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.

© 1995-2007 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.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, AppManager, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, IntelliPolicy, Knowing is Everything, Knowledge Scripts, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, NetIQ Change Administrator, NetIQ Change Guardian, NetIQ Compliance Suite, NetIQ Group Policy Administrator, NetIQ Group Policy Guardian, NetIQ Group Policy Suite, the NetIQ Partner Network design, NetIQ Patch Manager, NetIQ Risk and Compliance Center, NetIQ Secure Configuration Manager, NetIQ Security Administration Suite, NetIQ Security Analyzer, NetIQ Security Manager, NetIQ Vulnerability Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Server Consolidator, VigilEnt, Vivinet, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.
## Contents

### About This Guide
- Intended Audience ........................................... 5
- Conventions ...................................................... 6
- Using Online Help ............................................. 6
- Other Information in the Library ............................ 7
- About Attachmate .............................................. 8

### Chapter 1  The AppManager Connector for CA Unicenter NSM
- Integrating AppManager with CA Unicenter Framework . 12
- Understanding What the Connector Does .................. 12
- Understanding the Connector Components............... 13
- Understanding How an Event is Forwarded............... 13
- Viewing AppManager Events in the NSM Console ....... 14

### Chapter 2  Planning the Connector Installation
- System Requirements .......................................... 17
- Accounts Needed to Install the Connector ................. 18
- Establishing a Distribution Computer ...................... 19

### Chapter 3  Installing the Connector
- Installing the Connector ..................................... 21
- Updating the Connector Configuration .................... 27
Appendix A  Uninstalling the Connector

Appendix B  Windows Registry Information
CA Unicenter NSM Information ......................... 31
Event Category Information ............................. 32
Event Severity Information .............................. 34
About This Guide

The NetIQ AppManager Suite (AppManager Suite) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and server health for a broad spectrum of operating environments, applications, 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 staffs 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 Management Guide, AppManager Connector for CA Unicenter NSM, provides information to ensure a successful installation of NetIQ AppManager components. This guide is intended for system administrators and users responsible for installing all or part of the AppManager Suite software.

For more information about working with AppManager, see the User Guides for the Operator Console or Control Center. For more information about configuring and maintaining an AppManager management site, see the Administrator Guide.
Conventions

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>• Window and menu items</td>
</tr>
<tr>
<td></td>
<td>• Technical terms, when introduced</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>• Book and installation kit titles</td>
</tr>
<tr>
<td></td>
<td>• Variable names and values</td>
</tr>
<tr>
<td></td>
<td>• Emphasized words</td>
</tr>
<tr>
<td><strong>Fixed Font</strong></td>
<td>• File and folder names</td>
</tr>
<tr>
<td></td>
<td>• Commands and code examples</td>
</tr>
<tr>
<td></td>
<td>• Text you must type</td>
</tr>
<tr>
<td></td>
<td>• Text (output) displayed in the command-line interface</td>
</tr>
</tbody>
</table>

Using Online Help

AppManager provides task-based, reference, and context-sensitive online Help.

To access task-based Help or search for Help topics, click **Help Topics** on the Help menu. To view context-sensitive Help within dialog boxes, click **Help** or press **F1**.

You can get help on individual Knowledge Scripts in one of the following ways:

- On the **Values** tab of the Knowledge Script Properties dialog box, click **Help** or press **F1**.
- In the Knowledge Script pane of the Operator Console, highlight a Knowledge Script and press **F1**.
- In the Knowledge Script view of the Control Center Console, highlight a Knowledge Script and press **F1**.
Other Information in the Library

The library provides the following information resources:

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

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

- **Administrator Guide**: 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**: Provides complete information on how to upgrade from a previous version of AppManager.

- **Management Guides**: Provide information about installing and monitoring specific applications with AppManager.

The AppManager library is available in Adobe Acrobat (PDF) format and is located in the `Documentation` folder of the AppManager installation kit.

NetIQ Online Support and Extended Support Web sites provide other resources:

- Downloads, including hotfixes, service packs, and product upgrades.

- Documentation, including white papers and the most current information about version support for the systems and applications monitored by AppManager.

**Note** You can access NetIQ Support without a password or registration. To access the Extended Support site, you must be
a registered AppManager customer.

In addition to the AppManager documentation, you may want to consult the documentation for your Windows or UNIX operating system, or other application- or system-specific documentation for reference and conceptual information. This background information can help you get the most out of your AppManager installation.

About Attachmate

Attachmate, owned by an investment group led by Francisco Partners, Golden Gate Capital and Thoma Cressey Equity Partners, enables IT organizations to extend mission critical services and assure they are managed, secure and compliant. Attachmate’s leading solutions include host connectivity, systems and security management, and PC lifecycle management. Our goal is to empower IT organizations to deliver trusted applications, manage service levels, and ensure compliance by leveraging knowledge, automation and secured connectivity. For more information, visit www.attachmate.com.

NetIQ Solutions from Attachmate

Attachmate provides a wide selection of systems and security management solutions to help you manage and secure all your essential platforms, including Windows, UNIX, Linux, and iSeries. These Knowledge-Based Service Assurance products and solutions include embedded knowledge and tools to implement industry best practices and to better ensure operational integrity, manage service levels and risk, and ensure policy compliance. Our modular, best-of-breed solutions for Performance and Availability Management, Security Management, Configuration and Vulnerability Management, and Operational Change Control integrate through an open, service-oriented architecture allowing for common reporting, analytics and dashboards. Attachmate
offers the following systems and security management solutions:

- **Performance and Availability Management** These products offer rapid time-to-value solutions that enable you to align your IT operations with business priorities and optimize the delivery of your IT-based business services. This solution automates the complete IT service management lifecycle: assessment of requirements, definition of Service-Level Agreements, management of day-to-day operations, and review of operational metrics.

- **Security Management** These easy-to-install-and-deploy products provide effective protection from and response to security-related threats. This solution provides powerful features, such as real-time security event monitoring, mapping of threat indicators, policy violation alerts, and expedited incident forensics and resolution. These products reduce the time required to identify and resolve security threats.

- **Configuration and Vulnerability Management** These products allow you to quickly and easily assess vulnerabilities, manage security risks, and assure policy compliance. This powerful solution measures and enforces compliance to configuration baselines based on your corporate policies, regulations, and evolving security threats. You can use the latest security knowledge, which is updated in real time, to resolve compliance and configuration issues.

- **Operational Change Control** These products enable IT organizations to control, manage, and audit operational changes to servers, Active Directory, and Group Policy with unprecedented levels of accountability. NetIQ’s Operational Change Control (OCC) solutions enable enterprise customers to meet IT compliance and operational integrity needs in the most cost-effective manner, by delegating
access control, managing changes according to policy, and alerting and reporting on change activities and entitlements.

**Contacting NetIQ Solutions Support**

Please contact us with your questions and comments. We look forward to hearing from you.

**Sales Email:** info@netiq.com  
**Telephone:**  
713.418.5555 (United States)  
+353 (0) 91 782 677 (Europe, Middle East, and Africa)  
For other locations, see our Support Contact Information Web site at [www.netiq.com/support](http://www.netiq.com/support)

**Support Web Site:** [www.netiq.com/support](http://www.netiq.com/support)
Chapter 1

The AppManager Connector for CA Unicenter NSM

The NetIQ AppManager Connector for Computer Associates (CA) Unicenter NSM provides tight integration between the NetIQ AppManager Suite and CA Unicenter NSM Framework. With the AppManager connector in place, AppManager events are automatically formatted and forwarded to the CA Unicenter NSM repository and then displayed in the CA Unicenter NSM Console. This integrated solution allows existing AppManager customers to consolidate management information, and bring AppManager's Windows NT management functionality into CA Unicenter NSM.

This chapter provides an overview of the connector and how events are forwarded. The following topics are covered:

- “Integrating AppManager with CA Unicenter Framework” on page 12
- “Understanding What the Connector Does” on page 12
- “Understanding the Connector Components” on page 13
- “Understanding How an Event is Forwarded” on page 13
- “Viewing AppManager Events in the NSM Console” on page 14
Integrating AppManager with CA Unicenter Framework

Highlights of AppManager’s integration with CA Unicenter NSM Framework include:

- The AppManager SmartAdapter is a plug-in to the AppManager management server. It translates AppManager event information into CA Unicenter NSM format and forwards it to the CA Unicenter NSM repository.

- The AppManager SmartAdapter can intelligently filter AppManager events based on application type. For example, you might configure the SmartAdapter to forward AppManager events that were triggered on Microsoft Exchange and Microsoft SQL servers but not forward events triggered on Citrix WinFrame systems.

- Once you configure the SmartAdapter, AppManager events are automatically forwarded to CA Unicenter NSM without additional operator intervention.

- You can customize the SmartAdapter by assigning different ranges of AppManager event severity levels to the appropriate CA Unicenter NSM Console alarm conditions.

Understanding What the Connector Does

The AppManager Connector for CA Unicenter NSM formats and forwards AppManager events to the CA Unicenter NSM repository, which are then displayed in the NSM Enterprise Management’s EM Console.

An event is an alert and indicates that a condition or activity you are monitoring with AppManager has occurred on a managed client. Events are generated by AppManager Knowledge Script jobs. For more information about jobs and events, see the AppManager User Guide.
Understanding the Connector Components

The AppManager Connector for CA Unicenter NSM consists of an AppManager SmartAdapter and a framework integration component.

The SmartAdapter, a plug-in to the AppManager management server, monitors events received by the management server. It then translates AppManager event information into CA Unicenter NSM format and automatically forwards it to the CA Unicenter NSM repository. (For more information, see “Understanding How an Event is Forwarded” on page 13.)

The framework integration component configures CA Unicenter NSM so that the CA Unicenter NSM repository can receive the AppManager event information and the CA Unicenter NSM Console can display it.

The SmartAdapter is functional only when attached to the management server and, therefore, must reside on the same Windows Server as the management server.

The framework integration component supports CA Unicenter NSM running on Windows 2000 and Windows 2003 with the latest service pack.

For system requirements, see “System Requirements” on page 17.

Understanding How an Event is Forwarded

When a Knowledge Script job that is running on a managed client produces an event, the AppManager agent sends the event information to the AppManager management server. If the management server detects that the AppManager SmartAdapter is installed, the event information is forwarded to the SmartAdapter. If the SmartAdapter determines the event falls within the event categories and event severity levels that the SmartAdapter was configured to process, it then translates the event information into CA Unicenter NSM-readable format.
and forwards it the CA Unicenter NSM repository. The event information is then displayed in the CA Unicenter NSM Console. Other events are not forwarded. (For example, if the SmartAdapter is configured for Microsoft SQL Server and Exchange Server events, and an event is generated by Lotus Domino, then the SmartAdapter ignores it.)

The SmartAdapter log information (in the file named: msadpt_tng.log) is located in the NetIQ directory \temp\NetIQ_Debug\Computer folder (for example: c:\Program Files\NetIQ\Temp\NetIQ_Debug\Shasta).

**Viewing AppManager Events in the NSM Console**

AppManager events can be viewed in the NSM console.

**NSM Enterprise Management**

The steps necessary for using the NSM Enterprise Management to monitor AppManager events are:

1. In Programs > Unicenter TND > Enterprise Management, open EM Classic.

2. In the EM for Windows NT window, double-click the Windows NT icon.

3. In the Windows NT window, double-click the Event icon.

4. In the Event window, double-click the Console Logs icon. This displays the EM Console window. The AppManager events are displayed in this console window. Here is a typical EM Console display.
Chapter 1 • The AppManager Connector for CA Unicenter NSM
Chapter 2

Planning the Connector Installation

This chapter describes system and account requirements, and gives an overview of the procedures for installing the AppManager Connector for CA Unicenter NSM. The following topics are covered:

- System Requirements, below
- “Accounts Needed to Install the Connector” on page 18
- “Establishing a Distribution Computer” on page 19

System Requirements

Be sure your AppManager and framework environments meet the following software requirements before you install the AppManager Connector for CA Unicenter NSM:
**AppManager**

**Requirements:**

- AppManager management server version 7.0 running on a Windows 2000 Server or Windows 2003 with the latest service pack.

- The AppManager management server and AppManager Operator Console must be installed on the same computer as CA Unicenter NSM.

- The AppManager management server must be configured to log on using a Windows account that is part of the Administrator group.

**CA Unicenter NSM**

**Requirements:**

- CA Unicenter NSM 3.1 or r11 with Service Pack 1. The following components must be installed:
  - NSM Event Management
  - NSM World View Gateway

- The following CA Unicenter NSM services must be installed and running:
  For CA Unicenter NSM:
  - CA Unicenter
  - MSSQLServer
  For CA Unicenter NSM Framework:
  - NSM DB Server
  - CA Unicenter

**Accounts Needed to Install the Connector**

The AppManager connector installation program requires access to various administrator and user accounts.

The computer where the AppManager management server resides requires a valid Windows NT login account with Administrator privileges. The privileges can be for the local computer (required) or the Domain (optional).

**Note** If the SQL instance that accesses the AppManager repository is running in Integrated (Windows only) mode, then the account used by the netiqms service must have access to the
NSMDB database with the same permissions as the tngsa SQL account.

Establishing a Distribution Computer

In most cases, you’ll want to establish a distribution computer in your network where you will save the AppManager connector source files.

The AppManager Connector for CA Unicenter NSM source files are located on the AppManager CD-ROM in the <root>\connectors\ca_unicenter\ folder.

On a Windows 2000 Server or Windows 2003 computer, the distribution folder must:

- Be shared and accessible to the computer where the AppManager management server resides.
- Be readable to the Windows 2000 Server or Windows 2003 login account on the computer where the AppManager management server resides.
- Conform to UNC (Universal Naming Convention) format as a shared folder or network drive. For example, \mis\appmgr\ or \\mis\D$.

Copy the files from the <root>\connectors\ca_unicenter\windows folder to the distribution folder on the Windows 2000 Server or Windows 2003 computer.
Chapter 3

Installing the Connector

This chapter describes the procedures for installing the AppManager Connector for CA Unicenter NSM. These topics are covered:

- Installing the Connector, below
- “Updating the Connector Configuration” on page 27

Before installing the AppManager connector, be sure that you have installed AppManager 7.0 in your CA Unicenter NSM framework environment.

Installing the Connector

Run the AppManager Connector for CA Unicenter NSM setup program on the computer where the AppManager management server, AppManager Operator Console, and CA Unicenter NSM framework are all installed.

You need a valid Windows login account with Administrator privileges. The privileges can be for the local computer (required) or the Domain (optional).

**Note** Installation of the SmartAdapter requires that the netiq\bin folder be in the system path. If necessary, add the folder to the Path variable and then reboot the system.

1. Launch `SETUP.EXE` in the `connectors\ca_unicenter\directory on the AppManager CD-ROM or in the distribution folder you created.`
2. At the Welcome screen, click **Next**.

3. Read the license agreement, and if you agree, click **Yes**.
4 Set the options for CA Unicenter NSM, then click **Next**.

![NetIQ AppManager CA Unicenter NSM Settings](image)

<table>
<thead>
<tr>
<th>For:</th>
<th>Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSM Server</td>
<td>The hostname or IP address of the server where AppManager events are to be forwarded.</td>
</tr>
<tr>
<td>NSM Repository</td>
<td>The name of the NSM repository.</td>
</tr>
<tr>
<td>NSM User</td>
<td>The user name of the NSM repository login account. This account should have the same permissions to the NSMDB database as the tngsa SQL account.</td>
</tr>
<tr>
<td>NSM Password</td>
<td>The password of the NSM repository login account.</td>
</tr>
</tbody>
</table>
5. Select the AppManager events you want forwarded to the CA Unicenter NSM server, then click **Next**.

![Filter Categories](image1.png)

6. To change event severity levels, move the slider bars, then click **Next**.

![Select Severity Mappings](image2.png)
7 If prompted, select **Yes** to have Setup stop the AppManager management server service (**NetIQms**) and continue the setup procedure.

![Question dialog box](image)

**Note** When you stop and restart the AppManager services, the AppManager Connector for CA Unicenter NSM queries every device in the CA database. Depending on the number of devices, this query process can take several minutes to several hours to complete.

8 Click **Yes** to install the NetIQ World View Component. Click **No** to manually do the install at a later time.

![Question dialog box](image)
If you click **Yes**, the install process displays the **NetIQ Component Install** dialog box.

Enter:
- The name of the NSM repository host.
- The user name of the NSM repository login account. This account should have the same permissions to the NSMDB database as the `tngsa` SQL account.
- The password for the NSM repository login account.

**Note** If, after the installation, you do not see AppManager components in World View, do the following:

1. Run `tngdisc -r<repository> -user<username> -pwd <password>` at the command line.
2. Stop the **NetIQMS** service.
3. Restart the **NetIQMS** service.
Updating the Connector Configuration

After installing the connector, you can change the connector configuration. Updating the connector configuration only applies to the connector SmartAdapter, which is installed on the computer where the AppManager management server resides.

On the Windows 2000 Server or Windows 2003 computer (with the latest service pack installed) where the AppManager management server resides, click **Start**, then **Programs > NetIQ AppManager > Tools & Utilities > AppManager Connector for CA Unicenter NSM.**

Several quantities can *only* be configured by changing registry entries. For more information, see Appendix B, “Windows Registry Information.”

**Note** To install the connector for the first time on a computer, follow the instructions in “Installing the Connector” on page 21.
Appendix A

Uninstalling the Connector

The connector uninstall program removes the AppManager SmartAdapter component from the Windows 2000 or Windows 2003 computer where the AppManager management server resides.

To uninstall the connector:

1. Stop the NetIQ AppManager Management Service (NetIQms) on the computer where you installed the connector.

2. On the Windows 2000 Server or Windows 2003 computer where the AppManager management server resides, go to **Start > Settings > Control Panel**.

3. Double-click **Add/Remove Programs**, and select **NetIQ AppManager Connector for CA Unicenter NSM**.

4. Restart the NetIQ AppManager Management Service (NetIQms).
Appendix B

Windows Registry Information

This appendix describes the information that the AppManager Connector for CA Unicenter NSM writes to the Windows Registry. The following topics are covered:

- CA Unicenter NSM Information, below
- “Event Category Information” on page 32
- “Event Severity Information” on page 34

Note Altering the NODE NAME and NO SENDKEEP registry entries is the only way you can configure these quantities.

CA Unicenter NSM Information

CA Unicenter NSM information is stored in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0\NetIQms\Integration\TNG\Config

The key contains the following entries:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSM SERVER</td>
<td>The hostname or IP address of the server where AppManager events are to be forwarded</td>
</tr>
<tr>
<td>NSM REPOSITORY</td>
<td>The name of the NSM repository</td>
</tr>
<tr>
<td>NSM USER</td>
<td>The user name of the NSM repository login account</td>
</tr>
</tbody>
</table>
Event Category Information

Event categories correspond to AppManager Knowledge Script categories, such as IIS for Microsoft Internet Information Server or AMADMIN for AppManager administrative tasks.

Event category information is stored in the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0\NetIQms\Integration\TNG\Filter

The key contains an entry for each Knowledge Script category (such as WINFRAME for Citrix WinFrame). During Setup, selecting a category sets the DWORD value to 00000001; deselecting a category sets the DWORD value to 00000000. If the DWORD value is 00000001, the connector will send an event to the CA Unicenter NSM Console for an event generated by a Knowledge Script job in that category; if the DWORD value is 00000000, an event won’t be sent. In the example that follows, events generated on Citrix WinFrame by a WinFrame Knowledge Script will be forwarded to the CA Unicenter NSM Console; events generated on Compaq Insight Manager by a CIM Knowledge Script will not be forwarded.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSM PASSWORD</td>
<td>Password of the NSM repository login account (encrypted)</td>
</tr>
</tbody>
</table>
| NSM EVENT        | Sets event forwarding from the AppManager Management Server to CA Unicenter NSM.  
|                  | • 1 = ON                                        |
|                  | • 0 = OFF                                       |
|                  | The default is 1 (ON).                          |

### Entry Description

<table>
<thead>
<tr>
<th>Entry Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMADMIN=dword:00000001</td>
</tr>
<tr>
<td>AppManager administrative tasks</td>
</tr>
<tr>
<td>APPL=dword:00000001</td>
</tr>
<tr>
<td>Custom applications</td>
</tr>
<tr>
<td>BACKUPEXEC=dword:00000001</td>
</tr>
<tr>
<td>Veritas Backup Exec</td>
</tr>
<tr>
<td>Entry</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>BTS=dword:0000001</td>
</tr>
<tr>
<td>CIM=dword:0000000</td>
</tr>
<tr>
<td>COMMERCE=dword:0000001</td>
</tr>
<tr>
<td>CONF=dword:0000001</td>
</tr>
<tr>
<td>DB2=dword:0000001</td>
</tr>
<tr>
<td>DELL=dword:0000001</td>
</tr>
<tr>
<td>DISCOVERY=dword:0000001</td>
</tr>
<tr>
<td>DOMINO=dword:0000000</td>
</tr>
<tr>
<td>EXCH=dword:0000001</td>
</tr>
<tr>
<td>FW1=dword:0000001</td>
</tr>
<tr>
<td>GENERAL=dword:0000001</td>
</tr>
<tr>
<td>HPNS=dword:0000000</td>
</tr>
<tr>
<td>IIS=dword:0000001</td>
</tr>
<tr>
<td>ISA=dword:0000001</td>
</tr>
<tr>
<td>MFXP=dword:0000001</td>
</tr>
<tr>
<td>MQSeries=dword:0000001</td>
</tr>
<tr>
<td>MSCS=dword:0000001</td>
</tr>
<tr>
<td>MSMQ=dword:0000001</td>
</tr>
<tr>
<td>MTS=dword:0000001</td>
</tr>
<tr>
<td>NETBACKUP=dword:0000001</td>
</tr>
<tr>
<td>NETBACKUPUNIX=dword:0000001</td>
</tr>
<tr>
<td>NETFINITY=dword:0000001</td>
</tr>
<tr>
<td>NETFINITYDIR=dword:0000001</td>
</tr>
<tr>
<td>NETSERVICES=dword:0000001</td>
</tr>
<tr>
<td>NETSHIELD=dword:0000001</td>
</tr>
<tr>
<td>NETWORKER=dword:0000001</td>
</tr>
<tr>
<td>NT=dword:0000001</td>
</tr>
</tbody>
</table>
### Event Severity Information

Event severity information is stored in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0\NetIQms\  

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTADMIN=dword:00000001</td>
<td>Windows NT administrative tasks</td>
</tr>
<tr>
<td>ORACLE=dword:00000001</td>
<td>Oracle RDBMS Server</td>
</tr>
<tr>
<td>PROXY=dword:00000001</td>
<td>Microsoft Proxy Server</td>
</tr>
<tr>
<td>RDB=dword:00000001</td>
<td>Report database</td>
</tr>
<tr>
<td>QDB=dword:00000001</td>
<td>QDB reports</td>
</tr>
<tr>
<td>SAP=dword:00000001</td>
<td>SAP</td>
</tr>
<tr>
<td>SCANMAILEXCH=dword:00000001</td>
<td>TrendMicro ScanMail for Exchange</td>
</tr>
<tr>
<td>SIEMENS=dword:00000001</td>
<td>Siemens ServerView</td>
</tr>
<tr>
<td>SITE=dword:00000001</td>
<td>Microsoft Site Server</td>
</tr>
<tr>
<td>SEVERITY=dword:00000028</td>
<td>Events with a severity number 40 or greater won’t be sent.</td>
</tr>
<tr>
<td>SMS=dword:00000001</td>
<td>Microsoft Systems Management Server</td>
</tr>
<tr>
<td>SNA=dword:00000001</td>
<td>Microsoft SNA Server</td>
</tr>
<tr>
<td>SQL=dword:00000001</td>
<td>Microsoft SQL Server</td>
</tr>
<tr>
<td>UNIX=dword:00000001</td>
<td>UNIX Server Resources</td>
</tr>
<tr>
<td>WBEM=dword:00000001</td>
<td>Microsoft Web-Based Enterprise Management</td>
</tr>
<tr>
<td>WEBSERVICES=dword:00000001</td>
<td>Web Services</td>
</tr>
<tr>
<td>WIN2000=dword:00000001</td>
<td>Microsoft Windows 2000 Server</td>
</tr>
<tr>
<td>WINFRAME=dword:00000001</td>
<td>Citrix WinFrame Server</td>
</tr>
<tr>
<td>WLBS=dword:00000001</td>
<td>Microsoft Network Load Balancing Service</td>
</tr>
<tr>
<td>WMI=dword:00000001</td>
<td>Microsoft WMI Services</td>
</tr>
<tr>
<td>WTS=dword:00000001</td>
<td>Microsoft Terminal Server</td>
</tr>
<tr>
<td>OTHER=dword:00000001</td>
<td>Custom Knowledge Scripts that you have created that don’t fall into any of the standard categories.</td>
</tr>
</tbody>
</table>
### Integration\TNG\Severity

The key contains an entry for each severity level:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAILURE=dword:00000005</td>
<td>AppManager events with a severity level of 1 - 5</td>
</tr>
<tr>
<td>ERROR=dword:0000000a</td>
<td>AppManager events with a severity level of 6 - 10</td>
</tr>
<tr>
<td>WARNING=dword:00000014</td>
<td>AppManager events with a severity level of 11 - 20</td>
</tr>
<tr>
<td>INFORMATIONAL=dword:0000001e</td>
<td>AppManager events with a severity level of 21 - 30</td>
</tr>
<tr>
<td>SUCCESSFUL=dword:00000028</td>
<td>AppManager events with a severity level of 31 - 40</td>
</tr>
</tbody>
</table>