NetIQ® AppManager® for Cisco Unity Connection

Management Guide

May 2014

Legal Notice

Contents

About this Book and the Library

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

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

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

User Guide for AppManager Control Center

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

Administrator Guide for AppManager

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

Upgrade and Migration Guide for AppManager

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

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

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

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

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 Introducing AppManager for Cisco Unity Connection

Cisco Unity Connection is a scalable and full-featured voice and unified messaging application. As part of the Cisco AVVID (Architecture for Voice, Video, and Integrated Data) environment, Cisco Unity Connection works with Cisco Unified Communications Manager to provide advanced capabilities that unify data and voice, ensuring a smooth transition to IP telephony.

Cisco Unity Connection provides integrated messaging that allows users to access and manage messages and calls from anywhere at any time, regardless of device or media type. Users can listen to e-mail over the phone, check voice messages from their Microsoft Outlook Inbox, and forward faxes to any fax machine. In addition, the users can access messages in the sequence they prefer and can set up their own rules regarding management of callers.

Cisco Unity Connection keeps the messages highly secure and they cannot be played by someone outside the organization.

AppManager for Cisco Unity Connection helps you monitor Cisco Unity Connection application services and system resources on the Unity Connection server.

This module includes the following features:

- Monitors the system health and performance of all Unity Connection servers from a central location, including the Unity Connection application
- Monitors the incoming and outgoing call activity
- Monitors the CPU and memory utilization
- Monitors the usage of voice and text-to-speech ports
- Monitors the server ports that are available for use
- Monitors the active subscriber sessions
- Monitors the status of the Unity Connection servers

Counting AppManager Licenses

AppManager for Cisco Unity Connection consumes one AppManager license for each user configured on a Cisco Unity Connection system. The number of configured users is monitored using the Cisco Unity Connection Provisioning Interface during Discovery.

2 Installing AppManager for Cisco Unity Connection

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

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

2.1 System Requirements

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

AppManager for Cisco Unity Connection has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, on the agent computers through which you want to monitor Cisco Unity Connection servers (AppManager proxy agents), and on all console computers	7.0 or later Support for Windows Server 2008 on AppManager 7.x requires AppManager Windows Agent hotfix 71704 or later. For more information, see the AppManager Suite Hotfixes page.
Microsoft Windows operating system on the proxy agent computer	One of the following: ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (64-bit)
AppManager for Microsoft Windows module installed on the AppManager repository (QDB), on all proxy agents, and on all console computers	7.6.170.0 or later. For more information, see the AppManager Module Upgrades & Trials page.
Cisco Unity Connection on the computer that you want to monitor (through proxy agents)	10.0, 9.1, 9.0, 8.6, 8.5, or 8.0
Microsoft .NET Framework on proxy agent computers	4.0 or later

2.2 Installing the Module

Run the module installer on the Cisco Unity Connection 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-CiscoUC-8.x.x.0.msi` module installer from the `AM70_CiscoUC_8.x.x.0` self-extracting installation package on the AppManager Module Upgrades & Trials page.

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

- Log in to the server using the account named Administrator. Then run the module installer `CiscoUC.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 `CiscoUC.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 on a remote computer where an agent is installed. For more information, see Section 2.3, “Deploying the Module with Control Center,” on page 13. 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.
   - **All prerequisites are met:** In this scenario, the installer will install the agent components.

4 To install the Knowledge Scripts into the QDB:

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

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

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

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

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

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

9. Configure Cisco Unity Connection credentials in AppManager Security Manager for this module. For more information, see Section 2.5, "Configuring AXL Passwords in Security Manager," on page 14.
10. Export the HTTPS certificate from the Cisco Unity Connection website and save it to the trusted folder in the AppManager machine. For more information, see Section 2.6, "Accessing Cisco Unity Connection Resources," on page 15.
11. Run the **Discovery_CiscoUC** Knowledge Script on all agent computers where you installed the module to discover the Cisco Unity Connection resources. For more information, see Section 2.7, "Discovering Cisco Unity Connection Resources," on page 16.

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

2.3 Deploying the Module with Control Center

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

2.3.1 Deployment Overview

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

To deploy the module on an agent computer:

1. Verify the default deployment credentials.
2. Check in an installation package. For more information, see Section 2.3.2, "Checking In the Installation Package," on page 13.
3. Configure an e-mail address to receive notification of a deployment.
4. Create a deployment rule or modify an out-of-the-box deployment rule.
5. Approve the deployment task.
6. View the results.

2.3.2 Checking In the Installation Package

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

To check in a module installation package:

1. Log on to Control Center using an account that is a member of a user group with deployment permissions.
2. Navigate to the **Deployment** tab (for AppManager 8.x) or **Administration** tab (for AppManager 7.x).
3. In the Deployment folder, select **Packages**.
4. On the Tasks pane, click **Check in Deployment Packages** (for AppManager 8.x) or **Check in Packages** (for AppManager 7.x).

5 Navigate to the folder where you saved `AM70-CiscoUC-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.

2.4 Silently Installing the Module

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

```
msiexec.exe /i "AM70-CiscoUC-8.x.x.0.msi" /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-CiscoUC-x.x.x.0.msi.log"
```

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

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

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

Windows authentication:

```
AM70-CiscoUC-8.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_SQLSVR_WINAUTH=1
MO_SQLSVR_NAME=[SQL Server Name] MO_QDBNAME=[AM-Repository Name]
```

SQL authentication:

```
AM70-CiscoUC-8.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_SQLSVR_WINAUTH=0
MO_SQLSVR_USER=[SQL login] MO_SQLSVR_PWD=[SQL Login Password] MO_SQLSVR_NAME=[SQL
Server Name] MO_QDBNAME=[AM-Repository Name]
```

2.5 Configuring AXL Passwords in Security Manager

The Cisco Unified CM Serviceability APIs (SXML), a Cisco application programming interface, enable access to the Unity Connection server. Configure the password in AppManager Security Manager before running the Discovery_CiscoUC Knowledge Script.

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

Field	Description
Label	CiscoUC_AXL

Field	Description
Sub-label	Indicates whether the SXML information will be used for a single or for all Unity Connection servers. Specify one of the following locations: ◆ For a single server, provide the IP address or host name of the server. ◆ For all servers, type `default`.
Value 1	User ID that has the authority to use the API. In most cases, the Administrator user has this authority.
Value 2	Password associated with the user ID entered in *Value 1*.
Value 3	Use this field only if you used Cisco Unified Communications Manager Administration to change the number of the HTTPS port that the proxy agent computer uses to connect to the Communications Manager server. Type the new secure port number. Leave this field blank to use the default port number, 8443.
Extended application support	Required field. Encrypts the user name and password in Security Manager.

2.6 Accessing Cisco Unity Connection Resources

To access the Cisco Unity Connection resources, you must set up the browsers correctly on an administrator workstation. When you discover the Cisco Unity Connection resources, it might fail if the required HTTPS certificate is not saved to the trusted folder.

The system issues the certificate by using the host name. If you attempt to access a Web application by using the IP address, the Security Alert dialog box appears, even though you installed the certificate on the client.

Exporting the Certificate

This section describes how you can export the certificate from the Cisco Unity Connection website.

To export the certificate from the Cisco Unity Connection website:

1. Use Internet Explorer to browse to the Cisco Unity Connection Server. A security certificate alert page is displayed.
2. Click **Continue to this website (not recommended)**. The Cisco Unity Connection Administration Console is displayed.
3. Click **Certificate error**, which is to the right of the Address (URL) field, and then click **View Certificates**. The Certificate dialog box is displayed.
4. Click the **Details** tab, and then click **Copy to file** to open the Certificate Export Wizard.
5. Click **Next** twice.
6. Click **Browse** and browse to a location where you want to save the certificate, and then click **Save**.
7. Click **Next** and then click **Finish**.

8 Click **OK** twice.

9 Close the Cisco Unity Connection Administration Console.

Saving the Certificate to the Trusted Folder

This section describes how to save the certificate to the trusted folder.

To save the certificate to the trusted folder:

1 On the AppManager computer, open a Microsoft Management Console (mmc).

2 Select **File > Add/Remove Snap-in** to open the Add or Remove Snap-ins dialog box.

3 Click **Certificates** in the **Available snap-ins** list, and then click **Add**.

4 Select **Computer Account**, click **Next**, and then click **Finish**.

5 Click **OK** to close the Add or Remove Snap-ins dialog box.

6 Expand **Certificates** under **Console Root**, right-click **Trusted Root Certificate Authorities**, and then select **All Tasks > Import**.

7 Click **Browse** and browse to the location where you saved the certificate.

8 Select the certificate that you imported, and then click **Open**.

9 Click **Next**.

10 Click **Place All Certificates in the Following Store** and then click **Next**.

11 Click **Finish** and then click **OK**.

2.7 Discovering Cisco Unity Connection Resources

Use the Discovery_CiscoUC Knowledge Script to discover Cisco Unity Connection resources. You need to either specify a list of primary Unity Connection servers, separated by a comma, or specify the complete path to a file that contains a list of primary servers. The Cisco AXL Web service, Tomcat service, and SOAP API services must be active on all the servers in the cluster.

Prerequisite

Configure the AXL password in AppManager Security Manager before discovering Cisco Unity Connection resources. For more information see Section 2.5, "Configuring AXL Passwords in Security Manager," on page 14.

By default, this script runs once a week for each server.

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

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the Discovery_CiscoUC job fails. The default is 5.
Full path to file with list of primary Unity Connection servers	Specify the full path to the file that has the list of primary Unity Connection servers through which you want to discover other Cisco Unity Connection objects.

Parameter	How to Set It
Comma-separated list of primary Unity Connection servers.	Specify the name of the primary Unity Connection servers in the cluster, separated by commas, through which you want to discover other Cisco Unity Connection objects. For example: primarycluster1,primarycluster2,primarycluster4
Raise event if discovery succeeds?	Set to **Yes** to raise an event when the discovery job succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the discovery job succeeds. The default is 25.
Raise event if discovery succeeds with warnings?	Set to **Yes** to raise an event when the discovery job succeeds with warnings. The default is Yes.
Event severity when discovery succeeds with warnings	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the discovery job succeeds with warnings. The default is 15.
Raise event if discovery fails?	Set to **Yes** to raise an event when the discovery job fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the discovery job fails. The default is 5.

3 Cisco Unity Connection Knowledge Scripts

AppManager for Cisco Unity Connection provides the following Knowledge Scripts for monitoring Cisco Unity Connection resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AutoFailover	Monitors the Connection Server Role Manager logs for AutoFailover or AutoFailback events.
DRFStatus	Monitors the Cisco Unity Connection Disaster Recovery Framework (DRF) status.
GeneralCounter	Monitors a user-specified counter on a Unity Connection server.
ListUtil	Lists the counters, logs, and services on a Unity Connection server.
Logs	Monitors the user-specified Unity Connection server logs for matching text.
NumberofLogons	Monitors the number of active subscriber sessions for a Unity Connection server.
PortStatus	Monitors whether the Unity Connection server ports are available for use.
ServiceDown	Monitors the status of Unity Connection services.
SystemCPU	Monitors the percentage of CPU utilization for a Unity Connection server.
SystemMem	Monitors the physical and virtual memory utilization for a Unity Connection server.
VoicePortsinUse	Monitors the number of Unity Connection voice ports that are being used by callers.

3.1 AutoFailover

Use this Knowledge Script to monitor the Connection Server Role Manager logs for AutoFailover and AutoFailback events.

Cisco Unity Connection servers are a group of independent computers that work together to increase the availability of applications and services. If one of the cluster nodes fails, another node begins to provide service, and this process is called *failover*. Users experience minimum disruptions in service during a failover. A failover operation is followed by a *failback* operation, a process of returning the server to its original state. Any failover or failback event generates a set of logs.

This Knowledge Script helps you monitor the following failover or failback events:

- **AutoFailoverSucceeded:** Monitors the log entries that are created when automatic failover is successful.
- **AutoFailoverFailed:** Monitors the log entries that are created when automatic failover fails for any reason.
- **AutoFailbackSucceeded:** Monitors the log entries that are created when automatic failback is successful.
- **AutoFailbackFailed:** Monitors the log entries that are created when automatic failback fails for any reason

This script raises an event if it finds the failover or failback events, or cannot read the logs for failover or failback events. In addition, this script generates data streams for the number of failover or failback events.

Resource Object

Cisco Unity Connection server

Default Schedule

By default, this script runs every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the AutoFailover job fails. The default is 5.
Raise event if logs cannot be read?	Select **Yes** to raise an event if the script cannot read the failover or failback events in the logs. The default is Yes.
Event severity when logs cannot be read	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot read the failover or failback events in the logs. The default is 5.

Description	How to Set It
Raise event if lines are found?	Select **Yes** to raise an event if the script finds the failover or failback events in the log. The default is Yes.
Event severity when lines are found	Set the severity level, from 1 to 40, to indicate the importance of the event that is raised when the script finds the failover or failback events in the logs. The default is 15.
Raise event if no lines are found?	Select **Yes** to raise an event if the script does not find the failover or failback events in the logs. The default is unselected.
Event severity when no lines are found	Set the severity level, from 1 to 40, to indicate the importance of the event that is raised when the script does not find the failover or failback events in the logs. The default is 15.
Text to find	Select the failover or failback events that you want to monitor in the logs. You can choose from AutoFailoverSucceeded, AutoFailoverFailed, AutoFailbackSucceeded, and AutoFailbackFailed. The default is AutoFailoverSucceeded.
Log Name	Specify the name of the log to search for failover or failback events. The default log name is Connection Server Role Manager.
Scan entire log on first iteration?	Select **Yes** if you want to scan all entries in the failover or failback event logs during the first iteration of the Knowledge Script. The scanning depends on the number of hours specified in the *Previous hours to search for log* parameter. If you select Yes, this Knowledge Script scans the failover or failback events log for old failover or failback events during the first iteration, depending on the value specified in the *Previous hours to search for log* parameter. The default is Yes.
Previous hours to search for log	Specify how far back in the logs you want to search for failover or failback events during the first iteration of this script. For example, type 8 for the past 8 hours, 50 for the past 50 hours, and so on. By default, this Knowledge Script searches the logs from the previous 24 hours. You can specify a minimum of 1 hour and maximum of 100 hours.
Monitor Number of Lines Found	
Event Notification	
Raise event if number of lines found exceeds threshold?	Select **Yes** to raise an event if the number of failover or failback events exceeds the threshold. The default is Yes.
Threshold - Maximum number of lines found	Specify the maximum number of failover or failback events that the script may find between the last and current interval before it raises an event. The default is 0.
Event severity when number of lines found exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the number of failover or failback events exceeds the threshold. The default is 10.
Data Collection	
Collect data for number of lines found	Select **Yes** to collect data for charts and reports for the number of failover or failback events. The default is unselected.

3.2 DRFStatus

Use this Knowledge Script to monitor the Cisco Unity Connection Disaster Recovery Framework (DRF) backup status. By default, this Knowledge Script monitors the DRF backup status since the last iteration. This script can monitor the previous days' backups on the first iteration by setting the *Number of previous days to monitor on first iteration* parameter to a non-zero value.

This script raises events if it does not find a backup status, finds any successful or failed backup status, or finds one or more failed backups. In addition, this script generates data streams for the number of failed backups since the last iteration and the total number of backups on the DRF backup server.

Resource Object

Cisco Unity Connection server

Default Schedule

By default, this script runs **daily**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the DRFStatus job fails unexpectedly. The default is 5.
Raise event if DRF status cannot be determined?	Select **Yes** to raise an event if the script cannot determine the DRF status for any reason. The default is Yes.
Event severity when DRF status cannot be determined	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot determine the DRF status. The default is 5.
Raise event if no backups found?	Select **Yes** to raise an event if the script does not find a DRF backup. The default is Yes.
Event severity when no backups found	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script does not find the DRF backups. The default is 15.
Raise event if backups found?	Select **Yes** to raise an event if the script finds one or more DRF backups. The default is unselected.
Event severity when backups found	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script finds one or more DRF backups. The default is 15.
Raise event if failed backups found?	Select **Yes** to raise an event if the script finds a failed DRF backup. The default is Yes.

Description	How to Set It
Event severity when failed backups found	Set the event severity level, from 1 to 40, to indicate the importance of the event that is raised when the script finds the failed DRF backups. The default is 15.
Number of previous days to monitor on first iteration	Specify the value between 0 and 999 to specify the number of previous days that you want to monitor the DRF backup status on the first iteration. The default is 0. If the value is set to 0, this Knowledge Script monitors the DRF backups from the previous 24 hours.
Monitor Number of Backups	
Event Notification	
Raise event if number of backups exceeds threshold?	Select **Yes** to raise an event if the number of DRF backups exceeds the threshold. The default is unselected.
Threshold - Maximum number of backups	Specify the maximum number of successful backups that can exist on the DRF backup server before the script raises an event. The default is 0.
Event severity when number of backups exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the number of successful backups exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of backups?	Select **Yes** to collect data for charts and reports on the number of successful backups on the DRF backup server. The default is unselected.
Monitor Number of Failed Backups	
Data Collection	
Collect data for number of failed backups?	Select **Yes** to collect data for charts and reports on the number of failed backups since the previous iteration. The default is unselected.

3.3 GeneralCounter

Use this Knowledge Script to monitor a user-specified counter on a Unity Connection server.

This script raises events if it cannot obtain a counter, or the counter's value exceeds or falls below the threshold. In addition, this script generates data streams for the counter's value.

Resource Object

Cisco Unity Connection server

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the GeneralCounter job fails. The default is 5.
Raise event if counter cannot be obtained?	Select **Yes** to raise an event if the script cannot obtain a counter for any reason. The default is Yes.
Event severity when counter cannot be obtained	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot obtain a counter. The default is 5.
Counter's full path	Specify the counter's path, entered as [CounterObject\CounterName] or [CounterObject(Instance)\CounterName]. For example, `System\Total Processes` or `Processor(_Total)\User Percentage`.
Name of counter to use in messages	Specify the name of the counter that you want to use in messages. Leave blank if you want to use the counter's path.
Counter units	Specify the counter unit as a percentage, KB, or number. The default setting is no unit.
Monitor Counter's Current Value	
Event Notification	
Raise event if threshold is crossed?	Select **Yes** to raise an event if the counter value exceeds or falls below the threshold. The default is Yes.
Minimum threshold	Select **Enable** to raise an event if the value of the counter falls below the minimum threshold. The default is Enable.
Threshold - Minimum counter's current value	Specify the minimum threshold value for the counter. The default is 0.

Description	How to Set It
Event severity when counter’s current value falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of the event that is raised when the value of the counter falls below the minimum threshold. The default is 15.
Maximum threshold	Select **Enable** to raise an event if the value of the counter exceeds the maximum threshold. The default is Enable.
Threshold - Maximum counter’s current value	Specify the maximum threshold value for the counter. The default is 0.
Event severity when counter’s current value exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event that is raised when the value of the counter exceeds the maximum threshold. The default is 15.
Data Collection	
Collect data for counter’s current value	Select **Yes** to collect data for charts and reports about the current value of the counter. The default is unselected.

3.4 ListUtil

Use this Knowledge Script to list the counters, logs, or services on a Cisco Unity Connection server. This script raises events if it obtains a list or cannot obtain a list.

Resource Object

Cisco Unity Connection server

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the ListUtil job fails. The default is 5.
Raise event if list cannot be obtained?	Select **Yes** to raise an event if the script cannot obtain counters, logs, or services lists. The default is Yes.
Event severity when list cannot be obtained	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot obtain the selected list. The default is 5.
Raise event if list has been obtained?	Select Yes to raise an event if the script obtains the selected list.

Description	How to Set It
Event severity when list has been obtained	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script obtains the selected list. The default is 35.
Select list	Select the type of list you want to display. The options available are Counters, Logs, or Services. The default is Counters.

3.5 Logs

Use this Knowledge Script to search the user-defined Cisco Unity Connection logs for matching text. This Knowledge Script looks for lines with matching text in the user-specified logs.

This script raises an event if it cannot read the logs, finds matching lines, or does not find matching lines. This script also raises an event if the number of matching lines within the specified number of hours exceeds the threshold. In addition, this script generates data streams for the number of matching lines.

Resource Object

Cisco Unity Connection server

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the Logs job fails. The default is 5.
Raise event if logs cannot be read?	Select **Yes** to raise an event if the script cannot read the logs.
Event severity when logs cannot be read	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot read the logs. The default is 5.
Raise event if matching lines are found?	Select **Yes** to raise an event if the script finds matching lines in the logs. The default is Yes.
Event severity when matching lines are found	Set the severity level, from 1 to 40, to indicate the importance of the event that is raised when the script finds the matching lines in the logs. The default is 15.
Raise event if no matching lines are found?	Select **Yes** to raise an event if the script does not find the matching lines in the logs. The default is unselected.

Description	How to Set It
Event severity when no matching lines are found	Set the severity level, from 1 to 40, to indicate the importance of the event that is raised when the script does not find the matching lines in the logs. The default is 15.
Text to find	Specify a comma-separated list of regular expressions (as defined by Microsoft) to find in the specified Unity Connection log. The script raises an event when it finds one of more lines that match with one or more of the regular expressions.
Log Name	Specify the name of the log to search for the regular expressions. The default log name is `Cisco Syslog Agent`.
Scan entire log on first iteration	Select **Yes** if you want to scan all entries in the user-specified Unity Connection log during the first iteration of the Knowledge Script. The scanning depends on the number of hours specified in the *Previous hours to search for log* parameter. If you select Yes, this Knowledge Script scans the user-specified Unity Connection log for matching lines during the first iteration, depending on the value specified in the *Previous hours to search for log* parameter. The default is selected.
Previous hours to search for log	Specify how far back in the logs you want to search for matching lines during the first iteration of this script. For example, type 8 for the past 8 hours, 50 for the past 50 hours, and so on. By default, this Knowledge Script searches the logs from the previous 24 hours. You can specify a minimum of 1 hour and a maximum of 100 hours.
Monitor Number of Lines Found	
Event Notification	
Raise event if number of lines found exceeds threshold?	Select **Yes** to raise an event if the number of lines that the script finds exceeds the threshold. The default is Yes.
Threshold - Maximum number of lines found	Specify the maximum number of new lines that can be found since the last iteration before the script raises an event. The default is 0.
Event severity when number of lines found exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the number of matching lines exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of lines found	Select **Yes** to collect data for charts and reports on the number of matching lines. The default is unselected.

3.6 NumberofLogons

Use this Knowledge Script to monitor the number of active subscriber sessions on a Cisco Unity Connection server. This script raises an event if the maximum number of active subscriber sessions exceeds the threshold. In addition, this script generates data streams for the number of active subscriber sessions.

Resource Object

Cisco Unity Connection server

Default Schedule

By default, this script runs every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the NumberofLogons job fails. The default is 5.
Raise event if number of active subscriber sessions cannot be determined?	Select **Yes** to raise an event if the script cannot determine the number of active subscriber sessions. The default is Yes.
Event severity when number of active subscriber sessions cannot be determined	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot determine the number of active subscriber sessions. The default is 5.
Monitor the Number of Active Subscriber Sessions	
Event Notification	
Raise event if the number of active subscriber sessions exceeds threshold?	Select **Yes** to raise an event if the number of active subscriber sessions exceeds the threshold. The default is Yes.
Threshold - Maximum number of active subscriber sessions	Specify the maximum number of subscriber sessions that can be active before the script raises an event. Enter a number appropriate for the server you are monitoring. The default is 0.
Event severity when the number of active subscriber sessions exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the number of active subscriber sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data?	Select **Yes** to collect data for charts and reports on the number of active subscriber sessions. The default is unselected.

3.7 PortStatus

Use this Knowledge Script to monitor the utilization of Cisco Unity Connection voice ports on a Cisco Unity Connection server on a per-port basis. This script raises an event if a voice port in use exceeds the specified percentage utilization during an iteration. In addition, this script generates data streams for voice port utilization.

Resource Object

Cisco Unity Connection server

Default Schedule

By default, this script runs every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the PortStatus job fails. The default is 5.
Raise event if voice port utilization cannot be determined?	Select **Yes** to raise an event if the script cannot determine the voice port utilization of the Cisco Unity Connection server. The default is Yes.
Event severity when voice port utilization cannot be determined	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot determine the voice port utilization. The default is 5.
Exclude voice ports	List the voice ports, separated by commas, to exclude when the PortStatus job is running. By default, this script includes all the voice ports.
Monitor Voice Port Utilization	
Data Collection	
Collect data for voice port utilization	Select **Yes** to collect data for charts and reports on the voice port utilization. The default is unselected. The utilization data streams are expressed in seconds.
Event Notification	
Raise event if voice port utilization exceeds threshold?	Select **Yes** to raise an event if the maximum percentage of voice port utilization exceeds the threshold. The default is Yes.
Event severity when voice port utilization exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the voice port utilization exceeds the threshold. The default is 15.

Description	How to Set It
Threshold - Maximum voice port percent utilization	Specify the maximum utilization percentage of a voice port before the script raises an event. The default is 80%. The utilization percentage is based on the elapsed time between job iterations.

3.8 ServiceDown

Use this Knowledge Script to monitor the status of Cisco Unity Connection services to determine if any service is down. This script raises an event if a service is not running. You can use exclusion lists to exclude any services, which will prevent the script from raising events when those services are not started. In addition, this script generates data streams for service availability.

Resource Objects

- Cisco Unity Connection server
- Cisco Unity Connection service

Default Schedule

The default interval for this script is every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the ServiceDown job fails. The default is 5.
Raise event if service status cannot be obtained?	Select **Yes** to raise an event if the script cannot obtain the Cisco Unity Connection service status.
Event severity when service status cannot be obtained	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot obtain the Cisco Unity Connection service status. The default is 5.

Description	How to Set It
Dynamically observe services	Select **Yes** to observe the Cisco Unity Connection services dynamically. The default is Yes. If this parameter is set to No, then this Knowledge Script monitors only the services on which you run the script. If this parameter is set to Yes, the Knowledge Script ignores the individual services on which you run the script and instead monitors all of the activated services on the servers. NetIQ Corporation recommends a setting of Yes, which allows you to monitor new services in future releases of Cisco Unity Connection, without modifying this Knowledge Script. **NOTE:** If you set this parameter to Yes, you must select a server in the Knowledge Script's **Object** tab. This Knowledge Script does nothing if you set this parameter to Yes and you do not select a server.
Exclude services	List the Unity Connection services that you do not want to monitor. Separate multiple services with commas (no spaces).
Exclude reason codes	List the reason codes to ignore if a service is not running. If a service is not running due to one of the listed reasons, the script does not raise an event. Separate multiple reason codes with commas (no spaces).
Exclude services that are not activated	Select **Yes** to exclude Cisco Unity Connection services that are not activated. The default is Yes.
Monitor Service Availability	
Event Notification	
Raise event if service is down?	Select **Yes** to raise an event if a Cisco Unity Connection service is down. The default is Yes.
Event severity when service is down	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when a Unity Connection service is down. The default is 15.
Data Collection	
Collect data for service availability	Select **Yes** to collect data for charts and reports on the service availability. The default is **No**. In the data stream, 100 indicates that the service is running, and 0 indicates that the service is not running.

3.9 SystemCPU

Use this Knowledge Script to monitor the percentage of CPU utilization by the Cisco Unity Connection server. This script raises an event if it cannot determine the CPU utilization, or if the percentage of CPU utilization exceeds the threshold. In addition, this script generates data streams for the percentage of CPU utilization.

Resource Object

Cisco Unity Connection server

Default Schedule

The default interval for this script is every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the SystemCPU job fails. The default is 5.
Raise event if CPU percent utilization cannot be determined?	Select **Yes** to raise an event if the script cannot determine the percentage of CPU utilization. The default is Yes.
Event severity when CPU percent utilization cannot be determined	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot determine the percentage of CPU utilization. The default is 5.
Monitor CPU Percent Utilization	
Event Notification	
Raise event if CPU percent utilization exceeds threshold?	Select **Yes** to raise an event if the percentage of CPU utilization exceeds the threshold. The default is Yes.
Threshold - Maximum CPU percent utilization	Specify the maximum CPU utilization that can occur before the script raises an event. The default is 90%.
Event severity when maximum CPU percent utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event when the percentage of CPU utilization exceeds the threshold. The default is 15.
Data Collection	
Collect data for maximum CPU percent utilization	Select **Yes** to collect data for charts and reports on the percentage of CPU utilization. The default is unselected.

3.10 SystemMem

Use this Knowledge Script to monitor the physical and virtual memory usage by the Cisco Unity Connection server. This script raises an event if it cannot determine the memory usage, or the physical or virtual memory usage exceeds a threshold. In addition, this script generates data streams for the physical and virtual memory usage.

Resource Object

Cisco Unity Connection server

Default Schedule

The default interval for this script is every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the SystemMem job fails. The default is 5.
Raise event if system memory usage cannot be determined?	Select **Yes** to raise an event if the script cannot determine the system memory usage for a Cisco Unity Connection server. The default is Yes.
Event severity when system memory usage cannot be determined	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot determine the Cisco Unity Connection system memory usage. The default is 5.
Monitor Maximum Physical Memory Usage	
Event Notification	
Raise event if maximum physical memory usage exceeds threshold?	Select **Yes** to raise an event if the physical memory usage for a Cisco Unity Connection server exceeds the threshold. The default is Yes.
Threshold - Maximum physical memory usage	Specify the maximum physical memory usage that can occur before the script raises an event. The default is 90%.
Event severity when maximum physical memory usage exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the physical memory usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for maximum physical memory usage	Select **Yes** to collect data for charts and reports on the physical memory usage. The default is unselected.
Monitor Maximum Virtual Memory Usage	
Event Notification	

Description	How to Set It
Raise event if maximum virtual memory usage exceeds threshold?	Select **Yes** to raise an event if the virtual memory utilization exceeds the threshold. The default is Yes.
Threshold - Maximum virtual memory usage	Specify the maximum virtual memory utilization that can occur before the script raises an event. The default is 90%.
Event severity when maximum virtual memory usage exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the virtual memory utilization exceeds the threshold. The default is 15.
Data Collection	
Collect data for maximum virtual memory usage	Select **Yes** to collect data for charts and reports on the virtual memory utilization. The default is unselected.

3.11 VoicePortsinUse

Use this Knowledge Script to monitor the number of Cisco Unity Connection voice ports that are in use, the percentage of voice ports in use, and the number of voice ports that are locked. This script raises an event if the number of voice ports in use or voice ports locked exceeds a threshold. In addition, this script generates data streams for the number of voice ports in use and the number of voice ports that are locked.

You can use this script to identify episodes of high usage, and to determine whether there are sufficient voice port licenses on the Cisco Unity Connection server. In addition, you can use this script to determine the availability of voice ports, and to determine if are any ports cannot be used because they are locked.

Resource Object

Cisco Unity Connection server

Default Schedule

The default interval for this script is every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the VoicePortsinUse job fails. The default is 5.
Raise event if voice ports in use cannot be determined?	Select **Yes** to raise an event if the script cannot determine the voice ports of the Cisco Unity Connection server that are in use. The default is Yes.

Description	How to Set It
Event severity when voice ports in use cannot be determined	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the script cannot determine the voice ports of the Cisco Unity Connection server that are in use. The default is 5.
Monitor Number of Voice Ports in Use	
Event Notification	
Raise event if number of voice ports in use exceeds threshold?	Select **Yes** to raise an event if the number of voice ports in use exceeds the threshold. The default is unselected.
Threshold - Maximum number of voice ports in use	Specify the maximum number of voice ports that can be in use before the script raises an event. The default is 0.
Event severity when number of voice ports in use exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the number of voice ports that are in use exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of voice ports in use	Select **Yes** to collect data for charts and reports about the number of voice ports that are in use. The default is unselected.
Monitor Percentage Voice of Ports in Use	
Event Notification	
Raise event if percentage of voice ports in use exceeds threshold?	Select **Yes** to raise an event if the percentage of voice ports in use exceeds the threshold. The default is unselected.
Threshold - Maximum percentage of voice ports in use	Specify the maximum percentage of voice ports that can be in use before the script raises an event. The default is 80%.
Event severity when percentage of voice ports in use exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the percentage of voice ports that are in use exceeds the threshold. The default is 15.
Data Collection	
Collect data for percentage of voice ports in use	Select **Yes** to collect data for charts and reports about the percentage of voice ports that are in use. The default is unselected.
Monitor Voice Ports Locked	
Event Notification	
Raise event if locked voice ports exceeds threshold?	Select **Yes** to raise an event if the number of voice ports that are locked exceeds the threshold. The default is Yes.
Threshold - Maximum locked voice ports	Specify the maximum number of voice ports that can be locked before the script raises an event. The default is 0.
Event severity when locked voice ports exceeds threshold	Set the severity level, from 1 to 40, to reflect the importance of the event that is raised when the number of voice ports that are locked exceeds the threshold. The default is 15.
Data Collection	
Collect data for locked voice ports	Select **Yes** to collect data for charts and reports about the number of voice ports that are locked. The default is unselected.