NetIQ® AppManager® for Cisco Unified Communications Management

Management Guide

December 2019

Legal Notice

Contents

About this Book and the Library **5**
About NetIQ Corporation **7**

1 Introducing AppManager for Cisco Unified Communications **9**

Features and Benefits . . . 9
Counting AppManager Licenses . . . 10

2 Installing AppManager for CiscoUCM **11**

System Requirements . . . 11
Scalability Considerations . . . 12
Installing the Module . . . 13
Deploying the Module with Control Center . . . 14
Silently Installing the Module . . . 15
Configuring AXL Passwords in Security Manager . . . 16
Enabling Access to the Unified Communications Server . . . 16
Discovering CiscoUCM Resources . . . 18

3 CiscoUCM Knowledge Scripts **21**

CTIManager . . . 22
CUPS_ActiveCalendarSubscriptions . . . 24
CUPS_ActiveIMSessions . . . 26
CUPS_ActiveJsmSessions . . . 27
CUPS_IncomingSIPSubscriptions . . . 29
CUPS_JsmFailedLogins . . . 30
CUPS_JsmMsgsInLastSlice . . . 32
CUPS_JsmOnlineUsers . . . 33
CUPS_JsmTotalMessagePackets . . . 35
CUPS_OutgoingSIPSubscriptions . . . 36
CUPS_TotalAdhocChatRooms . . . 38
CUPS_TotalPersistentChatRooms . . . 39
ExtensionMobility . . . 41
GeneralCounter . . . 43
HealthCheck . . . 46
SystemUpTime . . . 48
SystemUsage . . . 49
UCCX_CUIC_Database_Unavailable . . . 53
UCCX_CUIC_DB_Replication_Failed . . . 54
UCCX_CUIC_Live_Data_Feeds_Stopped . . . 56
UCCX_CUIC_Report_Execution_Failed . . . 57
UCCX_CUIC_Service_Unavailable . . . 59
UCCX_CUIC_Unrecoverable_Error . . . 60
WebPageCheck . . . 62
Recommended Knowledge Script Groups . . . 64

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 website.

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
Website:	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
Website:	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 website 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

The Cisco Unified Communications server is a unified communications platform that provides services such as session management, voice, video, messaging, mobility, and web conferencing.

This chapter introduces AppManager for Cisco Unified Communications Management (CiscoUCM). AppManager for CiscoUCM allows you to monitor resources for Cisco Unified Communications servers such as the Cisco Universal Presence Server (CUPS) and the Cisco Unified Contact Center Express (UCCX).

You can use this module in combination with either the AppManager for Cisco Unified Communications Manager (CiscoCM) module or the Appmanager for Cisco Unified Connection (CiscoUC) module. The AppManager for CiscoCM module provides monitoring for Cisco CUCM call managers. The AppManager for CiscoUC module provides monitoring for Cisco Unity Connection voicemail servers. The AppManager for CiscoUCM module also provides monitoring for additional Cisco Communications servers, such Cisco CUPS, including those which are not call managers or voicemail systems.

Features and Benefits

The module includes Knowledge Scripts to create jobs that monitor the health, availability, and performance of key services, applications, and the operating system. These scripts allow you to monitor and manage any or all of these crucial Cisco Unified Communications servers and Cisco Universal Presence Server resources. Each Knowledge Script can be configured to send an alert, collect data for reporting, and perform automated problem management when an event occurs.

With AppManager for CiscoUCM, you can monitor a Cisco Unified Presence (CUPS) server for:

- Active instant message sessions between SIP and XMPP
- Ad-hoc and persistent text conferencing rooms
- Active incoming and outgoing subscriptions
- Calendar subscriptions that are currently active
- Client emulation sessions between Presence Engine and Jabber Session Manager
- Failed logins for the Jabber Session Manager
- Messages in the last time slice for the Jabber Session Manager
- Message packets through the Jabber Session Manager
- Online users being managed by the Jabber Session Manager

You can also monitor a Cisco Unified Contact Center Express (UCCX) server for:

- Critical errors with a database
- Database replication failures
- Live data feeds having stopped
- Reporting server being unable to run a report

- Cisco Unified Intelligence Center service unavailable
- Presence of internal errors within Reporting Server which may prevent it from functioning correctly.

This module also monitors general system properties relevant to the CUPS and UCCX servers as well other server types:

- User-specified Performance Monitor counters
- Operational status of active services on Unified Communications servers
- Number of hours the Unified Communications server has been operational since its last reboot
- CPU, memory, and disk usage for a Unified Communications server
- Availability of and round-trip time to the ccmadmin and ccmuser Web pages
- Cisco Unified Communications server CTI Manager and the Extension Mobility application

Counting AppManager Licenses

The module is licensed as part of the VoIP Licensing Pack.

2 Installing AppManager for CiscoUCM

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

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.

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 CiscoUCM has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, on all proxy agent computers, and on all console computers	8.0.3, 8.2, 9.1, or higher One of the following AppManager agents are required: ◆ AppManager agent 7.0.4 with hotfix 72616 or higher ◆ AppManager agent 8.0.3, 8.2, or 9.1 or higher For more information about hotfixes, see the AppManager Suite Hotfixes page.
Microsoft Windows operating system on agent computers	One of the following: ◆ Windows Server 2016 ◆ Windows 10 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows 8.1 (32-bit and 64-bit) ◆ Windows 8 (32-bit and 64-bit) ◆ Windows Server 2008 R2 **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	7.6.170.0 or later. For more information, see the AppManager Module Upgrades & Trials page.
Cisco Unified Communications Manager on the servers you want to monitor	12.5, 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

Software/Hardware	Version
Cisco Unified Presence Server on the servers you want to monitor	10.5, 10.0
Cisco Unified call Center Express (UCCX) on the servers you want to monitor	10.5,10.0
Cisco Unity Connection Servers	10.5, 10.0

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 CiscoUCM 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.

Installing the Module

Run the module installer on the CiscoUCM 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-CiscoUCM-8.x.x.0.msi` module installer from the `AM70_CiscoUCM_8.x.x.0` self-extracting installation package on the Download page following steps below:

1. Select VoIP Cisco Unified Communications Manager (UCM).
2. (Conditional) Select a version.
3. (Conditional) Select a date.
4. (Conditional) Enter keywords.
5. Click Submit.
6. On the Products tab, click VoIP Cisco Unified Communications Management (UCM) 8.1.0.2.
7. On the NetIQ VoIP Cisco Unified Communications Management (UCM) 8.1.0.2 page, click -> proceed to download.
8. Read the Downloads page, then click -> accept.
9. Click ->download next to the AM_CiscoUCM_8.1.0.2.exe.
10. (Conditional) Click ->download next to the the AppManagerForCiscoUCM_ReleaseMotes.html.

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 `CiscoUCM.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 `CiscoUCM.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 "Deploying the Module with Control Center" on page 14. 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.

Note Microsoft .NET Framework 3.5 is required on the computer where you run the installation program for the QDB portion of the module. For computers running more recent versions of Windows operating systems that use a newer version of NET, install.NET 3.5 with the Add Roles and Features wizard in Windows Server Manager, as described in this Microsoft article.

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 you want to monitor (agents) to install the agent components.

8 Configure AXL passwords in AppManager Security Manager. For more information, see "Configuring AXL Passwords in Security Manager" on page 16.

9 (Conditional) If you have not discovered CiscoUCM resources, run the Discovery_CiscoUCM Knowledge Script on all agent computers where you installed the module. For more information, see "Discovering CiscoUCM Resources" on page 18.

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

Deploying the Module with Control Center

You can use Control Center to deploy the module to 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.

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 "Checking In the Installation Package" on page 15.

3 Configure an email address to receive notification of a deployment.

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

5 Approve the deployment task.

6 View the results.

Checking In the Installation Package

You must check in the installation package, `AM70-CiscoUCM-8.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1 Log in 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-CiscoUCM-8.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.

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-CiscoUCM-8.x.x.0.m"si /qn
```

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

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

```
/L* "AM70-CiscoUCM-8.x.x.0.msi.l"og
```

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 Server 2008 R2 or Windows Server 2012, open a command prompt at the administrative level and select **Run as administrator** before you run the silent install command listed above.

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

Windows authentication:

```
AM70-CiscoUCM-8.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-CiscoUCM-8.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
```

Configuring AXL Passwords in Security Manager

AVVID XML Layer (AXL), a Cisco application programming interface, enables the Unified Communications server to access the HTTP server. Configure the AXL password in AppManager Security Manager *before* running the Discovery_CiscoUCM 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 Unified Communications server or for all Unified Communications servers. ◆ For a single Unified Communications server, provide the name of the Unified Communications server. ◆ For all Unified Communications servers, type `default`.
Value 1	AXL user ID that has the authority to use the AXL API. In most cases, the Unified Communications server Administrator user has this authority.
Value 2	AXL password that has the authority to use the AXL API. In most cases, the Unified Communications server 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 Unified Communications 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.

Enabling Access to the Unified Communications Server

By default, AppManager uses the `ccmadmin` account to access Unified Communications 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_CiscoUCM on the primary Unified Communications Manager server.

Configuring a New User

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

To configure a new user:

1. Navigate to the Administration Web site of your primary Unified Communications server.
2. In the **Username** and **Password** fields, type your user name and password, and then click **Submit**.
3. From the Cisco Unified application 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 application Web page, select **Access Control 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 CUM 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 application Web page, select **Access Control 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 application 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

Adding the New User in Security Manager

After you create a new user in a new access control 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 server for which you created the new user and user group in “Configuring a New User” on page 16.
Value 1	`netiq`
Value 2	Password you created for the new user in “Configuring a New User” on page 16.
Extended application support	Required field to encrypt the new password in Security Manager.

Running Discovery_CiscoUCM

After you create a new user and configure the new user in Security Manager, run the Discovery_CiscoUCM Knowledge Script on the proxy agent computer. For more information about the discovery process, see “Discovering CiscoUCM Resources” on page 18.

In the *Comma-separated list of primary servers* parameter of the Discovery_CiscoUCM script, provide the host name of the primary server for which you created the new user and user group in “Configuring a New User” on page 16.

Discovering CiscoUCM Resources

Use the Discovery_CiscoUCM Knowledge Script to discover configuration and resource information for Cisco Unified Communications servers and Cisco Universal Presence Server (CUPS) resources. 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 server. Therefore, run Discovery_CiscoUCM on only one Windows server at a time.

Configure your AXL password in AppManager Security Manager before discovering Cisco Unified Communications servers and Cisco Universal Presence Server (CUPS) resources. For more information, see “Configuring AXL Passwords in Security Manager” on page 16.

By default, this script runs once a week on Sundays for each computer.

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_CiscoUCM 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 following 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_CiscoUCM job fails. The default is 5.

Full path to file with list of primary 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_CiscoUCM job, note the name of the discovered cluster in the TreeView, which will look similar to the following example: `Proxy agent computer CiscoUCM:`**`CCM80-01`**`-Cluster`

Parameter	How to Set It
Comma-separated list of primary 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_CiscoUCM job, note the name of the discovered cluster in the TreeView, which will look similar to the following example: `Proxy agent computer CiscoUCM:`**`CCM80-01`**`-Cluster`

Comma-separated list of Communications 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 Unified Communications server.
	
	Type a list of IP address pairs for the Unified Communications 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 called 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 No.
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.
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.

3 CiscoUCM Knowledge Scripts

AppManager provides the following Knowledge Scripts for monitoring resources for Cisco Unified Communications servers such as the Cisco Universal Presence Server (CUPS), which are not call managers or voice mail systems, and the Cisco Unified Contact Center Express (UCCX) Server.

You can use this module in combination with either the AppManager for Cisco Unified Communications Manager (CiscoCM) module or the Appmanager for Cisco Unified Connection (CiscoUC) module. The AppManager for CiscoCM module provides monitoring for Cisco CUCM call managers. The AppManager for CiscoUC module provides monitoring for Cisco Unity Connection voice mail servers.

From the Knowledge Script view of Control Center, you can access more information about any 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
CTIManager	Monitors the activity and resource usage of the Cisco Unified Communications server CTI Manager.
CUPS_ActiveCalendarSubscriptions	Monitors the number of calendar subscriptions that are currently active on a Cisco Unified Presence server.
CUPS_ActiveIMSessions	Monitors the number of active instant message sessions between SIP and XMPP on a Cisco Unified Presence server.
CUPS_ActiveJsmSessions	Monitors the number of client emulation sessions between the Presence Engine and Jabber Session Manager for a Cisco Unified Presence server.
CUPS_IncomingSIPSubscriptions	Monitors the number of active incoming subscriptions for a Cisco Unified Presence server.
CUPS_JsmFailedLogins	Monitors the total number of failed logins for the Jabber Session Manager on a Cisco Unified Presence server.
CUPS_JsmMsgsInLastSlice	Monitors the total messages in the last time slice for the Jabber Session Manager on a Cisco Unified Presence server.
CUPS_JsmOnlineUsers	Monitors the current number of online users being managed by the Jabber Session Manager on a Cisco Unified Presence server.
CUPS_JsmTotalMessagePackets	Monitors the total message packets through the Jabber Session Manager on a Cisco Unified Presence server.
CUPS_OutgoingSIPSubscriptions	Monitors the number of active outgoing SIP subscriptions for a Cisco Unified Presence server.
CUPS_TotalAdhocChatRooms	Monitors the total number of ad-hoc text conferencing rooms for a Cisco Unified Presence server.
CUPS_TotalPersistentChatRooms	Monitors the total number of persistent text conferencing rooms for a Cisco Unified Presence server.
ExtensionMobility	Monitors activity for the Extension Mobility application.

Knowledge Script	What It Does
GeneralCounter	Monitors a user-specified performance counter.
HealthCheck	Monitors the operational status of active services on Unified Communications servers.
SystemUpTime	Monitors the number of hours the Unified Communications server has been operational since its last reboot.
SystemUsage	Monitors CPU, memory, and disk usage for a Unified Communications server.
UCCX_CUIC_Database_Unavailable	Monitors for critical errors with the database on a Cisco UCCX server.
UCCX_CUIC_DB_Replication_Failed	Monitors for database replication failures on a Cisco UCCX server.
UCCX_CUIC_Live_Data_Feeds_Stopped	Monitors for live data feeds having stopped on a Cisco UCCX server.
UCCX_CUIC_Report_Execution_Failed	Monitors for the reporting server being unable to run a report on a UCCX server.
UCCX_CUIC_Service_Unavailable	Monitors for the Cisco Unified Intelligence Center service being unavailable on a Cisco UCCX server.
UCCX_CUIC_Unrecoverable_Error	Monitors for internal errors within reporting server on a UCCX server, which might prevent it from functioning correctly.
WebPageCheck	Monitors the availability of and round-trip time to the ccmadmin and ccmuser Web pages.
Recommended Knowledge Script Groups	Perform essential monitoring of your Cisco Unified Communications environment and Cisco Unified Presence server environment.

CTIManager

Use the CTIManager Knowledge Script to monitor the activity and resource usage of the Computer Telephony Integration (CTI) Manager on a Cisco Unified Communications server.

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 Unified Communications links.

Resource Object

CiscoUCM_CTIMgrService

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following 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 the failure of the CTIManager job. The default is 5.
Monitor Connected Applications	
Event Notification	
Raise event if connected applications exceeds 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 exceeds 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. 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 number of open lines exceeds 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 open devices.

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

CUPS_ActiveCalendarSubscriptions

Use the CUPS_ActiveCalendarSubscriptions Knowledge Script to monitor the number of calendar subscriptions that are currently active on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of calendar subscriptions exceeds a threshold you set. The script also raises an event if the delta value for calendar subscriptions (the amount of present subscriptions minus previous subscriptions) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_ActiveCalendarSubscriptions job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco Presence Engine.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for calendar subscriptions. The default is ActiveCalendarSubscriptions.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for calendar subscriptions. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of current calendar subscriptions exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of current calendar subscriptions that must exist before an event is raised. The default is 500 subscriptions.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of current calendar subscriptions exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current calendar subscriptions for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for calendar subscriptions (the amount of present subscriptions minus previous subscriptions) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for calendar subscriptions that must exist before an event is raised. The default is 100 subscriptions.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for calendar subscriptions exceeds the threshold. The default is 10.

Parameter	How to Set It
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current calendar subscriptions for charts and reports. The default is unselected.

CUPS_ActiveIMSessions

Use the CUPS_ActiveIMSessions Knowledge Script to monitor the number of active instant message sessions between SIP and XMPP on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of active instant message sessions exceeds a threshold you set. The script also raises an event if the delta value for active instant message sessions (the amount of present subscriptions minus previous subscriptions) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_ActiveIMSessions job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco Presence Engine.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for active instant message sessions. The default is ActiveIMSessions.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for active instant message sessions. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.

Parameter	How to Set It
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of current active instant message sessions exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of current active instant message sessions that must exist before an event is raised. The default is 500 sessions.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of current active instant message sessions exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current active instant message sessions for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for active instant message sessions (the amount of present sessions minus previous sessions) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for active instant message sessions that must exist before an event is raised. The default is 100 sessions.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for active instant message sessions exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current active instant message sessions for charts and reports. The default is unselected.

CUPS_ActiveJsmSessions

Use the CUPS_ActiveJsmSessions Knowledge Script to monitor the number of client emulation sessions between the Presence Engine and Jabber Session Manager on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of client emulation sessions exceeds a threshold you set. The script also raises an event if the delta value for client emulation sessions (the amount of present subscriptions minus previous subscriptions) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_ActiveJsmSessions job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco Presence Engine.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for client emulation sessions. The default is ActiveJsmSessions.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for client emulation sessions. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of current client emulation sessions exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of current client emulation sessions that must exist before an event is raised. The default is 500 sessions.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of current client emulation sessions exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current client emulation sessions for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for client emulation sessions (the amount of present sessions minus previous sessions) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for client emulation sessions that must exist before an event is raised. The default is 100 sessions.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for client emulation sessions exceeds the threshold. The default is 10.

Parameter	How to Set It
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current client emulation sessions for charts and reports. The default is unselected.

CUPS_IncomingSIPSubscriptions

Use the CUPS_IncomingSIPSubscriptions Knowledge Script to monitor the number of incoming SIP subscriptions that are currently active on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of incoming SIP subscriptions exceeds a threshold you set. The script also raises an event if the delta value for incoming SIP subscriptions (the amount of present subscriptions minus previous subscriptions) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_IncomingSIPSubscriptions job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP SIP S2S.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for incoming SIP subscriptions. The default is SIPS2SSubscriptionsIn.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for incoming SIP subscriptions. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.

Parameter	How to Set It
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of current incoming SIP subscriptions exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of current incoming SIP subscriptions that must exist before an event is raised. The default is 500 subscriptions.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of current incoming SIP subscriptions exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current incoming SIP subscriptions for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for incoming SIP subscriptions (the amount of present subscriptions minus previous subscriptions) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for incoming SIP subscriptions that must exist before an event is raised. The default is 100 subscriptions.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for incoming SIP subscriptions exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current incoming SIP subscriptions for charts and reports. The default is unselected.

CUPS_JsmFailedLogins

Use the CUPS_JsmFailedLogins Knowledge Script to monitor the number of failed logins for the Jabber Session Manager on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of failed logins exceeds a threshold you set. The script also raises an event if the delta value for incoming failed logins (the amount of present failed logins minus previous amount of failed logins) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_JsmFailedLogins job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP JSM.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for failed logins. The default is JsmFailedLogins.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for failed logins. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of current failed logins exceeds the threshold you set. The default is Yes.
Threshold - Maximum current value	Specify the maximum number of current failed logins that must exist before an event is raised. The default is 1 failed login session.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of current failed logins exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current failed logins for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for failed logins (the amount of present logins minus previous logins) exceeds the threshold you set. The default is Yes.
Threshold - Maximum delta value	Specify the maximum delta value for failed logins that must exist before an event is raised. The default is 1 failed login.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for failed logins exceeds the threshold. The default is 10.
Data Collection	

Parameter	How to Set It
Collect data for delta value?	Select **Yes** to collect data about the delta value for current failed logins for charts and reports. The default is unselected.

CUPS_JsmMsgsInLastSlice

Use the CUPS_JsmMsgsInLastSlice Knowledge Script to monitor the total messages in the last time slice for the Jabber Session Manager on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of messages in the last time slice exceeds a threshold you set. The script also raises an event if the delta value for messages in the last time slice (the amount of present messages minus previous amount of messages) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_JsmMsgsInLastSlice job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP JSM.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for messages in the last time slice. The default is JsmMsgsInLastSlice.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for messages in the last time slice. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	

Parameter	How to Set It
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of total messages in the last time slice exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of total messages in the last time slice that must exist before an event is raised. The default is 500 messages.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of total messages in the last time slice exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current total messages in the last time slice for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for total messages in the last time slice (the amount of present messages in the last time slice minus previous messages) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for total messages in the last time slice that must exist before an event is raised. The default is 100 total messages in the last time slice.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for total messages in the last time slice exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current total messages in the last time slice for charts and reports. The default is unselected.

CUPS_JsmOnlineUsers

Use the CUPS_JsmOnlineUsers Knowledge Script to monitor the number of online users being managed by the Jabber Session Manager on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of online users being managed by Jabber Session Manager exceeds a threshold you set. The script also raises an event if the delta value for online users in the last time slice (the amount of present online users minus previous amount of online users) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_JsmOnlineUsers job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP JSM.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for online users. The default is JsmOnlineUsers.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for online users. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of online users exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of online users that must exist before an event is raised. The default is 500 online users.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of online users exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current online users for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for online users (the amount of present online users minus previous online users) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for online users that must exist before an event is raised. The default is 100 online users.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for online users exceeds the threshold. The default is 10.
Data Collection	

Parameter	How to Set It
Collect data for delta value?	Select **Yes** to collect data about the delta value for current online users for charts and reports. The default is unselected.

CUPS_JsmTotalMessagePackets

Use the CUPS_JsmTotalMessagePackets Knowledge Script to monitor the total message packets through the Jabber Session Manager on a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of total message packets exceeds a threshold you set. The script also raises an event if the delta value for total message packets in the last time slice (the amount of present total message packets minus previous amount of total message packets) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_JsmTotalMessagePackets job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP JSM.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for total message packets. The default is JsmTotalMessagePackets.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for total message packets. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	

Parameter	How to Set It
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of total message packets exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of total message packets that must exist before an event is raised. The default is 500 total message packets.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of total message packets exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current total message packets for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for total message packets (the amount of present total message packets minus previous total message packets) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for total message packets that must exist before an event is raised. The default is 100 total message packets.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for total message packets exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current total message packets for charts and reports. The default is unselected.

CUPS_OutgoingSIPSubscriptions

Use the CUPS_OutgoingSIPSubscriptions Knowledge Script to monitor the number of active outgoing SIP subscriptions for a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of active outgoing SIP subscriptions exceeds a threshold you set. The script also raises an event if the delta value for active outgoing SIP subscriptions in the last time slice (the amount of present active outgoing SIP subscriptions minus previous amount of active outgoing SIP subscriptions) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_OutgoingSIPSubscriptions job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP SIP S2S.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for active outgoing SIP subscriptions. The default is SIPS2SSubscriptionsOut.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for active outgoing SIP subscriptions. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of active outgoing SIP subscriptions exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of active outgoing SIP subscriptions that must exist before an event is raised. The default is 500 active outgoing SIP subscriptions.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active outgoing SIP subscriptions exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current active outgoing SIP subscriptions for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for active outgoing SIP subscriptions (the amount of present active outgoing SIP subscriptions minus previous active outgoing SIP subscriptions) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for active outgoing SIP subscriptions that must exist before an event is raised. The default is 100 active outgoing SIP subscriptions.

Parameter	How to Set It
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for active outgoing SIP subscriptions exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current active outgoing SIP subscriptions for charts and reports. The default is unselected.

CUPS_TotalAdhocChatRooms

Use the CUPS_TotalAdhocChatRooms Knowledge Script to monitor the total number of ad-hoc text conferencing rooms for a Cisco Unified Presence server.

This script raises an event if a counter or instance is not accessible, or if the current number of ad-hoc text conferencing rooms exceeds a threshold you set. The script also raises an event if the delta value for ad-hoc text conferencing rooms in the last time slice (the amount of present ad-hoc text conferencing rooms minus previous amount of ad-hoc text conferencing rooms) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_TotalAdhocChatRooms job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP TC.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for ad hoc text conferencing rooms. The default is TcAdhocRooms.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for ad hoc text conferencing rooms. Separate multiple instance names with commas.

Parameter	How to Set It
Raise event if counter or instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. The default is Yes.
Event severity when counter or instance not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of ad hoc text conferencing rooms exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of ad hoc text conferencing rooms that must exist before an event is raised. The default is 500 ad hoc text conferencing rooms.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of ad-hoc text conferencing rooms exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current ad hoc text conferencing rooms for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for ad hoc text conferencing rooms (the amount of present ad hoc text conferencing rooms minus previous ad-hoc text conferencing rooms) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for ad hoc text conferencing rooms that must exist before an event is raised. The default is 500 ad hoc text conferencing rooms.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for ad hoc text conferencing rooms exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current ad hoc text conferencing rooms for charts and reports. The default is unselected.

CUPS_TotalPersistentChatRooms

Use the CUPS_TotalPersistentChatRooms Knowledge Script to monitor the total number of persistent text conferencing rooms for a Cisco Unified Presence Server.

This script raises an event if a counter or instance is not accessible, or if the current number of persistent text conferencing rooms exceeds a threshold you set. The script also raises an event if the delta value for persistent text conferencing rooms in the last time slice (the amount of present persistent text conferencing rooms minus previous amount of persistent text conferencing rooms) exceeds a threshold. In addition, this script collects data for current and delta values.

Resource Object

CiscoUCM_PresenceApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the CUPS_TotalPersistentChatRooms job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Cisco XCP TC.
Name of the counter to monitor	Specify the name of the performance counter you want to monitor for persistent text conferencing rooms. The default is TcPersistentRooms.
Name of the instance(s) to monitor	Specify the name or names of the Unified Presence server instances you want to monitor for persistent text conferencing rooms. Separate multiple instance names with commas.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the number of persistent text conferencing rooms exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum number of persistent text conferencing rooms that must exist before an event is raised. The default is 500 persistent text conferencing rooms.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of persistent text conferencing rooms exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the number of current persistent text conferencing rooms for charts and reports. The default is Yes.
Monitor Delta Value	

Parameter	How to Set It
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value for persistent text conferencing rooms (the amount of present persistent text conferencing rooms minus previous persistent text conferencing rooms) exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for persistent text conferencing rooms that must exist before an event is raised. The default is 100 persistent text conferencing rooms.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value for persistent text conferencing rooms exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for current persistent text conferencing rooms for charts and reports. The default is unselected.

ExtensionMobility

Use the ExtensionMobility 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.

Resource Object

CiscoUCM_ExtMobility

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following 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 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.

GeneralCounter

Use the GeneralCounter Knowledge Script to monitor a user-specified performance monitor counter on a Cisco Unified Communications 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.

The GeneralCounter Knowledge Script has three configuration parameters: Object, Counter and Instance. Not all counters require an instance; however, many counters do. When GeneralCounter runs without an instance specified, it collects only the “no instance” version of the counter.

When monitoring by regular expression, the GeneralCounter Knowledge Script collects a list of all known instances of the specified Counter from the server. It then applies the regular expression provided against the instance list and selects only those instances. 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. If any instances are matched, the job will check against that list of counters on each subsequent iteration, as if the specific counter names had been entered by hand in the “Name of the instance to monitor” parameter.

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 a few examples of Boost regular expressions:

To search for:	Expression	Example
All Instances	`.*`	Calls rejected due to ICT throttling for all gateways. To limit your search to a specific object and counter, you can enter the object and counter name. For example: Object= `Cisco H323` Counter= CallsRejectedDueToICTCallThrottling Instance= `.*`
Everything on a specific device	`^devicename::.*`	◆ Calls completed for all ports on gateway Cisco MGCP FXS Device netiqrtp-tl0-r1-555.netiq.com Object= `Cisco MGCP FXS Device` Counter=`CallsCompleted` Instance=`^netiqrtp-tl0-r1-555\.netiq\.com::.*` ◆ Video calls for gateways within subnet 10.52.0.0 Object= `Cisco H323` Counter= VideoCallsActive Instance= `^10\.52\..*`
All things to, from, and within a named location	`(.*->)*(locationName)(->.*)*`	Calls completed for all ports on gateway Cisco MGCP FXS Device netiqrtp-tl0-r1-555.netiq.com Object= Cisco MGCP FXS Device Counter=CallsCompleted Instance=^netiqrtp-tl0-r1-555\.netiq\.com::.*

Resource Object

CiscoUCM_CMServer

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters on the **Values** tab 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 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 `TotalThreads`.
Instance Specification	
Name of the instance(s) to monitor	Type the name(s) 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.
Evaluate instance as regular expression?	Select the **Yes** check box to evaluate and monitor the instance names that you entered in the "Name of the instance(s) to monitor" field, as a regular expression. The default is unselected. **NOTE** ◆ If the check box is unselected, and the "Name of the instance to monitor" field contains at least one entry, CiscoUCM evaluates the instance(s) as a comma-separated values (CSV) list. ◆ If the check box is unselected, and the "Name of the instance to monitor" field is blank, CiscoUCM monitor the counter without specifying an instance.
Number of iterations between re-evaluation of instance names. (Enter 0 to never re-evaluate)	Set the number of iterations, from 0 to 8192, to re-evaluate between attempts to evaluate instance(s) for regular expressions. The default is 288.
Raise event if counter/ instance found?	Select **Yes** to raise an event if this script evaluates a regular expression and finds a match is for one or more counter instances. The default is No.
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 finds a match is for one or more counter after evaluating a regular expression. The default is 25.
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.
Threshold - Maximum current value	Specify the maximum current value the counter can attain before an event is raised. The default is 500.

Parameter	How to Set It
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 (the difference between the current value and the previous value) of the counter exceeds the threshold you set. The default is Yes.
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.

HealthCheck

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

- Cisco DB
- Cisco AMC Service
- Cisco Communications
- Cisco CDR Agent
- Cisco CTL Provider
- Cisco Database Layer Monitor
- Cisco DRF Local
- Cisco Extension Mobility
- Cisco Presence Datastore
- Cisco Presence Engine
- Cisco RIS Data Collector
- Cisco Extension Mobility
- Cisco Tftp
- Cisco Presence Engine

- Cisco Presence Datastore
- Cisco XCP Router

The script checks the target server to determine whether the default services are configured on that server, and it only monitors the services that are actually configured.

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.

You can exclude default services by specifying those services in the *Default services to exclude* parameter, and you can include additional services (not listed above by) specifying those services in the *Other services to include* parameter.

This script is a member of the CiscoUCM recommended Knowledge Script Group (KSG). For more information, see “Recommended Knowledge Script Groups” on page 64.

Resource Object

CiscoUCM_CMServer

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 to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following 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 the failure of the CiscoUCM_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 Unified Communications 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.

Parameter	How to Set 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.
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 which 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.
Skip event notification for uninstalled service	Select No to raise events for uninstalled services. The default is Yes.
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.

SystemUpTime

Use the SystemUpTime Knowledge Script to monitor the number of hours that a Cisco Unified Communications server 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 Unified Communications server has been operational since the last reboot.

This script is a member of the CiscoUCM recommended KSG. For more information, see “Recommended Knowledge Script Groups” on page 64.

Resource Object

CiscoUCM_CMServer

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 to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following 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 the failure of the SystemUpTime job. The default is 5.
Raise event if system has rebooted?	Select **Yes** to raise an event if the Unified Communications server 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 the Unified Communications server 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 Unified Communications server has been operational since the last reboot. The default is Yes.

SystemUsage

Use the SystemUsage Knowledge Script to monitor CPU, memory, and disk usage for a Unified Communications 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 CiscoUCM recommended Knowledge Script Group (KSG). For more information, see “Recommended Knowledge Script Groups” on page 64.

Resource Object

CiscoUCM_CMServer

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 to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following 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 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	

Parameter	How to Set It
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%.
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	

Parameter	How to Set It
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%.
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	

Parameter	How to Set It
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.
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.

UCCX_CUIC_Database_Unavailable

Use the UCCX_CUIC_Database_Unavailable Knowledge Script to monitor for critical errors with a database for a Cisco Unified Contact Center Express (UCCX) Server.

This script raises an event if a counter or instance is not accessible, or if the value of the Intelligence Center system condition table counter for critical database errors exceeds a threshold you set. This script also generates data streams for current and delta counter values.

Resource Object

CiscoUCM_UCCXApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the UCCX_CUIC_Database_Unavailable job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Intelligence Center System Condition Table.

Parameter	How to Set It
Name of the counter to monitor	Specify the name of the system condition counter you want to monitor. The default is CUIC_DATABASE_UNAVAILABLE.
Name of the instance(s) to monitor	Specify the name or names of the system condition counter instances you want to monitor. Separate multiple instance names with commas.The default is blank.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the value of the system condition counter for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value of the system condition counter exceeds the threshold you set. The default is Yes.
Threshold - Maximum delta value	Specify the maximum delta value for the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for the system condition counter for charts and reports. The default is unselected.

UCCX_CUIC_DB_Replication_Failed

Use the UCCX_CUIC_DB_Replication_Failed Knowledge Script to monitor for database replication failures on a Cisco Unified Contact Center Express (UCCX) Server.

This script raises an event if a counter or instance is not accessible, or if the value of the Intelligence Center system condition table counter for database replication failures exceeds a threshold you set. This script also generates data streams for current and delta counter values.

Resource Object

CiscoUCM_UCCXApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the UCCX_CUIC_DB_Replication_Failed job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Intelligence Center System Condition Table.
Name of the counter to monitor	Specify the name of the system condition counter you want to monitor. The default is CUIC_DB_REPLICATION_FAILED.
Name of the instance(s) to monitor	Specify the name or names of the system condition counter instances you want to monitor. Separate multiple instance names with commas. The default is blank, as an instance name is not required for this counter type.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum value of the system condition counter that must be exceeded before an event is raised. The system condition counters values are defined as 0=condition cleared or not set, 1=warning, 2=critical.The default is 0.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the value of the system condition counter for charts and reports. The default is Yes.
Monitor Delta Value	

Parameter	How to Set It
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value of the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for the system condition counter for charts and reports. The default is unselected.

UCCX_CUIC_Live_Data_Feeds_Stopped

Use the UCCX_CUIC_Live_Data_Feeds_Stopped Knowledge Script to monitor for live data feeds that have stopped on a Cisco Unified Contact Center Express (UCCX) Server.

This script raises an event if a counter or instance is not accessible, or if the value of the Intelligence Center system condition table counter for live data feeds having stopped exceeds a threshold you set. This script also generates data streams for current and delta counter values.

Resource Object

CiscoUCM_UCCXApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the UCCX_CUIC_Live_Data_Feeds_Stopped job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Intelligence Center System Condition Table.
Name of the counter to monitor	Specify the name of the system condition counter you want to monitor. The default is CUIC_LIVE_DATA_FEEDS_STOPPED.

Parameter	How to Set It
Name of the instance(s) to monitor	Specify the name or names of the system condition counter instances you want to monitor. Separate multiple instance names with commas. The default is blank, as an instance name is not required for this counter type.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. 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 the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the value of the system condition counter for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value of the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for the value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for the system condition counter for charts and reports. The default is unselected.

UCCX_CUIC_Report_Execution_Failed

Use the UCCX_CUIC_Report_Execution_Failed Knowledge Script to monitor whether the reporting server is able to run reports on a Cisco Unified Contact Center Express (UCCX) Server.

This script raises an event if a counter or instance is not accessible or if the value of the Intelligence Center system condition table counter if failed reports exceeds a threshold you set. This script also generates data streams for current and delta counter values.

Resource Object

CiscoUCM_UCCXApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the UCCX_CUIC_Report_Execution_Failed job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Intelligence Center System Condition Table.
Name of the counter to monitor	Specify the name of the system condition counter you want to monitor. The default is CUIC_REPORT_EXECUTION_FAILED.
Name of the instance(s) to monitor	Specify the name or names of the system condition counter instances you want to monitor. Separate multiple instance names with commas. The default is blank.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the value of the system condition counter for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value of the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value of the system condition counter that must be exceeded before an event is raised. The default is 0.

Parameter	How to Set It
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for the system condition counter for charts and reports. The default is unselected.

UCCX_CUIC_Service_Unavailable

Use the UCCX_CUIC_Service_Unavailable Knowledge Script to monitor the availability of the Cisco Unified Intelligence Center service on a Cisco Unified Contact Center Express (UCCX) Server.

This script raises an event if a counter or instance is not accessible, or if the value of the Intelligence Center system condition table counter if the availability of the Cisco Unified Intelligence Center service exceeds a threshold you set. This script also generates data streams for current and delta counter values.

Resource Object

CiscoUCM_UCCXApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the UCCX_CUIC_Service_Unavailable job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Intelligence Center System Condition Table.
Name of the counter to monitor	Specify the name of the system condition counter you want to monitor. The default is CUIC_SERVICE_UNAVAILABLE.
Name of the instance(s) to monitor	Specify the name or names of the system condition counter instances you want to monitor. Separate multiple instance names with commas. The default is blank.
Monitor Current Value	
Event Notification	

Parameter	How to Set It
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the value of system condition counter for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value of the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for the system condition counter for charts and reports. The default is unselected.

UCCX_CUIC_Unrecoverable_Error

Use the UCCX_CUIC_Unrecoverable_Error Knowledge Script to monitor for internal errors within the reporting server on a Cisco Unified Contact Center Express (UCCX) server which might prevent it from functioning correctly. You might need to restart the UCCX server when this counter is non-zero.

This script raises an event if a counter or instance is not accessible, or if the value of the Intelligence Center system condition table counter for internal errors within the reporting server exceeds a threshold you set. This script also generates data streams for current and delta counter values.

Resource Object

CiscoUCM_UCCXApp

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following 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 the failure of the UCCX_CUIC_Unrecoverable_Error job. The default is 5.
Counter Specifications	
Name of the object to monitor	Specify the name of the object you want to monitor. The default is Intelligence Center System Condition Table.
Name of the counter to monitor	Specify the name of the system condition counter you want to monitor. The default is CUIC_UNRECOVERABLE_ERROR.
Name of the instance(s) to monitor	Specify the name or names of the system condition counter instances you want to monitor. Separate multiple instance names with commas. The default is blank.
Raise event if counter or instance not found?	Select **Yes** to raise an event if the script cannot find the specified counter or instance. The default is Yes.
Event severity when counter or instance not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script cannot find the specified counter or instance. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold?	Select **Yes** to raise an event if the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum current value	Specify the maximum value of the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when current value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the system condition counter exceeds the threshold. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data about the value of the system condition counter for charts and reports. The default is Yes.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold?	Select **Yes** to raise an event if the delta value of the system condition counter exceeds the threshold you set. The default is unselected.
Threshold - Maximum delta value	Specify the maximum delta value for the system condition counter that must be exceeded before an event is raised. The default is 0.
Event severity when delta value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the delta value of the system condition counter exceeds the threshold. The default is 10.

Parameter	How to Set It
Data Collection	
Collect data for delta value?	Select **Yes** to collect data about the delta value for the system condition counter for charts and reports. The default is unselected.

WebPageCheck

Use the WebPageCheck 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, such as 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 from the AppManager ResponseTime for Web module.

Resource Object

CiscoUCM_CMServer

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following 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 the failure of the CiscoUCM_WebPageCheck job. The default is 5.
Is Web server secure?	Select **Yes** to indicate that your Unified Communications web server is a secure web server (HTTPS). The default is Yes.
Application web page customization	
Application web page to monitor (Leave blank for http>//(server)	Enter a comma-separated list of application web pages you want to monitor. The default is blank.
Monitor Admin 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.

Parameter	How to Set It
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 Admin 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 Admin Web Page Round-Trip Time	
Event Notification	
Raise event if Admin Web page round-trip time exceeds threshold?	Select **Yes** to raise an event if the round-trip connection time for the `Admin` 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 Admin Web page 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 `admin` web page exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for Admin Web page round-trip time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the round-trip connection time for the `ccmadmin` web page's during the monitoring period. The default is unselected.
Monitor User Web Page Availability	
Event Notification	
Raise event if Web page is unavailable?	Select **Yes** to raise an event if the `user` 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 User 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 User Web Page Round-Trip Time	
Event Notification	
Raise event if User Web page 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.
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 User Web page 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	

Parameter	How to Set It
Collect data for User Web page 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.
Monitor Application Web Page Availability	
Event Notification	
Raise event if Web page is unavailable?	Select **Yes** to raise an event if the web page is unavailable. The default is unselected.
Event severity when Web page is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event when the web page is unavailable.
Data Collection	
Collect data for Application Web page availability?	Select **Yes** to collect charts and reports. If enabled, data collection returns the application availability. The default is unselected.
Monitor Application Web Page Round-Trip Time	
Event Notification	
Raise an event if Application Web page round-trip time exceeds threshold?	Select **Yes** to raise an event if the Application web page round-trip time exceeds the threshold.
Threshold -- Maximum round-trip time	Specify the maximum round-trip time, from 0 to 100 ms. The default is 100.
Event severity when Application Web page 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 Application web page exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for Application Web page round-trip time?	Select **Yes** to collect charts and reports. If enabled, data collection returns the Application web page round-trip time. The default is unselected.

Recommended Knowledge Script Groups

The following Knowledge Scripts are members of the CiscoUCM recommended Knowledge Script Group (KSG):

- HealthCheck
- SystemUpTime
- SystemUsage

The following Knowledge Scripts are members of the CiscoUCM_CUPS recommended Knowledge Script Group (KSG):

- CUPS_ActiveCalendarSubscriptions
- CUPS_ActiveJsmSessions
- CUPS_IncomingSIPSubscriptions
- CUPS_JsmFailedLogins

- CUPS_JsmMsgsInLastSlice
- CUPS_JsmOnlineUsers
- CUPS_JsmTotalMessagePackets
- CUPS_OutgoingSIPSubscriptions
- CUPS_TotalAdhocChatRooms
- CUPS_TotalPersistentChatRooms
- HealthCheck

The following Knowledge Scripts are members of the CiscoUCM_UCCX recommended Knowledge Script Group (KSG):

- UCCX_CUIC_Database_Unavailable
- UCCX_CUIC_DB_Replication_Failed
- UCCX_CUIC_Live_Data_Feeds_Stopped
- UCCX_CUIC_Report_Execution_Failed
- UCCX_CUIC_Service_Unavailable
- UCCX_CUIC_Unrecoverable_Error

The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the KSG on a 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 CiscoUCM KSGs provide a "best practices" usage of AppManager for monitoring your Unified Communications environment. You can use these KSGs 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 Navigation pane or 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 CiscoUCM tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoUCM 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 CiscoUCM KSGs and want to restore it to its original form, you can reinstall AppManager for Cisco Unified Communications Server on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoUCM\RECOMMENDED_CiscoUCM` directory.