallRecords and CDR_RetrieveConfigData Knowledge Script to populate the database.

For more information, see Section 4.47.1, “Understanding the CiscoCM Supplemental Database,” on page 145.

4.13.2 Resource Object

CiscoCM_CDRMgmt

4.13.3 Default Schedule

By default, this script runs every five minutes.

4.13.4 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 the failure of the CallFailures job. The default is 5.

Parameter	How to Set It
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unchecked to suppress call details. The default is unselected. If you select **Yes**, an event includes the following details: ◆ Originating Device Name ◆ Originating IP Address ◆ Calling Party Number ◆ Originating Media Cap - Payload Capacity ◆ Destination Device Name ◆ Destination IP Address ◆ Original Called Party Number ◆ Final Called Party Number ◆ Originating Cause ◆ Destination Cause
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. Note that we do not mean there are no CDRs with abnormal termination codes, but that there are no CDRs at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.
Query Filters Despite the number of calls AppManager might find that match the filters you select, an event displays only the first 50 calls.	
Ignore unknown cause codes?	Select **Yes** if you want to ignore CDRs with cause codes of `Unknown`. The default is unselected.
Exclude these failure codes	Enter a list of termination codes (separated by commas) that are not to be considered failures. See Termination Codes for a list of available codes. **NOTE:** CiscoCM automatically excludes Codes 0, 16, 31, and 393216. They are normal termination codes. However, these codes might appear in events if the other side of the call has a failure code that has not been excluded.
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the 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 to ignore the filter for maximum call duration.
Calling directory number	Specify the number of the calling directory 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.

Parameter	How to Set It
Called directory number	Specify the number of the called directory 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.
Troubleshooting	
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.
Monitor Failed Calls	
Event Notification	
Raise event if number of failed calls exceeds threshold?	Select **Yes** to raise an event if the number of calls that failed with an abnormal termination code exceeds the threshold. The default is Yes.
Threshold - Maximum number of failed calls	Specify the maximum number of calls that can fail before an event is raised. The default is 0 calls.
Event severity when number of failed calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that failed with an abnormal termination code during the monitoring period. The default is unselected.

4.13.5 Termination Codes

Use this list of termination codes (also known as call release cause codes) to complete the *Exclude these failure codes* parameter.

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).

Termination Code	Description	Explanation
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 transit network that 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 was 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.
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 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 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	Preemption	Indicates a call was preempted.
9	Preemption - circuit reserved for reuse	Indicates a call was 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 might be generated by the called user or by the network. In the case of user-determined user busy, it is noted that 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 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).

Termination Code	Description	Explanation
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, indicating the call was cleared due to a supplementary service constraint.
22	Number changed	Indicates the called party number specified by the calling party is no longer assigned. The new called party number might optionally be included in the diagnostic field. If a network does not support this cause, then cause #1 shall be used.
26	Non-selected user clearing	Indicates the user has not been awarded the incoming call.
27	Destination out of order	Indicates the destination specified 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.

Termination Code	Description	Explanation
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.
41	Temporary failure	Indicates the network is not functioning correctly and the condition is not likely to last a long time. The user might 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. This might 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 Closed User Group (CUG)	Indicates the network does not allow the user to receive calls.
57	Bearer capability not authorized	Indicates the user requested a bearer capability 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.

Termination Code	Description	Explanation
58	Bearer capability not presently available	Indicates the user requested a bearer capability implemented by the equipment that generated this cause. However, bearer capability is unavailable at the present time. This problem might occur because of 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.
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 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 available (national use)	Indicates the calling party requested an unrestricted bearer service. However, the equipment sending this cause supports only 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 received a message with a call reference not currently in use on the user-network interface. This value applies only if the call reference value is 1 or 2 octets long and is not the global call reference.
82	Identified channel does not exist	Indicates the equipment sending this cause received a request to use a channel not active on the interface for a call.
83	A suspended call exists, but this call identity does not	Indicates 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, with the requested call identity, has cleared.
87	User not member of Closed User Group (CUG)	Indicates the call was not completed, probably because of one 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 the remote device is not authorized to use

Termination Code	Description	Explanation
88	Incompatible destination	Indicates the equipment sending this cause received a request to establish a call with low layer compatibility, high layer compatibility, or other compatibility attributes (such as data rate or DN subaddress) that cannot be accommodated. This call might be returned by a switch to a CPE when trying to route a call to an incompatible facility, or one without a data rate.
90	Destination number missing and DC not subscribed	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 the remote device is not authorized to use
91	Invalid transit network selection (national use)	Indicates an invalid transit network selection was requested.
95	Invalid message, unspecified	Indicates the entity sending this cause 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 received a message 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 received 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 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 non-existent or not implemented	Indicates the equipment sending this cause 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 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 was not implemented by the equipment sending this cause.

Termination Code	Description	Explanation
101	The message not compatible with the call state	Indicates one of the following: ◆ The equipment sending this cause received a message procedure indicating it is not a permissible message to receive at this time. ◆ The switch sending this cause is clearing the call because a threshold was exceeded for multiple protocol errors during an active call.
102	Call terminated when timer expired; a recovery routine executed to recover from the error	Indicates a procedure was initiated by the expiration of a timer in association with error-handling procedures.
103	Parameter non-existent or not implemented - passed on (national use)	Indicates the equipment sending this cause 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, then this cause indicates the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates the equipment sending this cause 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 might display if the user failed to dial a 9 or an 8 for an outside line. In addition, this cause might be returned in the event of certain types of restrictions as to number of calls.
122	Precedence level exceeded	Indicates users attempted to make a call with a higher level of precedence than the highest precedence level authorized for their line.
123	Device not preemptable	Indicates one of the following: ◆ The dialed number is non preemptable. That is, the dialed number registers as busy and has no call waiting, no call forwarding, and no alternate party designations. ◆ The dialed number has a higher precedence level (or priority) than the dialing number and cannot be preempted.
125	Out of bandwidth	Indicates not enough bandwidth was found to connect a call to the destination location.
127	Interworking, unspecified	Indicates an interworking call (usually a call to SW56 service) ended. This might also be seen in the event of a non-specific rejection by a long distance carrier.
129	Precedence out of bandwidth	Indicates not enough bandwidth was found to connect a precedence call to the destination location.
162144 0x40000	Conference full	A Cisco-specific code. Indicates a conference is at full capacity and can accept no new callers.

Termination Code	Description	Explanation
393216 0x60000	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 might help determine which calls were terminated as part of a feature operation.
458752 0x70000	Drop any party/drop last party	A Cisco-specific code. Indicates a call dropped from a conference by the new feature "drop any party/drop last party."

Related Topics

- CDR_CallFailures

4.14 CDR_CallQuality

Use this Knowledge Script to monitor call detail records (CDRs) and call management records (CMRs) retrieved from the primary Communications Manager for jitter, latency, packet loss, and MOS (Mean Opinion Score).

This script raises an event if a monitored value exceeds or falls below a threshold. In addition, this script generates data streams for average and minimum MOS, and maximum jitter, latency, and packet loss.

This script provides the following features:

- **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.
- **Troubleshooting**. In troubleshooting 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 troubleshooting mode, select **Run once** on the Schedule tab.
- **Diagnosing**. In diagnostic mode, this script works in conjunction with NetIQ Vivinet Diagnostics to diagnose VoIP quality problems detected during monitoring. If a call quality threshold is exceeded, then, by default, this script launches Action_DiagnoseVoIPQuality, a Knowledge Script that in turn launches Vivinet Diagnostics to generate a diagnosis of the problem.

  To turn off diagnostic mode, click on the Actions tab, select **Action_DiagnoseVoIPQuality**, and click **Delete**. Turning diagnostic mode off or on does not affect the events raised by this script.

4.14.1 Prerequisites

- Run the SetupSupplementalDB Knowledge Script to create the CiscoCM supplemental database that will house the call detail records.
- Run the CDR_RetrieveCallRecords and CDR_RetrieveConfigData Knowledge Script to populate the database.

For more information, see Understanding the CiscoCM Supplemental Database.

4.14.2 Resource Object

CiscoCM_CDRMgmt

4.14.3 Default Schedule

By default, this script runs every five minutes.

4.14.4 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 the failure of the CDR_CallQuality job. The default is 5.
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unchecked to suppress call details. If you select **Yes**, an event includes the following details: ◆ Average and minimum MOS ◆ Jitter ◆ Latency ◆ Lost Packets (%) ◆ Originating and Destination Devices ◆ Calling and Called Numbers ◆ Origination and Disconnect Times ◆ Duration (seconds) ◆ Calling and Called Number Partitions The default is Yes.
Sort call details table by this value	Select the value from the call details data by which you want to sort. Your can choose from all of the options listed in the previous parameter.
Sort type for call details table	Select a sort type for the call details data. Your options are `Ascending` or `Descending`.
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. Note that we do not mean there are no CDRs with call quality data, but that there are no CDRs at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.

Parameter	How to Set It
Query Filters	
◆ Despite the number of calls AppManager might find that match the filters you select, an event displays only the first 50 calls. ◆ Regardless of the filters you select (or if you select no filters at all), an event displays call data in two tables labeled Inbound and Outbound. The Inbound table contains details of calls coming into the Originating Device (according to the CMR table). The Outbound table contains details of calls going out from the Originating Device (according to the CMR table).	
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the filter for minimum duration.
Maximum duration	Set this parameter to filter out records whose call duration is more than or equal to the specified value. Accept the default of 0 to ignore the filter for maximum duration.
Directory number	Set this parameter to query for those calls whose directory number matches the specified value. Wildcard characters are acceptable. If you use multiple expressions, separate each expression with a comma, such as `123*,2345,234*`. Leave this parameter blank to search for any directory number.
Device name	Set this parameter to query for those calls whose device name matches the specified value. Wildcard characters are acceptable. If you use multiple expressions, separate each expression with a comma, such as `123*,2345,234*`. Leave this parameter blank to search for any device name.
Troubleshooting	
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.
Monitor Average Acceptable Listening MOS	
Event Notification	
Raise event if average MOS falls below threshold?	Select **Yes** to raise an event if the average MOS value falls below the threshold. The default is Yes.
Threshold - Average MOS	Specify the lowest average MOS value that must occur to prevent an event from being raised. The default is 3.60.
Event severity when average MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average MOS value falls below the threshold. The default is 5.
Data Collection	
Collect data for average MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average MOS value during the monitoring period. The default is unselected.
Monitor Minimum Acceptable Listening MOS	
Event Notification	

Parameter	How to Set It
Raise event if minimum MOS falls below threshold?	Select **Yes** to raise an event if the minimum MOS value falls below the threshold. The default is unselected.
Threshold - Minimum MOS	Specify the lowest MOS value that must occur to prevent an event from being raised. The default is 3.60.
Event severity when minimum MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the minimum MOS value falls below the threshold. The default is 5.
Data Collection	
Collect data for minimum MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the minimum MOS value during the monitoring period. The default is unselected.
Monitor Jitter	
Event Notification	
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if the jitter value exceeds the threshold. The default is unselected.
Threshold - Maximum jitter	Specify the highest jitter value that can occur before an event is raised. The default is 60 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the jitter value exceeds the threshold. The default is 15.
Data Collection	
Collect data for jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of jitter that occurred during the monitoring period. The default is unselected.
Monitor Latency	
Event Notification	
Raise event if latency exceeds threshold?	Select **Yes** to raise an event if the latency value exceeds the threshold. The default is unselected.
Threshold - Maximum latency	Specify the highest amount of latency that can occur before an event is raised. The default is 400 milliseconds.
Event severity when latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the latency value exceeds the threshold. The default is 15.
Data Collection	
Collect data for latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of latency that occurred during the monitoring period. the default is unselected.
Monitor Packet Loss	
Event Notification	
Raise event if packet loss exceeds threshold?	Select **Yes** to raise an event if the packet loss value exceeds the threshold. The default is unselected.
Threshold - Maximum packet loss	Specify the highest amount of packet loss that can occur before an event is raised. The default is 1%.

Parameter	How to Set It
Event severity when packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the packet loss value exceeds the threshold. The default is 15.
Data Collection	
Collect data for packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of packet loss that occurred during the monitoring period. The default is unselected.

4.15 CDR_Query

Use this Knowledge Script to search for call detail records (CDRs) retrieved from the primary Communications Manager and stored in the local SQL database. The search is based on query filters you select. This script raises an event if no CDRs are found or if the number of CDRs found exceeds the threshold you set. In addition, this script generates a data stream for the number of records found.

This script provides the following features:

- **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.
- **Troubleshooting**. In troubleshooting 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 troubleshooting mode, select **Run once** on the Schedule tab.

4.15.1 Resource Object

CiscoCM_CDRMgmt

4.15.2 Default Schedule

By default, this script runs every five minutes.

4.15.3 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 the failure of the CDR_Query job. The default is 5.
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. Note that we do not mean there are no CDRs with call quality data, but that there are no CDRs at all. The default is unselected.

Parameter	How to Set It
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.
Query Filters	
Despite the number of calls AppManager might find that match the filters you select, an event displays only the first 50 calls.	
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the 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 to ignore the filter for maximum call duration.
Calling directory number	Specify the number of the calling directory 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	Specify the number for the called directory you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any called directory number.
Called directory number type	Select the type of called directory number you want to find in the CDRs. You can filter the CDRs by the originally called directory number, the most recently called directory number, or by either directory number. The default is *either* 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 values for both the *Originating device name* and *Destination device name* parameters. 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.
Troubleshooting	
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.

Parameter	How to Set It
Call time range type	Select the type of call time range you want to use when troubleshooting. The time ranges can match on the following options: ◆ Origination time of calls ◆ Disconnect time of calls ◆ Either origination or disconnect time ◆ Both origination and disconnect time ◆ All calls that span some portion of the time range, including calls that started before the range, and calls that ended after the range. The default is DisconnectTime. **NOTE:** This filter will only work if you schedule the script to *Run Once*.
Monitor Records Found	
Event Notification	
Raise event if number of records exceeds threshold?	Select **Yes** to raise an event if the number of CDRs found exceeds the threshold. The default is Yes.
Threshold - Maximum number of records	Specify the maximum number of CDRs that can be found before an event is raised. The default is 0 CDRs.
Event severity when number of records exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of CDRs found exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of records?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of CDRs found during the monitoring period. The default is unselected.

4.16 CDR_RetrieveCallRecords

The primary Communications Manager sends call detail records (CDRs) to a folder you specified on the proxy agent computer. Use this script to retrieve the CDRs from the folder and insert them into the CiscoCM supplemental database. This script will archive the records, if indicated.

4.16.1 Prerequisite

Run the SetupSupplementalDB Knowledge Script to create the supplemental database. For more information, see Understanding the CiscoCM Supplemental Database.

4.16.2 Resource Object

CiscoCM_CDRMgmt

4.16.3 Default Schedule

By default, this script runs every five minutes.

4.16.4 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 the failure of the CDR_RetrieveCallRecords job. The default is 5.
Archive call detail records after processing?	Select **Yes** to copy CDRs to an archive folder after processing. If you leave this parameter unchecked, CDRs are deleted after processing. The default is unselected.
Archive folder	Specify the full path to a location on the agent computer in which to create the archive folder.

NOTE: Pruning is activated by default based on the **Phone Deregistration Parameters** and **CDR parameters** (Number of days to keep call detail records) specified during execution of CiscoCM_setupsupplementalDB knowledge script.

4.17 CDR_RetrieveConfigData

Use this Knowledge Script to retrieve Communications Manager configuration data from the primary Communications Manager and store it in the CiscoCM supplemental database.

4.17.1 Prerequisite

Run the SetupSupplementalDB Knowledge Script to create the supplemental database that will house the configuration data. For more information, see Section 4.47.1, “Understanding the CiscoCM Supplemental Database,” on page 145.

4.17.2 Resource Object

CiscoCM_CDRMgmt

4.17.3 Default Schedule

By default, this script runs once a day, at 3 A.M, so as to perform its possibly CPU-intensive function at a time when the Communications Manager is least busy.

However, because the PhoneDeregistrations script uses the configuration data this script retrieves, you might want to set this script to `Run Once` so the configuration data is retrieved immediately. When the “Run Once” job is complete, then you can run this script using the default schedule of once daily.

4.17.4 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 the failure of the CDR_RetrieveConfigData job. The default is 5.
Raise event if data collection succeeds?	Select **Yes** to raise an event if the data-collection process succeeds. The default is unselected.
Event severity when data collection succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data collection succeeds. The default is 25.

4.18 CFB_Hardware_Device

Use this Knowledge Script to monitor the resource usage of a registered hardware conference bridge device.

- Active conferences
- Completed conferences
- Resource usage
- Active resources
- Unavailable resources

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active and completed conferences, active resources, and resource usage (%).

4.18.1 Resource Object

CiscoCM_HW_CFBObj

4.18.2 Default Schedule

By default, this script runs every 15 minutes.

4.18.3 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 the failure of the CFB_Hardware_Device job. The default is 5.

Parameter	How to Set It
Monitor Active Conferences	
Event Notification	
Raise event if active conferences exceed threshold?	Select **Yes** to raise an event if the number of active hardware conferences exceeds the threshold you set. The default is Yes.
Threshold - Maximum active conferences	Specify the maximum number of hardware conferences that must be active before an event is raised. The default is 250 conferences.
Event severity when active conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active hardware conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for active conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conferences active during the monitoring period.The default is unselected.
Monitor Completed Conferences	
Data Collection	
Collect data for completed conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conferences completed during the monitoring period. The default is unselected.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of hardware conference usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of hardware conference usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of hardware conference usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of hardware conference usage at each script iteration.The default is unselected.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conferences active at each script iteration. The default is unselected.
Monitor Unavailable Resources	
Event Notification	

Parameter	How to Set It
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times hardware conferences were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times hardware conferences must be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times hardware conferences were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times hardware conferences were unavailable during the monitoring period. The default is unselected.

4.19 CFB_Software_Device

Use this Knowledge Script to monitor the resource usage of a registered software conference bridge device.

- Active conferences
- Completed conferences
- Resource usage
- Active resources
- Unavailable resources

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active and completed conferences, active resources, and resource usage (%).

4.19.1 Resource Object

CiscoCM_SW_CFBObj

4.19.2 Default Schedule

By default, this script runs every 15 minutes.

4.19.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CFB_Software_Device job. The default is 5.
Monitor Active Conferences	
Event Notification	
Raise event if active conferences exceed threshold?	Select **Yes** to raise an event if the number of active software conferences exceeds the threshold you set. The default is Yes.
Threshold - Maximum active conferences	Specify the maximum number of software conferences that must be active before an event is raised. The default is 250 conferences.
Event severity when active conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for active conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conferences active during the monitoring period. The default is unselected.
Monitor Completed Conferences	
Data Collection	
Collect data for completed conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conferences completed during the monitoring period. The default is unselected.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of software conference resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of software conference resource usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of software conference resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of software conference resource usage at each script iteration. The default is unselected.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conference resources active at each script iteration. The default is unselected.
Monitor Unavailable Resources	

Parameter	How to Set It
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times a software conference resource was unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times software conference resources must be unavailable before an event is raised. The default is 0 conferences.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times software conference resources were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times software conference resources were unavailable. The default is unselected.

4.20 CFB_Video_Device

Use this Knowledge Script to monitor the resource usage of a registered video conference bridge device.

- Active conferences
- Completed conferences
- Resource usage
- Active resources
- Unavailable resources

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active and completed conferences, active resources, and resource usage (%).

4.20.1 Resource Object

CiscoCM_VideoCFBObj

4.20.2 Default Schedule

By default, this script runs every 15 minutes.

4.20.3 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 event severity level, from 1 to 40, to indicate the importance of the failure of the CFB_Video_Device job. The default is 5.
Monitor Active Conferences	
Event Notification	
Raise event if active conferences exceed threshold?	Select **Yes** to raise an event if the number of active video conferences exceeds the threshold you set. The default is Yes.
Threshold - Maximum active conferences	Specify the maximum number of video conferences that must be active before an event is raised. The default is 250 conferences.
Event severity when active conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active video conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for active conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conferences active during the monitoring period.The default is unselected.
Monitor Completed Conferences	
Data Collection	
Collect data for completed conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conferences completed during the monitoring period. The default is unselected.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of video conference usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of video conference usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of video conference usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of video conference usage at each script iteration. The default is unselected.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conferences active at each script iteration.The default is unselected.

Parameter	How to Set It
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times video conferences were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times video conferences must be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times video conferences were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times video conferences were unavailable during the monitoring period. The default is unselected.

4.21 CTIManager

Use this Knowledge Script to monitor the usage of the Communications Manager CTI Manager. CTI Manager allows applications to access the resources and functionality of all Communications Managers in the cluster.

This script raises an event if a value exceeds or falls below its threshold. In addition, this script generates data streams for the number of connected applications, open lines, open devices, and active Communications Manager links.

4.21.1 Resource Object

CiscoCM_CTIMgrService

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	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CTIManager job. The default is 5.

Parameter	How to Set It
Monitor Connected Applications	
Event Notification	
Raise event if connected applications exceed threshold?	Select **Yes** to raise an event if the number of connected applications exceeds the threshold you set. The default is Yes.
Threshold - Maximum connected applications	Specify the maximum number of applications that must be connected before an event is raised. The default is 100 applications.
Event severity when connected applications exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of connected applications exceeds the threshold. The default is 15.
Data Collection	
Collect data for connected applications?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of applications connected at each script iteration. The default is unselected.
Monitor Open Lines	
Event Notification	
Raise event if open lines exceed threshold?	Select **Yes** to raise an event if the number of open lines exceeds the threshold you set. The default is Yes.
Threshold - Maximum open lines	Specify the maximum number of lines that must be open before an event is raised. The default is 100 lines.
Event severity when open lines exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of open lines exceeds the threshold. The default is 15.
Data Collection	
Collect data for open lines?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of lines open at each script iteration. The default is unselected.
Monitor Open Devices	
Event Notification	
Raise event if open devices exceed threshold?	Select **Yes** to raise an event if the number of open devices exceeds the threshold you set. The default is Yes.
Threshold - Maximum open devices	Specify the maximum number of devices that must be open before an event is raised. The default is 100 devices.
Event severity when open devices exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of open devices exceeds the threshold. The default is 15.
Data Collection	
Collect data for open devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of devices open at each script iteration. The default is unselected.
Monitor Active CallManager Links	
Event Notification	

Parameter	How to Set It
Raise event if active CallManager links fall below threshold?	Select **Yes** to raise an event if the number of active Communications Manager links falls below the threshold you set. The default is Yes.
Threshold - Minimum active CallManager links	Specify the minimum number of Communications Manager links that must be active before an event is raised. The default is 1 link.
Event severity when active CallManager links fall below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active Communications Manager links falls below the threshold. The default is 15.
Data Collection	
Collect data for active CallManager links?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Communications Manager links active at each script iteration. The default is unselected.

4.22 ExtensionMobility

Use this Knowledge Script to monitor the Extension Mobility application. Extension Mobility allows users to temporarily access their Cisco IP phone configuration, such as line appearances, services, and speed dials, from other Cisco IP phones.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of throttled requests, in-progress requests, login/logout requests, successful logins, successful logouts, and total requests.

4.22.1 Resource Object

CiscoCM_ExtMobility

4.22.2 Default Schedule

By default, this script runs every 15 minutes.

4.22.3 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 the failure of the ExtensionMobility job. The default is 5.
Monitor Login/Logout Requests	
Event Notification	

Parameter	How to Set It
Raise event if login/ logout requests exceed threshold?	Select **Yes** to raise an event if the number of requests to log in or log out exceeds the threshold you set. The default is Yes.
Threshold - Maximum login/ logout requests	Specify the maximum number of login and logout requests that must occur before an event is raised. The default is 100 requests.
Event severity when login/ logout requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of login and logout requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for login/logout requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of login and log out requests that occurred during the monitoring period. The default is unselected.
Monitor Successful Logins	
Data Collection	
Collect data for successful logins?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of logins that were successful during the monitoring period. The default is unselected.
Monitor Successful Logouts	
Data Collection	
Collect data for successful logouts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of logouts that were successful during the monitoring period. The default is unselected.
Monitor Requests in Progress	
Event Notification	
Raise event if requests in progress exceed threshold?	Select **Yes** to raise an event if the number of in-progress requests exceeds the threshold you set. The default is Yes.
Threshold - Maximum requests in progress	Specify the maximum number of requests that must be in progress before an event is raised. The default is 500 requests.
Event severity when requests in progress exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for requests in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests in progress at each script iteration. The default is unselected.
Monitor Throttled Requests	
Event Notification	
Raise event if throttled requests exceed threshold?	Select **Yes** to raise an event if the number of throttled requests exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum throttled requests	Specify the maximum number of requests that must be throttled before an event is raised. The default is 10 requests.
Event severity when throttled requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of throttled requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for throttled requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests throttled during the monitoring period. The default is unselected.
Monitor Total Requests	
Data Collection	
Collect data for total requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of all requests that occurred during the monitoring period. The default is unselected.

4.23 GatekeeperActivity

Use this Knowledge Script to monitor the activity on a gatekeeper. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following monitored activities:

- Received admission confirm messages (ACFs)
- Attempted admission requests
- Retried acknowledgement messages (RASs)
- Failed video stream requests

4.23.1 Resource Object

CiscoCM_GatekeeperObj

4.23.2 Default Schedule

By default, this script runs every 15 minutes.

4.23.3 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 the failure of the GatekeeperActivity job. The default is 5.

Parameter	How to Set It
Monitor Failed Video Stream Requests	
Event Notification	
Raise event if failed video stream requests exceed threshold?	Select **Yes** to raise an event if the number of failed video stream requests exceeds the threshold you set. The default is Yes.
Threshold - Maximum failed video stream requests	Specify the maximum number of video stream requests that must fail before an event is raised. The default is 0 requests.
Event severity when failed video stream requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed video stream requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for failed video stream requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video stream requests that failed during the monitoring period. The default is unselected.
Monitor Retries	
Event Notification	
Raise event if retries exceed threshold?	Select **Yes** to raise an event if the number of RASs exceeds the threshold you set. The default is Yes.
Threshold - Maximum retries	Specify the maximum number of acknowledgement messages that must be retried before an event is raised. The default is 50 messages.
Event severity when retries exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of RASs exceeds the threshold. The default is 15.
Data Collection	
Collect data for retries?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of acknowledgement messages that were retried during the monitoring period. The default is unselected.
Monitor Admission Confirm Messages	
Data Collection	
Collect data for admission confirm messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ACFs received during the monitoring period.
Monitor Admission Request Messages	
Data Collection	
Collect data for admission request messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of admission requests attempted during the monitoring period. The default is unselected.

4.24 GeneralCounter

Use this Knowledge Script to monitor a user-specified Performance Monitor counter on a Communications Manager server. You can monitor both the current value of the counter as well as the delta value (current value minus the previous value). This script raises an event if the value of the monitored counter exceeds the threshold and if the counter you want to monitor is not accessible.

This script generates data streams for current and delta counter values.

4.24.1 Resource Object

CiscoCM_CMServer

4.24.2 Default Schedule

By default, this script runs every five minutes.

4.24.3 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 the failure of the GeneralCounter job. The default is 5.
Counter Specifications	
Name of the object to monitor	Type the name of the performance object you want to monitor. An object is any resource, program or service for which performance data can be collected. The default object name is System.
Name of the counter to monitor	Type the name of the performance counter you want to monitor. A counter represents the data associated with aspects of an object. The default counter name is Total Threads.
Name of the instance to monitor	Type the name of the performance instance you want to monitor. An instance distinguishes between multiple objects of the same type on a single computer. You can type multiple instance names, separated by commas. Not all counters or objects require or have an instance.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if this script cannot find the counter or instance you specify. The default is Yes.
Event severity when counter/instance not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script cannot find the counter or instance you specify. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold	Select **Yes** to raise an event if the current value of the counter exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum current value	Specify the maximum current value the counter can attain before an event is raised. The default is 500.
Event severity when current value exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the current value of the counter exceeds the threshold you set. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the current value of the counter at each script iteration.The default is unselected.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold	Select **Yes** to raise an event if the delta value of the counter exceeds the threshold you set. The default is Yes. The delta value is the difference between the current value and the previous value.
Threshold - Maximum delta value	Specify the maximum delta value the counter can attain before an event is raised. The default is 100.
Event severity when delta value exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the delta value of the counter exceeds the threshold you set. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the delta value of the counter as measured during the monitoring period. The default is unselected.

4.25 H323_Gateway_CallActivity

Use this Knowledge Script to monitor completed, attempted, in-progress, and active calls on an H.323 gateway device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for completed calls, attempted calls, in-progress calls, and active calls.

4.25.1 Resource Object

CiscoCM_H323GatewayObj

4.25.2 Default Schedule

By default, this script runs every 15 minutes.

4.25.3 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 the failure of the H323_Gateway_CallActivity job. The default is 5.
Monitor Attempted Calls	
Event Notification	
Raise event if attempted calls exceed threshold	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the highest number of calls that must be attempted before an event is raised. The default is 500.
Event severity when attempted calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls attempted during the monitoring period. The default is unselected.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. The default is unselected.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active at each script iteration. The default is unselected.
Monitor Calls In Progress	
Event Notification	
Raise event if calls in progress exceed threshold	Select **Yes** to raise an event if the number of calls in progress exceeds the threshold you set. The default is Yes.
Threshold - Maximum calls in progress	Specify the highest number of calls that must be in progress before an event is raised. The default is 1000.
Event severity when calls in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of calls in progress exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration. The default is unselected.

4.26 H323_Trunk_CallActivity

Use this Knowledge Script to monitor attempted calls, completed calls, active calls, and calls in progress for H.323 trunks. This script can raise an event if any threshold is exceeded. In addition, this script generates data streams for attempted calls, completed calls, active calls, and calls in progress per trunk.

4.26.1 Resource Object

Cluster object

4.26.2 Default Schedule

By default, this script runs every 15 minutes.

4.26.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity if job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the H323_Trunk_CallActivity job. The default is 5.
Monitor Attempted Calls	
Event Notification	
Raise event if attempted calls exceed threshold	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the highest number of calls that must be attempted before an event is raised. The default is 500.
Event severity when attempted calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls attempted during the monitoring period. The default is unselected.

Parameter	How to Set It
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. The default is unselected.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active at each script iteration. The default is unselected.
Monitor Calls In Progress	
Event Notification	
Raise event if calls in progress exceed threshold	Select **Yes** to raise an event if the number of calls in progress exceeds the threshold you set. The default is Yes.
Threshold - Maximum calls in progress	Specify the highest number of calls that must be in progress before an event is raised. The default is 1000 calls.
Event severity when calls in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of calls in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration. The default is unselected.

4.27 HealthCheck

Use this Knowledge Script to monitor the operational status of active services on Communications Manager servers. Although the script monitors the following services by default, you can choose to exclude any default service, or include any service not mentioned in the list.

- A Cisco DB
- Cisco AMC Service
- Cisco CallManager
- Cisco CDR Agent
- Cisco CTL Provider
- Cisco Database Layer Monitor
- Cisco DRF Local
- Cisco Extension Mobility
- Cisco RIS Data Collector
- Cisco Tftp

This script raises an event if a stopped service is restarted or fails to restart, or if a service is stopped but the *Start service if it is stopped?* parameter has not been set to **Yes**. In addition, this script generates data streams for service availability.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.27.1 Resource Object

CiscoCM_CMServer

4.27.2 Default Schedule

By default, this script runs every two minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.27.3 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 the failure of the HealthCheck job. The default is 5.
Monitor Services	
Default services to exclude	Type the name of any default service you do not want to automatically start. You can specify the names of multiple services, separated by commas.
Other services to include	Type the name of any service you want to automatically start, but is not included in the list of default services. You can specify the names of multiple services, separated by commas.
Start service if it is stopped?	Select **Yes** to automatically start all stopped default services on Communications Manager servers. Any service you specify in *Default services to exclude* will not be started. The default is Yes. **NOTE:** Only “activated” services can be automatically started. If an administrator has “deactivated” a service, then AppManager cannot start it.
Event Notification	
Raise event if service is stopped and should not be started?	Select **Yes** to raise an event if a monitored service is stopped but *Start service if it is stopped?* is unchecked. The default is Yes.
Event severity when service is stopped and should not be started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is stopped but *Start service if it is stopped?* is unchecked. The default is 15.

Parameter	How to Set It
Raise event if service fails to start?	Select **Yes** to raise an event if AppManager cannot start a monitored service. The default is Yes.
Event severity when service fails to start	Set the event severity level, from 1 to 40, to indicate the importance of an event in AppManager cannot start a monitored service. The default is 5.
Raise event if stopped service has been started?	Select **Yes** to raise an event if AppManager successfully starts a monitored service. The default is Yes.
Event severity when stopped service has been started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully starts a monitored service. The default is 25.
Raise event if service is deactivated?	Select **Yes** to raise an event if a monitored service has been deactivated by an administrator. The default is unselected.
Event severity when service is not active	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service has been deactivated by an administrator. The default is 15.
Data Collection	
Collect data for service availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 0 for a stopped service or 1 for a started service. The default is Yes. **NOTE:** This script generates data streams for services running when the job starts or automatically restarted while the job runs. If a service is deactivated when the job starts, no data stream is generated.

4.28 HuntAndRouteList

Use this Knowledge Script to monitor hunt lists and route lists for availability and call activity. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of abandoned calls, busy attempts, unanswered calls, active calls, in-progress calls, and available members, and for hunt and route list availability.

4.28.1 Resource Object

CiscoCM_HuntListObj

4.28.2 Default Schedule

By default, this script runs every 15 minutes.

4.28.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the HuntAndRouteList job. The default is 5.
Monitor Abandoned Calls	
Event Notification	
Raise event if abandoned calls exceed threshold?	Select **Yes** to raise an event if the number of abandoned calls exceeds the threshold. The default is Yes.
Threshold - Maximum abandoned calls	Specify the maximum number of calls that must be abandoned before an event is raised. The default is 0 calls.
Event severity when abandoned calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for abandoned calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls abandoned during the monitoring period. The default is unselected.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected to prevent an event from being raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period. The default is unselected.
Monitor Unanswered Calls	
Event Notification	
Raise event if unanswered calls exceed threshold?	Select **Yes** to raise an event if the number of unanswered calls exceeds the threshold. The default is Yes.
Threshold - Maximum unanswered calls	Specify the maximum number of calls that must go unanswered before an event is raised. The default is 0 calls.
Event severity when unanswered calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unanswered calls exceeds the threshold you set. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for unanswered calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that went unanswered during the monitoring period. The default is unselected.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active at each script iteration.The default is unselected.
Monitor Calls In Progress	
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration. The default is unselected.
Monitor Hunt or Route List Availability	
Data Collection	
Collect data for hunt or route list availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the availability of a hunt or route list at each script iteration. The default is unselected.
Monitor Members Available	
Data Collection	
Collect data for members available?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hunt and route list members available at each script iteration. The default is unselected.

4.29 LicenseUsage

Use this Knowledge Script to monitor authorized, used, and remaining phone and node licenses on a Cisco Unified Communications Manager cluster. This script raises an event if the number of remaining licenses falls below a threshold, or if the percentage of licenses used exceeds a threshold you set.

In addition, this script generates data streams for authorized licenses, used licenses, and remaining licenses for both phones and Cisco Unified Communications Manager nodes. The script also generates data streams for the percentage of licenses used by phones and nodes.

4.29.1 Resource Object

Cluster object

4.29.2 Default Schedule

By default, this script runs every day.

4.29.3 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 the failure of the LicenseUsage job. The default is 5.
Phone License Units	
Monitor Phone License Units Authorized	
Data Collection	
Collect data for phone license units authorized?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of authorized phone licenses on the License Server. The default is Yes.
Monitor Phone License Units Used	
Data Collection	
Collect data for phone license units used?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of phone licenses currently being used on the License Server. The default is Yes.
Monitor Phone License Units Remaining	
Event Notification	
Raise event if phone license units remaining fall below threshold?	Select Yes to raise an event if the number of remaining phone licenses falls below the threshold you set. The default is unselected.
Threshold -- Minimum phone license units remaining	Specify the minimum number of phone license units that must be remaining and not in use before an event is raised. The default is 0.
Event severity when phone license units remaining fall below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of phone licenses that must be remaining and not in use falls below the threshold. The default is 25.
Data Collection	
Collect data for phone license units remaining?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of remaining phone licenses remaining on the License Server. The default is Yes.
Monitor the Percentage of Phone Licenses Used	
Event Notification	
Raise event if the percentage of phone licenses used exceeds threshold?	Select Yes to raise an event if the percentage of phone licenses in use exceeds the threshold you set. The default is unselected.
Threshold -- Maximum percentage of phone licenses used	Specify the highest percentage of phone licenses that must be in use before an event is raised. The default is 90%.

Parameter	How to Set It
Event severity when the percentage of phone licenses used exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of phone licenses that are in use exceeds the threshold. The default is 25.
Data Collection	
Collect data for the percentage of phone licenses used?	Select Yes to collect data for charts and reports. If enabled, data collection returns the percentage of phone licenses currently being used on the License Server. The default is Yes.
Node License Units	
Monitor Node License Units Authorized	
Data Collection	
Collect data for node license units authorized?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of authorized node licenses on the License Server. The default is Yes.
Monitor Node License Units Used	
Data Collection	
Collect data for node license units used?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of node licenses currently being used on the License Server. The default is Yes.
Monitor Node License Units Remaining	
Event Notification	
Raise event if node license units remaining fall below threshold?	Select Yes to raise an event if the number of remaining node licenses falls below the threshold you set. The default is unselected.
Threshold -- Minimum node license units remaining	Specify the minimum number of node licenses that must be remaining and not in use before an event is raised. The default is 0.
Event severity when node license units remaining fall below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of node licenses that must be remaining and not in use falls below the threshold. The default is 25.
Data Collection	
Collect data for node license units remaining?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of remaining node licenses remaining on the License Server. The default is Yes.
Monitor the Percentage of Node Licenses Used	
Event Notification	
Raise event if the percentage of node licenses used exceeds threshold?	Select Yes to raise an event if the percentage of node licenses in use exceeds the threshold you set. The default is unselected.
Threshold -- Maximum percentage of node licenses used	Specify the highest percentage of node licenses that must be in use before an event is raised. The default is 90%.
Event severity when the percentage of node licenses used exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of node license units exceed the threshold. The default is 25.

Parameter	How to Set It
Data Collection	
Collect data for the percentage of node licenses used?	Select Yes to collect data for charts and reports. If enabled, data collection returns the percentage of node licenses currently being used on the License Server. The default is Yes.
Overdraft License Options	
Include overdraft licenses in authorized counts and calculations?	Select Yes to count the overdraft value of your license into the authorized licenses and when calculating the remaining Units. The default is Yes.

4.30 Locations

Use this Knowledge Script to monitor Cisco locations for voice and video bandwidth availability and usage. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the bandwidth availability, bandwidth usage (%), bandwidth-related call failures, video bandwidth availability, video bandwidth usage (%), and bandwidth-related failures of video stream requests.

4.30.1 Resource Object

CiscoCM_LocationObj

4.30.2 Default Schedule

By default, this script runs every 15 minutes.

4.30.3 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 the failure of the Locations job. The default is 5.
Event Notification	
Raise event if performance recommendation exceeded?	Select Yes to raise an event if the performance recommendation is exceeded. The default is Yes.
Event severity when performance recommendation exceeded	Set the event severity to indicate the importance when the performance recommendation is exceeded. The default is 15.
Monitor Available Bandwidth	

Parameter	How to Set It
Data Collection	
Collect data for available bandwidth?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of bandwidth available at each script iteration. The default is unselected.
Monitor Bandwidth Usage	
Event Notification	
Raise event if bandwidth usage exceeds threshold?	Select **Yes** to raise an event if the percentage of bandwidth usage exceeds the threshold. The default is Yes.
Threshold - Maximum bandwidth usage	Specify the maximum percentage of bandwidth usage that must be detected before an event is raised. The default is 90%.
Event severity when bandwidth usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of bandwidth usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for bandwidth usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of bandwidth usage at each script iteration. The default is unselected.
Monitor Call Failures Caused By Insufficient Bandwidth	
Event Notification	
Raise event if call failures exceed threshold	Select **Yes** to raise an event if the number of calls that failed because of insufficient bandwidth exceeds the threshold. The default is Yes.
Threshold - Maximum failed calls	Specify the maximum number of calls that must fail before an event is raised. The default is 0 calls.
Event severity when failed calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of call that failed because of insufficient bandwidth exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of call failures caused by insufficient bandwidth during the monitoring period. The default is unselected.
Monitor Available Video Bandwidth	
Data Collection	
Collect data for available video bandwidth?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of video bandwidth available at each script iteration. The default is unselected.
Monitor Video Bandwidth Usage	
Event Notification	
Raise event if video bandwidth usage exceeds threshold?	Select **Yes** to raise an event if the percentage of video bandwidth usage exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum video bandwidth usage	Specify the maximum percentage of video bandwidth usage that must occur before an event is raised. The default is 90%.
Event severity when video bandwidth usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of video bandwidth usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for video bandwidth usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of video bandwidth usage at each script iteration. The default is unselected.
Monitor Failed Video Stream Requests Failures Caused by Insufficient Bandwidth	
Event Notification	
Raise event if failed video stream requests exceed threshold?	Select **Yes** to raise an event if the number of video stream requests that fail because of insufficient bandwidth exceeds the threshold. The default is Yes.
Threshold - Maximum failed video stream requests	Specify the maximum number of video stream requests that must fail before an event is raised. The default is 0 requests.
Event severity when failed video stream requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of video stream requests that fail because of insufficient bandwidth exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for failed video stream requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of bandwidth-related failures of video stream requests that occurred during the monitoring period. The default is unselected.

4.31 LocationsList

Use this Knowledge Script to monitor all combinations of Cisco's location bandwidth counters, including inter-location pairs. Raises an event if a threshold is exceeded. Generates data streams for available bandwidth, bandwidth usage (%), bandwidth-related call failures, available video bandwidth, video bandwidth usage (%), and bandwidth-related failures of video stream requests. This Knowledge Script provides the same data streams as the Locations Knowledge Script. with the difference in how the locations to be monitored are specified. The Locations knowledge script drops on location treeview objects and monitors bandwidth within each location. This script drops on the server object and monitors both bandwidth within the location as well as bandwidth usage between location pairs.

When monitoring by regular expression, the LocationsList Knowledge Script collects a list of all known location instance(s) from the server. The job created by this Knowledge Script compares the list of location instance names collected against the parameter, which can be either a csv list of the locations for which data is to be collected or, if the `evaluate instance name(s) as regular expression` is selected, a regular expression which can be applied to filter the location names to collect. If no names match, an error event is raised stating that the regular expression did not find any instances, and providing a list of the instances which were found but not matched.

Pattern matching is done using Perl syntax regular expression as provided by the 1.32.0 Boost library described at Boost.org (http://www.boost.org/doc/libs/1_32_0/libs/regex/doc/syntax.html).

The following table shows examples of Boost regular expressions:

To search for:	Expression	Example
All Instances	`.*`	Matches all location objects and inter-location pairs known to a server.
All things to, from, and within a named location	`(.*->)*(locationName)(->.*)*`	Matches both the location named "locationname" and all inter-location pairs to or from "locationname"

4.31.1 Resource Object

CiscoCM_CMServer

4.31.2 Default Schedule

By default, this script runs every 30 minutes.

4.31.3 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 the failure of the Location List job. The default is 5.
Locations Specifications	
Name of location instance(s) to monitor (leave blank for all locations)	Type the name of the location instance you want to monitor. An instance distinguishes between multiple objects of the same type on a single computer. You can specify comma-separated, multiple instance names. to monitor all locations instance(s), do not specify any location instances. The default is blank, so all location instances, including inter-location pairs are monitored.
Evaluate instance name(s) as regular expression?	Select **Yes** to evaluate the location instance name(s) as to evaluate the location name string as a Boost regular expression rather than a CSV list. The default is unselected, or a CSV list. **NOTE:** If entering CSV list, you must specify any inter-location pairs using the exact pair name because the location names are matched exactly. For example, the list `A,B` only matches the intra-location counters for A *and* B. To get the inter-location metrics, you must specify `A`, `B`, `A->B`, and `B->A`, as well. When inter location pair metrics are desired, regular expressions (such as ".*->.*") are recommended

Parameter	How to Set It
Intervals between re-evaluation of location matches (Enter 0 to never re-evaluate)	Specify the desired number of intervals to determine how often to re-evaluate the regular expression or *all locations* list against the CiscoCM location counters. The default is 96 intervals. The regular expression or location list will be re-evaluated to match against new locations when the specified number of intervals has elapsed. Type `0` to never re-evaluate. **NOTE:** It is recommended *not* to set the interval to 0 as the interval might have a negative impact in medium to large environments.
Raise event if filtered locations have been found?	Select **Yes** to raise an event if the filtered locations were found. The default is not to raise an event.
Event severity when filtered have found	Set the event severity level, from 1 to 40, to specify the number of filtered locations that were found. The default is 25.
Raise event if filtered locations have not been found?	Select **Yes** to raise an event if the filtered locations were not found. The default is 25.
Event severity when filtered have not been found	Set the event severity level, from 1 to 40, to specify the number of filtered locations that were found. The default is 25.
Monitor Available Bandwidth	
Data Collection	
Collect data for available bandwidth?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of bandwidth available at each script iteration. The default is unselected.
Monitor Bandwidth Usage	
Event Notification	
Raise event if bandwidth usage exceeds threshold?	Select **Yes** to raise an event if the percentage of bandwidth usage exceeds the threshold. The default is Yes.
Threshold - Maximum bandwidth usage	Specify the maximum percentage of bandwidth usage that must be detected before an event is raised. The default is 90%.
Event severity when bandwidth usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of bandwidth usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for bandwidth usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of bandwidth usage at each script iteration. the default is unselected.
Monitor Call Failures Caused By Insufficient Bandwidth	
Event Notification	
Raise event if call failures exceed threshold	Select **Yes** to raise an event if the number of calls that failed because of insufficient bandwidth exceeds the threshold. The default is Yes.
Threshold - Maximum failed calls	Specify the maximum number of calls that must fail before an event is raised. The default is 0 failures.
Event severity when failed calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of call that failed because of insufficient bandwidth exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of call failures caused by insufficient bandwidth during the monitoring period. The default is unselected.
Monitor Available Video Bandwidth	
Data Collection	
Collect data for available video bandwidth?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of video bandwidth available at each script iteration. The default is unselected.
Monitor Video Bandwidth Usage	
Event Notification	
Raise event if video bandwidth usage exceeds threshold?	Select **Yes** to raise an event if the percentage of video bandwidth usage exceeds the threshold. The default is Yes.
Threshold - Maximum video bandwidth usage	Specify the maximum percentage of video bandwidth usage that must occur before an event is raised. The default is 90%.
Event severity when video bandwidth usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of video bandwidth usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for video bandwidth usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of video bandwidth usage at each script iteration. The default is unselected.
Monitor Failed Video Stream Requests Caused by Insufficient Bandwidth	
Event Notification	
Raise event if failed video stream requests exceed threshold?	Select **Yes** to raise an event if the number of video stream requests that fail because of insufficient bandwidth exceeds the threshold. The default is Yes.
Threshold - Maximum failed video stream requests	Specify the maximum number of video stream requests that must fail before an event is raised. The default is 0 requests.
Event severity when failed video stream requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of video stream requests that fail because of insufficient bandwidth exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for failed video stream requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of bandwidth-related failures of video stream requests that occurred during the monitoring period. The default is unselected.

4.32 MediaStreamingApp

Use this Knowledge Script to monitor the resources handled by the Media Streaming Application: annunciators, conference bridges, and Music-on-Hold (MOH) resources. This script raises an event if a threshold is exceeded. In addition, this script generates the following data streams:

- Lost Communications Manager connections
- Active and total annunciator streams
- Active and total software conferences
- Active and total software conference streams
- Active MOH audio sources
- Active and total MOH streams
- Active and total Media Termination Point streams

4.32.1 Resource Object

CiscoCM_MediaStreamingApp

4.32.2 Default Schedule

By default, this script runs every 15 minutes.

4.32.3 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 the failure of the MediaStreamingApp job. The default is 5.
Monitor Lost CallManager Connections	
Event Notification	
Raise event if lost CallManager connections exceed threshold	Select **Yes** to raise an event if the number of lost Communications Manager connections exceeds the threshold. The default is Yes.
Threshold - Maximum lost CallManager connections	Specify the maximum number of Communications Manager connections that must be lost before an event is raised. The default is 0 connections.
Event severity when lost CallManager connections exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of lost Communications Manager connections exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for lost CallManager connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Communications Manager connections lost during the monitoring period. The default is unselected.

Parameter	How to Set It
Monitor Active Annunciator Streams	
Event Notification	
Raise event if active annunciator streams exceed threshold?	Select **Yes** to raise an event if the number of active annunciator streams exceeds the threshold you set. The default is Yes.
Threshold - Maximum active annunciator streams	Specify the maximum number of annunciator streams that can be active before an event is raised. The default is 200 streams.
Event severity when active annunciator streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active annunciator streams exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active annunciator streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator streams active at each script iteration. The default is unselected.
Monitor Total Annunciator Streams	
Data Collection	
Collect data for total annunciator streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of annunciator streams during the monitoring period. The default is unselected.
Monitor Active Software Conferences	
Event Notification	
Raise event if active software conferences exceed threshold?	Select **Yes** to raise an event if the number of active software conferences exceeds the threshold. The default is Yes.
Threshold - Maximum active software conferences	Specify the maximum number of software conferences that can be active before an event is raised. The default is 200 conferences.
Event severity when active software conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software conferences exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active software conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conferences active at each script iteration. The default is unselected.
Monitor Total Software Conferences	
Data Collection	
Collect data for total software conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of software conferences during the monitoring period. The default is unselected.
Monitor Active Software Conference Streams	
Event Notification	

Parameter	How to Set It
Raise event if active software conference streams exceed threshold?	Select **Yes** to raise an event if the number of active software conference streams exceeds the threshold you set. The default is Yes.
Threshold - Maximum active software conference streams	Specify the maximum number of software conference streams that can be active before an event is raised. The default is 500 streams.
Event severity when active software conference streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software conference streams exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active software conference streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conference streams active at each script iteration. The default is unselected.
Monitor Total Software Conference Streams	
Data Collection	
Collect data for total software conference streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of software conference streams during the monitoring period. The default is unselected.
Monitor Active Music-On-Hold Audio Sources	
Event Notification	
Raise event if active music-on-hold audio sources exceed threshold?	Select **Yes** to raise an event if the number of active MOH audio sources exceeds the threshold you set. The default is Yes.
Threshold - Maximum active music-on-hold audio sources	Specify the maximum number of MOH audio sources that can be active before an event is raised. The default is 200 sources.
Event severity when active music-on-hold audio sources exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MOH audio sources exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active music-on-hold audio sources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH audio sources active at each script iteration. The default is unselected.
Monitor Active Music-On-Hold Streams	
Event Notification	
Raise event if active music-on-hold streams exceed threshold?	Select **Yes** to raise an event if the number of active MOH streams exceeds the threshold you set. The default is Yes.
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 500 streams.

Parameter	How to Set It
Event severity when active music-on-hold streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MOH streams exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active music-on-hold streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH streams active at each script iteration. The default is unselected.
Monitor Total Music-on-Hold Streams	
Data Collection	
Collect data for total music-on-hold streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of MOH streams during the monitoring period. The default is unselected.
Monitor Active Media Termination Point Streams	
Event Notification	
Raise event if active media termination point streams exceed threshold?	Select **Yes** to raise an event if the number of active MTP streams exceeds the threshold you set. The default is Yes.
Threshold - Maximum active media termination point streams	Specify the maximum number of MTP streams that can be active before an event is raised. The default is 500 streams.
Event severity when active media termination point streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MTP streams exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active media termination point streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MTP streams active at each script iteration. The default is unselected.
Monitor Total Media Termination Point Streams	
Data Collection	
Collect data for total media termination point streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of MTP streams during the monitoring period. The default is unselected.

4.33 MGCP_FXO_CallActivity

Use this Knowledge Script to monitor completed calls, blocked calls, and outbound busy attempts on MGCP FXO (Media Gateway Control Protocol Foreign Exchange Office) devices. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of completed calls and busy attempts, percentage of blocked calls, and port status.

4.33.1 Resource Object

CiscoCM_MGCPFXSObj

4.33.2 Default Schedule

By default, this script runs every 15 minutes.

4.33.3 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 the failure of the MGCP_FXO_CallActivity job. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period. The default is unselected.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. Default is unselected.
Monitor Blocked Calls	
Data Collection	
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. The default is unselected. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.

Parameter	How to Set It
Monitor Ports Out of Service	
Data Collection	
Collect data for ports out of service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports out of service or that had an unknown status during the monitoring period. The default is unselected.

4.34 MGCP_FXS_CallActivity

Use this Knowledge Script to monitor completed calls, blocked calls, and outbound busy attempts on MGCP FXS (Media Gateway Control Protocol Foreign Exchange Station) devices. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of completed calls and busy attempts, and for port status.

4.34.1 Resource Object

CiscoCM_MGCPFXSObj

4.34.2 Default Schedule

By default, this script runs every 15 minutes.

4.34.3 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 the failure of the MGCP_FXS_CallActivity job. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	

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 that occurred during the monitoring period. The default is unselected.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. The default is unselected.
Monitor Blocked Calls	
Data Collection	
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. The default is unselected. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.
Monitor Ports Out of Service	
Data Collection	
Collect data for ports out of service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports out of service or that had an unknown status during the monitoring period. The default is unselected.

4.35 MGCP_GatewayUsage

Use this Knowledge Script to monitor active and in-service ports, active channels, and in-service spans for the following components of MGCP (Media Gateway Control Protocol) gateways:

- BRI (basic rate interface) spans
- FXO (foreign exchange office) ports
- FXS (foreign exchange station) ports
- PRI (primary rate interface) spans
- T1CAS (channel associated signaling) spans

An active port or channel is actively handling a call. An in-service port or span is registered to a Communications Manager and available for handling a call.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active ports and active channels.

4.35.1 Resource Object

CiscoCM_MGCPGatewayObj

4.35.2 Default Schedule

By default, this script runs every 15 minutes.

4.35.3 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 the failure of the MGCP_GatewayUsage job. The default is 5.
Event Notification	
Raise event if number of BRI spans in service decreases?	Select **Yes** to raise an event if the number of in-service BRI spans has decreased since the last monitoring interval. The default is unselected.
Event severity when number of BRI spans in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service BRI spans has decreased since the last monitoring interval. The default is 15.
Raise event if number of FXO ports in service decreases?	Select **Yes** to raise an event if the number of in-service FXO ports has decreased since the last monitoring interval. The default is unselected.
Event severity when number of FXO ports in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service FXO ports has decreased since the last monitoring interval. The default is 15.
Raise event if number of FXS ports in service decreases?	Select **Yes** to raise an event if the number of in-service FXS ports has decreased since the last monitoring interval. The default is unselected.
Event severity when number of FXS ports in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service FXS ports has decreased since the last monitoring interval. The default is 15.
Raise event if number of PRI spans in service decreases?	Select **Yes** to raise an event if the number of in-service PRI spans has decreased since the last monitoring interval. The default is unselected.
Event severity when number of PRI spans in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service PRI spans has decreased since the last monitoring interval. The default is 15.
Raise event if number of T1CAS spans in service decreases?	Select **Yes** to raise an event if the number of in-service T1CAS spans has decreased since the last monitoring interval. The default is unselected.
Event severity when number of T1CAS spans in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service T1CAS spans has decreased since the last monitoring interval. The default is 15.
Monitor Active BRI Channels	
Event Notification	

Parameter	How to Set It
Raise event if active BRI channels exceed threshold?	Select **Yes** to raise an event if the number of active BRI channels exceeds the threshold. The default is Yes.
Threshold - Maximum active BRI channels	Specify the maximum number of BRI channels that must be active before an event is raised. The default is 25 channels.
Event severity when active BRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active BRI channels exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active BRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of BRI channels active at each script iteration.The default is unselected.
Monitor Active FXO Ports	
Event Notification	
Raise event if active FXO ports exceed threshold?	Select **Yes** to raise an event if the number of active FXO ports exceeds the threshold. The default is Yes.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that must be active before an event is raised. The default is 100 ports.
Event severity when active FXO ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXO ports exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active FXO ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXO ports active at each script iteration. The default is unselected.
Monitor Active FXS Ports	
Event Notification	
Raise event if active FXS ports exceed threshold?	Select **Yes** to raise an event if the number of active FXS ports exceeds the threshold. The default is Yes.
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that must be active before an event is raised. The default is 100 ports.
Event severity when active FXS ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXS ports exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active FXS ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXS ports active at each script iteration. The default is unselected.
Monitor Active PRI Channels	
Event Notification	

Parameter	How to Set It
Raise event if active PRI channels exceed threshold?	Select **Yes** to raise an event if the number of active PRI channels exceeds the threshold. The default is Yes.
Threshold - Maximum PRI channels	Specify the maximum number of PRI channels that must be active before an event is raised. The default is 100 channels.
Event severity when active PRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active PRI channels exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active PRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of PRI channels active at each script iteration. The default is unselected.
Monitor Active T1CAS Channels	
Event Notification	
Raise event if active T1CAS channels exceed threshold?	Select **Yes** to raise an event if the number of active T1CAS channels exceeds the threshold. The default is Yes.
Threshold - Maximum T1CAS channels	Specify the maximum number of T1CAS channels that must be active before an event is raised. The default is 100 channels.
Event severity when active T1CAS channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active T1CAS channels exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active T1CAS channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of T1CAS channels active at each script iteration. The default is unselected.

4.36 MGCP_PRI_CallActivity

Use this Knowledge Script to monitor active calls, completed calls, blocked calls, outbound busy attempts, and data link availability on an MGCP PRI (Media Gateway Control Protocol Primary Rate Interface) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Active calls
- Completed calls
- Busy attempts
- Blocked calls

4.36.1 Resource Object

CiscoCM_MGCPPRIObj

4.36.2 Default Schedule

By default, this script runs every 15 minutes.

4.36.3 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 the failure of the MGCP_PRI_CallActivity job. The default is 5.
Event Notification	
Raise event if Data Link out of service?	Select **Yes** to raise an event if any data link is unavailable. The default is Yes.
Event severity when Data Link out of service	Set the event severity level, from 1 to 40, to indicate the importance of an event in which any data link is unavailable. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period. The default is unselected.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active during the monitoring period. The default is unselected.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. The default is unselected.

Parameter	How to Set It
Monitor Blocked Calls	
Data Collection	
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. The default is unselected. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.

4.37 MGCP_PRI_ChannelHealth

Use this Knowledge Script to monitor the status of channels for an MGCP PRI (Media Gateway Control Protocol Primary Rate Interface) device. This script raises an event if a channel is not available.

4.37.1 Resource Object

CiscoCM_MGCPPRIObj

4.37.2 Default Schedule

By default, this script runs every two minutes.

4.37.3 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 the failure of the MGCP_PRI_ChannelHealth job. The default is 5.
Monitor PRI Channels	
Select PRI channels to monitor	Select one or more PRI channels to monitor. To monitor all channels, select **All**. To select individual channels in the list, press `[Ctrl]` while clicking on the channels you want. To select an entire range of channels, press `[Shift]` while clicking on the first and last channel in the range. The default is All.
Treat unknown channel status as out-of-service	Select **Yes** to classify as out-of-service any selected channel whose status is unknown. The default is unselected. An out-of-service channel will trigger this script to raise an event.
Event Notification	
Raise event if channel is not available?	Select **Yes** to raise an event if the selected PRI channels are not available. The default is Yes.

Parameter	How to Set It
Event severity when channel is not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which at least one of the selected PRI channels is not available. The default is 5.

4.38 MGCP_T1CAS_CallActivity

Use this Knowledge Script to monitor active calls, completed calls, blocked calls, and outbound busy attempts on an MGCP T1CAS (Media Gateway Control Protocol Channel Associated Signaling) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Active calls
- Completed calls
- Blocked calls
- Busy attempts

4.38.1 Resource Object

CiscoCM_MGCPT1CASObj

4.38.2 Default Schedule

By default, this script runs every 15 minutes.

4.38.3 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 the failure of the MGCP_T1CAS_CallActivity job. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period. The default is unselected.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active during the monitoring period. The default is unselected.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. The default is unselected.
Monitor Blocked Calls	
Data Collection	
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. The default is unselected. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.

4.39 MGCP_T1CAS_ChannelHealth

Use this Knowledge Script to monitor the status of channels for an MGCP T1CAS (Media Gateway Control Protocol Channel Associated Signaling) device. This script raises an event if a channel is not available.

4.39.1 Resource Object

CiscoCM_MGCPT1CASObj

4.39.2 Default Schedule

By default, this script runs every two minutes.

4.39.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_T1CAS_ChannelHealth job. The default is 5.
Monitor T1CAS Channels	
Select T1CAS channels to monitor	Select one or more T1CAS channels to monitor. To monitor all channels, select **All**. To monitor selected channels, press `[Ctrl]` while clicking on the channels you want.
Treat unknown channel status as out-of-service?	Select **Yes** to classify as out-of-service any selected channel whose status is unknown. The default is unselected. An out-of-service channel will trigger this script to raise an event.
Event Notification	
Raise event if channel is not available?	Select **Yes** to raise an event if the selected T1CAS channels are not available. The default is Yes.
Event severity when channel is not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected T1CAS channels are not available. The default is 5.

4.40 MOH_Device

Use this Knowledge Script to monitor the resource usage for a registered Music-on-Hold (MOH) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for multicast resource usage (%), active multicast resources, unicast resource usage (%), active unicast resources, and resource availability.

4.40.1 Resource Object

CiscoCM_MOH_DeviceObj

4.40.2 Default Schedule

By default, this script runs every 15 minutes.

4.40.3 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 the failure of the MOH_Device job. The default is 5.
Monitor Multicast Resource Usage	
Event Notification	

Parameter	How to Set It
Raise event if multicast resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of multicast resource usage exceeds the threshold. The default is Yes.
Threshold - Maximum multicast resource usage	Specify the maximum percentage of multicast resource usage that must be detected before an event is raised. The default is 80%.
Event severity when multicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of multicast resource usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for multicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of multicast resource at each script iteration. The default is unselected.
Monitor Active Multicast Resources	
Data Collection	
Collect data for active multicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of multicast resources active at each script iteration. The default is unselected.
Monitor Unicast Resource Usage	
Event Notification	
Raise event if unicast resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of unicast resource usage exceeds the threshold. The default is Yes.
Threshold - Maximum unicast resource usage	Specify the maximum percentage of unicast resource usage that must be detected before an event is raised. The default is 80%.
Event severity when unicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of unicast resource usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for unicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of unicast resource usage at each script iteration. The default is unselected.
Monitor Active Unicast Resources	
Data Collection	
Collect data for active unicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of unicast resources active at each script iteration. The default is unselected.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MOH resources were unavailable exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times MOH resources can be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unavailability instances exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MOH resources were unavailable during the monitoring period. The default is unselected.

4.41 MTP_Device

Use this Knowledge Script to monitor the resource usage for a registered Media Termination Point (MTP) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for resource usage (%), active resources, and resource availability.

4.41.1 Resource Object

CiscoCM_MTP_DeviceObj

4.41.2 Default Schedule

By default, this script runs every 15 minutes.

4.41.3 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 the failure of the MTP_Device job. The default is 5.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of MTP resource usage exceeds the threshold. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of MTP resource usage that must be detected before an event is raised. The default is 80%.

Parameter	How to Set It
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of MTP resource usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MTP resource usage at each script iteration. The default is unselected.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MTP resources active at each script iteration. The default is unselected.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MTP resources were unavailable exceeds the threshold. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times MTP resources can be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times MTP resources were unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MTP resources were unavailable during the monitoring period. The default is unselected.

4.42 PhoneDeregistrations

Use this Knowledge Script to monitor phone deregistrations on a Unified Communications Manager and to maintain a history of phone deregistrations in the CiscoCM supplemental database. This script raises an event if the number or percentage of lost phones exceeds the threshold you set. You determine how long a phone must be deregistered before it is considered “lost.” In addition, you determine whether to group the events by cluster, device pool, location, or partition.

Unified Communications Manager reports a phone as deregistered even after that phone has been deleted from Communications Manager configuration, unplugged, and moved to a different cluster. As long as Unified Communications Manager indicates the phone is deregistered, AppManager continues to raise an event that identifies the deregistered phone. When Unified Communications Manager stops reporting the phone as deregistered, three days after the phone has been deleted, AppManager stops raising a “deregistered” event.

4.42.1 Prerequisites

- Run the SetupSupplementalDB Knowledge Script to create the CiscoCM supplemental database that will house the deregistration data.
- Run the CDR_RetrieveCallRecords and CDR_RetrieveConfigData Knowledge Scripts to populate the database.

For more information, see Section 4.47.1, “Understanding the CiscoCM Supplemental Database,” on page 145.

4.42.2 Resource Object

CiscoCM_CDRMgmt

4.42.3 Default Schedule

By default, this script runs every five minutes.

4.42.4 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 the failure of the PhoneDeregistrations job. The default is 5.
Event Notification	
Raise event if lost phones in group exceed threshold?	Select **Yes** to raise an event if the number or percentage of lost phones in a group exceeds the threshold you set. The default is Yes. Use *Select event grouping* to select how to group the lost phones. Use *Maximum time phone deregistered before counted as lost* to determine how long a phone must be deregistered before it is considered lost.
Select event grouping	Select whether to group lost phones by **Cluster**, **Device Pool**, **Location**, or **Partition**. AppManager raises an event based on whether the number of lost phones in *each* group exceeds the threshold you set. For example, you set *Maximum number of lost phones in the group* to 5, you set *Select event grouping* to Device Pool, and you have three device pools. If AppManager detects six lost phones in the first pool, two in the second, and seven in the third, it will raise two events: one for the six lost phones in the first pool and another for the seven lost phones in the third pool. Because you set the threshold to “5,” no event is raised for the lost phones in the second pool. The default is Cluster.
Maximum time phone deregistered before counted as lost	Specify the number of minutes that must elapse before a deregistered phone can be considered a “lost” phone. The default is 0 minutes. Accept the default if you want *all* deregistered phones to be considered lost.

Parameter	How to Set It
Type of threshold	Select whether you want to raise events based on the **Number** or **Percent** of lost phones. The default is Number.
Threshold - Maximum number of lost phones	Use this parameter if you selected **Number** in *Type of threshold*. Specify the maximum number of phones that can be lost before an event is raised. The default is 0.
Threshold - Maximum percent of lost phones	Use this parameter if you selected **Percent** in *Type of threshold*. Specify the maximum percentage of phones that can be lost before an event is raised. The default is 0.
Event severity when lost phones exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number or percentage of lost phones in a group exceeds the threshold you set. The default is 15.
Include lost phone details in event message	Select **Yes** to include details of the lost phones in the event message. Phone details can include device name, device IP address, directory number, description, name of device pool, time of deregistration, and the Communications Manager from which the phone was deregistered. The default is Yes.
Maximum number of detail rows to include in event detail	Specify the maximum number of detail rows to include in an event message. Each row contains details for one phone. Rows are sorted in order by most recently lost phone. Specify “0” to include all rows. The default is 20. This parameter is applicable only if you selected **Yes** for *Include lost phone details in event message*.

4.43 PhoneInventory

Use this Knowledge Script to create an inventory of the phones configured in a Communications Manager cluster. You choose both the search criteria for the inventory and the location of the output folder (for the results file containing the inventory list). Unless you specify a UNC path (`\\servername\sharename\directoryname\filename`), the results file is written to the computer on which the NetIQ AppManager agent is running. If you specify a UNC path, ensure the `NetIQmc` service is running as an account that has the proper permissions on the UNC path.

4.43.1 Monitoring Phone Registration After Failover

You can determine the status, registered or deregistered, of Communications Manager phones for Unified Communications Manager clusters on which failover has occurred. Failover occurs when Communications Manager status changes from Primary to Backup.

Communications Managers that fail over contain only a list of phones that registered since failover occurred. They do not provide a list of phones that deregistered as a result of failover. To determine which phones have deregistered, use the PhoneInventory Knowledge Script.

To determine whether failover has occurred, use the RoleStatus or CCM_RegisteredResources script.

4.43.2 Resource Object

CiscoCM_Devices

4.43.3 Default Schedule

By default, this script runs once.

4.43.4 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 the failure of the PhoneInventory job. The default is 5.
Raise event if phone inventory succeeds?	Select **Yes** to raise an event when a phone inventory file is successfully generated. The default is Yes.
Event severity when phone inventory succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the inventory file is successfully generated. The default is 25.
Raise event if no records found?	Select **Yes** to raise an event when the PhoneInventory job finds no phones based on the criteria you selected. The default is Yes.
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 PhoneInventory job found no phones based on the criteria you selected. The default is 25.
Search Options	

Parameter	How to Set It
Select by	Choose the type of selection criteria you want to use to create the list of phones. ◆ Name (the default) ◆ DirectoryNumber. If you select this option, you must also enable the *Include directory number and partition columns in report?* parameter. ◆ Description ◆ DevicePool ◆ CallingSearchSpace ◆ Location ◆ Partition. If you select this option, you must also enable the *Include directory number and partition columns in report?* parameter. ◆ Subnet. If you select this option, you must enter the subnet address in the *Selection criteria* parameter. Use the following format: `172.16.10.0/20` ◆ SubnetFilepath. If you select this option, then, 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. The file must be located on the agent computer.
Selection criteria	Type 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, then the items you enter must be device names or patterns. If *Select by* is DirectoryNumber, then the items you enter must be directory numbers or patterns. The default is blank.

Parameter	How to Set It
List only phones with status of	To further filter the list of phones, select a status. Only phones of this status type, matching the criteria you specified in *Selection criteria* and *Select by*, will be included in the inventory list. Select from the following status types: ◆ Any (the default) ◆ Not Registered ◆ Registered ◆ Unregistered ◆ Rejected **NOTE:** Setting this parameter to a value of **Not Registered** will also list those phones with a status of **Unregistered**.
Result File Options	
Full path to output folder for result file	Type the full path or a UNC path to a location on the agent computer in which to save the inventory `.csv` file. The default path is blank.
Order by	Select **Name** to display the contents of the results file in order by phone name. The default is Name. Select **DirectoryNumber** to display the contents of the results file in order by directory numbers. If you select DirectoryNumber, also enable the *Include directory number and partition columns in report?* parameter.
Include directory number and partition columns in report?	Because a phone can be associated with multiple directory numbers and partitions, your inventory report can present the same phone several times, once for each directory number or partition. Select **Yes** to include the directory number and partition columns in the inventory, allowing multiple entries per phone. Deselect Yes to remove the directory number and partition columns from the inventory, allowing only one entry per phone. **NOTE:** You must select **Yes** if you selected any of the following parameter options: ◆ The *Select by* parameter is set to **DirectoryNumber** or **Partition**. ◆ The *Order by* parameter is set to **DirectoryNumber**.

4.44 Report_PhoneDeregAudit

Use this Knowledge Script to create a history of phone deregistrations and reregistrations. This script uses the data stored in the CiscoCM supplemental database and collected by the PhoneDeregistrations script.

The completed Phone Deregistrations Audit report contains a column titled “Entry Type.” In this column, you might occasionally see an entry of “Reregister - Missed.” This entry indicates a phone that has, apparently, deregistered and then reregistered within a single iteration of this script.

AppManager can tell something happened because the timestamp on the reregistration is different from the last time the phone was polled. However, because the phone is registered, AppManager is unable to determine exactly what transpired.

4.44.1 Prerequisite

For the AppManager for Cisco Unified Communications Manager module, the Report agent pulls data from the CiscoCM supplemental database rather than from the AppManager repository. The `netiqmc` service on the Report agent computer must be running as an account that has permission to access the supplemental database you created using the SetupSupplementalDB Knowledge Script. The Report agent and supplemental database must be located on the same computer for the PhoneDeregAudit report to work.

4.44.2 Resource Object

Report agent

4.44.3 Default Schedule

By default, this script runs once.

4.44.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select cluster	Select the Communications Manager cluster for which you want to create a deregistered phone audit report.
CiscoCM SQL instance	Specify the SQL instance that contains the CiscoCM supplemental database from which the report should pull data. Use the same SQL instance you specified in the PhoneDeregistrations script parameters. Leave this parameter blank to accept the default instance.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Search Criteria	
Note for entering search criteria: If you enter only the wildcard (*) for a field (such as Partition name), then AppManager matches *only* those deregistered phones that have a value for that field. Phones for which that field has no value (i.e., is NULL) will not be matched. For example, if you enter * in the “Partition name” parameter, then the search matches only those phones that have been configured for some partition name. To match all deregistered phones (including phones that have no value for the selected field), leave the search criteria parameter blank.	
Directory number	Type the directory number for which you want to identify phone deregistrations.
Device name	Type the name of the device for which you want to identify phone deregistrations.

Parameter	How to Set It
Device IP address	Type the IP address of the device for which you want to identify phone deregistrations. You can use one of the following formats: ◆ Single dotted-decimal IP address, such as 10.41.2.31 ◆ Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. ◆ Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Device pool	Type the name of the device pool for which you want to identify phone deregistrations.
Location	Type the name of the device location for which you want to identify phone deregistrations. **NOTE:** The device location is the location configured on the Communications Manager.
Partition name	Type the name of the partition for which you want to identify phone deregistrations.
Report Settings	
Order rows by?	Select the column by which you want to sort the rows in the report. The default is DeregTimeDescending.
Show outage time in minutes or seconds?	Select whether the Outage Time column of the report displays the deregistration period in **Minutes** or **Seconds**. The default is Minutes. The outage time is calculated as the difference between the time of deregistration and the time of reregistration.
Include parameter help card?	Select y to include a table in the report that lists parameter settings for this script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is PhoneDeregistrationAudit.
Add job ID to output folder name?	Select y to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Phone Deregistration Audit.
Add time stamp to title?	Select 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. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select 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 successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which 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 an event in which the report fails. The default is 5.

4.45 Report_PhoneDeregWatchList

Use this Knowledge Script to create a list of phones that deregister frequently. This script uses the data stored in the CiscoCM supplemental database and collected by the PhoneDeregistrations script.

4.45.1 Prerequisite

For the AppManager for Cisco Unified Communications Manager module, the Report agent pulls data from the CiscoCM supplemental database rather than from the AppManager repository. The `netiqmc` service on the Report agent computer must be running as an account that has permission to access the supplemental database you created using the SetupSupplementalDB Knowledge Script. The Report agent and supplemental database must be located on the same computer for the PhoneDeregWatchList report to work.

4.45.2 Resource Object

Report agent

4.45.3 Default Schedule

By default, this script runs once.

4.45.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select cluster	Select the Communications Manager cluster for which you want to create a deregistered phone report.
CiscoCM SQL instance	Specify the SQL instance that contains the CiscoCM supplemental database from which the report should pull data. Use the same SQL instance you specified in the PhoneDeregistrations script parameters.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Search Criteria	

Parameter	How to Set It
Note for entering search criteria: If you enter only the wildcard (*) for a field (such as Partition name), then AppManager matches *only* those deregistered phones that have a value for that field. Phones for which that field has no value (i.e., is NULL) will not be matched. For example, if you enter * in the “Partition name” parameter, then the search matches only those phones that have been configured for some partition name. To match all deregistered phones (including phones that have no value for the selected field), leave the search criteria parameter blank.	
Minimum number of deregistrations	Specify the minimum number of deregistrations that must have occurred on a phone before that phone is included in the deregistration report. For example, if you specify “5” as the minimum, then any phone that has four or fewer deregistrations is not included in the report.
Directory number	Type the directory number for which you want to watch phone deregistrations.
Device name	Type the name of the device for which you want to watch phone deregistrations.
Device IP address	Type the IP address of the device for which you want to watch phone deregistrations. You can use one of the following formats: ◆ Single dotted-decimal IP address, such as 10.41.2.31 ◆ Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. ◆ Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Device pool	Type the name of the device pool for which you want to watch phone deregistrations.
Location	Type the name of the device location for which you want to watch phone deregistrations. **NOTE:** The device location is the location that is configured on the Communications Manager.
Partition name	Type the name of the partition for which you want to watch phone deregistrations.
Report Settings	
Order rows by?	Select the column by which you want to sort the rows in the report. The default is Deregistrations.
Include parameter help card?	Select y to include a table in the report that lists parameter settings for this script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is PhoneDeregistrationWatchList.
Add job ID to output folder name?	Select y to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Phone Deregistration Watch List.

Parameter	How to Set It
Add time stamp to title?	Select 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. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select 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 successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which 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 an event in which the report fails. The default is 5.

4.46 RoleStatus

Use this Knowledge Script to monitor a Communications Manager group for changes in the status of its primary and backup Communications Managers. This script raises an event if the initial status of the primary Communications Manager is “not active.” In addition, this script raises an event if the status of the primary or backup Communications Manager changes.

For more information, see PhoneInventory and Monitoring Cluster Up/Down Status.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.46.1 Resource Object

CiscoCM_CMGroupObj

4.46.2 Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.46.3 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 event severity level, from 1 to 40, to indicate the importance of the failure of the RoleStatus job. The default is 5.
Event Notification	
Raise event if primary CallManager is not active?	Select **Yes** to raise an event if the primary Communications Manager is not active when you start the RoleStatus job. The default is unselected.
Event severity when primary CallManager is not active	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the primary Communications Manager is not active when you start the RoleStatus job. The default is 5.
Raise event if primary CallManager status changes?	Select **Yes** to raise an event if the status of the primary Communications Manager changes while the RoleStatus job is running. The default is Yes.
Event severity when primary CallManager status changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of the primary Communications Manager changes while the RoleStatus job is running. The default is 5.
Raise event if backup CallManager status changes?	Select **Yes** to raise an event if the status of the backup Communications Manager changes while the RoleStatus job is running. The default is Yes.
Event severity when backup CallManager status changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of the backup Communications Manager changes while the RoleStatus job is running. The default is 5.

4.47 SetupSupplementalDB

Use this Knowledge Script to verify that Communications Manager is properly configured for the collection of Call Detail Records (CDRs). This script creates a CiscoCM supplemental database, plus the tables and stored procedures needed to store CDRs. In addition, this script creates a SQL job that removes old records from the supplemental database.

4.47.1 Understanding the CiscoCM Supplemental Database

The CiscoCM supplemental database is a SQL Server database you create on the proxy agent computer. The supplemental database fulfills three functions:

- **Storage for CDRs.** The Unified Communications Manager server pushes CDRs, which are flat files, to a folder on the proxy agent computer. From there, the CDRs are saved to tables in the CiscoCM supplemental database, from which the CDR_CallFailures, CDR_CallQuality, and CDR_Query Knowledge Scripts can easily monitor and retrieve data.

  When you create the supplemental database, you specify how long data is retained before being deleted and archived. AppManager automatically archives any flat files older than the retention age you specify. That way, no time or CPU is wasted by transferring to the supplemental database any files that will be immediately slated for deletion.
- **Data source for Call Data Analysis module.** By creating a supplemental database in which to store CDRs, you establish a means of using the AppManager for Call Data Analysis module for analyzing call activity for Unified Communications Manager. The Call Data Analysis module was

designed to analyze CDRs that are pushed to a supplemental database. The CDR_RetrieveConfigData script retrieves the Unified Communications Manager configuration information Call Data Analysis requires and stores it in the supplemental database.

When using AppManager for Call Data Analysis, simply identify the CiscoCM supplemental database as a Data Source when you run the CallDataAnalysis_AddDataSource_CiscoCM Knowledge Script.

- **Storage for phone deregistration data.** The PhoneDeregistrations Knowledge Script uses AXL queries to create a list of unregistered phones and to identify when they reregister. The script stores the deregistration data in an audit table in the CiscoCM supplemental database, from which it is easily accessed for reporting. The CDR_RetrieveConfigData script retrieves the Communications Manager configuration information the Report scripts need to accommodate your grouping choices and stores it in the supplemental database.

To use the supplemental database:

1. **Create the database**. Use the SetupSupplementalDB Knowledge Script to create one CiscoCM supplemental database per Unified Communications Manager cluster you are monitoring.
2. **Populate the database**. Use CDR_RetrieveConfigData to retrieve configuration data from Unified Communications Manager and save it to the CiscoCM supplemental database. Then run CDR_RetrieveCallRecords to retrieve the CDR flat files from the folder into which they were pushed (using FTP) by the primary Communications Manager. This folder is located on the proxy agent computer; you configure the primary Communications Manager to send CDRs to this location.

   Although the PhoneDeregistrations script does not monitor data in the supplemental database, it does populate the audit table in the database with phone deregistration data, which is subsequently used by the Report_PhoneDeregAudit and Report_PhoneDeregWatchList Report scripts.
3. **Monitor the data in the database**. Depending on your monitoring objectives, use the following scripts to analyze the data in the database.
   - CDR_CallFailures monitors CDRs for calls that ended with an abnormal termination code.
   - CDR_CallQuality monitors CDRs for jitter, latency, lost data, and MOS.
   - CDR_Query searches CDRs based on query filters you select.
   - PhoneDeregistrations monitors phone deregistrations and maintains a history of phone deregistrations in the supplemental database
4. **Run the Report Knowledge Scripts**. The Report_PhoneDeregAudit and Report_PhoneDeregWatchList scripts organize and display the information in the CiscoCM supplemental database. The reporting function requires the `netiqmc` service on the Report agent computer to be running as an account that has permissions on the supplemental database.

4.47.2 Resource Object

CiscoCM _CDRMgmt

4.47.3 Default Schedule

By default, this script runs once.

4.47.4 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 the failure of the SetupSupplementalDB job. The default is 5.
Raise event if database setup succeeds?	Select **Yes** to raise an event if the setup of the CiscoCM supplemental database is successful. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the success of the setup of the CiscoCM supplemental database. The default is 25.
Raise event if database setup fails?	Select **Yes** to raise an event if the setup of the CiscoCM supplemental database is unsuccessful. The default is selected.
Event severity when database setup fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the setup of the CiscoCM supplemental database. The default is 5.
Phone Deregistration Parameters	
Number of days to keep phone deregistration audit entries	Specify the number of days' worth of phone deregistration audit entries you want to keep in the CiscoCM supplemental database. Any data older than what you specify is discarded. The default is 180 days.
CDR Parameters	
Full path to call detail records	Specify the full path to the location of the CDRs on the proxy agent computer. The TreeView cluster name must appear in the path. Use the same TreeView cluster name you used when configuring the proxy agent computer as a billing server. The default is blank. For example, *if* you entered `CCM80-01\` as the host name of the primary server when you configured the billing server *and* your FTP server is installed in the default location, then enter the following: `c:\inetpub\ftproot\CCM80-01` For more information, see Appendix A, "Monitoring Deregistration for Communications Manager 4.x".
Number of days to keep call detail records	Specify the number of days' worth of call detail records you want to keep in the CiscoCM supplemental database. Any data older than what you specify is discarded. The default is 7 days.
SQL Server Information	
Local SQL Server Instance name	Specify the name of the local SQL Server instance (on the proxy agent computer) in which you want to create the new CiscoCM supplemental database. Leave this parameter blank to accept the default name.

4.48 SIP_Trunk_CallActivity

Use this Knowledge Script to monitor attempted, completed, in-progress, and active calls for SIP trunks. This script raises an event if any threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Attempted calls per trunk
- Completed calls per trunk
- In-progress calls per trunk
- Active calls per trunk

4.48.1 Resource Object

SIPTrunk object

4.48.2 Default Schedule

By default, this script runs every 15 minutes.

4.48.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity if job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SIP_Trunk_CallActivity job. The default is 5.
Monitor Attempted Calls	
Event Notification	
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 highest number of calls that must be attempted before an event is raised. The default is 500.
Event severity when attempted calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were attempted during the monitoring period. The default is unselected.
Monitor Completed Calls	
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 calls that were completed during the monitoring period. The default is unselected.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that are active at each script iteration. The default is unselected.
Monitor Calls In Progress	
Event Notification	
Raise event if calls in progress exceed threshold	Select **Yes** to raise an event if the number of calls in progress exceeds the threshold that you set. The default is Yes.
Threshold - Maximum calls in progress	Specify the highest number of calls that must be in progress before an event is raised. The default is 1000.
Event severity when calls in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of calls in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that are in progress at each script iteration. The default is unselected.

4.49 SNMPTrap_AddMIB

Use this Knowledge Script to add MIB (management information base) files to the MIB tree that is monitored by the SNMPTrap_Async Knowledge Script. The MIB files should be `ASN.1` text file with a `.txt` or `.my` file extension, and not compiled MIB files.

With this script you can copy a MIB file from an arbitrary directory to the MIB tree located in the `<AppManager directory>\bin\MIBs` directory. And, by using the *Reload MIB tree?* parameter, you can also reload all MIBs in the tree without restarting the AppManager agent. A restart of the AppManager agent automatically reloads the MIB tree, a directory of MIBs.

Scenarios for using this script include the following examples:

In This Scenario	Set These Parameters
You want to add a MIB file to the MIB tree, but do not want the addition to take effect until after the next restart of the AppManager agent.	*Full path to MIB files* and *List of MIB files*: Provide location and name of MIB file you want to add. *Reload MIB tree?*: Select **No** (unchecked).
You manually copied a MIB file to the MIB directory and want to reload all MIBs in the tree.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.

In This Scenario	Set These Parameters
Due to compiler errors, you edited some MIBs in the MIB directory. Now you want to reload the MIBs to ensure the errors have been fixed.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.

For more information, see Section 4.50.5, “Working with NetIQ SNMP Trap Receiver,” on page 154.

4.49.1 Resource Object

CiscoCM_TrapReceiver

4.49.2 Default Schedule

By default, this script runs once.

4.49.3 Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Full path to MIB files	Specify the full path to the folder that contains the MIB files you want to install. The AppManager agent on the proxy computer must have SNMP access to the location you specify.
List of MIB files	Type a comma-separated list of the MIB files you want to install. The MIB files should be `ASN.1` text files with a `.TXT` or `.MY` file extension. The MIB files should not be compiled MIB files. The MIB files you specify must be located in the folder you identified in the *Full path to MIB files* parameter.
Reload MIB tree?	Select **Yes** to update the MIB tree. The default is yes
MIB reload timeout	Specify the length of time AppManager should attempt to update the MIB tree before timing out and raising a failure event. The default is 10 seconds.
Event Notification	
Raise event if installation and reloading of MIB tree succeeds?	Select **Yes** to raise an event if installation of the MIB files and/or reloading of the MIB tree succeeds. The default is Yes. Note that reloading of the MIB tree can be successful even if no new MIB files are installed. Reloading of the MIB tree can proceed even if you provide no MIB files in the *List of MIB files* or *Full path to list of MIB files* parameters.
Event severity when installation and reloading of MIB tree succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation of MIB files and/or the reloading of the MIB tree succeeds. The default is 25.

Parameter	How to Set It
Raise event if "reload MIB parser" warnings received?	Select **Yes** to raise an event if warning messages are received during the reload process. The default is Yes. Warning scenarios include: ◆ MIBs are installed successfully but the *Reload MIB tree?* parameter is not set to Yes. ◆ Not all specified MIB files were loaded to the MIB tree.
Event severity when "reload MIB parser" warnings received	Set the severity level, from 1 to 40, to indicate the importance of an event in which warning messages are received during the reload process. The default is 15.
Raise event if installation and reloading of MIB tree fails?	Select **Yes** to raise an event if AppManager fails to install or reload the specified MIB files. The default is Yes. Failure scenarios include: ◆ MIB reload timeout period expired. ◆ Not all specified MIB files were installed.
Event severity when installation and reloading of MIB tree fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation or reloading of the MIB tree fails. The default is 10.
Raise event with the list of currently installed MIBs?	Select **Yes** to raise an informational event that provides a list of all MIBs installed in the MIB tree. The default is Yes.
Event severity for list of currently installed MIBs	Set the severity level, from 1 to 40, to indicate the importance of an event that provides a list of all MIBs installed in the MIB tree. The default is 25.

4.50 SNMPTrap_Async

Use this Knowledge Script to monitor SNMP traps forwarded from NetIQ SNMP Trap Receiver. This script raises an event when an SNMP trap is received and when Trap Receiver is unavailable or subsequently becomes available. In addition, this script generates data streams for Trap Receiver availability.

This script checks for SNMP traps in the MIB tree. You can add Management Information Bases (MIBs) to the MIB tree. For more information, see the SNMPTrap_AddMIB Knowledge Script.

In general, a trap receiver is an application that receives traps from SNMP agents. Trap Receiver receives SNMP traps, filters them, and then forwards the traps to AppManager. For more information, see Section 4.50.5, "Working with NetIQ SNMP Trap Receiver," on page 154.

4.50.1 Prerequisite

To allow this script to access the MIBs for Unified Communications Manager servers, configure your SNMP permissions in AppManager Security Manager *before* using the SNMPTrap_Async script. For more information, see Section 4.50.6, "Configuring SNMP Permissions in Security Manager," on page 157.

4.50.2 Resource Object

CiscoCM_TrapReceiver

4.50.3 Default Schedule

By default, this script runs on an asynchronous schedule.

4.50.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Trap Filters	
List of trap OIDs	Use this parameter to provide a list of the OIDs (object identifiers) of the traps you want to monitor. Separate multiple OIDs with a comma. For example: `1.3.6.1.2.1.2.2.1.1.1,1.3.6.1.2.1.2.2.1.7.1`

Full path to file with list of trap OIDs	If you have many OIDs to monitor, use this parameter to identify the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line. For example:
	
	`1.3.6.1.2.1.2.2.1.1.1`
	`1.3.6.1.2.1.2.2.1.7.1`
	
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path. The `netiqmc` service must be running as a user that has access to the UNC path.

List of MIB subtrees	Use this parameter to monitor an OID *and* all of its subtrees. Provide a comma-separated list of the OIDs you want to monitor. For example: `1.3.6,1.3.7`

Full path to file with list of MIB subtrees	If you have many subtrees to monitor, use this parameter to provide the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line. For example:
	
	`1.3.6`
	`1.3.7`
	
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path. The `netiqmc` service must be running as a user that has access to the UNC path.

Event Notification	
Format trap data according to SNMP version	Select the version of SNMP whose formatting should be used for trap event messages. The data provided by each format is the same; only the layout is different. The default is SNMPv2.
Raise emergency alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about an emergency alarm. The default is Yes.

Parameter	How to Set It
Event severity when emergency alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about an emergency alarm. The default is 1.
Raise alert alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about an alert alarm. The default is Yes.
Event severity when alert alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about an alert alarm. The default is 2.
Raise critical alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a critical alarm. The default is Yes.
Event severity when critical alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a critical alarm. The default is 3.
Raise error alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about an error alarm. The default is Yes.
Event severity when error alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about an error alarm. The default is 5.
Raise warning alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a warning alarm. The default is unselected.
Event severity when warning alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a warning alarm. The default is 15.
Raise notice alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a notice alarm. The default is unselected.
Event severity when notice alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a notice alarm. The default is 25.
Raise informational alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about an informational alarm. The default is unselected.
Event severity when informational alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about an informational alarm. The default is 35.
Raise unmapped alarm event?	Select **Yes** to raise an event an SNMP trap is received but is not reflected in the `.CSV` mapping file. The default is Yes. Disable this parameter if you do not want to be informed about SNMP traps that are not mapped in the `.CSV` file.
Event severity when unmapped alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP trap is not mapped in the `.CSV` file. The default is 15.
Raise Trap Receiver availability events?	Select **Yes** to raise an event when Trap Receiver becomes unavailable and when Trap Receiver becomes available once again. The default is Yes.
Event severity when Trap Receiver is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes unavailable. The default is 5.

Parameter	How to Set It
Event severity when Trap Receiver becomes available	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes available after being unavailable. The default is 25.
Data Collection	
Collect data for Trap Receiver availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a “1” if Trap Receiver is available and a “0” if Trap Receiver is unavailable. The default is unselected.
Interval for collecting Trap Receiver availability data	Specify the frequency with which the script collects Trap Receiver availability data. The default is every 5 minutes.

4.50.5 Working with NetIQ SNMP Trap Receiver

NetIQ SNMP Trap Receiver (Trap Receiver) is installed automatically when you install AppManager for Cisco Unified Communications Manager. Trap Receiver runs as a service, `NetIQTrapReceiver.exe`, and might compete for port usage with any other trap receiver installed on the same computer.

What is NetIQ SNMP Trap Receiver?

At its most basic, a trap receiver is an application that receives traps from SNMP agents. Trap Receiver receives, filters, and forwards SNMP traps to AppManager. When you use Trap Receiver with AppManager for Cisco Unified Communications Manager, the SNMPTrap_Async Knowledge Script raises events when SNMP traps are received.

What is an SNMP Trap?

Simple Network Management Protocol (SNMP) is a protocol-based system used to manage devices on TCP/IP-based networks. From devices on which an SNMP agent resides, such as routers and switches, SNMP sends unsolicited notifications, called traps, to network administrators when thresholds for certain conditions are exceeded. These conditions are defined by the vendor in a device’s MIB; the network administrator sets the thresholds.

Traps are composed of Protocol Data Units (PDUs). Each PDU contains the following information, organized in various ways depending on the version of SNMP in use:

- SNMP version number
- Community name of the SNMP agent
- PDU type
- Enterprise OID (object identifier), a unique number that identifies an enterprise and its system objects in the MIB
- IP address of the SNMP agent
- Generic trap type: Cold start, Warm start, Link down, Link up, Authentication failure, and Enterprise
- Specific trap type. When the Generic trap type is set to “Enterprise,” a specific trap type is included in the PDU. A specific trap is one that is unique or specific to an enterprise.
- Time the event occurred
- Varbind (variable binding), a sequence of two fields that contain the OID and a value

Understanding Trap Receiver Architecture

Trap Receiver operates on a Client-Server architecture: the *Server*—the stand-alone Trap Receiver application—receives, filters, and forwards SNMP traps to the *Client*—an application that receives traps, such as AppManager. The Server can receive traps on standard UDP port 162 or on any other configured port. The Client and the Server can reside on the same computer or on separate computers.

Communication between Client and Server is implemented as XML messages over a TCP connection. Only one Server is allowed per computer, however, several Clients are allowed per computer. Clients that are registered to the same Server share the same TCP connection. The Server TCP port should be known to all potential Clients.

Understanding the Trap Receiver Configuration File

The configuration file for Trap Receiver, `NetIQTrapReceiver.conf`, identifies the UDP and TCP ports used by Trap Receiver: the UDP port is used for receiving traps; the TCP port is used for communicating with the Client, such as AppManager or another supported NetIQ application. The configuration file also identifies the level of logging you want to use and whether port forwarding is enabled.

By default, the configuration file is installed in `[installation directory]\config`, and has the following format:

```
#################################################################
#
# NetIQTrapReceiver.conf
#
# A configuration file for NetIQ SNMP Trap Receiver
#
#################################################################
#########################
# TCP port
# Syntax: tcp_port [port]
# E.g. : tcp_port 2735
#########################
tcp_port 2735
#########################
# UDP port
# Syntax: udp_port [port]
# E.g. : udp_port 162
#########################
udp_port 162
#########################
# Forwarding
# Syntax: forward [address]:[port] [v1]
# E.g. : forward 127.0.0.1:1000 v1
#########################
#########################
# Log level
# Syntax: log_level error|warning|info|debug|xml
# E.g. : log_level info
#########################
log_level debug
```

If the configuration file cannot be found, cannot be parsed, or does not contain one of the required values, Trap Receiver is initialized with the default configuration as shown above.

When changing values in the configuration file, take into account the following:

- If you change the TCP port number, stop all asynchronous Knowledge Script jobs associated with the modules that support Trap Receiver. Run the Discovery Knowledge Script on all monitored devices to enable the devices to recognize the new TCP port number.
- If you change the UDP port number, also change the UDP port number configured on the devices that send traps to Trap Receiver.
- If another service uses port 2735 or port 162, Trap Receiver *will not start*. The Trap Receiver log file will contain different levels of messages, based on the log_level you choose. Either change the port numbers in the configuration file, stop the service that is using the default Trap Receiver port numbers, or forward the traps coming in to UDP port 162.
- To forward incoming traps to another trap receiver, such as Microsoft SNMP Trap Service, set the Forwarding values as follows:

  ```
  forward [IP address of other trap receiver]:[port number of other trap receiver] [SNMP version]
  ```

  For example: `forward 10.40.40.25:167 v1`. By default, incoming traps are not forwarded. For more information, see Coexisting with Microsoft SNMP Trap Service.
- Restart Trap Receiver after any change to the configuration file. From Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **NetIQ Trap Receiver** and select **Restart**.

Coexisting with Microsoft SNMP Trap Service

Two trap receivers cannot be in use on the same computer while using the same standard UDP port (162). If NetIQ SNMP Trap Receiver and another trap receiver such as Microsoft SNMP Trap Service are installed on the same computer and both are receiving traps, configure Trap Receiver to use the standard UDP port and to forward incoming traps (UDP forwarding) to the other trap receiver. For more information, see “Understanding the Trap Receiver Configuration File” on page 155.

Then, configure the other trap receiver to use a different, non-standard, UDP port that is not in use by another application. The following are instructions for configuring Microsoft SNMP Trap Service.

To configure Microsoft SNMP Trap Service to use another port:

1. Navigate to `c:\Windows\system32\drivers\etc`.
2. Open the **services** file.
3. In the row for `snmptrap`, change the value for **udp** from 162 to another port number that is not in use by any other application. Use the same port number you set as the forwarding port in the Trap Receiver configuration file.
4. Save and close the **services** file.
5. Restart Windows SNMP Trap Service. In Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **SNMP Trap Service** and select **Restart**.

TIP: To see which ports are in use, run netstat.exe from a command prompt. Then select an available port as the port for the other trap receiver service.

4.50.6 Configuring SNMP Permissions in Security Manager

To allow the SNMPTrap_Async Knowledge Script to access the Management Information Bases (MIBs) for Unified Communications Manager servers, configure your SNMP permissions in AppManager Security Manager *before* using the SNMPTrap_Async script. The SNMP permissions act as a filter for incoming SNMP traps.

The type of information you configure varies according to the version of SNMP that is implemented in your network. AppManager for Cisco Unified Communications Manager supports SNMP versions 1, 2, and 3.

Adding Permissions for SNMP Versions 1 and 2

Configure community string and version information for each Unified Communications Manager server that is monitored by the proxy agent computer. Complete the following fields in the Custom tab of Security Manager.

Field	Description
Label	`SNMP`
Sub-label	Indicates whether the community string information you are configuring will be used for a single Communications Manager or for all Communications Managers. ◆ type `default`.
Value 1	Appropriate read-only community string value, such as `private` or `public`.

Adding Permissions for SNMP Version 3

SNMP trap monitoring in AppManager for Cisco Unified Communications Manager supports the following modes for SNMPv3:

- No authentication; no privacy
- Authentication; no privacy
- Authentication and privacy

In addition, the module supports the following protocols for SNMPv3:

- MD5 (Message-Digest algorithm 5, an authentication protocol)
- SHA (Secure Hash Algorithm, an authentication protocol)
- DES (Data Encryption Standard, encryption protocol)

Your SNMPv3 implementation might support one or more combinations of mode and protocol. That combination dictates the type of information you configure in AppManager Security Manager: user name (or entity), context name, protocol name, and protocol passwords.

Configure community string and version information for each Unified Communications Manager server that is monitored by the proxy agent computer. Complete the following fields in the Custom tab of Security Manager.

Field	Description
Label	`SNMP`

Field	Description
Sub-label	Indicates whether the community string information you are configuring will be used for a single Communications Manager or for all Communications Managers. ◆ For a single device supported by a particular proxy agent computer, provide the name of the Communications Manager. ◆ For all devices supported by a particular proxy agent computer, type `default`.
Value 1	SNMP user name or entity configured for the device. All SNMPv3 modes require an entry in the **Value 1** field.
Value 2	Name of the context associated with the user name or entity you entered in the **Value 1** field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides access to all MIBS for a device. If the device does not support context, type an asterisk (*). All SNMPv3 modes require an entry in the **Value 2** field.
Value 3	Combination of protocol and password appropriate for the SNMPv3 mode you have implemented. ◆ For *no authentication/no privacy mode*, leave the **Value 3** field blank. ◆ For *authentication/no privacy mode*, type `md5` or `sha` and the password for the protocol, separating each entry with a comma. For example, type `md5,abcdefgh` ◆ For *authentication/privacy mode*, type `md5` or `sha` and the associated password, and then type `des` and the associated password, separating each entry with a comma. For example, type `sha,hijklmno,des,nopqrstu`

4.51 SystemUpTime

Use this Knowledge Script to monitor the number of hours that the Communications Manager system has been up since the last reboot. This script raises an event if a reboot occurs. In addition, this script generates a data stream for the number of hours that the Communications Manager system has been operational since the last reboot.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.51.1 Resource Object

CiscoCM_CMServer

4.51.2 Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.51.3 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 the failure of the SystemUpTime job. The default is 5.
Raise event if system has rebooted?	Select **Yes** to raise an event if Communications Manager has rebooted during the monitoring period. The default is Yes.
Event severity when system has rebooted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Communications Manager has rebooted. The default is 10.
Monitor System Uptime	
Data Collection	
Collect data for system uptime?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hours that the Communications Manager system has been operational since the last reboot. The default is Yes.

4.52 SystemUsage

Use this Knowledge Script to monitor CPU, memory, and disk usage for a Communications Manager server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- CPU usage (%)
- Physical and virtual memory usage (%)
- Swap space usage (%)
- Active, common, and swap partition usage (%)
- Total processes
- Total threads

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see Section 4.57, “Recommended Knowledge Script Group,” on page 171.

4.52.1 Resource Object

CiscoCM_CMServer

4.52.2 Default Schedule

By default, this script runs every two minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

4.52.3 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 the failure of the SystemUsage job. The default is 5.
Monitor CPU Usage	
Event Notification	
Raise event if CPU usage exceeds threshold?	Select **Yes** to raise an event if CPU usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CPU usage	Specify the highest percentage of CPU usage that must occur before an event is raised. The default is 80%.
Event severity when CPU usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for CPU usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU usage during the monitoring period. The default is Yes.
Monitor Physical Memory Usage	
Event Notification	
Raise event if physical memory usage exceeds threshold?	Select **Yes** to raise an event if physical memory usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum physical memory usage	Specify the highest percentage of physical memory usage that must occur before an event is raised. The default is 80%.
Event severity when physical memory usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which physical memory usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for physical memory usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of physical memory usage during the monitoring period. The default is Yes.
Monitor Virtual Memory Usage	
Event Notification	
Raise event if virtual memory usage exceeds threshold?	Select **Yes** to raise an event if virtual memory usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum virtual memory usage	Specify the highest percentage of virtual memory usage that must occur before an event is raised. The default is 80%.

Parameter	How to Set It
Event severity when virtual memory usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which virtual memory usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for virtual memory usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of virtual memory usage during the monitoring period. The default is Yes.
Monitor Swap Space Usage	
Event Notification	
Raise event if swap space usage exceeds threshold?	Select **Yes** to raise an event if swap space usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum swap space usage	Specify the highest percentage of swap space that must be in use before an event is raised. The default is 80%.
Event severity when swap space usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which swap space usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for swap space usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of swap space usage during the monitoring period. The default is unselected.
Monitor Active Partition Usage	
Event Notification	
Raise event if active partition usage exceeds threshold?	Select **Yes** to raise an event if active partition usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum active partition usage	Specify the highest percentage of active partition usage that must occur before an event is raised. The default is 80%.
Event severity when active partition usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which active partition usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active partition usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of active partition usage during the monitoring period. The default is unselected.
Monitor Common Partition Usage	
Event Notification	
Raise event if common partition usage exceeds threshold?	Select **Yes** to raise an event if common partition usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum common partition usage	Specify the highest percentage of common partition usage that must occur before an event is raised. The default is 80%.

Parameter	How to Set It
Event severity when common partition usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which common partition usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for common partition usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of common partition usage during the monitoring period. The default is unselected.
Monitor Swap Partition Usage	
Event Notification	
Raise event if swap partition usage exceeds threshold?	Select **Yes** to raise an event if swap partition usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum swap partition usage	Specify the highest percentage of swap partition usage that must occur before an event is raised. The default is 50%.
Event severity when swap partition usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which swap partition usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for swap partition usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of swap partition usage during the monitoring period. The default is unselected.
Monitor Total Processes	
Event Notification	
Raise event if total processes exceed threshold?	Select **Yes** to raise an event if the number of active processes exceeds the threshold that you set. The default is Yes.
Threshold - Maximum total processes	Specify the highest number of processes that must be active before an event is raised. The default is 250 processes.
Event severity when total processes exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of active processes exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for total processes?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of processes that are active at each script iteration. The default is unselected.
Monitor Total Threads	
Event Notification	
Raise event if total threads exceed threshold?	Select **Yes** to raise an event if the number of threads exceeds the threshold that you set. The default is Yes.
Threshold - Maximum total threads	Specify the highest number of threads that must be created before an event is raised. The default is 2500 threads.

Parameter	How to Set It
Event severity when total threads exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of threads exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for total threads?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of threads detected at each script iteration. The default is unselected.

4.53 TFTPActivity

Use this Knowledge Script to monitor activity on the Cisco TFTP server. This script raises an event when the number of change notifications for the monitored activity exceeds the threshold that you set. In addition, this script generates data streams for the following metrics:

- Change notifications
- Builds
- Aborted requests
- Not-found requests
- Rejected requests
- Total requests
- Successful requests

4.53.1 Resource Object

CiscoCM_TFTP

4.53.2 Default Schedule

By default, this script runs every 15 minutes.

4.53.3 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 the failure of the TFTPActivity job. The default is 5.
Monitor Change Notifications	
Event Notification	

Parameter	How to Set It
Raise event if change notifications exceed threshold?	Select **Yes** to raise an event if the number of change notifications exceeds the threshold that you set. The default is Yes.
Threshold - Maximum change notifications	Specify the highest number of change notifications that must occur before an event is raised. The default is 10 notifications.
Event severity when change notifications exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of change notifications exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for change notifications?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of change notifications that occurred during the monitoring period. The default is unselected.
Monitor Builds	
Event Notification	
Raise event if builds exceed threshold?	Select **Yes** to raise an event if the number of builds exceeds the threshold that you set. The default is Yes.
Threshold - Maximum builds	Specify the highest number of builds that must occur before an event is raised. The default is 50 builds.
Event severity when builds exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of builds exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for builds?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of builds that occurred during the monitoring period. The default is unselected.
Monitor Aborted Requests	
Event Notification	
Raise event if aborted requests exceed threshold?	Select **Yes** to raise an event if the number of aborted requests exceeds the threshold that you set. The default is Yes.
Threshold - Maximum aborted requests	Specify the highest number of aborted requests that must occur before an event is raised. The default is 0 requests.
Event severity when aborted requests exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of aborted requests exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for aborted requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of aborted requests that occurred during the monitoring period. The default is unselected.
Monitor Requests Not Found	
Event Notification	

Parameter	How to Set It
Raise event if requests not found exceed threshold?	Select **Yes** to raise an event if the number of requests that are not found exceeds the threshold that you set. The default is Yes.
Threshold - Maximum requests not found	Specify the highest number of requests that must be “not found” before an event is raised. The default is 0 requests.
Event severity when requests not found exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of requests that are not found exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for requests not found?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests that were not found during the monitoring period. The default is unselected.
Monitor Rejected Requests	
Event Notification	
Raise event if rejected requests exceed threshold?	Select **Yes** to raise an event if the number of rejected requests exceeds the threshold that you set. The default is Yes.
Threshold - Maximum rejected requests	Specify the highest number of rejected requests that must occur before an event is raised. The default is 0 requests.
Event severity when rejected requests exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of rejected requests exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for rejected requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests that were rejected during the monitoring period. The default is unselected.
Monitor Total Requests	
Data Collection	
Collect data for total requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of requests, which includes aborted, not-found, rejected, and successful requests. The default is unselected.
Monitor Successful Requests	
Data Collection	
Collect data for successful requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of requests that were successful during the monitoring period. The default is unselected.

4.54 Transcoder_Device

Use this Knowledge Script to monitor the usage of registered transcoder devices. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of active resources and for resource usage (%).

4.54.1 Resource Object

CiscoCM_XCode_DeviceObj

4.54.2 Default Schedule

By default, this script runs every 15 minutes.

4.54.3 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 the failure of the Transcoder_Device job. The default is 5.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of transcoder device usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum resource usage	Specify the highest percentage of transcoder device usage that must occur before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the percentage of transcoder usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of transcoder usage at each script iteration. The default is unselected.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of transcoder devices that are active at each script iteration. The default is unselected.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times that transcoder devices were unavailable exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times that transcoder devices can be unavailable before an event is raised. The default is 0 instances.
Event severity number of times resources were unavailable exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of times that transcoder devices were unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times that transcoder devices were unavailable during the monitoring period. The default is unselected.

4.55 WebDialer

Use this Knowledge Script to monitor activity for the Cisco Web Dialer application. Web Dialer enables users to place calls from their computers.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following monitored activities:

- Failed calls
- Completed calls
- In-progress CTI sessions
- Total CTI sessions
- In-progress HTTP sessions
- Total HTTP sessions

4.55.1 Resource Object

CiscoCM_WebDialer

4.55.2 Default Schedule

By default, this script runs every 15 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 the failure of the WebDialer job. The default is 5.

Parameter	How to Set It
Monitor Failed Calls	
Event Notification	
Raise event if failed calls exceed threshold?	Select **Yes** to raise an event if the number of failed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum failed calls	Specify the highest number of calls that must fail before an event is raised. The default is 0 calls.
Event severity when failed calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of failed calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that failed during the monitoring period.The default is unselected.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were completed during the monitoring period. The default is unselected.
Monitor CTI Sessions in Progress	
Event Notification	
Raise event if CTI sessions in progress exceed threshold?	Select **Yes** to raise an event if the number of CTI sessions in progress exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CTI sessions in progress	Specify the highest number of CTI sessions that must be in progress before an event is raised. The default is 100 sessions.
Event severity when CTI sessions in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of CTI sessions in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for CTI sessions in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of CTI sessions that are in progress at each script iteration. The default is unselected.
Monitor CTI Sessions	
Data Collection	
Collect data for CTI sessions?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of CTI sessions that were handled during the monitoring period. The default is unselected.
Monitor HTTP Sessions in Progress	
Event Notification	
Raise event if HTTP sessions in progress exceed threshold?	Select **Yes** to raise an event if the number of HTTP sessions in progress exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum HTTP sessions in progress	Specify the highest number of HTTP sessions that must be in progress before an event is raised. The default is 100 sessions.
Event severity when HTTP sessions in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of HTTP sessions in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for HTTP sessions in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of HTTP sessions that are in progress at each script iteration. The default is unselected.
Monitor HTTP Sessions	
Data Collection	
Collect data for HTTP sessions?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of HTTP sessions that were handled during the monitoring period. The default is unselected.

4.56 WebPageCheck

Use this Knowledge Script to monitor the availability of and round-trip connection time to the `ccmadmin` and `ccmuser` Web pages. This script raises an event if either Web page is unavailable or if round-trip connection time exceeds the threshold that you set. In addition, this script generates data streams for Web page availability and round-trip time.

If either Web page is unavailable, the detail message records the reason, for example, because the format of the request was invalid or the server name was not found.

This script monitors Web page availability only. To monitor Web page content and usage, use the Knowledge Scripts in a different module: AppManager ResponseTime for Web.

4.56.1 Resource Object

CiscoCM_CMServer

4.56.2 Default Schedule

By default, this script runs every 30 minutes.

4.56.3 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 the failure of the WebPageCheck job. The default is 5.

Parameter	How to Set It
Is Web server secure?	Select **Yes** to indicate that your Communications Manager Web server is a secure Web server (HTTPS). The default is Yes.
Monitor CCMAdmin Web Page Availability	
Event Notification	
Raise event if Web page is unavailable?	Select **Yes** to raise an event if the `ccmadmin` Web page is unavailable. The default is Yes.
Event severity when Web page is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the `ccmadmin` Web page is unavailable. The default is 15.
Data Collection	
Collect data for ccmadmin Web page availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the Web page is available and 0 if the Web page is unavailable. The default is unselected.
Monitor CCMAdmin Web Page Round-Trip Time	
Event Notification	
Raise event if round-trip time exceeds threshold?	Select **Yes** to raise an event if the round-trip connection time for the `ccmadmin` Web page exceeds the threshold that you set. The default is Yes.
Threshold - Maximum round-trip time	Specify the longest round-trip connection time that can occur before an event is raised. The default is 100 milliseconds.
Event severity when round-trip time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which round-trip connection time for the `ccmadmin` Web page exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for round-trip time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the `ccmadmin` Web page's round-trip connection time during the monitoring period. The default is unselected.
Monitor CCMUser Web Page Availability	
Event Notification	
Raise event if Web page is unavailable?	Select **Yes** to raise an event if the `ccmuser` Web page is unavailable. The default is Yes.
Event severity when Web page is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the `ccmuser` Web page is unavailable. The default is 15.
Data Collection	
Collect data for ccmuser Web page availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the Web page is available and 0 if the Web page is unavailable. The default is unselected.
Monitor CCMUser Web Page Round-Trip Time	
Event Notification	
Raise event if round-trip time exceeds threshold?	Select **Yes** to raise an event if the round-trip connection time for the `ccmuser` Web page exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum round-trip time	Specify the longest round-trip connection time that can occur before an event is raised. The default is 100 milliseconds.
Event severity when round-trip time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which round-trip connection time for the `ccmuser` Web page exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for round-trip time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the round-trip connection time for the `ccmuser` Web page during the monitoring period. The default is unselected.

4.57 Recommended Knowledge Script Group

The following Knowledge Scripts are members of the CiscoCM recommended Knowledge Script Group (KSG).

- CCM_CallActivity
- CCM_MGCPResources
- CCM_RegisteredResources
- CCM_ResourceAvailability
- CCM_SystemPerformance
- HealthCheck
- RoleStatus
- SystemUpTime
- SystemUsage

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 CiscoCM group on a Unified Communications Manager resource.

Run the KSG on only one cluster at a time. Running the KSG on multiple clusters all at once hinders the proxy agent's ability to spread out processing over time. You can monitor multiple clusters by running the KSG on the first cluster, and then repeating the process for each additional cluster.

The CiscoCM KSG provides a "best practices" usage of AppManager for monitoring your Unified Communications Manager environment. You can use this 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 CiscoCM tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoCM tab are not affected.

When deployed as part of a KSG, a script's default script parameter settings might 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 CiscoCM KSG and want to restore it to its original form, you can reinstall AppManager for Cisco Unified Communications Manager on the repository computer or check in the appropriate script from the AppManager\qdb\kp\CiscoCM\RECOMMENDED_CiscoCM directory.

4.58 Troubleshooting Missing Data Points

AppManager for Cisco Unified Communications Manager sends consolidated requests to the Unified Communications Manager server to collect the data used by several CiscoCM Knowledge Scripts. AppManager sends these requests 30 seconds before a script begins each iteration. This 30-second data-collection offset allows enough time for AppManager to execute the query before a script requires the data.

If you notice data points are missing from a job's data stream, it may be that 30 seconds is not enough time for AppManager to execute all of the queries you need, most likely because you are running several scripts on the same schedule.

You can increase the data-collection offset time by changing a Registry setting:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0\NetIQmc\DataRecorder
\CollectionOffset
```

In the right pane of the Registry Editor, double-click **CiscoCM** and change the **Decimal** value from 30 seconds to a larger value that will allow enough time for AppManager to execute the queries for all of the scripts you are running. Keep the value *less* than the shortest interval specified by any Knowledge Script. For example, if one script runs every one minute, but the others run every five minutes, do not change the Registry setting to a value equal to or greater than 60 seconds.

Changes to this Registry setting affect the data-collection offset time for the following Knowledge Scripts:

AnalogAccess_GatewayUsage
Annunciator_Device
AttendantConsole
CCM_CallActivity
CCM_MediaResources
CCM_MGCPResources
CCM_RegisteredResources
CCM_ResourceAvailability
CCM_SystemPerformance
CFB_Hardware_Device
CFB_Software_Device
CFB_Video_Device
CTIManager
ExtensionMobility
GatekeeperActivity
GeneralCounter
H323_Gateway_CallActivity
H323_Trunk_CallActivity
HuntAndRouteList
Locations
MediaStreamingApp
MGCP_FXO_CallActivity
MGCP_FXS_CallActivity
MGCP_GatewayUsage
MGCP_PRI_CallActivity
MGCP_PRI_ChannelHealth
MGCP_T1CAS_CallActivity
MGCP_T1CAS_ChannelHealth
MOH_Device
MTP_Device
SIP_Trunk_CallActivity
SystemUpTime
SystemUsage
TFTPActivity
Transcoder_Device
WebDialer

A Monitoring Deregistration for Communications Manager 4.x Clusters

AppManager for Cisco Unified Communications Manager (CiscoCM) provides limited support for monitoring and reporting on deregistered phones on Cisco Communications Manager 4.x clusters.

The AppManager for Cisco CallManager (CiscoCallMgr) module, was designed to monitor Communications Manager 4.x clusters and uses a traditional agent architecture whereby the AppManager management agent is installed directly on the Communications Manager computer. In contrast, AppManager for Cisco Unified Communications Manager uses a proxy agent architecture to monitor 10.0, 9.1, 9.0, 8.6, 8.5, 8.0, 7.1(2), 7.0, 6.1, 6.0, 5.1, and 5.0 appliance-based systems. This architecture allows for the creation of a supplemental database, installed on the same computer as the proxy agent, in which phone deregistration data is stored.

The phone deregistration monitoring function is supported for both Cisco Communications Manager 4.x clusters and Cisco Unified Communications Manager 10.0, 9.1, 9.0, 8.6, 8.5, 8.0, 7.1(2), 7.0, 6.1, 6.0, 5.1, and 5.0 clusters.

A.1 Getting Started

Take the following steps to monitor deregistered phones on Cisco Communications Manager 4.x clusters.

To monitor deregistered phones:

1. **Discover a Communications Manager 4.x cluster**. Run Discovery_CiscoCM_4x to discover the cluster. Configure Security Manager with the AXL password *before* running the Discovery script. For more information, see Section A.2, “Discovering Communications Manager 4.x Resources,” on page 174 and Section A.3, “Configuring AXL Passwords in Security Manager,” on page 175.
2. **Create the database**. Run 4x_SetupSupplementalDB to create one CiscoCM supplemental database per Communications Manager 4.x cluster that you are monitoring.
3. **Retrieve Communications Manager 4.x configuration data**. Run 4x_RetrieveConfigData to populate the supplemental database with Communications Manager configuration data. The phone deregistration Report scripts need this information.
4. **Monitor deregistered phones**. Run 4x_PhoneDeregistrations to monitor deregistered phones on the Communications Manager 4.x cluster. This script populates the audit table in the database with phone deregistration data, which is subsequently used by the phone deregistration Report scripts.
5. **Create deregistration reports**. Run Report_PhoneDeregAudit to create a history of phone deregistrations and reregistrations. Run Report_PhoneDeregWatchList to create a list of phones that frequently deregister.

A.2 Discovering Communications Manager 4.x Resources

Use the Discovery_CiscoCM_4x Knowledge Script to discover a Communications Manager 4.x cluster. You can then use the CiscoCM_4x Knowledge Scripts to monitor phone deregistrations on Communications Manager 4.x clusters. Only one computer can act as proxy agent for any given Communications Manager cluster. Therefore, run this script on only one Windows computer at a time.

By default, this script runs once.

NOTE: Prerequisites

- The proxy agent computer for the Communications Manager 4.x cluster must be running SQL Server 2005, SQL Server 2008, or SQL Server 2008 R2 to provide a local database in which to store the collected deregistration information.
- You must configure the AXL user ID and password in AppManager Security Manager before you can discover a Communications Manager 4.x cluster. For more information, see Section A.3, “Configuring AXL Passwords in Security Manager,” on page 175.

Set the parameters on the Values tab 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 Discovery_CiscoCM_4x job fails. The default is 5.

Full path to file with list of CallManager Publishers	Specify the full path to a file on the agent computer that contains a list of Publisher names or IP addresses. Include the names or IP addresses on one or more lines in the file. If you specify the names on one line, separate each item with a comma. For example,
	`10.0.1.1, 10.0.1.254, 10.0.4.1, 10.0.4.254`
	
	If you specify the names on multiple lines, ensure that each line contains only one entry. For example:
	
	`primarycluster1`
	
	`primarycluster2`
	`primarycluster4`

Comma-separated list of CallManager Publishers	If you do not have a file that contains a list of Publisher names or addresses, you can use this parameter to type the names or IP addresses of the Communications Manager Publisher in the clusters that you want to monitor. Use commas to separate more than one name or address. For example: `primarycluster1,primarycluster2,primarycluster4`
Raise event if discovery succeeds?	Select **Yes** to raise an event when discovery succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery succeeds with warnings	Select **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.

Parameter	How to Set It
Event severity when discovery succeeds with warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discover generates warning messages. The default is 15.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.

A.3 Configuring AXL Passwords in Security Manager

AVVID XML Layer (AXL), a Cisco application programming interface, enables Communications Manager 4.x to access the HTTP server.

Configure the AXL password in AppManager Security Manager *before* you can discover Communications Manager 4.x resources. If, after running the Discovery script, you do not see the expected devices in the TreeView pane of the Operator Console, ensure that you have configured the correct AXL password. To do so, perform the following procedure again.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`CiscoCM_AXL`
Sub-label	If the AXL information will be used for a single device, type the <*device name*>. If the AXL information will be used for all devices, type `default`.
Value 1	AXL user ID that has the authority to use the AXL API. In most cases, the Communications Manager Administrator user has this authority.
Value 2	AXL password that has the authority to use the AXL API. In most cases, the Communications Manager Administrator user has this authority.
Extended application support	Required field to encrypt the new password in Security Manager.

A.4 Understanding the CiscoCM Supplemental Database

The CiscoCM supplemental database is a SQL Server database that you create on the proxy agent computer. In terms of monitoring Communications Manager 4.x clusters, the database fulfills one function: **storage for phone deregistration data**.

The 4x_PhoneDeregistrations script uses AXL queries to create a list of unregistered phones and to identify when they reregister. The script stores the deregistration data in an audit table in the CiscoCM supplemental database, from which it is easily retrieved for reporting. The Communications Manager configuration information that the Report scripts need to accommodate the grouping choices you make is retrieved by the 4x_RetrieveConfigData and also stored in the supplemental database.

A.5 Understanding Cluster Details In the Operator Console

After you discover a Communications Manager 4.x cluster, the **Details** tab of the Operator Console displays information about the cluster in several columns. To review the information, click the cluster name in the TreeView pane and then click the **Details** tab.

Column Name	Description
Name	Name that AppManager has assigned to the cluster, based on the primary node name with a suffix of "`-Cluster`."
Cluster ID	Cluster ID parameter from the Communications Manager configuration for the cluster.
Cluster Support	Either 5.x or 4.x, depending on the cluster that has been discovered.
Cisco Node Licenses	This field is always blank.
Cisco Phone Licenses	This field is always blank.
NetIQ License Count	This field is always "0." Communications Manager 4.x phones do not count toward your AppManager license for AppManager for Cisco Unified Communications Manager. The licensing for these phones is covered by the AppManager for Cisco CallManager (CiscoCallMgr) module.
NetIQ MO Version	The build number of the most recently installed version of the managed object for AppManager for Cisco Unified Communications Manager.

A.6 Monitoring Phone Status

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

For active Communications Manager clusters

In this scenario, use the phone deregistration support provided by the 4x_PhoneDeregistrations Knowledge Script. By using this script, you can determine which phones have deregistered and maintain a history of phone deregistrations in the CiscoCM supplemental database.

For Communications Managers that have failed over

Communications Managers 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. To determine which phones have deregistered, use the CiscoCallMgr_CCM_PhoneInventory Knowledge Script from the AppManager for Cisco CallManager (CiscoCallMgr) module. This script takes an inventory of phones based on specified search criteria. Make sure to use the *Monitor for new/missing phone registrations?* parameter to monitor for phone registrations that are new or missing since the last time this script was run.

To determine whether failover has occurred, use the CiscoCallMgr_CCM_RoleStatus or CiscoCallMgr_LossOfHardwarePhones Knowledge Script.