

NetIQ® AppManager® for Microsoft Windows Management Instrumentation

Management Guide

April 2010



Legal Notice

NetIQ AppManager is covered by United States Patent No(s): 05829001, 05986653, 05999178, 06078324, 06397359, 06408335.

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.

© 2010 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

Chapter 1	
Introducing AppManager for Microsoft Windows Management Instrumentation	1
Chapter 2	
Installing AppManager for WMI	3
System Requirements.....	3
Installing the Module	5
Deploying the Module with Control Center.....	6
Verifying Your Installed Module	7
Propagating Knowledge Script Changes.....	7
Chapter 3	
WMI Knowledge Scripts	9
Configure	10
EventConsumer	11
LogSizes	12
RepositoryUsage	13
ResourceHigh.....	14
RunWQL	15
ServiceDown	17
UserManager.....	18
Discovery_WMI.....	20

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.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	<ul style="list-style-type: none">• Window and menu items• Technical terms, when introduced
<i>Italics</i>	<ul style="list-style-type: none">• Book and CD-ROM titles• Variable names and values• Emphasized words
Fixed Font	<ul style="list-style-type: none">• File and folder names• Commands and code examples• Text you must type• Text (output) displayed in the command-line interface
Brackets, such as <i>[value]</i>	<ul style="list-style-type: none">• Optional parameters of a command
Braces, such as <i>{value}</i>	<ul style="list-style-type: none">• Required parameters of a command
Logical OR, such as <i>value1 value2</i>	<ul style="list-style-type: none">• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

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

Contacting Sales Support

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

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

Contacting Technical Support

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

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

Contacting 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>.

Chapter 1

Introducing AppManager for Microsoft Windows Management Instrumentation

Microsoft Windows Management Instrumentation (WMI) is the infrastructure for managing data and operations on Windows-based operating systems. It provides an interface through which scripting languages such as VBScript or Windows PowerShell manage local and remote computers.

AppManager for WMI provides Knowledge Scripts that enable you to monitor WMI processes and services, and execute WMI queries. You can configure each Knowledge Script to raise an event, collect data for reporting, and perform automated problem management when an event occurs.

With AppManager for WMI, you can perform the following tasks:

- Configure the frequency of the WMI repository backup and the type, size, and location of the logging files
- Monitor for events generated by the WMI event provider and search for events in the database
- Monitor the size of WMI log files
- Monitor the size of the WMI repository
- Monitor the CPU and memory consumption for WMI processes
- Run WQL statements
- Monitor the availability of the WMI CIMOM service
- Add, delete, or edit a WMI user account or WMI group account for the WMI service

Chapter 2

Installing AppManager for WMI

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

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 Web site: <https://www.netiq.com/support/am/extended/documentation/default.asp>.

System Requirements

AppManager for WMI has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, on the servers you want to monitor (agents), and on all console computers	7.0, at minimum For support of Windows Server 2008, hotfix 71704 is required. For more information, see the AppManager Suite Hotfixes Web page.
Microsoft Windows operating system on agent computers	One of the following: <ul style="list-style-type: none">• Windows 7• Windows Vista• 32-bit or 64-bit Windows Server 2008 SP2, including R2• 32-bit or 64-bit Windows Server 2003 SP2, including R2• 32-bit Windows XP Professional SP3• 64-bit Windows XP Professional
Windows Management Instrumentation on agent computers	5.2, 5.1, 6.0, or 6.1
AppManager for Microsoft Windows module installed on repository, agent, and console computers	The most recent version, for support of Windows Server 2008. For more information, see the AppManager Module Upgrades & Trials Web page.

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page at www.netiq.com/support/am/supportedproducts/default.asp. If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

For more information about system requirements for the AppManager agent, repository, and management server, see the *Installation Guide for AppManager*.

Installing the Module

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

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

- Run the module setup program, `AM70-WMI -7. x. x. 0. msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager*.
- Use Control Center to install the module on the remote computer where an agent is installed. For more information, see “[Deploying the Module with Control Center](#)” on page 6.

To install the module:

1. Run the module setup program on all AppManager repository (QDB) computers to install the Knowledge Scripts and reports.
 - Run the setup program on the primary repository computer first. Then run the setup program on all other repository computers.
 - For repositories running in active/active and active/passive clusters, run the setup program on the active node. Then, copy the following Registry key to the non-active node.
`HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0`
2. Install the module on the WMI computer you want to monitor (agent computer). Use one of the following methods:
 - Run the module setup program.
 - Use Control Center to deploy the installation package.
3. Run the module setup program on all Operator Console and Control Center computers to install the Help and console extensions.
4. *If you have not already discovered WMI resources*, run the [Discovery_WMI](#) 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 `WMI_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\ServerName` folder.

Deploying the Module with Control Center

You can use Control Center to deploy the module on a remote computer where an agent is installed. This topic briefly describes the steps involved in deploying a module and provides instructions for checking in the module installation package. For more information, see the *Control Center User Guide for AppManager*, which is available on the AppManager Documentation Web site: <https://www.netiq.com/support/am/extended/documentation/default.asp>.

Deployment Overview

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

To deploy the module on an agent computer:

1. Verify the default deployment credentials.
2. Check in an installation package.
3. Configure an email address to receive notification of a deployment.
4. Create a deployment rule or modify an out-of-the-box deployment rule.
5. Approve the deployment task.
6. View the results.

Checking In the Installation Package

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

To check in a module installation package:

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

Verifying Your Installed Module

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

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

To verify your installed module with the Operator Console:

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

Propagating Knowledge Script Changes

This release of AppManager for WMI may contain updated Knowledge Scripts. You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups.

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 your attention.

You can propagate only properties (specified in the Schedule, Values, Actions, and Advanced 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 Running Jobs

You can propagate the properties and the logic of a Knowledge Script to running jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

To propagate changes to running Knowledge Script jobs:

1. In the Knowledge Script pane, select the Knowledge Script for which you want to propagate changes.
2. On the KS menu, select **Properties propagation**, and then select **Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated running jobs:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	The Knowledge Script properties, including schedule, monitoring values, actions, and advanced options.

4. Click OK.

Propagating Changes to Knowledge Script Groups

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

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see [“Propagating Changes to Running Jobs”](#) on page 7.

To propagate Knowledge Script changes to Knowledge Script Groups:

1. In the Knowledge Script pane, select the Knowledge Script for which you want to propagate changes.
2. On the KS menu, select **Properties propagation**, and then select **Knowledge Script Group Members**.
3. 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	The Knowledge Script properties, including schedule, monitoring values, actions, and advanced options.

4. Click OK.

Chapter 3

WMI Knowledge Scripts

The WMI category provides the following Knowledge Scripts for monitoring Microsoft Windows Management Instrumentation (WMI) services and executing WMI queries.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and pressing **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Configure	Configures the frequency of the WMI repository backup and the type, size, and location of the logging files.
EventConsumer	Monitors for events generated by the WMI event provider and allows you to search for events in the database.
LogSizes	Monitors the size of WMI log files.
RepositoryUsage	Monitors the size of the WMI repository.
ResourceHigh	Monitors the CPU and memory consumption for WMI processes.
RunWQL	Allows you to run WQL statements.
ServiceDown	Monitors the availability of the WMI CIMOM service.
UserManager	Allows you to add, delete, or edit a WMI user account or WMI group account for the WMI service.
Discovery_WMI	Discovers Microsoft Windows Management Instrumentation (WMI) server configuration and resources.

Configure

Use this Knowledge Script to configure the frequency of the WMI repository backup and the type, size, and location of the logging files.

Resource Object

WMI server

Note

This Knowledge Script is not supported for WMI servers running Windows Server 2008, Windows Vista, or Windows 7.

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if operation succeeds?	Set to y to raise an event when the selected operation succeeds. The default is y . Note This script always raises an event if a selected operation fails.
Time between repository backup attempts	Enter the number of minutes between WMI backup repository attempts. The default is 60 minutes.
Logging type: disable(d)/error(e)/verbose(v)	Specify the type of log files you want created by the WMI repository backup operation. Valid values are: <ul style="list-style-type: none">• d to disable logging (no log file is created)• e to enable error logging (log file records any errors encountered)• v to enable verbose logging (log file includes error and informational messages) The default is e .
Maximum log file size	Enter the maximum size of the log file in bytes. If the log file exceeds this size, the file is truncated. The default is 65535 bytes.
Logging directory	Enter the name of the directory to use for log files.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: <ul style="list-style-type: none">• ...configuration succeeded. The default is 25 (blue event indicator).• ...configuration failed. The default is 5 (red event indicator).

EventConsumer

Use this Knowledge Script to search a specific WMI repository namespace for events generated by the event provider. Enter the search criteria using the Windows Management Instrumentation Query Language (WQL). You can perform event queries with this script using the **SELECT** statement and related **WITHIN**, **GROUP**, and **HAVING** clauses. For more information about WQL, refer to the Microsoft documentation.

This script raises an event when events matching your query are found in the WMI repository. You specify the WMI event properties to display in the AppManager event.

Resource Object

WMI server

Default Schedule

The default schedule for this script is **Asynchronous**. This script will run indefinitely until you stop the script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Path to the WMI namespace	Specify the path to the WMI namespace you want to monitor. The default is <code>root\cimv2</code> .
WMI event query	Specify the information you want to find in the WMI repository using the WQL query format. The default query is: <pre>select * from __InstanceCreationEvent within 1 where TargetInstance is a 'Win32_NTLogEvent'</pre>
Fields to display for the event in the List pane	Specify the type of event information to display in the Message field in the List pane of the Operator Console. By default, the Source Name and Event ID fields are displayed. For example, if the source of an event is <code>MSSQLSERVER</code> and the Event ID is <code>17055</code> , the information displayed in the Message field would be <code>MSSQLSERVER - 17055</code> . Note This parameter requires case-sensitive entries. For example, do not enter <code>sourcename</code> if the actual field name is <code>SourceName</code> .
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

LogSizes

Use this Knowledge Script to monitor the size of the following WMI log files:

- cimom.log
- mofcomp.log
- wbemcore.log
- wbemprox.log

This Knowledge Script allows you to set a maximum log file size for individual log files and a maximum size for the sum of all log files. If either threshold is exceeded, an event is raised.

Note

This Knowledge Script is not supported on the Microsoft Windows Vista, or later, operating system.

Resource Object

WMI Log file object

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to y to raise events. The default is y .
Collect data for all log files?	Set to y to collect data for all log files. If set to y , the script returns the total file size used by all log files. The default is n .
Collect data for individual log files?	Set to y to collect data for individual log files. If set to y , the script returns the file size used by each log file. The default is n .
All log files size maximum threshold	Enter a threshold in MB for the maximum total file size used by all log files. The default is 1000 MB.
Individual log files size maximum threshold	Enter a threshold in MB for the maximum size of each log file. The default is 50 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

RepositoryUsage

Use this Knowledge Script to monitor the size of the WMI repository. If the repository size exceeds the threshold you set, an event is raised.

Resource Object

WMI Repository folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to y to raise events. The default is y .
Collect data?	Set to y to collect data for graphs and reports. If set to y , the script returns the size of the WMI repository in MB. The default is n .
Repository size	Enter a threshold in MB for the repository size. The default is 500 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

ResourceHigh

Use this Knowledge Script to monitor CPU and memory consumption by the WMI service (`Wmi nmgmt`). This script raises an event if CPU usage or memory usage exceeds the threshold you set.

Note

Beginning with Microsoft Windows XP, the `Wmi nmgmt` service runs with several other services under an instance of the `svchost.exe` process. Therefore, when the ResourceHigh Knowledge Script monitors CPU and memory for the `Wmi nmgmt` service, it is actually monitoring these same metrics for all services hosted by the instance of the `svchost.exe` process.

If you set the `Collect data?` parameter to `y`, the values returned for percentage of CPU used and MB of memory used are sums of CPU usage and memory usage for all services hosted by the `svchost.exe` process. The values do not represent CPU and memory usage for only the `Wmi nmgmt` service.

Resource Object

WMI server

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data?	Set to <code>y</code> to collect data for graphs and reports. If set to <code>y</code> , the script returns the percentage of CPU resources and the MB of memory used by the WMI service. The default is <code>n</code> .
% CPU maximum threshold	Enter a threshold for the maximum percentage of CPU resources that WMI should be allowed to consume. The default is 60%.
Memory maximum threshold (in MB)	Enter a threshold in MB for the maximum amount of memory WMI should be allowed to consume. The default is 6 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8 (red event indicator).

RunWQL

Use this Knowledge Script to run WQL queries. You can enter the WQL query to be executed as a parameter of this Knowledge Script, or you can load the query from a script file. You can choose the data output to be a specified number of data rows (all columns) or the value of the first row of a specific column (the column is specified by either number or name).

Examples of simple WQL queries:

```
/* Command to get the path setting for a computer. */  
Select * from Environment where Name = 'Path'
```

```
/* Command to get information about the provider CIMWmi n32. */  
Select * from _Wmi n32Provider where Name = 'CIMWmi n32'
```

Resource Object

WMI server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to y to raise events. The default is y .
Collect data?	Set to y to collect data for graphs and reports. The default is y .
WQL query	Enter the WQL query that will run. The default query is: <code>SELECT Caption, ThreadCount FROM wmi n32_Process</code> Tip Unless you are entering very simple queries, you may find that typing WQL statements in this field is error-prone. To avoid errors, you can use the <i>Load WQL script from file</i> parameter. Alternatively, if you have an AppManager Developer's license, you can check this Knowledge Script out of the repository, use the Knowledge Script Editor to paste the desired WQL statements into the WQL query field, and then check in the modified Knowledge Script.
Load WQL script from file?	Set to y to load an existing WQL script. The file containing the script must be present on the computer on which the Knowledge Script job will run. The default is n .
WQL script file (full path)	Enter the full path to the file that contains the WQL script (for example: <code>C:\netiq\Sample.wql</code>). Note This path is relative to the computer on which the Knowledge Script job will run.
WMI server\namespace	Enter the name of the managed WMI server and CIM namespace. The default is <code>root\CIMv2</code> .

Description	How to Set It
Return N rows (set to 0 for all rows)	<p>Enter the number of rows to return as data output when the <i>Collect data?</i> parameter is set to y. The default is 10.</p> <p>Note You can set this value to 0 to set no limit on the number of rows returned. However, there is a limit of 32K for the total of returned data.</p>
Return first row of specified column?	<p>Set to y to use a specified column number or column name from which data will be returned (specify the column number or name in one of the two following parameters). Setting this parameter to y will override the <i>Return N rows</i> parameter. The default is n.</p>
Column number	<p>If the <i>Return first row of specified column?</i> parameter is set to y, the value of the first row of the column specified here (by number), rather than the number of rows, is used as data output. The default is 0.</p>
Column name	<p>If the <i>Return first row of specified column?</i> parameter is set to y, the value of the first row of the column specified here (by name), rather than the number of rows, is used as data output. The default is blank.</p>
GivenLegend	<p>String used in the Legend column of graph data. If this value is left blank, the Legend column will read: "WQL query results on WMI Server: <machine name>."</p>
Maximum threshold	<p>Set the high watermark for the return value of the WQL query (this value can be the number of rows returned or the value of the first row of a specified column, depending on the type of data output you chose). If the return value exceeds this limit, an event will be raised. The default is 10000.</p>
Minimum threshold	<p>Set a low watermark for the return value of the WQL query (this value can be the number of rows returned or the value of the first row of a specified column, depending on the type of data output you chose). If the return value is below this limit, an event will be raised. The default is 10.</p>
Event severity level	<p>Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).</p>

ServiceDown

Use this Knowledge Script to monitor the WMI CIMOM (Common Information Model Object Manager) service. If the CIMOM service is not running, an event is raised. Optionally, you can set the Knowledge Script to attempt to restart the service automatically.

Resource Object

WMI service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to y to collect data for graphs and reports. The default is n . If set to y , the script returns a value of 100 if the CIMOM service is running and a value of 0 if the service is not running.
Auto-start service?	Set to y to automatically restart down services. The default is y .
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: <ul style="list-style-type: none">• ...service down; restart failed. The default is 5 (red event indicator).• ...service down; restart succeeded. The default is 25 (blue event indicator).• ...service down; don't restart. The default is 18 (yellow event indicator).

UserManager

Use this Knowledge Script to add, delete, or edit WMI user or group accounts for the WMI service on the computer where the Knowledge Script job is running. You can also use this Knowledge Script to manage user access to CIM objects.

This script can add or modify domain accounts or groups. The account or group you are modifying must belong to the same domain as the computer on which the script is running.

By default, this script raises an event whose message informs you of the success or failure of the operation.

If you want to use this script to manage an account that was added from the WMI Control, that account must meet the following requirements:

- Permissions must be granted for **This namespace and subnamespaces**.
- Permissions must allow Provider Write, Enable Account, and Remote Enable.

Resource Object

WMI server

Note

This Knowledge Script is not supported for WMI servers running Windows Server 2008, Windows Vista, or Windows 7.

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if operation succeeds?	Set to y to raise an event when the selected operation succeeds. The default is y . Note This script always raises an event if a selected operation fails.
Manage user or group?	Set to u to manage user accounts. Set to g to manage group accounts. The default is u .
Operation to perform: add(a)/delete(d)/edit(e)	Indicate the type of operation you want to perform. Set to one of the following: <ul style="list-style-type: none">• a to Add users or groups• d to Delete users or groups• e to Edit users or groups The default is a .
User or Group names to be managed	Enter the user or group account name you want to manage. You can enter multiple names, separated by commas with no spaces. For example: guest, adm i n, user1 The default is guest.
Domain name	Enter the domain name associated with the user or group account. You must specify the local machine name when deleting or editing a local user.

Description	How to Set It
Enable this account?	Set to y to enable the specified accounts if you are adding new user or group accounts or editing existing accounts. Set to n to disable an account. The default is y .
Can this account execute methods?	Set to y to give the specified accounts permission to execute methods exported from the CIM Object Manager. The default is n .
Schema access privileges: Read-only(r) / Write instance(i) / Write class(c)?	<p>Indicate the WMI schema access allowed for the specified accounts. Set to:</p> <ul style="list-style-type: none"> • r to authorize read-only access (users can execute queries or retrieve instances and classes, but cannot create, delete, or modify CIM objects). • i to allow the account read/write/delete access to instances in the WMI schema and read-only access to classes. • c to allow the account full read/write/delete access to all CIM objects, classes, and instances in the WMI schema. <p>The default is r.</p>
Can this account edit security?	Set to y to give the specified accounts permission to edit security. When set to y , the user has read and write access to the ROOT\Security namespace. When set to n , the user cannot access the ROOT\Security namespace. The default is n .
Group account type: NTLM Local(l)/NTLM Global(g)	<p>Indicate whether the specified group accounts are local to the managed computer or global. Set to:</p> <ul style="list-style-type: none"> • l to create a local Windows group (that can only access the local workstation or domain). • g to create a domain global group (that can access its own domain, member servers and workstations in the domain, and trusting domains). <p>This parameter is used only for managing group accounts. The default is l.</p>
Event severity level	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 12 (yellow event indicator).

Discovery_WMI

Use this Knowledge Script to discover the Microsoft Windows Management Instrumentation (WMI) server configuration and resources.

Resource Object

WMI server

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n .
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: <ul style="list-style-type: none">• ...succeeds. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator).• ...fails. The default is 5 (red event indicator).• ...is not applicable. This type of failure usually occurs when the target computer does not have WMI installed. The default is 15 (yellow event indicator).