

NetIQ[®] AppManager[®] for Cisco Unity

Management Guide

February 2012



Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2009 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

Contents

About this Book and the Library	5
About NetIQ Corporation	7
1 Introducing AppManager for Cisco Unity	9
2 Installing AppManager for Cisco Unity	11
2.1 System Requirements	11
2.2 Installing the Module	12
2.3 Silently Installing the Module	12
2.4 Upgrading Knowledge Script Jobs	13
3 CiscoUnity Knowledge Scripts	15
3.1 CU_BackupAndRestoreStatus	17
3.2 CU_CallActivity	17
3.3 CU_CpuHigh	19
3.4 CU_CurrentDiskQueueLength	20
3.5 CU_EventLog	21
3.6 CU_FailoverStatus	23
3.7 CU_HealthCheck	24
3.8 CU_LicenseCompliance	25
3.9 CU_MemoryHigh	26
3.10 CU_MessageDeliveryFailure	29
3.11 CU_MessageStoreAvailability	30
3.12 CU_MessageStoreLock	31
3.13 CU_NumberOfLogons	32
3.14 CU_PortStatus	32
3.15 CU_ProcessorQueueLength	33
3.16 CU_RestartService	34
3.17 CU_Silence	35
3.18 CU_SystemUsage	36
3.19 CU_TTSPortsInUse	37
3.20 CU_UMRServiceHung	38
3.21 CU_VoicePortsInUse	39
3.22 IIS_CpuHigh	39
3.23 IIS_HealthCheck	40
3.24 IIS_KillTopCPUProcs	41
3.25 IIS_MemoryHigh	42
3.26 IIS_RestartServer	43
3.27 IIS_ServiceUpTime	44
3.28 Report_PortUsage	44
3.29 Report_ServicesAvailability	46
3.30 Report_SystemUsage	47
3.31 SQL_Accessibility	49
3.32 SQL_CPUUtil	50
3.33 SQL_DataGrowthRate	51

3.34	SQL_DBGrowthRate	52
3.35	SQL_MemUtil	53
3.36	SQL_RestartServer	54
3.37	Recommended Knowledge Script Groups	55
3.38	Discovery_CiscoUnity	56

About this Book and the Library

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

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

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

User Guide for AppManager Control Center

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

Administrator Guide for AppManager

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

Upgrade and Migration Guide for AppManager

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

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

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

The AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

About NetIQ Corporation

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

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

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

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

1 Introducing AppManager for Cisco Unity

Cisco Unity 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 works with Cisco Unified Communications Manager to provide advanced capabilities that unify data and voice, ensuring a smooth transition to IP telephony.

Cisco Unity allows users to access and manage messages and calls from anywhere at anytime, 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.

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

The following are just a few of the highlights of monitoring Cisco Unity with AppManager:

- ♦ Monitors system health and performance of all Unity servers from a central location, including the Unity application, SQL, IIS, system resources, and mailbox activity
- ♦ Monitors incoming and outgoing call activity
- ♦ Monitors CPU and memory usage
- ♦ Monitors usage of voice and text-to-speech ports
- ♦ Monitors the number of processes in queue for the Processor
- ♦ Allows you to launch Cisco Unity Administration Web pages from the Extensions menu of the AppManager Operator Console

AppManager consumes one license for each discovered Cisco Unity mailbox.

2 Installing AppManager for Cisco Unity

This chapter lists system requirements and describes how to install AppManager for Cisco Unity. Only the following AppManager modules should be installed on a Cisco Unity server:

- ◆ Cisco Unity (qciscoUnitya4.dll)
- ◆ CIM (qcima4.dll)
- ◆ Dell (qdella4.dll)
- ◆ IBM Netfinity (qnfda4.dll)
- ◆ NT (qnta4.dll)
- ◆ WTS (qwtsa4.dll)
- ◆ SQL (qsqla4.dll)

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 has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the repository, agent, and console computers	7.0 or later
Microsoft operating system installed on the agent computers	32-bit Windows Server 2003 R2
Cisco Unity installed on the agent computers	7.0(2), 7.0, 5.0, 4.x, or 3.x
Microsoft SQL Server installed on the agent computers	SQL Server 2000 or Desktop Engine (MSDE)
Microsoft Exchange Server installed on agent computers	5.5 (or later) Directory Connector and Message Store
Internet Explorer installed on the agent computers	5.5 or later

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

2.2 Installing the Module

You can install the module in one of the following ways:

- ♦ Run the module setup program, `AM70-CiscoUnity-7.x.x.xx.0.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager*.
- ♦ Use Control Center to install the module on the remote computer where an agent is installed. Ensure you check in the installation package, which is the `.XML` file included with the module setup program. For more information about the `.XML` file, see the *AppManager for Cisco Unity Readme*. For more information about deploying modules on agent computers, see the *Control Center User Guide for AppManager*.

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

To install the module:

- 1 Stop the Cisco Security Agent (CSA) service on each Cisco Unity server you want to monitor.
- 2 Run the module setup program on all repository computers to install the Knowledge Scripts and reports. For repositories running in a clustered environment, run the setup program on the node that currently owns the cluster resource.
- 3 Install the module on the Cisco Unity server you want to monitor. Use one of the following methods:
 - ♦ Run the module setup program.
 - ♦ Use Control Center Console to deploy the installation package.
- 4 Run the module setup program on all Operator Console and Control Center computers to install the Help.
- 5 Start the CSA service each Cisco Unity server where you installed the module.
- 6 If you have not already discovered Cisco Unity resources, run the [“Discovery_CiscoUnity” on page 56](#) Knowledge Script on all agent computers where you installed the module.

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

2.3 Silently Installing the Module

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

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

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

```
MO_CommunityString=string name
```

where *string name* is the name of the community string, such as `public`.
- 3 Save and close the `.ini` file.

4 Run the following command from the folder in which you saved the module installer:

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

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

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

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

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

2.4 Upgrading Knowledge Script Jobs

This release of AppManager for Cisco Unity may contain updated Knowledge Scripts. You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

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

2.4.1 Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. In addition, the repository computer must have hotfix 72040 installed, or the most recent AppManager Repository hotfix. To download the hotfix, see the [AppManager Suite Hotfixes](#) Web page.

Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

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

2.4.2 Propagating Knowledge Script Changes

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

Before propagating script changes, verify that the script parameters are set to your specifications. Customized script parameters may have reverted to default parameters during the installation of the module. New parameters may need to be set appropriately for your environment or application.

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

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

Propagating Changes to Ad Hoc Jobs

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

To propagate changes to ad hoc Knowledge Script jobs:

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

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options.

Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic (script) of a Knowledge Script to corresponding Knowledge Script Group members.

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see [“Propagating Changes to Ad Hoc Jobs” on page 14](#).

To propagate Knowledge Script changes to Knowledge Script Groups:

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

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

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

3 CiscoUnity Knowledge Scripts

AppManager Knowledge Scripts can help you better manage Cisco Unity resources. From within the Operator Console, you can select a Knowledge Script in the CiscoUnity tab of the Knowledge Script pane and press **F1** for complete details.

Knowledge Script	What It Does
CU_BackupAndRestoreStatus	Monitors the success or failure of the Cisco Disaster Recovery Tool (DiRT) Backup and Restore utility.
CU_CallActivity	Monitors the number of incoming and outgoing calls to the Unity server during an interval you specify.
CU_CpuHigh	Monitors the CPU resource consumption for Unity processes.
CU_CurrentDiskQueueLength	Monitors the number of requests outstanding on the disk.
CU_EventLog	Scans the Event Log for Cisco Unity errors and status events.
CU_FailoverStatus	Monitors whether failover or failback has occurred on the current server.
CU_HealthCheck	Monitors the status of Cisco Unity services. Can automatically restart any service that is down.
CU_LicenseCompliance	Monitors the number of Unified Messaging and/or Voice Mail licences and determines how many of those licenses are actively used.
CU_MemoryHigh	Monitors the memory consumption for Unity processes.
CU_MessageDeliveryFailure	Determines whether errors prohibited the Unity Message Repository (UMR) or the Message Transfer Agent (MTA) from successfully delivering all messages.
CU_MessageStoreAvailability	Monitors the number of offline message stores.
CU_MessageStoreLock	Monitors the number of tics it takes to acquire a Message Store Lock.
CU_NumberOfLogons	Monitors the number of active logons to Cisco Unity.
CU_PortStatus	Monitors whether a Unity port is unavailable and unable to handle further calls.
CU_ProcessorQueueLength	Monitors the number of processes in queue for the Processor.
CU_RestartService	Schedules a Unity service to stop and then restart after a specified interval.
CU_Silence	Monitors all of the silence performance counters for the Unity Manager Service in tenths of a second.
CU_SystemUsage	Monitors the CPU usage and memory for the Cisco Unity Manager process and for system processes.
CU_TTSPortsInUse	Monitors the number of text-to-speech ports being used by callers.

Knowledge Script	What It Does
CU_UMRServiceHung	Determines whether the AvUMRSyncSvr service is hung. This script is supported only for Cisco Unity version 3.0(x).
CU_VoicePortsInUse	Determines the number of voice ports currently in use on the Unity server.
CiscoUnity Knowledge Scripts	Monitors CPU usage for Cisco ICS processes on a Unity blade within an ICS chassis. This script monitors CPU usage for each process individually and the total CPU usage for all processes.
CiscoUnity Knowledge Scripts	Monitors the status of Cisco ICS services on a Unity blade within an ICS chassis. Can automatically restart any service that is down.
CiscoUnity Knowledge Scripts	Monitors the memory usage and memory pool usage of Cisco ICS processes on a Unity blade within an ICS chassis. This script checks the memory used by each process individually, and the total memory used by all processes.
CiscoUnity Knowledge Scripts	Schedules an ICS service (on a Unity blade within an ICS chassis) to stop and then restart after a specified interval.
IIS_CpuHigh	Monitors CPU usage for IIS processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors the CPU usage of the dllhost and MTX processes. Can automatically stop a process that exceeds the threshold.
IIS_MemoryHigh	Monitors memory usage and memory pool usage for IIS application processes.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors Web sites and the uptime for Web services.
Report_PortUsage	Summarizes the number of Unity ports in use. This script uses the data collected by the CU_TTSPortsInUse and CU_VoicePortsInUse scripts.
Report_ServicesAvailability	Summarizes the average availability of Unity services.
Report_SystemUsage	Summarizes average CPU and memory usage per Unity server.
SQL_Accessibility	Monitors whether the SQL Server database is accessible.
SQL_CPUUtil	Monitors CPU usage for SQL Server processes.
SQL_DataGrowthRate	Monitors data growth and shrink rates for all SQL Server databases.
SQL_DBGrowthRate	Monitors database growth and shrink rates.
SQL_MemUtil	Monitors memory usage for SQL Server processes.
SQL_RestartServer	Restarts a SQL Server.
Recommended Knowledge Script Groups	Performs essential monitoring of your Cisco Unity environment.
CiscoUnity Knowledge Scripts	Discovers Cisco Unity resources and configuration information.

3.1 CU_BackupAndRestoreStatus

Use this Knowledge Script to monitor the success or failure of the Cisco Disaster Recovery Tool (DiRT) Backup and Restore utility.

You use the DiRT utility to back up Cisco Unity-specific data — including SQL databases, registry settings, greetings, recorded names, switch file configuration, routing rules, and subscriber passwords — and then restore the information onto the Cisco Unity unified messaging server.

This script raises an event if backup/restore succeeds or fails. In addition, this script generates data streams for successful backup/restore operations.

3.1.1 Resource Object

CiscoUnity

3.1.2 Default Schedule

By default, this script runs every 10 minutes.

3.1.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for successful backup/restore?	Set to y to collect data about a successful backup and restore. The default is n .
Raise event if backup/restore succeeds?	Set to y to raise an event when a backup or restore is successful. The default is y .
Event severity if backup/restore succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a backup or restore is successful. The default is 25.
Raise event if backup/restore fails?	Set to y to raise an event when a backup or restore fails. The default is y .
Event severity if backup/restore fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a backup or restore fails. The default is 5.

3.2 CU_CallActivity

Use this Knowledge Script to monitor incoming and outgoing calls to the Unity server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for number and percentage of incoming calls, number and percentage of outgoing calls, number and percentage per second of incoming calls, and number and percentage per second of outgoing calls.

3.2.1 Resource Object

CiscoUnity

3.2.2 Default Schedule

By default, this script runs every five minutes.

3.2.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to y to collect data about incoming and outgoing calls for graphs and reports. The default is y .
Threshold type	Select whether you want to set a threshold based on a Percentage or a Value . The default is Percentage.
Monitor incoming calls?	Set to y to monitor incoming calls. The default is y .
Threshold - Maximum percentage of incoming calls	Specify the highest percentage of incoming calls that can occur before an event is raised. The default is 80%.
Threshold - Maximum number of incoming calls	Specify the highest number of incoming calls that can occur before an event is raised. The default is 18 calls.
Event severity if incoming calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of incoming calls exceeds the threshold. The default is 15.
Monitor outgoing calls?	Set to y to monitor outgoing calls. The default is y .
Threshold - Maximum percentage of outgoing calls	Specify the highest percentage of outgoing calls that can occur before an event is raised. The default is 80%.
Threshold - Maximum number of outgoing calls	Specify the highest number of outgoing calls that can occur before an event is raised. The default is 18 calls.
Event severity if outgoing calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of outgoing calls exceeds the threshold. The default is 15.
Monitor incoming calls per second?	Set to y to monitor incoming calls per second. The default is y .
Threshold - Maximum percentage of incoming calls per second	Specify the highest percentage of incoming calls that can occur per second before an event is raised. The default is 80%.
Threshold - Maximum number of incoming calls per second	Specify the highest number of incoming calls that can occur per second before an event is raised. The default is 18 calls.
Event severity if incoming calls per second exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of incoming calls per second exceeds the threshold. The default is 15.
Monitor outgoing calls per second?	Set to y to monitor outgoing calls per second. The default is y .
Threshold for percentage of outgoing calls per second	Specify the highest percentage of outgoing calls that can occur per second before an event is raised. The default is 80%.
Threshold for number of outgoing calls per second	Specify the highest number of outgoing calls that can occur per second before an event is raised. The default is 18 calls.

Parameter	How to Set It
Event severity for outgoing calls per second	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of incoming calls per second exceeds the threshold. The default is 15.

3.3 CU_CpuHigh

Use this Knowledge Script to monitor CPU usage for the following Unity processes:

- ◆ Unity Manager
- ◆ Secure Gateway
- ◆ Message Repository
- ◆ Directory Change Writer
- ◆ Active Directory Datastore
- ◆ Global Catalog Datastore
- ◆ Event Reporter
- ◆ Report Handler
- ◆ Exchange 5.5 Datastore
- ◆ Text-To-Speech
- ◆ Bridge Connector
- ◆ AvLic
- ◆ AvMMProxySvr
- ◆ AvMsgStoreMonitorSvr
- ◆ AvNotifierMgr
- ◆ AvSqlChangeWriter

This script raises an event if CPU usage exceeds the thresholds you set. The script generates data streams for CPU usage for each process individually and the total CPU usage for all processes. If a process is not found, the script assumes the process is not running, and reports zero for CPU usage.

3.3.1 Resource Object

CiscoUnity

3.3.2 Default Schedule

By default, this script runs every 15 minutes.

3.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when CPU utilization exceeds threshold?	Set to y to raise an event when CPU usage exceeds a threshold. The default is y .
Collect data?	Set to y to collect data about CPU usage for graphs and charts. The default is n .
Event severity when CPU utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds a threshold. The default is 8.
Threshold - Maximum CPU usage for ...	Specify the maximum amount of CPU usage that must be detected before an event is raised. Set to 0 if you do not want to monitor this process. The default is for Unity Manager is 80%. The default for all other services is 20%.

3.4 CU_CurrentDiskQueueLength

Use this Knowledge Script to monitor the number of requests outstanding on the disk. This script raises an event if a threshold is exceeded. In addition, this script generates a data stream for the number of requests in queue.

3.4.1 Resource Object

CiscoUnity

3.4.2 Default Schedule

By default, this script runs every 30 minutes.

3.4.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if requests in queue exceed threshold?	Set to y to raise event an event if the number of requests in queue exceeds the threshold you set. The default is y .
Collect data?	Set to y to collect data for graphs and reports. The default is n .
Threshold - Maximum requests in queue	Specify the maximum number of requests that can be in the disk queue before an event is raised. The default is 10 requests.
Event severity if requests in queue exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of requests in queue exceeds the threshold. The default is 25.

3.5 CU_EventLog

Use this Knowledge Script to monitor the event log entries from Cisco Unity during the past *n* hours. This script raises an event when log entries are detected. In addition, this script generates data streams for those log entries.

3.5.1 Resource Object

CiscoUnity

3.5.2 Default Schedule

By default, this script runs every 10 minutes.

3.5.3 Setting Parameter Values

Set the following parameters as needed:

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

Parameter	How to Set It
Type: Success Audit	Set to y to monitor for success audit events. If set to n , this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the <i>Collect data</i> parameter. The default is n .
Type: Failure Audit	Set to y to monitor for failure audit events. If set to n , this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the <i>Collect data</i> parameter. The default is n .
<p>Instructions for filtering: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.</p> <ul style="list-style-type: none"> ◆ Separate include and exclude criteria with a colon (:). For example, <code>net : logon</code>. ◆ Separate multiple include or exclude entries with commas. For example, <code>finance , sales : corp00 , HQ</code> ◆ If you specify only include criteria, the colon is not necessary. For example, <code>SQL</code> ◆ If you specify only exclude criteria, start the search string with a colon. For example, <code>: defragmentation , cleanup</code> 	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. For example: <code>NTDS KCC , NTDS General</code>
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: <code>1094 , 1404 - 1463</code>
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: <code>Pat , Chris , Alex</code>
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: <code>SHASTA , MARS</code>
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: <code>data loss during system failures , corrupt indices , Inter-Site Transport objects failed</code>
Maximum number of entries per event report	<p>Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30.</p> <p>The Message column on the Events tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.</p>
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries for which you have filtered. You may want to adjust the severity depending on the types of events for which you are checking. The default is 8.

3.6 CU_FailoverStatus

Use this Knowledge Script to determine whether failover or failback has occurred on the current server. The first time you run this script on a particular server, you can choose to raise an informational event indicating whether the current computer is the active computer. The word “Primary” or “Secondary” accompany each computer name in the event.

- ♦ **Failover.** A feature that provides simple redundancy, allowing voice messaging functions to continue if the Cisco Unity server fails or when you need to perform maintenance. A primary and secondary Unity server (failover pair) allow for continuous voice messaging functionality. When the status of the primary server changes from active to inactive, the secondary server takes over the tasks of the primary server.
- ♦ **Failback.** A feature that allows the secondary Unity server to shutdown down its functionality and allows the primary Unity server to take back the ability to answer calls.
- ♦ **Primary Unity server.** As the primary server of a failover pair, this server replicates all the appropriate Unity data to its backup counterpart (the secondary).
- ♦ **Secondary Unity server.** This server is basically an identical copy of the primary Unity server. The secondary server takes over for the primary server in the event of a failover.
- ♦ **AvCsNodeMgr.exe.** The Unity service responsible for determining whether failover or failback needs (or is scheduled) to occur.

The failover feature of Cisco Unity provides simple redundancy, allowing voice messaging functions to continue if the Cisco Unity server fails or when you need to perform maintenance. A primary and secondary Unity server (failover pair) allow for continuous voice messaging functionality. When the status of the primary server changes from active to inactive, the secondary server takes over the tasks of the primary server.

Use this script to monitor the status of failover and failback, which occurs when the primary server resumes its tasks.

To create a failover pair, set the *Create failover pair server group* parameter in the *Discovery_CiscoUnity* Knowledge Script to *y*. An Action Knowledge Script — *AddComputerToServerGroup* — runs by default and creates a server group composed of the two computers on which you run the *Discovery* script.

3.6.1 Resource Object

CiscoUnity

3.6.2 Default Schedule

By default, this script runs every minute.

3.6.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when failover occurs?	Set to y to raise an event when failover occurs. A failover event message will indicate which computer is now the primary computer in the failover scenario. In addition, the event will indicate when the next failback is scheduled to occur. The event indicates if failback is not scheduled. The default is y .
Event severity when failover occurs	Set the severity level, from 1 to 40, to indicate the importance of a failover event. The default is 15.
Raise event when failback occurs?	Set to y to raise an event when failback occurs. A failback event message will indicate which computer is now the primary computer in the failback scenario. The default is y .
Event severity when failback occurs	Set the severity level, from 1 to 40, to indicate the importance of a failback event. The default is 15.
Raise event for initial failover configuration and status?	Set to y to raise an informational event indicating the current configuration — Primary or Secondary — and status — active or inactive — of the Unity server. The default is y .
Collect data?	Set to y to collect data about failover status values (1 for active and 0 for inactive) for graphs and reports. The default is n .

3.7 CU_HealthCheck

Use this Knowledge Script to monitor the status of the following Cisco Unity services:

- ♦ Unity Manager
- ♦ Secure Gateway
- ♦ Message Repository
- ♦ Directory Change Writer
- ♦ Active Directory Store
- ♦ Global Catalog Datastore
- ♦ Event Reporter
- ♦ Report Handler
- ♦ Exchange 5.5 Datastore
- ♦ Text-To-Speech
- ♦ Bridge Connector
- ♦ Node Manager
- ♦ Licensing
- ♦ Media Master Proxy Server
- ♦ Message Store Monitor
- ♦ Notifier
- ♦ SQL Change Writer

This script raises an event if any service is not running. In addition, this script can automatically restart any service that is not running, as well as generate data streams for service status.

3.7.1 Resource Object

CiscoUnity

3.7.2 Default Schedule

By default, this script runs every minute.

3.7.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to y to collect data about service status for charts and graphs. The default is y .
Auto-start the monitored services?	Set to y to auto-start the services you choose to monitor. The default is y .
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which auto-start fails. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which auto-start succeeds. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager has not been set to restart the service. The default is 5.
Event severity when service doesn't exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service does not exist. The default is 25.
Monitor service?	Set to y to monitor Unity services. The default for Unity Manager is y . The default for all other services is n .

3.8 CU_LicenseCompliance

Use this Knowledge Script to monitor the number of Unified Messaging and/or Voice Mail licences and determine how many of those licenses are actively used. This script raises an event a threshold is exceeded. In addition, this script generates data streams for number and percentage of licenses used.

NOTE: This script supports Cisco Unity version 4.0(3) and later.

3.8.1 Resource Object

CiscoUnity

3.8.2 Default Schedule

By default, this script runs every 24 hours.

3.8.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for licenses used?	Set to y to collect data about in-use licenses for reports and graphs. The default is n.
Threshold type	Select the type of threshold you want to set. Select Percentage to set a threshold for a percentage of in-use licenses. Select Value to set a threshold for a number of in-use licenses. The default is Percentage.
Threshold - Maximum percentage of licenses used	Specify the threshold for the highest percentage of licenses that can be in use before an event is raised. The default is 80%.
Threshold - Maximum number of licenses used	Specify the threshold for the highest number of licenses that can be in use before an event is raised. The default is 24 licenses.
Event severity if used licenses exceed threshold	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number or percentage of in-use licenses exceeds the threshold you set. The default is 15.

3.9 CU_MemoryHigh

Use this Knowledge Script to monitor memory usage for the following Unity processes:

- ♦ Unity Manager
- ♦ Secure Gateway
- ♦ Message Repository
- ♦ Directory Change Writer
- ♦ Active Directory Datastore
- ♦ Global Catalog Datastore
- ♦ Event Reporter
- ♦ Exchange 5.5 Datastore
- ♦ Text-To-Speech
- ♦ Bridge Connector
- ♦ Licensing Service
- ♦ Media Master Proxy Server
- ♦ Message Store Monitor
- ♦ Notifier
- ♦ SQL Change Writer

This script checks the memory used by each process individually and the total memory used by all processes. If a process is not found, the script assumes the process is not running, and reports zero as the memory result.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for memory usage for all monitored applications.

3.9.1 Resource Object

CiscoUnity

3.9.2 Default Schedule

By default, this script runs every five minutes.

3.9.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when threshold exceeded?	Set to y to raise an event if a threshold is exceeded. The default is y .
Collect data?	Set to y to collect data for graphs and reports. The default is n .
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.
Monitor Unity Manager memory usage?	Set to y to monitor the memory usage of Unity Manager. The default is y .
Threshold - Maximum memory usage for Unity Manager	Specify the maximum memory usage that can occur before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Unity Manager	Specify the maximum memory pool usage that can occur before an event is raised. The default is 5000 KB.
Monitor Secure Gateway memory usage	Set to y to monitor the memory usage of Secure Gateway. The default is y .
Threshold - Maximum memory usage for Secure Gateway	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Secure Gateway	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Message Repository memory usage?	Set to y to monitor the memory usage of Message Repository. The default is y .
Threshold - Maximum memory usage for Message Repository	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Message Repository	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Directory Change Writer memory usage?	Set to y to monitor the memory usage of Directory Change Writer. The default is y .
Threshold - Maximum memory usage for Directory Change Writer	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Directory Change Writer	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.

Parameter	How to Set It
Monitor Active Directory Datastore memory usage?	Set to y to monitor the memory usage of Active Directory Datastore. The default is y .
Threshold - Maximum memory usage for Active Directory Datastore	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Active Directory Datastore	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Global Catalog Datastore memory usage?	Set to y to monitor the memory usage of Global Catalog Datastore. The default is y .
Threshold - Maximum memory usage for Global Catalog Datastore	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Global Catalog Datastore	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Event Reporter memory usage?	Set to y to monitor the memory usage of Event Reporter. The default is y .
Threshold - Maximum memory usage for Event Reporter	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Event Reporter	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Report Handler memory usage?	Set to y to monitor the memory usage of Report Handler. The default is y .
Threshold - Maximum memory usage for Report Handler	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Report Handler	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Exchange 5.5 Datastore memory usage?	Set to y to monitor the memory usage of Exchange 5.5 Datastore. The default is y .
Threshold - Maximum memory usage for Exchange 5.5 Datastore	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Exchange 5.5 Datastore	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Text-To-Speech memory usage?	Set to y to monitor the memory usage of Text-To-Speech. The default is y .
Threshold - Maximum memory usage for Text-To-Speech	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Text-To-Speech	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Bridge Connector memory usage?	Set to y to monitor the memory usage of the Bridge Connector. The default is y .
Threshold - Maximum memory usage for Bridge Connector	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Bridge Connector	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.

Parameter	How to Set It
Monitor Licensing Service memory usage?	Set to y to monitor the memory usage of the Licensing Service. The default is y .
Threshold - Maximum memory usage for the Licensing Service	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for the Licensing Service	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Media Master Proxy Server memory usage?	Set to y to monitor the memory usage of the Media Master Proxy Server. The default is y .
Threshold - Maximum memory usage for the Media Master Proxy Server	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the Media Master Proxy Server	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Message Store Monitor memory usage?	Set to y to monitor the memory usage of the Message Store Monitor. The default is y .
Threshold - Maximum memory usage for the Message Store Monitor	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the Message Store Monitor	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Notifier memory usage?	Set to y to monitor the memory usage of the Notifier. The default is y .
Threshold - Maximum memory usage for the Notifier	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the Notifier	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor SQL Change Writer memory usage?	Set to y to monitor the memory usage of the SQL Change Writer. The default is y .
Threshold - Maximum memory usage for the SQL Change Writer	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the SQL Change Writer	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.

3.10 CU_MessageDeliveryFailure

Use this Knowledge Script to determine whether errors prohibited the Unity Message Repository (UMR) or the Message Transfer Agent (MTA) from successfully delivering all messages. Messages not delivered successfully are stored locally on the Unity server. You can set this script to retrieve a count of the messages that are in storage awaiting delivery.

This script raises an event if messages are not delivered successfully. In addition, this script generates data streams for the number of unsuccessful deliveries for UMR and MTA.

NOTE: This script replaces CU_MTAFailures, which has been removed from the CiscoUnity category of Knowledge Scripts.

3.10.1 Resource Object

CiscoUnity

3.10.2 Default Schedule

By default, this script runs every 10 minutes.

3.10.3 Setting Parameter Values

Set the following parameters as needed

Parameter	How to Set It
Event Notification	
Raise event if MTA failure prevents message delivery	Set to Yes to raise an event if MTA messages are not delivered. The default is Yes.
Event severity if MTA failure prevents message delivery	Set the event notification level, from 1 to 40, to indicate the importance of an event in which MTA messages are not delivered. The default is 10.
Raise event if UMR failure prevents message delivery	Set to Yes to raise an event if UMR messages are not delivered. The default is Yes.
Event severity if UMR failure prevents message delivery	Set the event notification level, from 1 to 40, to indicate the importance of an event in which UMR messages are not delivered. The default is 10.
Data Collection	
Collect data for failed message deliveries due to MTA failure?	Set to Yes to collect data about undelivered MTA messages for reports and graphs.
Collect data for failed message deliveries due to UMR failure?	Set to Yes to collect data about undelivered UMR messages for reports and graphs.

3.11 CU_MessageStoreAvailability

Use this Knowledge Script to monitor the number of offline message stores. This script raises an event if a message store goes offline. In addition, this script generates data streams for the number of offline message stores.

NOTE: This script supports Cisco Unity versions 4.0(3) and later.

3.11.1 Resource Object

CiscoUnity

3.11.2 Default Schedule

By default, this script runs every 600 seconds.

3.11.3 Setting Parameter Values

Set the following parameters as needed

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MessageStoreAvailability job fails. The default is 5.
Monitor Message Store Availability	
Event Notification	
Raise event if message store goes offline?	Set to Yes to raise an event if a message store goes offline. The default is Yes.
Event severity when message store goes offline	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a message store goes offline. The default is 5.
Data Collection	
Collect data for number of offline message stores?	Set to Yes to collect data about offline message store for reports and graphs. The default is unchecked.

3.12 CU_MessageStoreLock

Use this Knowledge Script to monitor the number of tics it takes to acquire a Message Store Lock. This script raises an event a threshold is exceeded. In addition, this script generates data streams for number of tics.

NOTE: This script does not support Cisco Unity versions 4.0(3) and later.

3.12.1 Resource Object

CiscoUnity

3.12.2 Default Schedule

By default, this script runs every 30 minutes.

3.12.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when number of tics exceeds threshold?	Set to y to raise event if the number of tics required to acquire a Message Store Lock exceeds the threshold. The default is y.

Parameter	How to Set It
Collect data?	Set to y to collect data about tics for charts and graphs. The default is n .
Threshold - Maximum number of tics to acquire a Message Store Lock	Specify the maximum number of tics it takes to acquire a Message Store Lock before an event is raised. The default is 4 tics.
Event severity when number of tics exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

3.13 CU_NumberOfLogons

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

3.13.1 Resource Object

CiscoUnity

3.13.2 Default Schedule

By default, this script runs every 30 minutes.

3.13.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if active subscriber sessions exceed threshold?	Set to y to raise event if the number of active subscriber sessions exceeds the threshold you set. The default is y .
Collect data?	Set to y to collect data about subscriber sessions for charts and graphs. The default is n .
Threshold - Maximum number of active subscriber sessions	Specify the maximum number of subscriber sessions that can be active before an event is raised. Enter a number appropriate for the server you are monitoring. The default is 20 sessions.
Event severity when active subscriber sessions exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active subscriber sessions exceeds the threshold. The default is 25.

3.14 CU_PortStatus

Use this Knowledge Script to monitor whether a Unity port is unavailable and unable to handle further calls. This script raises an event if a port is unavailable. In addition, this script generates data streams for port availability.

3.14.1 Resource Object

CiscoUnity

3.14.2 Default Schedule

By default, this script runs every 10 minutes.

3.14.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if a port is unavailable?	Set to y to raise an event when a port is unavailable. The default is y .
Collect data?	Set to y to collect data about unavailable ports for charts and graphs. The default is n .
Event severity when a port is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which a port is unavailable. The default is 8.

3.15 CU_ProcessorQueueLength

Use this Knowledge Script to monitor the number of processes in queue for the processor. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for queue length.

3.15.1 Resource Object

CiscoUnity

3.15.2 Default Schedule

By default, this script runs every 30 minutes.

3.15.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if queue length exceeds threshold?	Set to y to raise event if the queue length exceeds the threshold you set. The default is y .
Collect data?	Set to y to collect data about queue length for charts and graphs. The default is n .
Threshold - Maximum number of processes in queue	Specify the maximum number of processes that can be in the queue before an event is raised. The default is 10 processes.

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

3.16 CU_RestartService

Use this Knowledge Script to schedule the following Unity services to stop and then restart after a specified interval:

- ◆ Unity Manager
- ◆ Secure Gateway
- ◆ Message Repository
- ◆ Directory Change Writer
- ◆ Active Directory Datastore
- ◆ Global Catalog Datastore
- ◆ Event Reporter
- ◆ Exchange 5.5 Datastore
- ◆ Text-To-Speech
- ◆ Bridge Connector
- ◆ Licensing Service
- ◆ Media Master Proxy Server
- ◆ Message Store Monitor
- ◆ Notifier
- ◆ SQL Change Writer

This script raises an event when a stop or restart fails, when service status is unavailable, and when a stop or restart succeeds. In addition, this script generates data streams for service status.

NOTE: This script does not support Cisco Unity versions 4.0(3) and later.

3.16.1 Resource Object

CiscoUnity

3.16.2 Default Schedule

By default, this script runs every hour.

3.16.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to y to collect data about service status for charts and graphs. The default is n .
Wait N seconds before restarting	Specify the number of seconds that should elapse before a service is restarted. The default is 5 seconds.
Event severity when stop fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to stop a service. The default is 5.
Event severity when restart fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to restart a service. The default is 5.
Event severity when status of service is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which service status is unavailable. The default is 10.
Event severity when stop succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops a service. The default is 25.
Event severity when restart succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts a service. The default is 25.
Restart service?	Set to y to restart any of the listed Unity services. The default is n .
Unity 3.1-only Services	
Restart ... service?	Set to y to restart any of the listed 3.1 Unity services. The default is n .

3.17 CU_Silence

Use this Knowledge Script to monitor all of the silence performance counters for the Unity Manager Service in tenths of a second. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for silence length for all monitored performance counters.

NOTE: This script does not support Cisco Unity versions 4.0(3) and later.

3.17.1 Resource Object

CiscoUnity

3.17.2 Default Schedule

By default, this script runs every 30 minutes.

3.17.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if a counter exceeds its threshold?	Set to y to raise an event if any of the counters exceeds its threshold. The default is y .
Collect data?	Set to y to collect data about silence counters for charts and graphs. The default is n .
Threshold - Maximum time for any silence performance counter	Specify the maximum amount of time for any silence performance counter. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Header silence	Specify the maximum amount of time for Header silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Logon silence	Specify the maximum amount of time for Logon silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Message Delete silence	Specify the maximum amount of time for Message Delete silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Opening silence	Specify the maximum amount of time for Opening silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Play Message silence	Specify the maximum amount of time for Play Message silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Record silence	Specify the maximum amount of time for Record silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Event severity when a counter exceeds its threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 25.

3.18 CU_SystemUsage

Use this Knowledge Script to monitor CPU usage and memory for the Cisco Unity Process. This script raises an event if any threshold is exceeded. In addition, this script generates data streams for maximum and total CPU usage (%) and maximum and total memory usage (%).

To generate reports based on the data collected by this script, run [Report_SystemUsage](#) and [Report_ServicesAvailability](#).

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

3.18.1 Resource Object

CiscoUnity

3.18.2 Default Schedule

By default, this script runs every five minutes.

3.18.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when threshold is exceeded?	Set to y to raise event if a threshold is exceeded. The default is y .
Collect data?	Set to y to collect data for reports and graphs. The default is y .
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Threshold - Maximum Unity CPU usage	Specify the maximum Unity CPU usage that must occur before an event is raised. The default is 65%.
Threshold - Maximum total CPU usage	Specify the maximum total CPU usage that must occur before an event is raised. The default is 80%.
Threshold - Maximum Unity memory usage	Specify the maximum Unity memory usage that must occur before an event is raised. The default is 65%.
Threshold - Maximum total memory usage	Specify the maximum total memory usage that must occur before an event is raised. The default is 80%.

3.19 CU_TTSPortsInUse

Use this Knowledge Script to monitor the number of Cisco Unity text-to-speech (TTS) ports that are in use. This script raises an event if a threshold is exceeded. A port is considered “in use” when a Unity subscriber is having his or her email read back over the phone.

This script generates data streams for number of ports in use.

Administrators can use this script to determine whether there are sufficient TTS port licenses and to gather usage statistics.

3.19.1 Resource Object

CISCOUNTY_TTSPorts

3.19.2 Default Schedule

By default, this script runs every five minutes.

3.19.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when number of in-use TTS ports exceeds threshold?	Set to y to raise an event when the number of ports in use exceeds the threshold. The default is y .
Collect data?	Set to y to collect data about TTS ports for charts and graphs. The default is y . NOTE: If the status of the Unity server changes from "active" to "inactive," data collection for this script will stop. Data collection will resume when status changes back to "active."
Threshold - Maximum number of TTS ports in use	Specify the maximum number of TTS ports that can be in use before an event is raised. Enter a number appropriate for the server you are monitoring. The default is 4 ports.
Event severity when number of in-use TTS ports exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use TTS ports exceeds the threshold. The default is 5.

3.20 CU_UMRServiceHung

Use this Knowledge Script to determine whether the AvUMRSyncSvr service is unresponsive. By default, this script always raises an event if AvUMRSyncSvr is unresponsive. In addition, you can choose to raise an event if AvUMRSyncSvr is *not* unresponsive.

UMR is the Unity Message Repository.

NOTE: This script supports Cisco Unity version 3.0(x) only.

3.20.1 Resource Object

CISCOUNITY

3.20.2 Default Schedule

By default, this script runs every 30 minutes.

3.20.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event when AvUMRSyncSvr service is not hung?	Set to y to raise an event if the AvUMRSyncSvr service is <i>not</i> unresponsive. The default is n .
Event severity when AvUMRSyncSvr service is hung	Set the severity level, from 1 to 40, to indicate the importance of an event in which the AvUMRSyncSvr service is unresponsive. The default is 8.

3.21 CU_VoicePortsInUse

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

Administrators can use this script to identify episodes of high usage, to determine whether there are sufficient voice port licenses on the Unity server, and to determine the availability of voice ports.

3.21.1 Resource Object

CISCOUNTY_Ports

3.21.2 Default Schedule

By default, this script runs every five minutes.

3.21.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if in-use voice ports exceed threshold?	Set to y to raise an event when the number of ports in use exceeds the threshold. The default is y .
Collect data?	Set to y to collect data about voice ports for charts and graphs. The default is y . NOTE: If the status of the Unity server changes from "active" to "inactive," data collection for this script will stop. Data collection will resume when status changes back to "active."
Threshold - Maximum voice ports in use	Specify the maximum number of voice ports that can be in use before an event is raised. Enter a value appropriate for the server you are monitoring. The default is 4 ports.
Event severity when in-use voice ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use voice ports exceeds the threshold. The default is 5.

3.22 IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for CPU usage (%) for each monitored process.

3.22.1 Resource Object

CISCOUNTY_IIST_Server

3.22.2 Default Schedule

By default, this script runs every five minutes.

3.22.3 Setting Parameter Values

Set the following parameters as needed:

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

3.23 IIS_HealthCheck

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

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

3.23.1 Resource Objects

- ◆ CISCOUNTY_IIST_Server
- ◆ CISCOUNTY_IIST_FTPSRV
- ◆ CISCOUNTY_IIST_W3SRV
- ◆ CISCOUNTY_IIST_WebInst

3.23.2 Default Schedule

By default, this script runs every five minutes.

3.23.3 Setting Parameter Values

Set the following parameters as needed:

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

3.24 IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if a threshold is exceeded. In addition, this script can automatically stop a process that exceeds the CPU usage threshold.

3.24.1 Resource Object

CISCOUNTY_IIST_Server

3.24.2 Default Schedule

By default, this script runs every three minutes.

3.24.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if kill is successful or unsuccessful?	Set to y to raise an event if the stop process is successful or unsuccessful. The default is y .
Kill CPU-intensive processes?	Set to y to automatically stop any process that exceeds the CPU usage threshold. The default is n .

Parameter	How to Set It
Threshold - Maximum CPU usage allowed	Specify the maximum percentage of CPU usage allowed by the <code>dllhost</code> and <code>mtx</code> processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager has successfully stopped the process. The default is 20.

3.25 IIS_MemoryHigh

Use this Knowledge Script to monitor the memory usage of specified processes. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for memory usage per process.

3.25.1 Resource Object

CISCOUNTY_IIST_Server

3.25.2 Default Schedule

By default, this script runs every three minutes.

3.25.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold exceeded?	Set to y to raise an event if a threshold is exceeded. The default is y .
Collect data?	Set to y to collect data for reports and graphs. If enabled, data collection returns memory usage for the specified process. The default is n .
Process names	Enter the name of the application process to monitor. Use a comma to separate multiple entries — do not use spaces. For example: <code>inetinfo,dllhost</code> . The default is <code>inetinfo</code> . NOTE: Do not append <code>.exe</code> to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.

Parameter	How to Set It
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

3.26 IIS_RestartServer

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

3.26.1 Resource Object

CISCOUNTY_IIST_Server

3.26.2 Default Schedule

By default, this script runs once.

3.26.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Restart server?	Set to y to automatically restart a server that is down. The default is y .
Wait N seconds before restarting	Enter the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the AppManager fails to stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the service is unavailable. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

3.27 IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if any value falls below the threshold. In addition, this script generates data streams for service uptime.

NOTE: This script runs on IIS version 5 and later.

3.27.1 Resource Objects

- ♦ CISCOUNTY_IIST_WebInst
- ♦ CISCOUNTY_IIST_FTPInst

3.27.2 Default Schedule

By default, this script runs every hour.

3.27.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if uptime falls below threshold?	Set to y to raise an event if uptime falls below the threshold. The default is y .
Collect data?	Set to y to collect data for reports and graphs. If enabled, data collection returns the length of time a service has been running. The default is n .
Threshold - Minimum uptime	Specify the minimum number of seconds that discovered Web sites and services and FTP sites and services are required to be up to prevent an event from being raised. If up time for sites and services is less than this threshold, an event is raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

3.28 Report_PortUsage

Use this Knowledge Script to summarize the number of Unity ports in use for a given time frame. This script uses the data collected by the [CU_TTSPortsInUse](#) and [CU_VoicePortsInUse](#) scripts.

3.28.1 Resource Object

Report agent

3.28.2 Default Schedule

By default, this script runs once.

3.28.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Port type	Select the type of port for which you are running the report: TTS or Voice. The default is Voice.
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts you want to include in the report.
Select time range	Select a Specific or Sliding date/time range from which the report should pull data. The default is Sliding.
Select peak weekdays	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by n minutes?	Specify the interval in minutes in which time-period data will be grouped. The default is 60 minutes.
Report Settings	
Include parameter help card?	Set to y to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to y to include a table of information in the report. The default is y.
Include chart?	Set to y to include a chart in the report. The default is y.
Select chart style	Define chart properties in the Chart Settings dialog box. The default style is Area.
Select output folder	Select the output folder. The default folder name is CiscoUnityVoicePortUsage.
Add job ID to output folder name?	Set to y to append the job ID to the name of the output folder. The default is n. The job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set report properties as desired. The default report name is Cisco Unity Voice Port Usage.
Add time stamp to title?	Set to y to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to y to raise an event when the report is successfully generated. The default is y.

Parameter	How to Set It
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

3.29 Report_ServicesAvailability

Use this Knowledge Script to summarize the average availability of Unity services within a time frame you specify. This script uses the data collected by the [CU_HealthCheck](#) script.

3.29.1 Resource Object

Report agent

3.29.2 Default Schedule

By default, this script runs once.

3.29.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts you want to include in the report.
Select time range	Select a Specific or Sliding date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Decimal accuracy for % values	Enter the number of decimal places you want to see in the values displayed in this report. The default is 3.
Include parameter help card?	Set to y to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to y to include a table of data stream values in the report. The default is y.
Include chart?	Set to y to include a chart of data stream values in the report. The default is y.

Parameter	How to Set It
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoUnityServicesAvailability.
Add job ID to output folder name?	Set to y to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set report properties as desired. The default report name is Cisco Unity Services Availability.
Add time stamp to title?	Set to y to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to y to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

3.30 Report_SystemUsage

Use this Knowledge Script to summarize the average CPU and memory usage within a time frame you specify. This script uses the data collected by the [CU_SystemUsage](#) script.

3.30.1 Resource Object

Report agent

3.30.2 Default Schedule

By default, this script runs once.

3.30.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the computers you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts you want to include in the report.
Select time range	Select a Specific or Sliding date/time range from which the report should pull data. The default is Sliding.
Charts	
Include % CPU chart?	Set to y to include a chart that details the CPU usage for the selected cluster. The default is y.
Include memory usage chart?	Set to y to include a chart that details the memory usage for the selected cluster. The default is y.
% CPU chart threshold	Enter the CPU percentage threshold to display on the charts in the report. The default is 0%.
Memory usage chart threshold	Enter the physical memory threshold (in KB) to display on the charts in the report. The default is 0 KB.
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to y to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to y to include a table of information in the report. The default is y.
Select output folder	Locate and select the output folder. The default folder name is CiscoUnitySystemUsage.
Add job ID to output folder name?	Set to y to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set report properties as desired. The default report name is Cisco Unity System Usage.
Add time stamp to title?	Set to y to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	

Parameter	How to Set It
Raise event when report succeeds?	Set to y to raise an event when the report is successfully generated. The default is y .
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

3.31 SQL_Accessibility

Use this Knowledge Script to monitor SQL Server and database accessibility. This script raises an event if SQL Server or a specified database is not accessible. In addition, this script generates a data stream for database accessibility.

3.31.1 Resource Object

CISCOUNTY_SQLT_Server

3.31.2 Default Schedule

By default, this script runs every hour.

3.31.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to y to collect data for reports and graphs. If enabled, data collection returns 100 if all specified databases are accessible, 50 if some of the specified databases are accessible and some are not, or 0 if none of the specified databases is accessible. The default is n .
SQL login	Type the database username that provides access SQL Server. The username must have permission to access the database names for which you want to check accessibility. To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Database name	Type the names of the databases to which you want to check access, separated by commas. For example, type <code>master, pubs, tempdb</code> . If you leave this field blank, the script checks access to all databases. The default is <code>master</code> .

Parameter	How to Set It
Timeout	<p>Specify the number of seconds to wait for a response before retrying or determining the database is inaccessible. The default is 0 seconds.</p> <p>NOTE: Keep in mind the Knowledge Script continues waiting until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep the time out period at a minimum for regular monitoring jobs. If you run this script to troubleshoot a particular problem and not as part of a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow a longer time out period.</p>
Number of retries	<p>Specify the number of times to retry connecting to the database before determining the database is inaccessible. The default is 0 retries.</p> <p>NOTE: Keep in mind the script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep retry attempts at a minimum for regular monitoring jobs. If you run this script to troubleshoot a particular problem and not as part of a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow more retry attempts.</p>
Event severity if SQL Server or database inaccessible	<p>Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server or the database is not accessible. The default is 5.</p>

3.32 SQL_CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr` and `sqlagent` processes. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for CPU usage (%) for all monitored processes.

3.32.1 Resource Object

CISCOUNTY_SQLT_Server

3.32.2 Default Schedule

By default, this script runs every 15 minutes.

3.32.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if CPU usage exceeds threshold?	Set to y to raise an event if CPU usage exceeds the threshold. The default is y .

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

3.33 SQL_DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the data space utilization from the current interval from the data space utilization from the last interval. This script raises an event if growth and shrink rates exceed the thresholds you set. In addition, this script generates data streams for data growth and shrink rates for each monitored database.

3.33.1 Resource Objects

- ♦ CISCOUNTY_SQLT_DatabaseF
- ♦ CISCOUNTY_SQLT_DatabaseObj

3.33.2 Default Schedule

By default, this script runs every hour.

3.33.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to y to automatically count databases at each monitoring interval. The default is y .
Exclude these objects	Type the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example, enter <code>master,model,mdb</code> NOTE: Ignore this parameter if you are not dynamically enumerating databases.

Parameter	How to Set It
Raise event if threshold exceeded?	Set to y to raise an event if a threshold is exceeded. The default is y .
Collect data?	Set to y to collect data for reports and graphs. If enabled, data collection returns the data growth and shrink rates for each database. The default is n .
SQL login	<p>Enter the database username that provides access to SQL Server. You can use the "sa" account or other user login account that has been set up in the managed client's SQL Server.</p> <p>To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.</p> <p>NOTE: If you are monitoring SQL Server 7, use a <code>sysadmin</code> role account. Only members of the <code>sysadmin</code> role can retrieve file statistics on SQL Server 7.0.</p>
Threshold - Maximum growth rate	Specify the maximum percentage of data growth allowed between the last and current interval before an event is raised. Enter 0 to ignore this parameter. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of data shrinkage allowed between the last and current interval before an event is raised. Enter 0 to ignore this parameter. The default is 25%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

3.34 SQL_DBGrowthRate

Use this Knowledge Script to monitor database growth and shrink rates. Growth and shrink rates are calculated by taking the difference between the database space utilization from the current interval and the database space utilization from the last interval. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for database growth and shrink rates.

3.34.1 Resource Objects

- ◆ CISCOUNTY_SQLT_DatabaseF
- ◆ CISCOUNTY_SQLT_DatabaseObj

3.34.2 Default Schedule

By default, this script runs every hour.

3.34.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to y to automatically count databases at each monitoring interval. The default is y .

Parameter	How to Set It
Exclude these objects	<p>Enter the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example, enter <code>master,model,mdb</code></p> <p>NOTE: Ignore this parameter if you are not dynamically enumerating databases.</p>
Raise event if threshold exceeded?	Set to y to raise an event if a threshold is exceeded. The default is y .
Collect data?	Set to y to collect data for reports and graphs. If enabled, data collection returns database growth and shrink rates. The default is y .
SQL login	<p>Enter the database username that provides access to SQL Server. You can use the "sa" account or other user login account that has been set up in the managed client's SQL Server.</p> <p>To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.</p> <p>NOTE: If you are monitoring SQL Server 7, use a <code>sysadmin</code> role account. Only members of the <code>sysadmin</code> role can retrieve file statistics on SQL Server 7.0.</p>
Update usage?	Set to y to have SQL Server recalculate the space usage. The default is n .
Threshold - Maximum growth rate	Enter the maximum percentage of data growth allowed between the last and current interval before an event is raised. Enter 0 to ignore this parameter. The default is 25%.
Threshold - Maximum shrink rate	Enter the maximum percentage of data shrinkage allowed between the last and current interval before an event is raised. Enter 0 to ignore this parameter. The default is 25%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

3.35 SQL_MemUtil

Use this Knowledge Script to monitor the amount of memory used by SQL Server processes. This script monitors the `sqlservr` and `sqlagent` processes.

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

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for memory usage for SQL Server processes.

3.35.1 Resource Object

CISCOUNITY_SQLT_Server

3.35.2 Default Schedule

By default, this script runs every 10 minutes.

3.35.3 Setting Parameter Values

Set the following parameters as needed:

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

3.36 SQL_RestartServer

Use this Knowledge Script to restart SQL Server. This script raises an event if the server successfully restarts or fails to restart. In order to restart SQL services, this script will also stop dependent Unity services, such as AvCsMgr and AvUMRSyncSvr. This script automatically restarts any service that it stops.

3.36.1 Resource Object

CISCOUNTY_SQLT_Server

3.36.2 Default Schedule

By default, this script runs once.

3.36.3 Setting Parameter Values

Set the following parameters as needed:

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

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

3.37 Recommended Knowledge Script Groups

The following Knowledge Scripts are members of the CiscoUnity recommended Knowledge Script Group. You can find these scripts individually on the CiscoUnity tab and in a group on the RECOMMENDED tab of the Operator Console.

- ◆ [CU_HealthCheck](#)
- ◆ [CU_NumberOfLogons](#)
- ◆ [CU_Silence](#)
- ◆ [CU_SystemUsage](#)
- ◆ [CU_VoicePortsInUse](#)

The following scripts are members of the CiscoUnity_Reports recommended KSG:

- ◆ [Report_PortUsage.](#)
- ◆ [Report_ServicesAvailability.](#)
- ◆ [Report_SystemUsage.](#)

All scripts in the KSGs have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the KSG on a Cisco Unity or Report resource.

The KSGs enable a “best practices” usage of AppManager for monitoring your Cisco Unity environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView.

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 CiscoUnity tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoUnity tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it 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 CiscoUnity or CiscoUnity_Report KSG and want to restore it to its original form, you can reinstall AppManager for Cisco Unity on the repository computer or check in the appropriate script from the AppManager\qdb\kp\CiscoUnity directory.

3.38 Discovery_CiscoUnity

Use this Knowledge Script to discover Cisco Unity resources, including the TSP version, and ports.

3.38.1 Resource Object

NT_MachineFolder

3.38.2 Default Schedule

By default, this script runs once.

3.38.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	This script always raises an event when the discovery fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n .
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discover fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery partially succeeds. The default is 15.
SQL username	If appropriate, enter your SQL username. Leave this field blank to use Windows Authentication. NOTE: If a SQL username is required, then you must configure the user name into AppManager Security Manager.
Create failover pair server group?	Set to y to create a server group composed of a failover pair (primary and secondary Unity servers). This server group is visible in the TreeView pane from the Master view only. The default is y .