

Installation Guide

NetIQ® AppManager®

September 2007



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.

© 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.

Part Number: 10045-701

Contents

About This Book and the Library

Intended Audience	xv
Other Information in the Library	xvi
Conventions	xvii
Using Online Help	xvii
About NetIQ Corporation	xviii
Contacting NetIQ Corporation	xviii

Chapter 1 Introduction to AppManager

Understanding AppManager Components	1
Understanding the AppManager Architecture	4
Monitoring in Different Environments	5
Monitoring in a Windows Environment	6
Monitoring in a UNIX Environment	8
Working With Both Windows And Unix Computers	10
Understanding AppManager Reports	12

Chapter 2 Planning to Install AppManager

Getting Started	14
Recommended Implementation Scenarios	14
Small-Scale Implementation: Basic Requirements	14

Medium-Scale Implementation:	
Basic Requirements	15
Large-Scale Implementation.	17
Assembling a Project Team	18
Evaluating the Environment to Be Monitored	19
Understanding Network Connection Requirements	20
Testing Network Connectivity	21
Reviewing AppManager Port Usage	22
Understanding Default Ports for Agent Deployment	24
Understanding Management Sites	25
Understanding Management Server and Repository Locations	25
Understanding AppManager System Resources	26
Sizing the AppManager Repository	27
Accounting for Database Growth	28
Adjusting the Size of Other Databases.	30
Reviewing Security Recommendations	30
Reviewing Your Security Requirements	32
Planning for Localization	33
Planning a Staged Deployment	33
Documenting Decisions and Policies	34

Chapter 3 System Requirements

Understanding System Requirements	36
Module Requirements	36
General Requirements for All Components	37
Supported Platforms and Operating Systems	39
Console Program Requirements	40

Repository Requirements	41
Management Server Requirements	45
AppManager Web Management Server	47
AppManager Operator Web Console	49
AppManager Windows Agent	49
AppManager UNIX Agent	52
Control Center Console	53
Control Center Repository Database	54
Control Center Command Queue Service	55
Control Center Services for Deploying Agents and Modules Remotely	57
Reviewing Required Accounts and Permissions	60

Chapter 4

Installing AppManager

Previewing AppManager Installation	64
AppManager Implementation Checklist	65
Installing Components in Order	65
Understanding the AppManager Installation Kit	67
Saving Installation Kits to a Distribution Computer	67
Installing with Remote Desktop	68
Understanding The AppManager Pre-Installation Check	68
Upgrading from a Previous Version of AppManager ..	69
Running the AppManager Setup Program	70
Reviewing AppManager Log Files	72

Chapter 5	Installing AppManager for Evaluation Purposes	
	Evaluating AppManager	75
	Reviewing Evaluation Installation Requirements	76
	Installing AppManager in Evaluation Mode	77
	Repository Settings in Evaluation Mode	80
Chapter 6	Installing the Repository	
	Understanding the AppManager	
	Repository Installation	81
	Understanding Repository Security Options.	82
	Restricting Knowledge Script Check in.	82
	Installing the AppManager Repository	83
Chapter 7	Installing the Management Server	
	Understanding Management Server Installation	91
	Reviewing Port Information for Management Server	91
	Installing the Management Server	92
Chapter 8	Installing the Operator Console Programs	
	Understanding Operator Console Installation	95
	Installing the Operator Console	96
Chapter 9	Installing Agents	
	Understanding Agent Installation	99
	Understanding Prerequisites for Installing	
	Agents on Windows Server 2003 SP1	100
	Installing Agents in a Windows Environment	102
	Understanding Space Considerations	103
	Understanding Agent Reporting Capabilities	104

Understanding Agent Automatic Discovery	105
Understanding MAPI Mail Settings	105
Understanding Windows User Accounts	106
Understanding Management Server Designation ...	107
Installing the Agent Locally	109
Installing Agents Remotely	114
Post-Installation Tasks	115
Manually Discovering the Agent	115
Firewall Considerations	115
Changing the Default AppManager Listening Ports	117
Installing UNIX Agents	117

Chapter 10

Installing Modules

About AppManager Modules	119
Introducing Module Installation	120
Installing Modules on Managed Clients	121
Installing Modules by Downloading From the Web ..	122
Installing Modules Using the AppManager Installation Kit	125
Installing Modules Remotely by Using Control Center	125
Installing Modules in a VoIP Environment	126

Chapter 11

Installing the Web Management Server

Understanding Web Management Server Installation	129
Installing the Web Management Server	130
Configuring Web Server Security	130

Verifying the Chart Component	132
-------------------------------------	-----

Chapter 12 **Installing Control Center**

Understanding Control Center Installation	135
Understanding the Command Queue Service Options	137
Understanding Optional Configuration for the Command Queue Service	138
Understanding the SQL Server Agent Service Account	140
Understanding the SQL Server Account for Control Center Administration	140
Installing Control Center	141
Installing Components for Deploying Agents Remotely	145
Creating the Web Depot	146
Installing the Deployment Web Service	147
Importing Deployment Rules After Installing Deployment Web Service	148
Installing the Deployment Service	149
Installing SSL Certificates	150
Deployment Service Account Information	151
Post-Installation Tasks	152
SQL Server Security	152
Optional Configuration for the Deployment Service	153
Changing the User Account for the Deployment Service	155
Registering the Location of the Deployment Web Service	156

	Changing the User Account for the Deployment Web Service	157
Chapter 13	Post-Installation Configuration	
	Understanding Security Manager	159
	Starting Security Manager for the First Time	160
	Configuring SNMP for Monitoring Hardware	161
	Checking the SNMP Service	161
	Checking SNMP Security	162
	Using the Microsoft SNMP Utility	163
	Configuring a Mailbox for MAPI Mail	164
	Installing an Exchange Client	165
	Creating an Account for the Agent	165
	Creating an Exchange Mailbox	166
	Using Security Manager to Update Information	167
	Identifying Modules that Require Secure Information	167
	Entering Secure Information	168
	Working with AppManager Connectors	168
Chapter 14	Staging the Deployment	
	Installing in a Lab Environment	169
	Preparing to Install the Pilot Group	170
	Running the Recommended Core Knowledge Scripts	172
	Setting Thresholds for Recommended Scripts	176
	What You Should See	177
	Using the Data Collected	178
	Adjusting Thresholds and Intervals	179

The Next Stage of Deployment	179
Expanding the Scope of Your Deployment	180
Deploying Additional Knowledge Scripts	180
Identifying Your Reporting Requirements.	182
Deploying Actions and Notification Policies	182
Reviewing and Refining the Deployment	183
Extending AppManager	184
Roadmap for a Staged Deployment	185

Appendix A Updating License Information

Understanding AppManager License Keys	187
Managing AppManager Licenses	188
Requesting a License Key	189
Starting License Manager	190
Updating an Expired License	191
Adding and Deleting a License Key	191
Requesting License Information	192
Importing License Keys from a File	193
Running a License Report	193

Appendix B Performing a Silent Installation

Understanding Silent Installation	195
Understanding Silent Installation on Windows Vista . .	196
Repository Installation	197
Sample Repository Installation File	200
Management Server Installation	200
Operator Console Programs Installation	203
AppManager Agent Installation	204

	Module Installation	210
	Web Management Server Installation	212
	Control Center Installation	213
	Control Center Log File Options	216
	Silent Installation on UNIX	217
	Executing UNIX Agent Silent Installation	217
	Performing an Evaluation Installation Silently	218
Appendix C	Uninstalling AppManager	
	Understanding AppManager Uninstallation	221
	Understanding the Uninstallation Sequence	222
	Uninstalling AppManager	223
	Uninstalling AppManager from a Remote Computer .	224
	Uninstalling Agents and Modules Remotely	225
	Uninstalling the Control Center Console	225
	Uninstalling the UNIX Agent	226
Appendix D	Using SMS to Install AppManager Agents	
	Working with Packages	227
Appendix E	Reviewing Microsoft DTC and Control Center Installation	
	Verifying DTC Connectivity before Installation	231
	Reconfiguring DTC in Microsoft Windows Server 2003 SP1 for a Non-Clustered System	233
	Reconfiguring DTC in Microsoft Windows Server 2003 SP1 for a Clustered System	234
	Reconfiguring MSDTC Through a Firewall	236
	Troubleshooting DTC Connectivity	236

Server Name Resolution Failure	237
DTC Fails To Communicate In Windows Server 2003	238
The SID Of One Of The DTCS Is Not Unique . . .	240
SQL Server System Variable @@servername Is Incorrect Or Null	243
Double Hop Error With Kerberos Credentials. . . .	244
Delay In Syncing Of Data From The Appmanager Repository To The Control Center Repository	244

Appendix F VMware Support

AppManager Suite	247
AppManager 7.0	248
AppManager Performance Profiler (AMPP)	250
AppManager Analysis Center	250
VMware Versions Supported	251
Additional Limitations	251

Appendix G Installing in a Clustered Environment

Installing the Repository on a Cluster	253
Understanding MSCS Terminology	253
Reviewing Account Requirements to Install the Repository on a Cluster	255
Installing the Repository on a Virtual Server	256
Installing the Management Server on a Cluster	257
Preparing to Install on a Cluster	258
Running Setup on a Cluster Node	258
Operating in Active/Passive Mode on a Cluster . .	260

Installing AppManager Agents on Each Cluster Node	261
Configuring Communication with Managed Clients	261
Installing Agents on a Cluster	262
Installing on an Active Cluster Node	262
Communicating with a Clustered Management Server	263
Installing Modules on a Cluster	263

About This Book and the Library

The NetIQ AppManager Suite (AppManager) 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 guide provides information to ensure a successful installation of AppManager components. This guide is intended for system administrators and users responsible for installing all or part of the AppManager Suite software.

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.

Conventions

This guide 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 installation kit 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

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**.

About NetIQ Corporation

NetIQ Corporation, an Attachmate business, is a leading provider of comprehensive systems and security management solutions that help enterprises maximize IT service delivery and efficiency. With more than 12,000 customers worldwide, NetIQ solutions yield measurable business value and results that dynamic organizations demand. Best-of-breed solutions from NetIQ Corporation help IT organizations deliver critical business services, mitigate operational risk, and document policy compliance. The company's portfolio of award-winning management solutions includes Systems Management, Security Management, Configuration Control and Enterprise Administration. For more information, please visit www.netiq.com.

Contacting NetIQ Corporation

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

Sales Email: info@netiq.com

Telephone: 1-713-418-5555 (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

Support Web Site: www.netiq.com/support

Introduction to AppManager

AppManager is a client/server application that helps monitor and manage a broad spectrum of IT environments. Before installing AppManager, it is important to understand the crucial components of the AppManager architecture. Understanding how AppManager works helps you develop a workable implementation plan and ensures successful deployment.

This chapter contains the following sections:

- [“Understanding AppManager Components” on page 1](#)
- [“Understanding the AppManager Architecture” on page 4](#)
- [“Monitoring in Different Environments” on page 5](#)
- [“Understanding AppManager Reports” on page 12](#)

If you are not familiar with AppManager components and how these components communicate with each other, read this chapter for an overview. If you already understand the AppManager architecture, proceed to [Chapter 2, “Planning to Install AppManager,”](#) which provides guidelines to help you plan your AppManager installation before you begin to install it.

For a more complete discussion of AppManager architecture, see the *Operator Console User Guide for AppManager*.

Understanding AppManager Components

AppManager’s flexible, multi-tiered architecture consists of required and optional components. The components can be installed together

on a single computer or separately on multiple computers. Each component has unique requirements or configuration options.

The following table describes AppManager components and their usage.

Component	Description	Required/Optional
AppManager repository	The repository is a SQL Server database that stores all of your management information, such as jobs, events, data, and Knowledge Scripts.	Required
Management server	The management server is a Windows service (NetIQms) that manages the event-driven communication between the AppManager repository and the AppManager agents.	Required
AppManager Control Center Console	The Control Center Console offers enhancements over the Operator Console and allows you to easily manage large environments with thousands of servers. Using the Control Center Console, you can quickly push out agents and modules to hundreds of remote computers.	Required/Optional Note: You can use either the Control Center Console or the Operator Console. NetIQ Corporation recommends using the Control Center Console for more powerful monitoring and deployment activities.
AppManager Operator Console	An Operator Console is used to view and control the jobs that monitor and manage your computers and server applications. There are two Operator Console environments: the standard Windows interface Operator Console and the Web browser-based Operator Web Console. In addition to the Operator Console, AppManager includes several other console programs to help you manage your environment, such as the AppManager Security Manager and the Developer's Console.	Required/Optional For more information, see the note under the Control Center Console.

Component	Description	Required/Optional
AppManager agent	<p>The AppManager agent is responsible for monitoring system and application resources, such as CPU utilization or active processes, on the managed computer.</p> <p>For Windows computers, the AppManager agent consists of the NetIQ AppManager Client Resource Monitor (NetIQmc) Windows service, the NetIQ AppManager Client Communication (NetIQccm) Windows service, a local repository database, and at least one module, all of which reside locally on each computer you are managing.</p> <p>For UNIX computers, the agent is a daemon and the supporting files and directories that provide data persistence, equivalent to the local repository, and access to system statistics, equivalent to modules.</p>	Required
AppManager Web management server	<p>Install this component if you want to use the Operator Web Console to check the status of jobs and events, view charts and reports, run Knowledge Script jobs, and view details about the computers you are monitoring using a Web browser.</p>	Optional
AppManager report-enabled agent	<p>Reporting capability is an optional supplement to the AppManager agent that allows you to create and configure reports on selected computers in your environment. You discover report-related elements on managed computers to enable different types of reporting.</p>	Optional

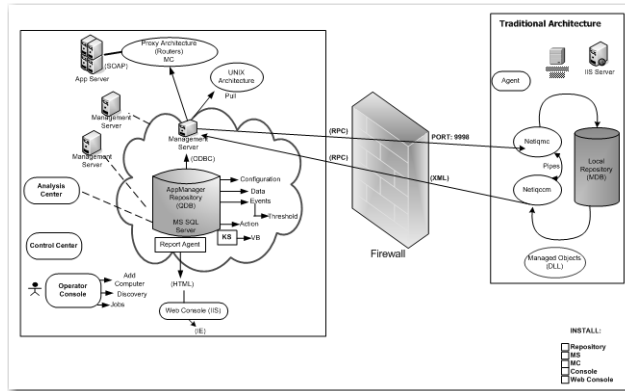
Component	Description	Required/Optional
Developer's Console Utilities	These utilities are used for developing custom Knowledge Scripts.	Optional
Control Center components	Control Center components include the Control Center repository database, the Command Queue Service, the Deployment Service, and the Deployment Web Service. Most Control Center components are required to run Control Center. The Deployment components are only required to install agents, modules, updates, hotfixes, and service packs on remote computers. For more information, see the <i>Control Center User Guide for AppManager</i> .	Optional

Understanding the AppManager Architecture

To provide the best combination of efficiency, scalability, and flexibility, AppManager uses a multi-tier architecture. This multi-tier architecture gives you flexibility in distributing process load across

multiple components and allows for efficient communication between components.

The following graphic illustrates the complete AppManager architecture and how components interact with each other.



For more information about the options for distributing AppManager components across multiple computers, see the *Administrator Guide for AppManager*.

For more information about using consoles to monitor your environment, see the *Operator Console User Guide for AppManager* and the *Control Center User Guide for AppManager*.

Monitoring in Different Environments

The computer on which you install an AppManager agent becomes a managed client that you can monitor. AppManager enables you to

manage both Windows and UNIX clients by running Knowledge Scripts.

Knowledge Scripts are programs that run on managed clients and help you collect data, monitor for events, and perform specific actions in response to events.

A job is an instance of a Knowledge Script running on a managed client. Each time you run a Knowledge Script you are creating a job. For more information, see the *Operator Console User Guide for AppManager*.

At a minimum, every job involves:

- Discovering your managed clients.
- Running Knowledge Script jobs on those managed clients.

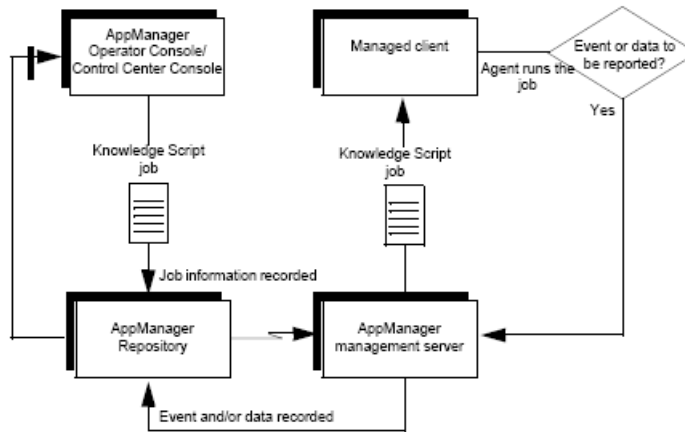
When you start a job, AppManager inserts a new record into the repository and notifies the management server of the job request. This process is common irrespective of the environment you are monitoring. However, some differences may exist depending on the operating environments you intend to monitor. Typically these differences relate to port requirements and deployment options.

After you install and configure all of the appropriate AppManager components, monitoring Windows and UNIX computers is a seamless process with no operational difference.

Monitoring in a Windows Environment

When you start a job on a Windows computer, the NetIQ AppManager Management Service (**NetIQms**) sends the job request to the NetIQ AppManager Client Resource Monitor service (**NetIQmc**).

The **NetIQmc** service receives the request and runs the job locally. The following diagram illustrates this process:



As the agent runs a job, it uses the code in the Knowledge Script to collect the information it needs. The method used to collect the requested information varies. For example, the Knowledge Script may check the value of performance counters, read log files, execute queries, or access system tables.

In a Windows environment, Knowledge Scripts use an OLE automation call to one or more modules to get information. A module is a collection of lower-level COM/OLE objects, packaged in a DLL. The appropriate DLLs are copied to the managed client during setup when you select the servers and applications you want to monitor. For more information, see [“About AppManager Modules” on page 119](#).

Each time the Knowledge Script runs, it evaluates the information returned by the module and determines whether an event has occurred or data needs to be inserted into the repository. If an event condition is detected or a data point collected, the NetIQmc service notifies the NetIQ AppManager Client Communication service

(**NetIQccm**). The **NetIQccm** service then communicates with the management server to upload the information to the repository.

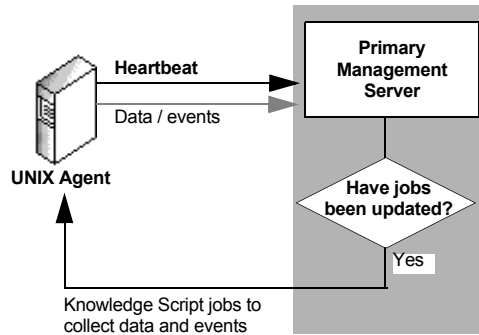
If the **NetIQccm** or **NetIQmc** service cannot communicate with the management server for any reason, the **NetIQccm** service writes the data to the local managed client repository. When connectivity is reestablished, the **NetIQccm** service uploads any data stored locally to the management server.

Monitoring in a UNIX Environment

If you are monitoring UNIX servers, the AppManager agents you install are called UNIX agents. Every 30 seconds, UNIX agents send a heartbeat message to the management server (**NetIQms**) to indicate that they are working properly. Each heartbeat message also requests new or updated job information.

When the UNIX agent contacts the management server, the management server determines whether any of the Knowledge Script jobs for the managed client have been added or updated. If job properties have changed or if new jobs have been added since the last heartbeat interval, the management server delivers the revised job information to the UNIX agent. If there is no change to the Knowledge Script job the managed client is running, the management server simply acknowledges the heartbeat and waits for

the next heartbeat. The following diagram illustrates this communication flow:



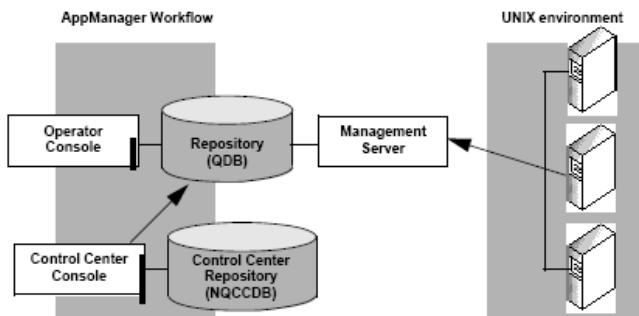
After it receives a job from the management server, the UNIX agent runs the job to access log files, system tables, or other data providers and retrieves the information requested.

Each time the Knowledge Script job runs, it determines whether an event has occurred or data needs to be inserted into the repository. If an event condition is detected or a data point collected, the UNIX agent communicates with the management server to upload the information to the repository.

If the UNIX agent service cannot communicate with the management server for some reason, the agent writes the data to the db directory on the UNIX computer. When connectivity is reestablished, the UNIX agent uploads any data stored locally to the management server.

The management server inserts events and data from the UNIX agent into the standard AppManager workflow. You can see events stored in the repository using the Control Center Console and

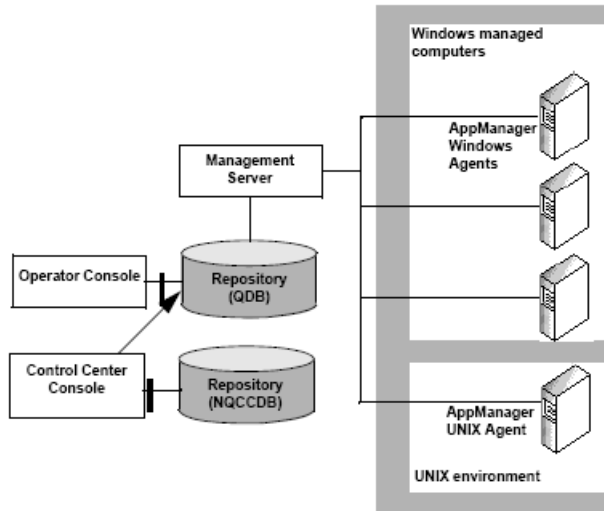
Operator Console. The following diagram illustrates this communication flow:



Working With Both Windows And Unix Computers

Although slight differences in communication exist for Windows-based agents and UNIX-based agents, the AppManager workflow is the same in a heterogeneous monitoring environment. The following

figure illustrates the basic relationship between AppManager components and the UNIX environment:



In an environment with both Windows computers and UNIX computers, a single management server can communicate with:

- Multiple Windows agents
- Multiple UNIX agents
- A combination of Windows and UNIX agents

You can also install multiple management servers in your environment to distribute processing and to provide failover support for both Windows and UNIX computers.

For more information on:

- Configuring a management site to use multiple management servers, see the *Administrator Guide for AppManager*.
- Monitoring in a UNIX environment, see the *AppManager for UNIX Management Guide*.

Understanding AppManager Reports

AppManager reports derive information that Knowledge Scripts collect and store in the repository. To create reports, enable the reporting capability when you install the agent.

For more information about enabling reporting capability on the AppManager agent, see [Chapter 9, “Installing Agents.”](#)

When you enable reporting capability on the agent, report Knowledge Scripts collect monitoring data and generate reports. AppManager reports are typically stored in the following location:
`<InstallDir>:\Program Files\NetIQ\Common\Report`

Note Apart from AppManager reports, you can also install NetIQ Analysis Center in your environment to meet more complex reporting needs. Analysis Center extends AppManager reporting capabilities to provide more sophisticated data access and specialized report scripts. For more information about AppManager reporting and Analysis Center, see the AppManager Help and the *Analysis Center User Guide*.

Planning to Install AppManager

This chapter guides you through the planning issues to consider before installing AppManager.

The following topics are covered in this chapter:

- [“Getting Started” on page 14](#)
- [“Recommended Implementation Scenarios” on page 14](#)
- [“Assembling a Project Team” on page 18](#)
- [“Evaluating the Environment to Be Monitored” on page 19](#)
- [“Understanding Network Connection Requirements” on page 20](#)
- [“Testing Network Connectivity” on page 21](#)
- [“Reviewing AppManager Port Usage” on page 22](#)
- [“Understanding Default Ports for Agent Deployment” on page 24](#)
- [“Understanding Management Sites” on page 25](#)
- [“Understanding Management Server and Repository Locations” on page 25](#)
- [“Understanding AppManager System Resources” on page 26](#)
- [“Sizing the AppManager Repository” on page 27](#)
- [“Reviewing Security Recommendations” on page 30](#)
- [“Planning for Localization” on page 33](#)
- [“Planning a Staged Deployment” on page 33](#)
- [“Documenting Decisions and Policies” on page 34](#)

Getting Started

The planning steps vary depending on what you want to accomplish using AppManager. The following installation paths are typical:

- **Evaluation:** A stand-alone configuration with all AppManager components on a single computer. An Evaluation installation contains just the most basic features of AppManager. For more information, see [Chapter 5, “Installing AppManager for Evaluation Purposes.”](#)
- **Production:** A full-fledged deployment of AppManager based on the environment-specific implementation scenarios. For more information, see [“Recommended Implementation Scenarios” on page 14.](#)

Recommended Implementation Scenarios

Because you can deploy AppManager in almost any scenario, there is no standard implementation formula that is applicable to all scenarios. Consider the following three typical implementation scenarios:

- **Small-scale:** A management site with 150 or fewer managed clients.
- **Medium-scale:** A management site with 151–600 managed clients.
- **Large-scale:** A management site with more than 600 managed clients.

The following sections provide basic requirements and recommendations for each implementation scenario.

Small-Scale Implementation: Basic Requirements

For a small-scale deployment, install the repository, management server, report agent, Operator Console, and Control Center on a

single computer. This computer should be completely dedicated to AppManager and should meet the following basic requirements:

Item	Requirements
Processor	Dual processor of current type, such as Pentium III and later
Memory	2 GB
Disk drive	3 physical disk drives for: <ul style="list-style-type: none">• the operating system• data• logs
Storage	RAID 10 or SAN attached

Note Because all components are installed on the same computer, this implementation creates a single point of failure.

Medium-Scale Implementation: Basic Requirements

For a medium-sized deployment, install the repository, management server, report agent, Operator Console and Control Center

components on three separate computers, as described in the following table:

AppManager Components	Requirements	Notes
Dedicated repository and Web management server	Dual processor (such as Pentium III and later) 4 GB memory 3 physical disk drives: <ul style="list-style-type: none">• operating system• data• logs RAID 10 or SAN attached.	For security reasons, the Web management server should be installed on the same computer as your SQL Server. For more information, see “Installing the Web Management Server” on page 129 . At a minimum, the server should be on a 100 Mbps or faster backbone on the same IP subnet.

AppManager Components	Requirements	Notes
Dedicated management server	Single processor 512 MB memory	<p>A Blade server is ideal. An agent is always installed along with the management server.</p> <p>A secondary management server is recommended for fault tolerance and load balancing.</p> <p>At a minimum, the server should be on a 100 Mbps or faster backbone on the same IP subnet.</p>
Dedicated report agent and Operator Console	Single processor 512 MB memory	<p>A Blade server or computer is fine.</p> <p>You may want to place the report agent on a separate computer, depending on your reporting requirements.</p> <p>The report agent interacts with the processor and memory on the video card and will run better with a higher-end video card.</p>

Large-Scale Implementation

For an AppManager implementation larger than 600 managed clients, NetIQ Corporation recommends that you consult NetIQ Professional Services before you begin installing it. AppManager has a great deal of flexibility and options to improve scalability, and NetIQ Professional Services can help you get the best performance with the smallest hardware investment. For more information, see [Chapter 14, “Staging the Deployment.”](#)

Assembling a Project Team

In larger organizations, where the AppManager installation is likely to involve cross-functional or interdepartmental groups, you may need to assemble a project team and identify the key tasks and responsibilities of each member. The size and technical expertise of the team should reflect the size and management requirements of the deployment. For example, if you are monitoring Exchange Servers, your team should include an Exchange Administrator or individuals with similar experience; if you are monitoring SQL Server, the team should include individuals with database administration experience.

All team members should have fairly comprehensive knowledge of the Windows operating system and administration and the network configuration of the organization. If you are also monitoring UNIX, the team should have at least one UNIX administrator.

The following table provides guidelines for the information that team members should possess:

Area of Expertise	Training or Access Required
Windows	<ul style="list-style-type: none">• Domain structure and trust relationships.• Administrator passwords for all computers where AppManager components are to be installed.• Ability to create and modify user accounts.
Network	<ul style="list-style-type: none">• Network bandwidth and topology.• Latency and the configuration of switches and routers.• Any DNS, WINS, or DHCP setup in use.

Area of Expertise	Training or Access Required
SQL Server	<ul style="list-style-type: none"> • System administrator or local administrator privileges for the AppManager repository server. • Knowledge of SQL Server login IDs and users with permission to access system tables. • Experience with SQL Server security modes. • Ability to evaluate the hardware configuration for the computer that will serve as the AppManager repository server. • Knowledge of SQL Server scheduled tasks. • Understanding of ongoing database maintenance, such as backup / restore and consistency checking.
Applications	<p>Depends on the applications monitored. For example:</p> <ul style="list-style-type: none"> • Monitoring hardware may require knowledge of SNMP community names in use. • Monitoring SQL Server may require knowledge of SQL Server logins or Windows accounts for each server and knowledge of login accounts with special privileges. • Monitoring Exchange requires knowledge of mailboxes and profiles, granting view access, and turning on tracking logs. • Monitoring Oracle requires knowledge of database and instance names, access to system-level (V\$ tables), and the ability to create and modify users.

Evaluating the Environment to Be Monitored

An essential part of planning an AppManager installation is to understand the characteristics of your environment and the network you are going to monitor. This involves determining the following:

- The number of Windows and UNIX servers to be monitored.
- The number and type of application and database servers to be monitored.
- The hardware types to be monitored.
- Specific components to be monitored—for example, operating systems, email servers, clustered applications, and so on.
- The specific objectives of monitoring your environment.

These factors influence how you size the repository and how you distribute AppManager components. Your monitoring goals may also require extra configuration after installation.

Understanding Network Connection Requirements

Reviewing your network configuration is important to determine where to install AppManager components. The following represents the typical network connections in a basic AppManager set up:

- The Operator Console computer and the repository computer require TCP/IP and ODBC connectivity.
- Control Center requires Microsoft Distributed Transaction Coordinator (DTC) connectivity between the Control Center repository and every managed AppManager repository.

DTC connectivity can be checked just before Control Center installation. For more information, see [Appendix E, “Reviewing Microsoft DTC and Control Center Installation.”](#)

- The AppManager repository and the management server, if installed on separate servers, require TCP/IP and ODBC connectivity.
- The management server and each managed client require TCP/IP and RPC connectivity. The management server and managed clients must resolve each other's names or IP addresses.
- The AppManager repository and Web management server, if installed on separate servers, require TCP/IP and ODBC connectivity.
- To enable reporting on a managed client, ODBC connectivity between the managed client and repository is required.
- The Web management server and the Operator Web Console require TCP/IP connectivity.

However, specific types of network connectivity must exist between the computers where specific AppManager components are installed. For more information, see [Chapter 3, “System Requirements.”](#)

Testing Network Connectivity

Test the network connectivity between the following computers in your network:

- AppManager Operator Console computer and the repository computer.
- AppManager repository computer and the management server, if installed on separate servers.
- AppManager management server and each managed client on which the AppManager agent is to be installed.
- AppManager repository computer and the Web management server, if installed on separate servers.
- AppManager Web management server and the Operator Web Console.
- Control Center console and AppManager repositories.
- Control Center console and Control Center repository.
- Control Center Command Queue Service and Control Center repository.

No special domain security requirements apply to network communication between components.

To test network connectivity:

- 1 Log on to a computer you want to test.

For example, to test the connection between the repository and the management server, log on to the computer where the repository is installed.

- 2 Open a command prompt.

3 Enter `ping computer`

where *computer* is the name of the computer to which you want to test the connection. For example, enter the name of the computer where the management server is installed.

If there is network connectivity between the two computers, you will typically see a reply like the following:

```
F:\Mgmt_Server> ping corp08
pinging corp08.west.com [192.90.38.11]
Reply from 192.90.38.11
```

If you do not get a reply, contact your network administrator.

Reviewing AppManager Port Usage

AppManager components communicate with each other through default ports. Check for any port restrictions specific to your site or firewall protections that may prevent you from using certain ports.

The following table lists the default ports that AppManager uses:

Components Communicating	Ports Used	Protocols
Repository from Operator Console	1433 †	SQL ODBC
Repository from management server	1433 †	SQL ODBC
Repository from Web management server	1433 †	SQL ODBC
Operator Console from repository	135 * ‡	SQL ODBC
Installation on target computer from deployment service		TCP/IP
Control Center Command Queue Service to AppManager repository		UDP
Operator Web Console, Web management server		HTTP
Deployment Web Service from agents	80	
Deployment Web Service from Deployment		
Service running in proxy mode		

Components Communicating	Ports Used	Protocols
Deployment Web Service from Deployment Service running in proxy mode	443	HTTPS
Agents from management server	9998	TCP/IP
Management server from agents	9999	TCP/IP
Management server from UNIX agents	9001	TCP/IP
Installation on target computer from deployment service	139	TCP/IP
Control Center Console to Control Center repository	1433 †	SQL ODBC
Control Center Command Queue Service to Control Center repository	1433 †	SQL ODBC
Troubleshooter and NetIQCtrl (Operator Console to agent)	8996 *	TCP/IP
ResponseTime for Networks	10115 *	TCP/IP

Notes * Indicates a bidirectional port requirement.

† Indicates additional port requirements. If you are using a named instance of SQL Server, or if you are not using the default SQL Server port (1433), additional port requirements include:

- the SQL Server Browser port, 1434.
The SQL Server Browser service helps clients determine the associated SQL Server port to use. Once a client establishes a connection to the SQL Server running on the non-default port, it will not use the SQL Browser again unless the SQL Server port changes.
- the SQL Server port for the instance that is hosting your AppManager repository and Control Center repository.

‡ Indicates that an additional port range is needed. If you plan to remotely install agents and updates across a firewall, you need to decide how many ports you want to allocate to DCOM processes on the agents.

You can change the listening ports that the agent services use. However, be particularly careful if you intend to change the port settings. Setting ports incorrectly can disable communication between components. Consult a security administrator before installing if you intend to change communication ports.

Understanding Default Ports for Agent Deployment

In past versions of AppManager, the AMAdmin_AgentInstallProxy Knowledge Script handled agent deployments across a firewall. Port 9979 had to be open on the agent computer to allow the agent services to receive connections from the Knowledge Script. Port 9998 must be open on the agent to enable management server-to-agent communications. A few additional ports are also required to install agent or module updates remotely on managed clients behind a firewall.

Note If you are upgrading from AppManager version 7.0, the port requirements stated in [“Reviewing AppManager Port Usage” on page 22](#) are not applicable.

NetIQ Corporation recommends that you install a separate Deployment Service in each firewall-separated network that contains agents on which you want to remotely deploy updates. If you cannot install a Deployment Service outside the firewall, open the following ports on the agent to allow the Deployment Service to perform deployment tasks across a firewall:

- 139 – Needed to enable NetBIOS processes to install agents and modules.
- 135 – Needed to enable WMI processes to install agents and modules.

Additional ports are required by WMI. Determine how many ports you want to allocate to DCOM processes on the agents. Select a port range, and then open all UDP and TCP ports corresponding to the port numbers you choose.

For more information, see <http://msdn2.microsoft.com/en-us/library/ms809327.aspx>.

Note Opening Port 135 or 139 may expose a computer to vulnerabilities. Both ports are general administrative ports for Windows. NetIQ Corporation recommends that you close both ports after completing your deployment. However, a safer alternative is to co-locate your Deployment Service outside the firewall.

Understanding Management Sites

A management site comprises one AppManager repository and one or more AppManager management servers. Installing multiple management servers allows you to distribute processing and communication for managed clients.

Each managed client needs at least one management server. Consider the following issues if you plan to install multiple management servers:

- Volume of events and data, which directly impact the size and growth of your repository.
- Intensity of network traffic from event and data reporting, which might slow down your connectivity.
- Access-control based on your organization's internal policies.
- Heterogeneity of your environment (for instance, using UNIX servers to handle emails and Windows computers for general business tasks), which affects how you set up your management servers.

Understanding Management Server and Repository Locations

Typically, the AppManager repository and management server are both installed on the same computer. However, you might decide to

install them on separate computers depending on your specific needs. Consider the following factors before making this decision:

- Access control and administration of each managed server in a management site.
- The geographical distribution of servers and management groups.
- Network bandwidth, latency, and normal load on the network.

The management server accesses the repository every 5 seconds and manipulates the data in the repository. This continuous process results in dense network traffic and requires a highly-available connection between the management server and the repository.

For more information about recommended implementations, see [“Recommended Implementation Scenarios” on page 14.](#)

Understanding AppManager System Resources

The following table provides guidelines to plan the resources required to suit your specific environment and monitoring needs:

AppManager Components	Factors Affecting System Resource Requirements
Repository	<ul style="list-style-type: none">• Number of computers, jobs, events, and data streams in your environment.• Network bandwidth and latency and where other components are installed.• Historical reporting requirements.
Management server	<ul style="list-style-type: none">• Number of computers you are monitoring.• Number and frequency of events in your environment.• Number and frequency of data points collected.• Network bandwidth and latency.

AppManager Components	Factors Affecting System Resource Requirements
Operator Console	<ul style="list-style-type: none"> • The preferences and options you have set (for example, the Views, panes, and tabs you decide to display). • Number of computers and details displayed in the TreeView. • Number of jobs, events, data streams, and active, real-time graphs you elect to display.
Agent	<ul style="list-style-type: none"> • Number of jobs running on the computer. • Number of server applications you are monitoring. • Interval at which the jobs run. • Types of jobs you run. Some jobs perform multiple tasks or more complex tasks.

A major factor that can affect management server performance, and agent performance is the number of data streams collected. Each Knowledge Script can potentially collect several data streams. To improve management server performance, configure Knowledge Scripts to collect only the data you need for reporting.

In addition, you can maximize performance by setting up your Operator Console or Control Center Console optimally. For more information, see the *Administrator Guide for AppManager*, the *Operator Console User Guide for AppManager* and the *Control Center User Guide for AppManager*.

Sizing the AppManager Repository

Two important factors that influence the configuration of the AppManager repository database are:

- The number of events you expect to generate
- The number of data points you intend to collect and save for historical reporting or trend analysis

Note AppManager can support up to 25 repositories.

Because this information is difficult to estimate before you install AppManager, and changes as you expand and refine your deployment strategy, NetIQ Corporation recommends the following process a starting point to size your repository.

To estimate the initial size of the repository:

- 1 Count the number of managed clients you plan to monitor and multiply that number by 1 MB to account for the events and data each will generate.
- 2 Multiply the result by the number of days you intend to keep data in the repository. For example:

Number of managed clients=180

Number of days to retain data=30

(Estimated) Repository size= 180 MB X 30 = 5400 MB (5.4 GB)

- 3 Set the initial database size (during installation) to 2 GB and the initial log device size to 600 MB.

Sizing the initial database along these guidelines is a good starting point in most environments. It is roughly one-third of the size for a full deployment.

- 4 Keep the data and the log on separate devices.

Note NetIQ Corporation recommends that you do not use a single repository to monitor more than **600** managed clients.

Accounting for Database Growth

The repository installation displays 100 MB as the default data device size. This size is adequate only for a small network with moderate monitoring activities. Larger AppManager deployments will need additional space.

Note A small network typically comprises 10 computers and generates a data point or an event only about every 10 seconds.

Setting the initial size to about a third of what you think you will need avoids reserving space you will not use during the early stages of deployment, when you are unlikely to run a full set of Knowledge Script jobs or collect all the data you will eventually want to use. Instead, you will probably increase the number of managed clients and the number of jobs you run over time. In addition, maintenance operations, such as backup and restore, are easier if you create smaller data devices and plan for growth rather than sizing the data device at the onset to handle your eventual database requirements.

Although SQL Server can dynamically increase the size of database files and memory, this is not a reliable method for managing database growth. The default setting for the size increase is only 1 MB, which can lead to multiple size increases and corresponding disk fragmentation. Letting the database grow dynamically can also cause fragmentation of the SQL space, which can severely impede performance.

Instead, you should plan for periodic repository database maintenance. Plan to monitor the size of the repository database by running AppManager Knowledge Script jobs to check the size of the repository at regular intervals. If you install the management server and the repository on the same computer, you may also want to set a fixed amount of memory for SQL Server to minimize resource contention between the management server and the repository.

To estimate the potential growth of your AppManager repository, assume it will grow at a rate of about 2 MB per server, per day. NetIQ Corporation recommends installing NetIQ Analysis Center to manage and report on your data if you need to keep data for longer than 90 days. Typically, AppManager performance will start to deteriorate as the repository surpasses 50 GB in size. If repository size exceeds 100 GB, its impact on performance may be quite severe.

AppManager provides many options for managing the repository database and keeping it healthy. For example, you can configure the repository to consolidate older data into daily, weekly, and monthly averages. For more information, see the *Administrator Guide* for

AppManager.

To achieve optimal SQL Server and AppManager performance, place the data and transaction logs on separate physical drives. You can select the locations of these logs during repository installation. For more information, see [Chapter 6, “Installing the Repository.”](#)

Adjusting the Size of Other Databases

As you increase the amount of data you store, you may also need to increase the size of the temp database to handle queries that require temporary space. By default, this database is usually 10 MB. The more data you store and access, and the more you plan to use AppManager’s reporting capabilities, the more space you should set aside for the temp database.

You typically do not need to change the size of the other databases, such as the master database.

Reviewing Security Recommendations

NetIQ Corporation recommends that you use Windows authentication on the SQL Server where you have installed the AppManager repository. Using Windows authentication simplifies several tasks for you when you need to set up permissions for users or groups to access AppManager components and features. If the SQL Server is set up to use mixed mode authentication, users can log into the AppManager repository using either Windows authentication or SQL Server authentication. Then you must not only communicate with users about which login account they should use to access the repository, but you must also configure access permissions on two separate accounts for each user or group. This process is called “assigning AppManager roles.”

We also recommend using Windows groups to provide secure access to AppManager data and components. This approach entails using Windows administrative tools to create and manage user and group accounts and mapping those groups and users to SQL Server login

accounts. You can then use the SQL Server Enterprise Manager to set specific database permissions for these accounts. Finally, you can use AppManager Security Manager to indicate which of your SQL Server login accounts should have access to AppManager.

To configure the SQL Server to set AppManager security roles:

- 1** In the **Security** folder of the SQL Enterprise Manager, double-click **Logins**.
- 2** Double-click the group name to open the SQL Server Login Properties dialog box.
- 3** On the **Database Access** tab, select the repository and make sure the **public** database role is enabled.

All other security configuration is performed from AppManager Security Manager. Information about logins and passwords needed by specific Knowledge Scripts can always be found in the Knowledge Script Help, which also provides guidance on entering security information in Security Manager.

Agent installation offers extra security options to encrypt agent-to-management server communications, or to encrypt communications and require agents to authenticate the management server. For more information, see [“Installing the Agent Locally” on page 109](#). In most cases, you do not need to use these extra options, which add some overhead to production servers and the management server.

AppManager always encrypts passwords, so even without extra agent security options, only user names are sent as clear text over the network. If you require a password for access to a particular application, like SQL, the password is encrypted in a special table. That encrypted password is sent to the agent, which records it locally, still encrypted. Only when a job executes will the password be unencrypted and used to gain access to the application.

Reviewing Your Security Requirements

To assess your security requirements before installing AppManager, do the following:

- Verify the SQL Server security mode you are using.

For more information about the relationship between SQL Server security and AppManager, see the *Administrator Guide for AppManager*. For more information about using security modes, see the Microsoft SQL Server documentation. For more information about adding AppManager users, see [Chapter 13, “Post-Installation Configuration.”](#)

- Determine the AppManager user roles you need and the AppManager-related rights associated with each role. In general, NetIQ Corporation recommends that you stringently restrict user rights initially, and expand rights over time as you refine AppManager roles.

You can use role-based security profiles to restrict access to specific AppManager activities, views, computers, or Knowledge Script categories.

For more information, see the *Administrator Guide for AppManager* and [Chapter 13, “Post-Installation Configuration.”](#)

- Determine the level of security appropriate for the management server and managed clients (agents). To secure communication between the management server and agents, you can choose either encrypted communication only or management server authentication and encrypted communication.

Encrypted communication provides a basic level of security with little impact on performance. Using authentication and encryption provides an additional layer of security, but it requires you to perform additional steps to manage and distribute keys.

Note Although secure communication is managed separately for Windows-based agents and UNIX-based agents, all management servers and managed clients in a single repository should use the

same level of security. For either platform, you cannot mix security levels. For example, you cannot set some Windows managed clients to use clear text or encryption while other Windows managed clients use authentication and encryption.

- Determine any security-related information needed to run Knowledge Scripts (for example, community names, user account or password information). Typically, you need to enter this information when you install the module for an application that requires it. For example, AppManager for Microsoft Exchange Server requires a user account, profile, and mailbox alias name. For more information, [“Configuring a Mailbox for MAPI Mail” on page 164](#).

Planning for Localization

AppManager is supported on the US English version of supported Windows operating systems, using the US English locale. In addition, we support the use of AppManager on some additional regional settings (locales), as listed below:

- German
- Spanish (Spain)

For information on support for the Italian and French locales of AppManager version 7.0 and later, contact NetIQ Technical Support.

Planning a Staged Deployment

Typically, you deploy an AppManager installation in stages. A staged deployment is recommended because you can fine-tune your implementation with each step. For more information about staged deployment, see [Chapter 14, “Staging the Deployment.”](#)

Documenting Decisions and Policies

An important part of a successful deployment is complete and accurate documentation. Throughout the deployment cycle, document your plans, testing, results, and policy decisions. Ideally, each stage of the project should include a document that records the tasks completed and the strategies implemented. For example, articulate specific policies determining who should respond to certain types of events, how individuals should receive notification, who is responsible for closing or deleting events, and how or when events should be closed or deleted.

AppManager can even help with documentation tasks. While AppManager does not automatically document your monitoring policies, the Report_JobInfo Knowledge Script records all jobs and their settings. Schedule this Knowledge Script to run regularly to help keep documentation up to date. You can also use Report_JobInfo when an agent suddenly begins sending several simultaneous events. You can compare current job settings to previous job settings to see whether the events are being generated due to a configuration change.

System Requirements

This chapter describes system requirements to install AppManager successfully.

The following topics are covered:

- [“Understanding System Requirements” on page 36](#)
- [“Module Requirements” on page 36](#)
- [“General Requirements for All Components” on page 37](#)
- [“Supported Platforms and Operating Systems” on page 39](#)
- [“Console Program Requirements” on page 40](#)
- [“Repository Requirements” on page 41](#)
- [“Management Server Requirements” on page 45](#)
- [“AppManager Windows Agent” on page 49](#)
- [“AppManager UNIX Agent” on page 52](#)
- [“Control Center Console” on page 53](#)
- [“Control Center Repository Database” on page 54](#)
- [“Control Center Command Queue Service” on page 55](#)
- [“Control Center Services for Deploying Agents and Modules Remotely” on page 57](#)
- [“Reviewing Required Accounts and Permissions” on page 60](#)

Understanding System Requirements

Before running the AppManager Setup program, review the AppManager system requirements and verify that the computers where you plan to install AppManager components meet all system requirements.

Although the AppManager pre-installation check program verifies most system requirements, you might need to verify some requirements manually. This chapter provides specific information about all AppManager system requirements. In addition, you can also check the AppManager Release Notes and the NetIQ Support Web site for the latest information about system requirements and supported products.

The following table provides a pre-installation check legend for each AppManager system requirement listed in the following sections

Symbol	Meaning
v	Verified by the pre-installation check program. Although these requirements represent the minimum configuration needed, they may not be recommended for your environment. In adjusting the minimum requirements to your organization's needs, consider the number of servers monitored, the number of jobs, the data you collect and other factors. For more information about the factors to consider, see Chapter 2, "Planning to Install AppManager."
n	Not verified by the pre-installation check program. You must check this requirement manually.

Module Requirements

AppManager offers monitoring support for a large number of modules and each module may have unique requirements. The pre-installation check program verifies most module-specific

requirements. If a computer does not pass the requirements to monitor an application with a module, that module does not appear in the list of available modules during installation.

For up-to-date information regarding supported product versions and unique requirements for monitoring third-party systems, see the AppManager Supported Products Web site at www.netiq.com/support/am/supportedproducts.asp.

General Requirements for All Components

On all Windows computers, ensure that the version number of `msi.dll` is 3.1.4000.1823 or higher to avoid the following error:

Error 1723. There is a problem with this windows Installer package. A DLL required for this install to complete could not be run. Contact your support personnel or package vendor.

`msi.dll` is typically located in the `\windows\system32` folder.

`windowsInstaller-KB893803-v2-x86.exe` verifies the version number of `msi.dll`. This file is located in the `\appmanager\extras\utilities\instmsi` folder.

Restart the computer after the Windows Installer installation.

The following table summarizes the requirements that are common to all AppManager components:

Pre-install Check Verified?	Requirements
v	For AppManager Operator Console, repository, management server, and Web management server, and for Control Center components, an Intel-based Pentium III computer running at 733 MHz (or higher).
v	Valid Windows login account with Administrator privileges. The privileges can be for the local computer (required) or the Domain (optional).

Pre-install Check Verified?	Requirements
v	Windows Installer 3.1 or later. Included with Windows XP and Windows Server 2003, and with the .NET Framework. If your computer does not have it, you may need a Windows Update. Check the Microsoft Web site for more information. A copy of Windows Installer is provided in the AppManager installation kit, in the \Prerequisites\Microsoft windows Installer folder.
v	Valid temp or tmp Path environment. AppManager may require up to approximately 80 MB of temporary disk space on the drive where the temp or tmp directory resides. For more information, see “Understanding Space Considerations” on page 103 .
n	Appropriate ODBC drivers (ODBC32.DLL, ODBC32.DLL, ODBCINT.DLL, ODBC32.DLL) installed in the system directory.
n	Event Viewer closed during the installation. If open, it may cause locking contention with processes trying to write to the Windows Log. No Event Viewers—local or remote—should be viewing the computer where you plan to install AppManager.
n	All Control Panel applets, such as Services, closed.
n	Network connectivity between computers. For more information, see “Understanding Network Connection Requirements” on page 20 .

Supported Platforms and Operating Systems

The following table lists the platforms and operating systems that AppManager supports:

Component	Operating System Version
Repository Management server	Windows 2000 Server
Web management server	Windows Server 2003*
Console programs (including Control Center Console)	Windows 2000 Server Windows XP Professional Windows Server 2003* Windows Vista (Business and Enterprise editions) on 32 bit systems
Windows Agent	Windows 2000 Server Windows XP Professional Windows Server 2003 Windows Vista (Business and Enterprise editions) on 32 bit systems
UNIX agent	Sun Solaris Red Hat Linux SuSE Linux HP-UX IBM AIX For more information about UNIX platform support, see the <i>AppManager for UNIX Management Guide</i> .
Control Center repository	Windows 2000 Server
Command Queue Service	Windows Server 2003*
Deployment Service	Windows Server 2003*
Deployment Web Service	

Note *At this time only 32-bit Operating System versions of Windows 2003 Server are supported for all Windows components.

In general, AppManager can monitor current, generally available versions of supported systems and applications including 64-bit systems and applications. In some cases, however, not all versions or

platforms are supported for specific applications. For up-to-date information regarding the systems, applications, and versions of those products that AppManager currently supports, check the AppManager Supported Products Web site at <http://www.netiq.com/support/am/supportedproducts.asp>.

Console Program Requirements

AppManager console programs include a collection of programs that operators and administrators use to manage various aspects of their environment. You can install one or all of the following consoles:

- Control Center Console
- Operator Console
- Security Manager
- Developer's Console

The following table describes the requirements for Console programs.

Pre-install Check Verified?	Requirements
v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	At least 256 MB of RAM.
v	At least 64 MB of available disk space. Depending on the number of managed clients, events you expect to generate, and amount of data you expect to collect, you may need to allow additional disk space for the local cache folder and paging files.
v	256-color display monitor configured for at least 1024x768 display resolution.
v	MDAC 2.6 or 2.7.
n	Windows 2000 Server, Windows Server 2003, or Windows XP Professional. <ul style="list-style-type: none"> Windows 2000 Server (SP 4 or later), Advanced Server, or Windows 2000 Professional. Windows Server 2003 Standard Edition, Enterprise Edition, Web Edition, or Windows XP Professional (SP 2). Windows Vista Business and Enterprise editions (on 32-bit systems)
n	ODBC SQL Server driver (SQLSRV32.DLL) and DBNMPNTW.DLL installed in the System directory.
n	Microsoft Internet Explorer 6.0 (or later).
n	Microsoft XML Parser, version 3.0 (msxm13) SP1 or later.
n	Network connectivity between this computer and the computer where the repository is to be installed. For more information, see "Testing Network Connectivity" on page 21 .

Repository Requirements

The following table lists repository requirements.

Pre-install Requirements	
Check	Verified?
	v Intel-based Pentium III computer running at 733 MHz (or higher).
	v Windows 2000 Server or Windows Server 2003: <ul style="list-style-type: none"> • Windows 2000 Server or Advanced Server (SP 4 or later). • Windows Server 2003 Standard Edition or Enterprise Edition.
	v Microsoft SQL Server 2000 (SP 3a or later). SQL collation must be set to the default, which is SQL_Latin1_General_CP1_CI_AS. To check the version of SQL Server: 1 Start SQL Enterprise Manager. 2 Select the SQL Server in the list. 3 Select Tools > SQL Query Tool . 4 In the Query dialog box, type the following query: select @@version Note There are no spaces in @@version. 5 Click Execute Query . 6 Check the results. Note For installing the AppManager Repository on SQL Server 2005, Windows 2003 Server Service Pack 1 is required.
	v ODBC SQL Server driver (SQLSRV32.DLL) and DBNMPNTW.DLL installed in the System directory. Setup installs these files if they are not found on the system. If the computer already has ODBC drivers, the AppManager setup program leaves the existing drivers in place.
	v At least 512 MB of RAM.
	v At least 200 MB of available disk space. <ul style="list-style-type: none"> • At least 100 MB is required for the repository's data device. Note AppManager uses 13 MB of the data device space to store Knowledge Scripts, tables, and stored procedures. At least 9 MB is required for AppManager executable files and tools. • At least 50 MB is required for the repository's log device. Note Values for the data and log devices can be reduced for small, departmental solutions or increased for large-scale deployments.
	v MDAC 2.6 or 2.7.

Pre-install Requirements
Check
Verified?

- y
- Account access and password for the SQL Server sa login account.
- Setup uses this account to create a NetIQ SQL Server login account, and prompts you for a password. The default account name and password are netiq.
 - The netiq account should be db_owner of the repository. Otherwise, it needs rights enough to use DBCC as it reindexes during the scheduled tasks. And it has to be able to delete and move data from the repository.
 - The management server needs enough rights on the repository account to do reads, inserts, and deletes from any table and to execute any stored procedure. Neither needs to have access to any other database except for the ability to invoke extended stored procedures.

Notes

- If the SQL Server 2005 on which the AppManager Repository is being installed has a strong password policy, you must specify a netiq account password that meets the requirements. If the specified password does not meet the password policy, the installation will fail and you must manually uninstall the repository database.
- For successful installation, ensure that the netiq SQL login does not already exist in your SQL Server environment. If it exists, it may create a conflict unless the database administrator uses SQL Enterprise Manager to set the Login Properties on the Database Access tab for the account to use a fully qualified account name (DOMAIN\login).

-
- n
- Security mode configured to run in **Windows Authentication** or **Mixed** security mode.
- Note** When running in mixed security mode, use a SQL Server login account to access the AppManager Operator Console, Security Manager, and Operator Web Console.

Pre-install Requirements**Check****Verified?**

v	<p>The Named Pipes network protocol. Required for SQL Server. (You can have other protocols in addition).</p> <p>If SQL Server is not configured for any network protocol, run SQL Server Setup again before installing AppManager and at a minimum add the Named Pipes protocol.</p>
v	<p>The following services started:</p> <ul style="list-style-type: none">• For SQL Server 2000 without instances: MSSQLServer and SQLServerAgent.• For SQL Server 2000 with instances: MSSQL\$<instance> and SQLAgent\$<instance> <p>You can manually start these services, or let AppManager Setup automatically start them. The startup type for the SQLServerAgent service is set to Manual by default. AppManager Setup will start the service; you do not have to set the startup type to Automatic.</p>
n	<p>MSDB database. MSDB must exist in SQL Server.</p> <p>To check for the database:</p> <ol style="list-style-type: none">1 Start SQL Enterprise Manager.2 In the list, right-click the SQL Server where the AppManager repository is installed.3 Select Tools > SQL Query Tool.4 In the Query dialog box, type the following query: <code>sp_helpdb msdb</code>5 Click Execute Query.6 Check the results. <p>If msdb does not exist:</p> <ol style="list-style-type: none">1 Start SQL Enterprise Manager.2 Stop the SQLServerAgent service.3 In the list, right-click the SQL Server where the AppManager repository is installed.4 Select Tools > SQL Query Tool.5 In the Query dialog box, click Load SQL Script.6 Select <code>MSSQL\INSTALL\INSTMSDB.SQL</code>. Click Open.7 In the Query dialog box, click Execute Query.8 Load and execute <code>MSSQL\INSTALL\SERVMSG.SQL</code>.9 Restart the SQLServerAgent service.

Management Server Requirements

The management server needs excellent network access to the repository. Install it on the same computer as the repository for smaller AppManager deployments (150 managed clients or fewer). For more information, see [“Recommended Implementation Scenarios” on page 14](#).

The following table describes the requirements for installing the management server.

Pre-install Check Verified?	Requirements
v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	Windows 2000 Server or Windows Server 2003: <ul style="list-style-type: none">• Windows 2000 Server or Advanced Server (SP 4 or later).• Windows Server 2003 Standard Edition or Enterprise Edition. Note If you want to use authentication and encryption between the management server and the agent, be sure the Windows High Encryption Pack is installed in your environment. The Windows High Encryption Pack is normally included in Windows 2000 Server and Windows Server 2003.
v	ODBC SQL Server driver (SQLSRV32.DLL) and DBNMPNTW.DLL installed in the System directory. Setup will install these files, if they are not found on the system. If the computer already has ODBC drivers, the AppManager setup program leaves the existing drivers in place.
v	At least 256 MB of RAM.
v	At least 70 MB of available disk space.
v	MDAC 2.6 or 2.7.

Pre-install Check Verified?	Requirements
n	<p>A service account (sometimes called the run-as account) for the NetIQms service, either:</p> <ul style="list-style-type: none"> • The Local System account. • A valid Windows login account. <p>Note If running SQL Server in Windows Authentication mode, you must specify a valid Windows login account as the service account for the AppManager management server service (NetIQms). During the setup process for the management server, disable Management server service runs as Local System account and specify a Windows login account.</p>
v	<p>Availability of TCP port 9999. If this port is being used by another application, reconfigure the application to use another port.</p>
n	<p>Static IP address (highly recommended). DHCP is supported but should not be used if a static IP address is available.</p> <p>Note If using DHCP, run the AMAdmin_ConfigSiteCommType Knowledge Script, with Communication via IP address disabled, on the managed clients. The AppManager agent service on the managed client will then communicate with the management server using the server hostname instead of the IP address. Resolving the hostname incurs more overhead on the managed client.</p>
n	<p>Install the AppManager agent component on this computer.</p> <p>Installing the agent allows you to run recovery actions (such as sending e-mail) and use AppManager's centralized-installation procedure to install the agent on managed clients.</p> <p>Note NetIQ Corporation recommends installing the agent when you install the management server. Otherwise, Setup automatically installs the agent with the appropriate Windows module, but you will not be able to specify any agent options such as enabling MAPI mail.</p>
n	<p>Network connectivity between this computer and the repository computer. For more information, see "Understanding Network Connection Requirements" on page 20.</p>
n	<p>Network connectivity between this computer and the managed clients. For more information, see "Understanding Network Connection Requirements" on page 20.</p>
v	<p>Microsoft XML Parser, version 6.0 (msxm16), SP1 or later.</p>

AppManager Web Management Server

NetIQ Corporation recommends installing the Web management server on the same computer as the AppManager repository for additional security.

The following table lists system requirements for Web management servers.

Pre-install Check Verified?	Requirements
v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	Windows 2000 Server or Windows Server 2003 and Internet Information Server (IIS). Either: <ul style="list-style-type: none">• Windows 2000 Server or Advanced Server with SP3 or later and IIS 5.0 or later.• Windows Server 2003 Standard Edition or Enterprise Edition and IIS 6.0. Notes: <ul style="list-style-type: none">• IIS must be running the World Wide Web Publishing Service (a standard Windows service).• If you are using Windows Server 2003 and IIS 6.0, you must allow Active Server Page extensions on the computer where you plan to install the Web management server. If the setup program finds you do not have Active Server Page extensions enabled, it displays a warning.
v	At least 256 MB of RAM.
v	At least 40 MB of available disk space in the IIS Web folder (the default folder is c:\inetpub\wwwroot) and 30 MB of temporary space.
v	Active Server Pages (ASP) installed and enabled.
v	Active Data Objects (ADO) installed and enabled.
v	MDAC 2.6 or 2.7.
n	ODBC SQL Server driver (SQLSRV32.DLL) and DBNMPNTW.DLL installed in the System directory.

Pre-install Check Verified?	Requirements
n	The Web server must be able to communicate with the SQL Server where the AppManager repository resides. This means that these two computers should be connected on the same network.
n	Microsoft XML Parser, version 3.0 (msxm13), SP1 or later.

AppManager Operator Web Console

The Operator Web Console allows you to view AppManager information published by the AppManager Web management server.

The following table lists system requirements for Operator Web Console computers.

Pre-install Requirements	
Check	Verified?
v	Windows 2000 Server or Windows Server 2003: <ul style="list-style-type: none">• Windows 2000 Server (SP 4 or later) or Advanced Server, or Windows 2000 Professional.• Windows Server 2003 Standard Edition, Enterprise Edition, Web Edition, or Windows XP Professional.
v	Microsoft Internet Explorer 6.0 (or later) on Windows Server 2003 or Windows 2000 Server, Advanced Server, or Professional (with SP3 or later). Be sure your Web browser has the following settings: <ul style="list-style-type: none">• Java- and JavaScript-enabled.• Can accept cookies.• Supports frames and tables.
v	MDAC 2.6 or later (to view charts in Internet Explorer). The setup program is included in the AppManager installation kit.
n	Microsoft XML Parser, version 3.0 (msxm13), SP1 or later.
n	AppManager version checker (to install the chart component).
n	AppManager chart component (to view charts in Internet Explorer). If the chart component is not installed, when you click Charts in the navigation bar, the Charts page provides instructions on how to install the chart component.

AppManager Windows Agent

The requirements in the following table apply to all Windows-based managed clients. The table does not include requirements for applications you want to monitor with modules. For more

information about module requirements, see [“Module Requirements” on page 36](#).

Pre-install Requirements	
Check	
Verified?	
v	Intel-based Pentium computer running at 100 MHz (or higher).
v	<p>Windows 2000 Server, Windows XP Professional, or Windows Server 2003:</p> <ul style="list-style-type: none">• Windows 2000 Server or Advanced Server, or Windows Server Professional with SP 3 or later.• Windows XP Professional.• Windows Server 2003 Standard Edition, Enterprise Edition, or Web Edition.• Windows Vista Business and Enterprise editions <p>Note If you want to use authentication and encryption between the management server and the agent, be sure you have the Windows High Encryption Pack installed. The Windows High Encryption Pack is normally included in Windows 2000 Server and Windows Server 2003. If you are installing on Windows NT 4.0, however, you should verify check your version of the operating system for the Windows High Encryption Pack.</p>
v	At least 32 MB of RAM.
v	At least 55 MB of available disk space.
v	<p>MDAC 2.0 or later is supported. However, the minimum recommended version is MDAC 2.1, SP2 or later.</p> <p>You should use MDAC 2.5 or later for the report-enabled agent or MDAC 2.6 or later if the report-enabled agent is used for Analysis Center reports.</p> <p>Note If you use MDAC 2.6 or later, you may need to install the JetPack driver separately. This driver is required for the local repository on the managed client, but is not included in MDAC 2.6 or later.</p>
v	<p>ODBC Access driver installed (required for the local repository).</p> <p>If the computer already has a driver, the AppManager setup program leaves the existing driver in place.</p>
v	<p>Availability of TCP port 9998. If this port is being used by another application, reconfigure the application to use another port.</p> <p>For more information, see “Reviewing AppManager Port Usage” on page 22.</p>

Pre-install Requirements

Check

Verified?

y	<p>(Optional) For disk array subsystems, Performance Monitor for disk activities enabled. Run the program %systemroot%\system32\diskperf.exe with the -y switch. Reboot your system after enabling the disk counters.</p> <p>Note You only have to enable disk counters if you plan to run disk-related Knowledge Scripts, such as NT_LogicalDiskIO and NT_PhysicalDiskIO.</p>
n	<p>A service account for the NetIQmc and NetIQccm services to use. Either:</p> <ul style="list-style-type: none">• The Local System account, or• A valid Windows login account.
n	<p>Microsoft XML Parser, version 3.0 (msxm13), SP1 or later, for the report agent, or if the report agent is used for Analysis Center reports.</p>
n	<p>(Optional) SNMP Service does not need to be running when you install AppManager; however, some Knowledge Scripts, such as SNMPGet, require the SNMP Service to be installed and running.</p>
n	<p>(Optional) Install Microsoft Exchange Client.</p> <ul style="list-style-type: none">• Exchange Client is required if selecting the setup option to enable MAPI mail on a computer that is not an Exchange Server. Installing the Exchange Client allows AppManager to initiate MAPI mail recovery actions. In addition to installing the Exchange client, you need to create a mailbox for AppManager to use. For more information, see “Configuring a Mailbox for MAPI Mail” on page 164.• If installing the Exchange module, with or without the MAPI mail option, you can select to have the setup program create an Exchange mailbox. This option does not require Exchange Client to be previously installed. If, however, you do not select the mailbox option, you will need to create a mailbox before running Setup. For more information, see “Using Security Manager to Update Information” on page 167.
n	<p>Network connectivity between this computer and the computer where the management server is to be installed. For more information, see “Understanding Network Connection Requirements” on page 20.</p>
n	<p>A static IP address is recommended; however, DHCP is supported.</p>

If you want to enable reporting for an AppManager agent, check for the following report-specific requirements:

- MDAC 2.6 or MDAC 2.7.
- SQL Server 2000 Analysis Services Client components. SQL Server 2000 Analysis Services components are required if you want to generate reports using the Analysis Center data warehouse. For more information, see the *Analysis Center User Guide*.
- Internet Explorer 6.0 or later with Scripting Support.

AppManager UNIX Agent

The system requirements for UNIX agents are platform- dependent and checked by the pre-installation check program as soon as Setup begins. In addition to the basic system requirements check, each

module you install verifies application-specific requirements. The following table lists basic requirements. For more information, see the *AppManager for UNIX Management Guide*.

Pre-install Check Verified?	Requirements
v	<p>Operating systems:</p> <p>Refer to the <i>AppManager for UNIX Management Guide</i>, provided in the UNIX Components installation kit, for a list of supported platforms.</p> <p>Different operating systems and versions may require specific patches or system libraries to work correctly. Because this information changes frequently, NetIQ Corporation recommends that you check the NetIQ Web site and the Web site of your operating system vendor for up-to-date patch information.</p>
v	<p>Disk space for installed files:</p> <ul style="list-style-type: none"> • On Sun Solaris, approximately 120 MB. • On Linux, approximately 105 MB. • On HP-UX, approximately 155 MB. • On IBM AIX, approximately 175 MB.
v	(All platforms) Approximately 10 MB of disk space for temporary files.
v	(All platforms) At least 16 MB of available memory.

For the most up-to-date information about system requirements and platform support for UNIX agents and applications, see the NetIQ Web site <http://www.netiq.com/support/am/supportedproducts.asp#Unix>.

Control Center Console

The Control Center Console, the Control Center repository database, and the Command Queue Service can all reside on the same computer, but distributing them among multiple different Windows computers can improve performance.

The following table lists system requirements for the Control Center

Console.

Pre-install Check Verified?	Requirements
v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	At least 512 MB of RAM.
v	At least 1 GB of available disk space. Depending on the number of managed clients, events you expect to generate, and jobs you expect to run in data collection mode, you may need to allow additional disk space for the local cache folder and paging files. 110 MB are recommended for large environments.
v	256-color display monitor configured for at least 1024x768 display resolution.
v	Operating systems: <ul style="list-style-type: none">• Windows 2000 Server (SP 4 or later)• Windows XP (SP 2 or later)• Windows Server 2003• Windows Vista Business and Enterprise editions (on 32-bit systems)
v	Microsoft .NET Framework 1.1 or later.
v	Microsoft Background Intelligent Transfer Service (BITS) Client Component, version 1.5 (or later). Provided with the AppManager installation kit in the Prerequisites folder.
v	Microsoft Terminal Services Client ActiveX Control.

Control Center Repository Database

Some requirements for the Control Center repository are different from those of the AppManager repository.

The following table lists system requirements for the Control Center

Repository.

Pre-install Requirements	
Check	Verified?
v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	At least 256 MB of RAM.
v	At least 64 MB of available disk space. 110 MB are recommended for large environments.
v	<ul style="list-style-type: none">• Windows 2000 Server (SP 4 or later).• Windows Server 2003.
v	Microsoft .NET Framework 1.1 or later.
v	<ul style="list-style-type: none">• SQL Server 2000 with SP3 or 3a.• SQL Server 2005, running on Windows Server 2003 with SP1. <p>Note SQL Server and the SQL server agent must be running. Make sure that SQL Server services are set to auto start, and that you have security access. Pre-installation checking does not check for these conditions.</p>
n	Microsoft DTC (Distributed Transaction Coordinator), running as a service. If you install Control Center components on Windows Server 2003 with Service Pack 1, you will have to do some extra configuration to make sure Control Center can find and use the DTC service. For more information, see Appendix E, “Reviewing Microsoft DTC and Control Center Installation.”
n	Network connectivity: If you decide to install the Command Queue Service on a separate system from the Control Center database, both systems should reside on the same LAN.

Control Center Command Queue Service

The following table lists system requirements for the Control Center

Command Queue Service.

Pre-install Check Verified?	Requirements
v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	At least 256 MB of RAM.
v	At least 64 MB of available disk space. 110 MB are recommended for large environments.
v	<ul style="list-style-type: none">• Windows 2000 Server (SP 4 or later).• Windows Server 2003.
n	<p>A valid Windows user account that is part of the local Administrators group.</p> <p>An account with Domain Admin privileges is not sufficient unless it is also a <i>direct</i> member of the local Administrators group. The credentials for this account are needed to install and run the Command Queue Service and Deployment services for deploying agents and modules remotely.</p> <p>You are asked to supply credentials for this account as part of the installation.</p>
v	Microsoft .NET Framework 1.1 or later.
n	Network connectivity: If you decide to install the Command Queue Service on a separate system from the Control Center repository database, both systems should reside on the same LAN.

Note Only one Command Queue Service may be connected to any single Control Center repository.

Control Center Services for Deploying Agents and Modules Remotely

To use the Control Center for deploying agents and modules remotely, install either the Deployment Service, the Deployment Web Service, or both.

Note The Deployment Service uses port 139 by default to remotely deploy agents and modules. However, if port 139 is not available and a firewall is not present, you can use port 445 to remotely deploy agents and modules.

The following table lists system requirements for the Deployment Service and the Deployment Web Service.

Deployment Service	
Pre-install	Requirements
Check	
Verified?	
v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	At least 256 MB of RAM.
v	At least 64 MB of available disk space.
v	Windows Server 2003.
n	<p>A valid Windows user account that is part of the local Administrators group.</p> <p>An account with Domain Admin privileges is not sufficient unless it is also a <i>direct</i> member of the local Administrators group. The credentials for this account are needed to install and run the Command Queue Service and Deployment services for deploying agents and modules remotely.</p> <p>You are asked to supply credentials for this account as part of the installation.</p>
v	Microsoft .NET Framework 1.1 or later.
n	Network connectivity: If you decide to install the Deployment Service on a separate system from the Control Center repository database, both systems should reside on the same LAN.
v	<p>Microsoft Background Intelligent Transfer Service (BITS) Client Component, version 1.5 (or later).</p> <p>Provided with the AppManager installation kit in the Prerequisites folder.</p>
n	SSL Certificate installed. Allows the Deployment Service to run in proxy mode to access the Deployment Web Service across a firewall. For more information, see "Installing SSL Certificates" on page 150 .

Deployment Web Service

Pre-install Requirements

Check

Verified?

v	Intel-based Pentium III computer running at 733 MHz (or higher).
v	At least 256 MB of RAM.
v	At least 64 MB of available disk space.
v	Windows Server 2003.
v	Microsoft .NET Framework 1.1 or later.
n	Network connectivity: If you decide to install the Deployment Web Service on a separate system from the Control Center repository database, both systems should reside on the same LAN.
v	<p>Microsoft IIS with the following optional components enabled:</p> <ul style="list-style-type: none">• ASP.NET.• BITS Server Extensions.• Default IIS Web site• Default port bindings <p>Notes:</p> <ul style="list-style-type: none">• On some systems, ASP.NET and BITS Server Extensions are not installed or enabled by default. You need to manually install and configure the same. For information on installing ASP.NET and BITS Server Extensions, see the documentation for your version of Microsoft Windows Server.• If the pre-installation check does not detect a default IIS Web site, the Deployment Web service installation fails.• The default port bindings are 80 for HTTP and 443 for secure connections.
n	SSL Certificate installed. Allows the Deployment Service to run in proxy mode to access the Deployment Web Service across a firewall. For more information, see "Installing SSL Certificates" on page 150 .

Notes Uploading and downloading packages using BITS has a limitation. If the Control Center interface runs on Windows 2000 and on a terminal client session, BITS is not supported. This

limitation is applicable if the Control Center interface runs on a Windows 2000 VMware image. For more information about VMware support, see [Appendix F, “VMware Support.”](#)

You cannot install Control Center if Microsoft SQL Server Desktop Engine (MSDE) is present on the system where you are installing AppManager. ASP.NET and the BITS Server Extensions must be manually installed if they are not installed or not running.

Reviewing Required Accounts and Permissions

The AppManager setup program requires access to various user accounts with administrator privileges and prompts you for user account information needed to install AppManager components.

For more information about installing AppManager on a cluster, see [Appendix G, “Installing in a Clustered Environment.”](#)

The following table lists the accounts Setup requires:

Component	Accounts Required
Any AppManager component	A valid Windows login account with Administrator privileges for the local computer (required) or the domain (optional) to run the Setup program.
Repository	<p>Windows or SQL Server login account with a sysadmin role or permission to create tables, users, and stored procedures. The SQL Server sa login account is not required.</p> <p>Setup creates a SQL Server login account. The default password for the “netiq” SQL Server login is netiq. You can specify a different password, if desired.</p>

Component	Accounts Required
Management server	<p>A service account (sometimes called the run-as account) for the NetIQ AppManager Management Service (NetIQms) to use. Either:</p> <ul style="list-style-type: none"> • The Local System account. • A valid Windows login account. <p>A valid Windows login account is required if you use Windows Authentication security mode for SQL Server. If you do not use Windows Authentication security for SQL Server, the NetIQms service runs under the LocalSystem account by default. You can specify a different Windows login account, if desired.</p>
Agent	<p>A service account (sometimes called the “run-as account”) for the agent services—the Client Resource Monitor (NetIQmc) and Client Communication Manager (NetIQccm)—or the AppManager UNIX agent (nqmagt) to use.</p> <ul style="list-style-type: none"> • For Windows, the account can be either the LocalSystem account or a valid Windows login account. • For UNIX, the account can be a valid UNIX login account. <p>Note In some cases, the agent must use a valid login account. For example, if you enable reporting capability for the agent, you must provide a valid Windows login account.</p>
Microsoft Exchange Server or Exchange 2000 Server module	<p>A valid Windows login account with Log on as Service privileges for each domain that contains an Exchange Server to be monitored. For Exchange Server, you need to specify the domain, user name, and password for the account the agent services run as. For Exchange 2000 Server, you also need a Windows account for the monitoring service on each virtual server to use.</p> <p>Note For Setup to create an Exchange profile (automatic) and (optional) mailbox, the Windows login account must be an Exchange Administrator with the Permissions Admin role for the Recipients configuration level.</p> <p>For more information about the requirements for Exchange and Exchange 2000, see the appropriate <i>AppManager for Microsoft Exchange Server Management Guide</i> in the AppManager installation kit.</p>

Component	Accounts Required
Microsoft SQL Server module	<p>Account access and password for either a SQL Server login account or a Windows account with permission to access SQL Server.</p> <p>Note Some SQL Knowledge Scripts require special permissions to access specific performance statistics or server activity. If necessary, you can add login accounts for monitoring SQL Server after installation using Security Manager.</p>
Control Center Command Queue Service	<p>One of the following:</p> <ul style="list-style-type: none"> • A Windows account with Administrator privileges in the Control Center repository and in each managed AppManager repository. Must be configured as an Administrator in Control Center. Must be part of the local Administrators group. An account with Domain Admin privileges is not sufficient unless it is also a direct member of the local Administrators group. <p>Use the AppManager Security Manager to add this account as an AppManager user on each repository.</p> <ul style="list-style-type: none"> • A SQL Server account with access to each managed repository.
Control Center Repository	<p>An account to run the SQL Server Agent (Cache Manager) Service and to give the Cache Manager access to each managed repository.</p> <p>One of the following:</p> <ul style="list-style-type: none"> • A Windows account with Administrator privileges in the Control Center repository that is also configured as an Administrator in Control Center. <p>NetIQ Corporation recommends using the same account that you are using for the Command Queue Service.</p> <ul style="list-style-type: none"> • A SQL Server account with access to each managed repository.
Deployment Service and Deployment Web Service	<p>A valid Windows account that is part of the local Administrators group. An account with Domain Admin privileges is not sufficient unless it is also a direct member of the local Administrators group.</p>

Installing AppManager

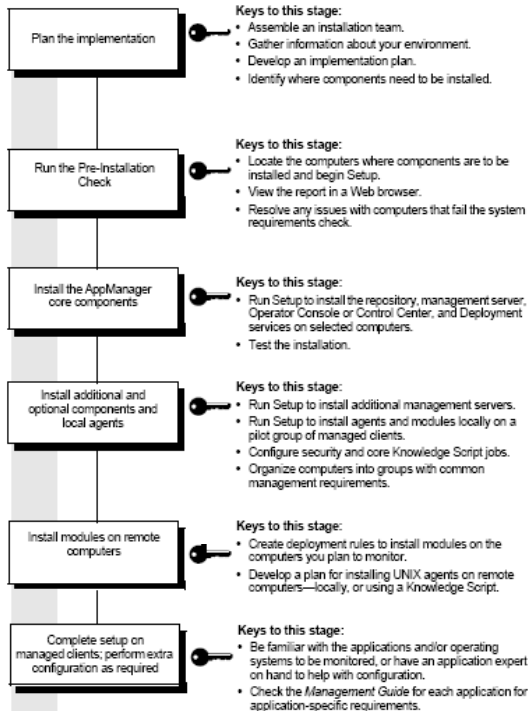
Ensure that you complete all the steps described in [Chapter 2, “Planning to Install AppManager,”](#) before beginning the AppManager installation. The AppManager setup program allows you to select the specific components you want to install. Because AppManager components can be installed together or separately, this chapter describes the recommended order of component installation. The actual order of component installation may vary depending on your environment.

The following topics are covered:

- [“Previewing AppManager Installation”](#) on page 64
- [“AppManager Implementation Checklist”](#) on page 65
- [“Installing Components in Order”](#) on page 65
- [“Understanding the AppManager Installation Kit”](#) on page 67
- [“Understanding The AppManager Pre-Installation Check”](#) on page 68
- [“Upgrading from a Previous Version of AppManager”](#) on page 69
- [“Running the AppManager Setup Program”](#) on page 70
- [“Reviewing AppManager Log Files”](#) on page 72

Previewing AppManager Installation

The following diagram summarizes the typical installation process for most environments:



AppManager Implementation Checklist

Use the following checklist as a guide to installing AppManager in your environment.

<input checked="" type="checkbox"/>	Steps	Section to Review
<input type="checkbox"/>	1 Plan your AppManager installation.	Chapter 2, “Planning to Install AppManager.”
<input type="checkbox"/>	2 Review system requirements.	Chapter 3, “System Requirements.”
<input type="checkbox"/>	3 Run the pre-installation check program.	“Understanding The AppManager Pre-Installation Check” on page 68
<input type="checkbox"/>	4 Review information about staging an AppManager implementation.	Chapter 14, “Staging the Deployment.”
<input type="checkbox"/>	5 Review DTC connectivity.	Appendix E, “Reviewing Microsoft DTC and Control Center Installation.”
<input type="checkbox"/>	6 Install AppManager components.	Chapter 6, “Installing the Repository” through Chapter 12, “Installing Control Center.”
<input type="checkbox"/>	7 Review the post-installation configuration steps if it applies to your environment.	Chapter 13, “Post-Installation Configuration.”
<input type="checkbox"/>	8 Implement special installation scenarios if they apply to your environment.	Appendix B, “Performing a Silent Installation,” Appendix D, “Using SMS to Install AppManager Agents,” and Appendix G, “Installing in a Clustered Environment.”

Installing Components in Order

You can install AppManager components in any of these combinations:

- All components at once
- Individual components one at a time
- A few components at a time

The AppManager installation provides this flexibility to accommodate your unique installation scenario.

If you are installing AppManager components one at a time, install the components in the following order:

- 1 Always install the AppManager repository first.** Because the repository is where all AppManager management information such as events, data, and statistics are stored, it is the first component you need to install. In addition, because almost every component interacts with the repository, it is important to first install the repository.

- 2 Install at least one management server and agent.** The management server enables communication between the repository and agents.

Note Because the agent is required to enable the management server, it is automatically selected when you install the management server. Collocating the repository, management server, and agent on a single computer is typical.

- 3 Install agents on managed clients.** Typically, managed clients are automatically discovered during agent installation provided the repository and management server are already installed. However, you might need to manually discover some managed clients. For more information, see [Chapter 9, “Installing Agents.”](#)

- 4 Install Control Center.** You need to install the Control Center to deploy agents and modules on remote computers.

- 5 Install other components.** You can install the remaining components in any order.

Note If you are upgrading from AppManager version 6.0.2 to AppManager 7.0, verify whether you have disabled Data Execution Prevention. Data Execution Prevention restricts certain AppManager setup files from being run, which will cause AppManager installation to fail. This information applies only to Microsoft Windows XP SP2 or later, and Microsoft Windows Server 2003 SP1.

Understanding the AppManager Installation Kit

You can obtain the AppManager installation kit either as separate downloads from the NetIQ Web site or on a CD-ROM. If you downloaded the installation kit from the NetIQ Web site, unpack the AppManager installation kit to launch the setup program.

Note AppManager software is available for download from the NetIQ Web site. AppManager suites are available as CD images or directory structures. You can save the suites you want on a distribution computer, or transfer them to a CD-ROM.

The AppManager installation kit for Windows includes the following:

- **connectors:** Contains the AppManager Connector software, programs to help AppManager communicate with third-party monitoring frameworks, such as Microsoft Operations Manager and Hewlett-Packard OpenView.
- **suite_installation:** Contains software that works in conjunction with AppManager to provide a comprehensive monitoring, reporting, and diagnostic solution, including NetIQ Analysis Center, and Diagnostic Console.
- **windows_installation:** Contains the AppManager software, documentation, and some prerequisite software.

Note The installation kit also contains an **update** folder to enable you to update AppManager from version 7.0 to 7.0.1. For more information, see the *Upgrade and Migration Guide for AppManager*.

A separate installation kit for installing AppManager UNIX Components is also available for all UNIX agent and module installations.

Saving Installation Kits to a Distribution Computer

Because AppManager ships with a large number of supporting files, it is recommended to unpack and preserve these directories on a

network location so that other members of the AppManager team can access them. Consider this network location to be a AppManager distribution computer.

Establishing a distribution computer is useful when you want to download and install AppManager modules from the Web.

Installing with Remote Desktop

If you try to use Windows Terminal Services (or Remote Desktop) to install AppManager on a remote computer, you may see failures during the installation of individual components if you are taking the necessary setup files from a mapped network drive. This failure is caused by a known issue, documented in Microsoft Knowledge Base article [Q278603](#).

To resolve this problem:

- Copy all source files to the Terminal Services computer, replicating the structure of the AppManager installation directories, and then run the AppManager setup program from this location.
- Use the full universal naming convention (UNC) path to the source files. For example:
`\\servername\sharename\Setup_Files\[ModuleName - BuildN].msi`

Understanding The AppManager Pre-Installation Check

When you launch the setup program, the AppManager pre-installation check script verifies system requirements for each component you select to install. The pre-installation check displays

an HTML-formatted report that indicates whether the each component passed or failed the system requirement check.

The pre-installation check results are classified as:

- **Passed:** The component has passed all system requirement checks.
- **Warning:** The component has passed all system requirement checks but configuration issues may exist.
- **Failed:** The component has failed one or all system requirement checks.

Upgrading from a Previous Version of AppManager

If you plan to upgrade from a previous version of AppManager, NetIQ Corporation recommends that you upgrade all components, including your repository, management server, console, Web

management server and all of your managed clients (agents) and modules.

Upgrading the agent is required if the agent is collocated with another AppManager component, such as the repository or management server.

For more information on upgrading AppManager, see the *Upgrade and Migration Guide for AppManager*.

Running the AppManager Setup Program

The installation steps in this section are common to all AppManager components, whether you are installing individual or multiple components.

Do not install AppManager on a network drive. If you are installing multiple AppManager components on a computer, install them all in the same location.

To install AppManager:

- 1 Ensure that you have logged in with either local or domain Administrator privileges on the computer where you want to install AppManager.
- 2 Run the AppManager setup program from either the AppManager CD or the installation kit located on your hard drive.

Note If autorun is enabled, the AppManager setup program opens in your default Web browser.

- 3 Click the **Production Setup** tab.
- 4 Click **Begin AppManager 7.0 Setup**.

Note Depending on your Internet security settings, the File Download dialog box may be displayed. In such cases, click **Run** in the File Download dialog box.

- 5 In the Welcome dialog box, select **Evaluation** or **Production**.

The Evaluation option installs the recommended minimum components with default settings on the computer where you are running Setup. For more information, see [Chapter 5, “Installing AppManager for Evaluation Purposes.”](#)

- 6 If you select **Production**, select the AppManager components you want to install.
- 7 Click **Next**.
- 8 A pre-installation check report indicates if any pre-installation check has failed. Click **Next** if the pre-installation check is successful.
- 9 In the License Agreement dialog box, select **I accept the terms of the license agreement** to accept the license agreement and click **Next**.
- 10 In the License Manager dialog box, select the appropriate license key and click **Next**.

For more information about AppManager licenses, see [“Managing AppManager Licenses”](#) on page 188.

- 11 Select the folder where you want to install AppManager. If you do not want to use the default folder location (**C:\Program Files\NetIQ**), click the **Browse** button to install AppManager in a different location.

Note The default folder location on a 64-Bit computer is **C:\Program Files(x86)\NetIQ**.

Note The installation steps from this point vary depending on the component or combination of components you are installing. After you have completed the installation steps for a given component, the setup program runs in the background to copy files and make the necessary configuration changes.

For more information about installing each AppManager component, see the appropriate section listed in the following table.

Component	Setup Instructions
AppManager repository	Chapter 6, “Installing the Repository.”
AppManager management server	Chapter 7, “Installing the Management Server.”
Operator Console	Chapter 8, “Installing the Operator Console Programs.”
AppManager agent	Chapter 9, “Installing Agents.”
Modules	Chapter 10, “Installing Modules.”
AppManager Web management server	Chapter 11, “Installing the Web Management Server.”
Control Center	Chapter 12, “Installing Control Center.”

12 After all components have been installed, click **Finish** to complete AppManager installation.

Note Installing agents and modules on Windows Vista (Business and Enterprise editions) operating systems will generate warning log events. The warning log events detect some files as potential risks.

Reviewing AppManager Log Files

Each AppManager component has at least a custom log and an MSI/InstallShield log associated with it. The custom log is usually named `nq*.log`. The MSI/InstallShield log is usually named the same as the

installation package, with .log appended. The location of the log files is \Netiq\Temp\NetIQ_Debug\<computer_name>.

Component	Log Files
AppManager Suite Installation	<ul style="list-style-type: none">• nqAMInst_Setup.log
Repository Installation	<ul style="list-style-type: none">• kscheckin.log• nqAMInst_QDB.log• qdbinstall.log
Management Server	<ul style="list-style-type: none">• nqAMInstMS.log• ms.log
Management Client (Agent)	<ul style="list-style-type: none">• nqAMInstMC.log• ccmtrace.log• mctrace.log
Control Center	<ul style="list-style-type: none">• nqCC_Install.log• ccdbinstall.log• <CC_ADSTrace>DeploymentService.log• <CC_CQSTrace> CQSLog.txt• SyncQDBLog.txt• nqXmlUtil.log• rplib.log
Module	<ul style="list-style-type: none">• <ModuleName>_Install.log• AM70-App1-7.0.87.0.msi.log

Installing AppManager for Evaluation Purposes

The following sections describe how to install AppManager for evaluation purposes. An evaluation installation helps you explore the features and benefits of using AppManager to monitor your environment. In an evaluation installation, you cannot use AppManager to monitor large-scale environments.

The following topics are covered:

- [“Evaluating AppManager” on page 75](#)
- [“Reviewing Evaluation Installation Requirements” on page 76](#)
- [“Installing AppManager in Evaluation Mode” on page 77](#)
- [“Repository Settings in Evaluation Mode” on page 80](#)

Evaluating AppManager

An evaluation installation of AppManager contains all AppManager components including Control Center, installed on a single computer. It comprises just the most basic features of AppManager.

The following list provides the typical features and benefits of an evaluation installation:

- You can quickly understand your monitoring needs.
- You can assess your environment and plan for a full-scale AppManager deployment.
- All AppManager components are installed using default settings, which you can change later.

- You can monitor up to 100 managed clients (recommended). Performance may decline when you add more managed clients to your environment.
- You can evaluate AppManager for a 30-day period that begins on the date you install the repository component. For more information about evaluation licensing, see [Appendix A, “Updating License Information.”](#)

Because installation in evaluation mode locates all components on a single Windows computer, some installation options that concern UNIX agents are not included. However, you can monitor UNIX platforms and applications with AppManager in evaluation mode. You will need to install UNIX agents as a separate step to enable UNIX monitoring. For more information, see the *AppManager for UNIX Management Guide*, provided with the AppManager UNIX Components installation kit.

Reviewing Evaluation Installation Requirements

Installing AppManager in evaluation mode is a simple and quick process, where many decisions are made on your behalf, based on recommended settings.

The following table describes the system requirements to install AppManager in evaluation mode.

Requirement	Recommended Configuration for Evaluation
CPU	Pentium III (733 Mhz or higher), Single or Dual Processor
RAM	1 GB (or more)
Available disk space	1700 MB (or more)
Operating System	Microsoft Windows Server 2003

Requirement	Recommended Configuration for Evaluation
Database server	<ul style="list-style-type: none"> Microsoft SQL Server 2000 with Service Pack 3a or later Microsoft SQL Server 2005 <p>Note: The evaluation installation only supports a default instance of SQL Server. You cannot install the AppManager evaluation program on a SQL Server named instance.</p>
Database driver	ODBC SQL Server driver (included with MDAC)
Internet	<p>Microsoft Internet Information Services (IIS) 5.0 or later with ASP and ADO installed with the following optional components enabled:</p> <ul style="list-style-type: none"> ASP.NET BITS Server Extensions
Web browser	Microsoft Internet Explorer version 6.0 or later
Installer	Windows Installer 3.1 or later
Software	<ul style="list-style-type: none"> Microsoft .NET Framework 1.1 or later Microsoft Distributed Transaction Coordinator (DTC), running as a service Microsoft Background Intelligent Transfer Service (BITS) Client Component, version 1.5 or later Microsoft XML Parser, version 6.0 (msxml6), SP1 or later
Windows account	User account with Domain Administrator privileges

Installing AppManager in Evaluation Mode

The initial installation steps described in this section are common to both the evaluation and production modes. For more information about installing AppManager in production mode, see [“Running the AppManager Setup Program” on page 70](#).

To install AppManager in evaluation mode:

- 1 Ensure that you have logged in with either local or domain Administrator privileges on the computer where you want to install AppManager in evaluation mode.

- 2 Run the AppManager setup program:
 - from the AppManager CD or
 - by double-clicking the setup program in the installation kit.
- 3 Click the **Trial Setup** tab.
- 4 Click **Begin AppManager Setup**.
- 5 In the Welcome dialog box, ensure that **Evaluation** is selected.
- 6 Click **Next**.
- 7 A pre-installation check report indicates if any pre-installation check has failed. Click **Next** if the pre-installation check is successful.
- 8 In the License Agreement dialog box, select **I accept the license agreement** to accept the license agreement and click **Next**.
- 9 Select the folder where you want to install AppManager. If you do not want to use the default folder location (**C:\Program Files\NetIQ**), click **Browse** to install AppManager in a different location.
- 10 Click **Next**.
- 11 In the Windows User Account Information dialog box, enter a valid **User name** and **Password** of a Windows account with administrator privileges.

The Windows user account must have permissions to log on as a service. The following AppManager components use this account:

- AppManager agent
- Control Center Command Queue
- Deployment Service
- Deployment Web Service

- 12 Click **Next**.

13 In the Monitoring Modules dialog box, select the modules you want to install.

Note The list of modules only shows modules that passed the pre-installation check, organized into categories as described in the following table.

Category	Description
AppManager	Third-party application modules. Operating-system modules (Windows only). Note: The AppManager for SQL Server module requires additional configuration. You need to specify the type of authentication to use when connecting to the SQL Server instance. Some of the Knowledge Scripts in the SQL category must connect to the SQL Server for monitoring purposes.
ResponseTime	ResponseTime modules, which run network tests between network clients (where you have installed agents) and your application servers to measure server response time and availability.
VoIP	Modules to monitor and manage voice over IP servers and applications. If you select any of the VoIP modules shown here, the local computer will be used as a proxy for the agent in cases where an agent cannot be installed on the VoIP hardware.

Note NetIQ Corporation recommends selecting at least a couple of modules to try them out. Some of the ResponseTime modules, the AppManager for Microsoft SQL Server, and Microsoft IIS modules are recommended choices. Typically, your computer will have the necessary prerequisites to install them.

14 Click **Next**.

15 Review the installation summary and click **Install** to install AppManager in evaluation mode.

Repository Settings in Evaluation Mode

The AppManager repository stores all of your management information, such as events and data, and Knowledge Scripts. For more information about repository installation, see [Chapter 6, “Installing the Repository.”](#)

For an evaluation installation, the AppManager setup program installs the repository with default settings as described in the following table.

Setting	Default Value	Notes
SQL Server Login: <ul style="list-style-type: none">• SQL Server Name	SQL Server instance on the local computer.	You need to install an instance of SQL Server on the computer to enable installation in evaluation mode.
<ul style="list-style-type: none">• SQL Server Authentication	Windows authentication (with administrator permissions) is used to access the AppManager repository.	For more information about repository authentication, see “Installing the AppManager Repository” on page 83.
Repository Name	The default name for the AppManager repository is QDB.	You cannot specify or change the default repository database name.
Repository Database Options	Default sizes and locations for the new database data and log files.	Default sizes are appropriate for a small deployment (150 managed clients or fewer).
Netiq User Password	The default password for the netiq user account is netiq.	The netiq user account is a SQL Server login account that will act as repository owner. For more information, see “Installing the AppManager Repository” on page 83.
Windows Agent Security Level	cleartext communications (no security) are used for agent-to-management server communications. In evaluation mode, AppManager only installs an agent for Windows. You can install UNIX agents yourself as a separate step.	For more information about security levels, see “Installing the AppManager Repository” on page 83.

Installing the Repository

This chapter describes the steps for installing the repository.

The following topics are covered:

- [“Understanding the AppManager Repository Installation” on page 81](#)
- [“Installing the AppManager Repository” on page 83](#)

Understanding the AppManager Repository Installation

Typically, you need to install the repository and management server on the same computer. NetIQ Corporation recommends that you at least install an agent on the same computer as the repository to facilitate database management.

Note When you install the repository on one computer using Windows-only authentication, and install the management server on another computer, the setup program does not allow you to enter a domain account by disabling the local system account. If you enter a local system account, the management server service fails and the setup program displays errors. In addition, AppManager uninstallation does not work properly.

If the repository uses Windows authentication, then the account used to log in must be from the same domain or a trusted domain. An account from a non-trusted domain will not be able to log into the repository if the repository database is configured to use Windows authentication.

If the repository and the management server are on different computers, you should configure the "log on as" account for the AppManager management server to use an account that has Network Access to the registry of the repository server.

For more information about security and managing site communications between the management server and managed clients, see the *Administrator Guide for AppManager*.

Understanding Repository Security Options

During installation, you need to specify security options for the managed clients that report to the repository. Depending on your environment, you can choose to configure security for Windows agents only, for UNIX agents only, or for both Windows and UNIX agents. The security level you select affects all communications between the management servers and managed clients within the management site.

If you are upgrading from a previous version of AppManager, the setup program retains all of your existing security information to prevent communication failures between management servers and agents. This process also ensures a smooth transition to the new version of AppManager across all components. To change the security level after an upgrade, you must use the `NQkeyGenWindows.exe` and `NQkeyGenUnix.exe` utilities to create new security keys and new security levels.

For more information, see the *Upgrade and Migration Guide for AppManager* or *Administrator Guide for AppManager*.

Restricting Knowledge Script Check in

The setup program checks a copy of every current AppManager Knowledge Script into your repository during installation.

You can exclude checking in Knowledge Scripts that you do not require. If you want to exclude Knowledge Script categories (that is, to exclude all the Knowledge Scripts associated with a particular

application, such as BlackBerry Enterprise Server), you can make the relevant change to the AppManager installation kit.

Note NetIQ Corporation recommends caution before deleting any of the files from the **Setup Files** folder. Do not remove any executable files, such as **ckBES.exe**.

The repository installer looks for Knowledge Scripts in the module-specific files in the **\setup\Setup Files** folder. For example, to exclude all Knowledge Scripts in the AppManager for BlackBerry and AppManager for BES Knowledge Script categories, delete the following files from the Setup Files folder, where **xx** is the version of AppManager or the module:

- **AMxx-BES-xx.ini**
- **AMxx-BlackBerry-xx.ini**
- **AMxx-BES-xx.msi**
- **AMxx-BlackBerry-xx.msi**

For information about installing the repository in a clustered environment, see [“Installing the Repository on a Cluster” on page 253](#).

Installing the AppManager Repository

Ensure that the Microsoft SQL Server Agent service is set to run automatically to avoid a warning message at the end of the repository installation.

To install the AppManager repository:

- 1 After selecting a location to install the repository (see [“Running the AppManager Setup Program” on page 70](#)), click **Next**.

- 2 In the SQL Server Login dialog box, type the following information, and click **Next**.

Field	Description
SQL Server Name	<p>The name of the SQL Server computer and instance, if applicable, for the AppManager repository database.</p> <p>The default is "local", or the name of the SQL Server on the computer where you are running the setup program. If there are multiple SQL Server instances on the computer, use the format:</p> <p>ServerName\InstanceName</p> <p>Note If you are installing on a cluster node, type the network name for the virtual SQL Server. The network name is the virtual server name or computer name that the SQL Client uses to connect to the clustered SQL Server. For more information, see "Installing the Repository on a Virtual Server" on page 256.</p>
Windows Authentication	<p>Use your current Windows account and password to log in to SQL Server. If you use your Windows account, be sure this account is a local Administrator with permission to access SQL Server, or an account that is a member of the sysadmin server role.</p>
SQL Server Authentication	<p>Use SQL Server authentication to log in to SQL Server. If you are using SQL Server authentication, you must also specify the SQL Server username and password to log in.</p>
Username	<p>The username associated with a user account for this SQL Server.</p> <p>The user associated with this account must be one of the following:</p> <ul style="list-style-type: none">• A member of the sysadmin server role.• A user who has the db_owner database role.• A user who has permission to create databases and database user accounts.
Password	<p>The password for the user account.</p> <p>The login access you provide here for the SQL Server login account is used by the setup program to create a NetIQ SQL Server login account. The default account name and password for the NetIQ SQL Server login account are netiq.</p>

- 3 In the AppManager Repository Database Name dialog box, type a name for your repository. You can also accept the default, which is **QDB**. Click **Next**.

Notes If you do not want to upgrade a backlevel repository database, specify a different name for the new repository. For more information about upgrading a repository to the latest version, see the *Upgrade and Migration Guide for AppManager*.

If Control Center is installed on SQL Server 2000, the name of the repository must not contain any periods. If you specify a repository name with periods, the Control Center Daily Task fails and the Cache Manager shows error status.

- 4 In the AppManager Repository Database Options dialog box, type the following information or accept the default values, then click **Next**.

Field	Description
Initial Data File Size (MB)	<p>The size in MB for the AppManager repository data device. The default is 110 MB.</p> <p>Note AppManager uses 13 MB to store Knowledge Scripts, tables, and stored procedures, but your sizing requirements are largely dependent on your monitoring environment (number of servers, events, and data you expect). Generally, 1 MB for data and events per server, per day, is an appropriate starting point for calculating the size of the repository. SQL Server can be configured to dynamically increase the size of databases, as needed.</p>
Data File Name and Location	<p>The name of the AppManager repository database data file. The default name is <code>DBNameData</code>. The file created is named <code>DBNameData.mdf</code>, for example, <code>QDBData.mdf</code>.</p> <p>The location of the folder where the AppManager database data is stored. For example: <code>C:\Program Files\Microsoft SQL Server\MSSQL\Data</code></p> <p>The disk space available on the target drive must be larger than the size specified by the Data device size option. Many environments with significant amounts of SQL Server database data save their data devices on a large drive.</p> <p>To browse for the folder location, click the Browse [...] button.</p>
Initial Log File Size (MB)	<p>The size in MB for the AppManager repository log device. The default is 51 MB.</p> <p>Note: The default size is adequate for a small AppManager deployment of only about 10 managed clients.</p>
Log File Location	<p>The location of the folder where the AppManager database log is stored. <code>DBNameLog.ldf</code> is created in <code>C:\Program Files\Microsoft SQL Server\MSSQL\LOG</code></p> <p>The other three log files are created in <code>\Netiq\Temp\NetIQ_Debug\<computer_name>.</code></p> <p>The disk space available on the target drive must be larger than the size specified by the Log device size option. Many environments with significant amounts of SQL Server database data save their log devices on a large drive.</p> <p>To browse for the folder location, click Browse [...].</p>

Note You may need to adjust the data size and log file options based on the amount of data you intend to collect and the number of computers you plan to monitor. For repository sizing guidelines, see [“Sizing the AppManager Repository” on page 27](#).

- 5 In the Netiq User Password dialog box, type a password for the **netiq** user.

Make sure the password format complies with any network- or computer-specific requirements. If this is not done, the repository installation fails and must be manually uninstalled.

- 6 Retype the new password to confirm it and click **Next**.

Note You need to enter the **netiq** SQL Server account password during the management server installation to grant the management server access to the repository.

- 7 In the Security Configuration dialog box, select whether you want to configure security for Windows agents only, for UNIX agents only, or for both Windows and UNIX agents, and click **Next**.

Note NetIQ Corporation recommends that you configure all Windows agents and all UNIX agents to use the same security level when you run the setup program. After installation, or when upgrading from a previous release, you can manage security separately for Windows and UNIX agents using the **NQkeyGenWindows.exe** and **NQkeyGenUnix.exe** utilities. For more information about using these utilities, see the *Administrator Guide for AppManager*.

- 8 Based on the type of agent and level of security you have selected, the appropriate Security Level dialog box is displayed—for

example, the Windows Security Level dialog box. Select the appropriate level of security.

Option	Description
Cleartext communications	No security. Allows communication in clear text messages between all management servers and managed clients within the site. If you select this security level, no further configuration is necessary.
Encrypted communications only	Medium security. Encrypts all communication between the management server and managed clients.
Authentication and encrypted communications	Highest security. Requires managed clients to authenticate the identity of the management server before sending encrypted communications. Note If you select this option, all communication between management servers and managed clients is encrypted, but you provide an additional layer of security by requiring all managed clients to authenticate the management server before sending any data.

9 If you selected **Cleartext communications**, the Confirmation dialog box displays your confirmation choices.

Note The following steps apply if you select either **Encrypted communications only** or **Authentication and encrypted communications**.

10 If you selected **Encrypted communications only** or **Authentication and encrypted communications**, the Repository Key Password dialog box is displayed.

11 Type a password for the encryption key stored in the repository, and then confirm the password by retyping it.

For more information about the repository key, see the *Administrator Guide for AppManager*.

12 Click **Next**. The Agent Key Password and Optional Key location dialog box is displayed. The agent uses a password to access its portion of the repository encryption key. You are asked to supply this key.

13 Type the password for the agent key file, then confirm the password by retyping it.

Note If you have already installed the agent, enter the same password you supplied during agent installation.

14 Select **Export Windows Agent Key Password to a file** to export the key file information to a text file.

15 Type a location where Setup should save the agent key file, or accept the default location.

Note The filename of the exported agent key file for Windows is `nqwindowsPublic0.key`, and `nqUNIXPublic0.key` for UNIX. After the installation is complete, a message is displayed indicating the name and location of the key. You can optionally rename or move these files after installation. You will need the location of the agent key file when you install Windows agents. NetIQ Corporation recommends safeguarding the key file in a secure location.

16 Click **Next**. The Confirmation dialog box displays your confirmation choices.

17 Click **Install**.

18 After the repository is successfully installed, click **Finish**.

Installing the Management Server

This chapter describes the steps for installing the AppManager management server.

The following topics are covered:

- [“Understanding Management Server Installation” on page 91](#)
- [“Reviewing Port Information for Management Server” on page 91](#)
- [“Installing the Management Server” on page 92](#)

Understanding Management Server Installation

Before you start the management server installation, ensure that you have either local or domain Administrator privileges.

Because the management server enables you to remotely install agents and manage actions, an AppManager agent must:

- Be installed on the management server.
- Run under a Windows user account.

When you select the management server for installation, the agent is automatically selected.

Reviewing Port Information for Management Server

To enable communication between the NetIQ AppManager management server and the AppManager agents for Windows or UNIX, you may want to change the default ports that the management server and agents use.

Ensure that you use the correct ports on both the management server and each managed client that the management server communicates with. For example, if you change the port to which the management server binds for receiving information from the managed client but do not set corresponding port information when you install the agent, no communication can occur between the management server and the managed client.

If you decide to change the ports after installing the management server and agents, you can change listening ports automatically by editing a registry key. For more information, see the *Administrator Guide for AppManager*.

Typically, the following default ports are appropriate:

Default Port	Use
9999	Agents on Windows and UNIX platforms listen on this port for communications from the management server service (NetIQms).
9998	Management server listens on this port for communications from the Windows agent services: <ul style="list-style-type: none">• Client Resource Monitor Service (NetIQmc)• Client Communication Manager Service (NetIQccm)
9001	Management server listens on this port for communications from the UNIX agent.

Note Consult a network security administrator before changing port information.

Installing the Management Server

Installing the AppManager management server comprises several steps such as specifying port information, specifying a repository, and providing user account information.

Note If a previous installation of the management server exists on your computer, the new installation will overwrite the existing registry settings. However, you can retain your existing registry settings. For

information about registry key settings, see the *Administrator Guide for AppManager*.

To install the Management Server:

- 1 After selecting a location to install the management server (see [“Running the AppManager Setup Program” on page 70](#)), click **Next**.
- 2 In the Port Designation dialog box, accept the default ports or change the port information and click **Next**.
- 3 In the Repository Information dialog box, specify the appropriate information, or accept the default values and click **Next**.

Option	Description
Repository Server	<p>Name of the SQL Server (or SQL Server instance) where the AppManager repository is installed.</p> <p>If there are multiple SQL Server instances on this computer, use the following format:</p> <p>ServerName\InstanceName</p> <p>The location of the database is required for DSN configuration. The default location is the SQL Server computer on which the management server component is being installed.</p> <p>Note If the repository is installed on a virtual SQL Server on a cluster, enter the <i>network name</i> of the virtual server (not the local computer name). For more information, see “Installing the Management Server on a Cluster” on page 257.</p>
Repository Name	<p>Name of the AppManager repository that the management server will connect to.</p> <p>The default name of the repository is QDB.</p>

Note The ODBC32 Data Source Name (DSN) for the repository is created during repository installation. The management server service (**NetIQms**) uses this DSN to communicate with the AppManager repository database. The default data source name is **[RepositoryName]ms**, for example, **QDBms** where “**QDB**” is the default repository database name.

4 In the Windows User Account Information dialog box, select the type of account for the NetIQ AppManager Management Service (**NetIQms**) to use and click **Next**.

- Accept the default **Local system account**.
- If you want the management server to run using a Windows user account, select **Windows user account** and enter the **Username** (in the **domain\username** format) and **Password**.

Note If the setup program can connect to the SQL Server where the AppManager repository is installed and it detects the Windows Authentication mode, this step is skipped and you are prompted for the domain, username, and password directly.

5 In the Repository Password dialog box, type the password for the **netiq** account and click **Next**. The default password for the **netiq** SQL Server login account is **netiq**.

For more information about the **netiq** repository account, see [“Installing the AppManager Repository” on page 83](#).

Notes If you install the AppManager repository and management server at the same time, the Repository Password dialog box does not appear.

For successful installation, make sure that the **netiq** SQL login does not already exist in your SQL Server environment to avoid conflicts.

6 In the Installation Summary dialog box, click **Install**.

7 After the management server is successfully installed, click **Finish**.

Installing the Operator Console Programs

This chapter describes the steps for installing AppManager Operator Console programs.

The following topics are covered:

- [“Understanding Operator Console Installation” on page 95](#)
- [“Installing the Operator Console” on page 96](#)

Understanding Operator Console Installation

Installing the Operator Console programs is essential if you want to administer and manage the AppManager system. Operator Console programs include the following:

- **AppManager Operator Console:** The user interface to configure and control the execution of jobs.
- **AppManager Security Manager:** A utility that lets you identify users who are allowed to access AppManager, define user roles and rights, and maintain passwords and other secure information.
- **Developer’s Console:** A utility that provides tools to develop custom Knowledge Scripts. For information, see *Developer’s Tools and Reference* in the AppManager Help.

AppManager requires at least one Operator Console or Control Center Console to be installed in your environment.

You can also use the Browser-based version of the Operator Console, known as the Operator Web Console to monitor your AppManager environment.

Installing the Operator Console

Before you begin the Operator Console installation, ensure that you have either local or domain Administrator privileges on your computer.

To install the Operator Console programs:

- 1 After selecting a location to install the AppManager Operator Console (see [“Running the AppManager Setup Program” on page 70](#)), click **Next**.

Note If you install the Operator Console in a non-default location (the default location is `C:\Program Files\NetIQ\`) and use a semicolon in the specified path, the Chart Console fails to create the ChartWizard object. As a result, you will not be able to add new charts.

- 2 In the User Information dialog box, enter the appropriate information and click **Next**.
- 3 In the Component Selection dialog box, select the Operator Console programs you want to install.

By default, all console programs and all their “subfeatures” are installed. Click the down arrow adjacent to any component and select **This feature will not be installed** if you *do not* want to install it.

Note NetIQ Corporation recommends installing the Security Manager program.

- 4 Click **Space** to check your hard drives for the required free disk space. The Disk Space Requirements dialog box indicates if any drives lack the necessary space for the selected features.
- 5 Click **OK** to return to the Component Selection dialog box and click **Next**.

- 6 In the Installation Summary dialog box, click **Install**. You can review the updated system path the next time you restart the computer.

Note If you plan to immediately install any AppManager Connector product (such as the AppManager Connector for Tivoli Enterprise), restart the system so that the system path is updated with the `\NetIQ\AppManager\bin` folder. For information about installing AppManager connectors, see the Connector documentation in the AppManager installation kit.

- 7 Click **Finish** after the selected console programs are successfully installed.

Installing Agents

This chapter describes the steps for installing the AppManager agent.

The following topics are covered:

- [“Understanding Agent Installation” on page 99](#)
- [“Understanding Prerequisites for Installing Agents on Windows Server 2003 SP1” on page 100](#)
- [“Installing Agents in a Windows Environment” on page 102](#)
- [“Understanding Space Considerations” on page 103](#)
- [“Understanding Agent Reporting Capabilities” on page 104](#)
- [“Understanding Agent Automatic Discovery” on page 105](#)
- [“Understanding MAPI Mail Settings” on page 105](#)
- [“Understanding Windows User Accounts” on page 106](#)
- [“Understanding Management Server Designation” on page 107](#)
- [“Installing the Agent Locally” on page 109](#)
- [“Installing Agents Remotely” on page 114](#)
- [“Post-Installation Tasks” on page 115](#)
- [“Installing UNIX Agents” on page 117](#)

Understanding Agent Installation

The steps you take to install the agent vary depending on the environment you are monitoring.

In a **Windows** environment, you can install the agent:

- **Locally** by running the setup program from the AppManager installation kit or from an AppManager distribution directory. For more information, see [“Installing the Agent Locally” on page 109](#).
- **Remotely** by using Control Center. You must install Control Center before you try to deploy agents on remote computers. For more information, see the *Control Center User Guide for AppManager*.

Note The AppManager agent version 7.0 monitors Windows Vista computers running on 32-bit systems. However, the agent does not monitor applications running on these operating systems.

In a **UNIX** environment, you can install the agent:

- **Locally** by running the installation script `netiq_agent_install` from the `unixclient` directory. You must first extract the directory from the `unixclient.tar` file, which is included with the AppManager UNIX Components installation kit.
- **Remotely** by running the `AMAdminUNIX_AgentInstallProxy` Knowledge Script.

For information about installing the agent on UNIX, see the *AppManager for UNIX Management Guide*, included with the UNIX Components installation kit.

This chapter describes the steps for installing the agent component on a Windows computer. For additional information about installing and working with the Windows or UNIX agents, see *Administrator Guide for AppManager*.

Understanding Prerequisites for Installing Agents on Windows Server 2003 SP1

On a computer where Windows Firewall is enabled (it is disabled by default with Windows Server 2003 SP1 but enabled by default with Windows XP SP2), you must manually open some TCP ports to

enable communication between AppManager components. This is because Windows Firewall closes required TCP ports on Windows Server 2003 SP1.

The following table summarizes the default AppManager TCP port settings. Note that you can change the listening ports the NetIQ AppManager Management Service (**netiqms**) and NetIQ AppManager Client Resource Monitor (**netiqmc**) use. Depending on your firewall requirements and the configuration of your management site, your organization may use different ports. In addition, if you use any ResponseTime modules, those modules have their own port requirements. For information about the ports required for ResponseTime modules, see the appropriate *AppManager ResponseTime Management Guide*.

This Component	Requires TCP Port	For
Operator Console	135	Communication with the repository and automatic discovery.
Management server	9999 9001	Communication from the Windows agent using RPC. Communication from the UNIX agent using XML and TCP/IP.
AppManager repository	1433 445 39	Communication from the Operator Console and the management server using ODBC and communication with the report-enabled agent using ADO. Using the AMAdmin_UpgradeJobs Knowledge Script.
Windows agent services	9998 9979	Communication from the management server using RPC. Receiving remote AgentInstall connections.
Web management server	80	Communication from the Web Operator Console using TCP/IP.
Troubleshooter and NetIQCtrl	9998 9999 135	Communication from the management server or agent using TCP/IP.

On the repository computer, you must open the TCP port required by Microsoft SQL Server. Note that the default TCP port for SQL Server is 1433.

To verify the default TCP port for SQL Server:

- 1** Click **Programs > Microsoft SQL Server > Server Network Utility**.
- 2** In the SQL Server Network Utility, click **TCP/IP** and click **Properties**.
- 3** In the <computer> - TCP/IP dialog box, the default port displayed.

To open a TCP port using Windows Firewall:

- 1** Click **Start > Control Panel > Windows Firewall**.
- 2** In the **General** tab of the Windows Firewall dialog box, make sure the **On** option is selected. This indicates Windows Firewall is enabled.
- 3** In the **Exceptions** tab, click the **Add Port** button.
- 4** In the Add a Port dialog box, enter a name for the port you want, for example, netiqms, and specify the port, for example, 9999. Make sure **TCP** is selected.
- 5** Click **OK** to add the port. To add another port, repeat Steps 3 and 4, or click **OK** again to close the dialog box.

Installing Agents in a Windows Environment

When you install the AppManager agent on Windows computers, you install a package that consists of:

- NetIQ AppManager Client Resource Monitor (**netiqmc**)
- NetIQ AppManager Client Communication Manager (**netiqccm**)
- Local repository for storing data and events

Note The recommended method for installing agents is by using the Control Center Console. This is especially useful if you are installing multiple agents, or agents on remote computers. For more information, see [“Installing Agents Remotely” on page 114](#). However, you can install the AppManager agent by running either the `AMSetup.exe` or `NetIQ AppManager agent.msi` on a local computer.

After you install the agent, NetIQ Corporation recommends that you install at least one module that you plan to monitor using the agent. For more information about installing modules, see [Chapter 10, “Installing Modules.”](#)

Understanding Space Considerations

Agent installation is handled by a mechanism that launches `.msi` packages for individual agents and modules. If you launch the installation manually (`NetIQ AppManager agent.msi`) or from the main AppManager setup program (`AMSetup.exe`), the installer for each `.msi` package unpacks its contents into the `Temp` directory as defined by the System environment variable on the local computer. In such a case, you can avoid a failed agent or module installation by ensuring that the `Temp` directory is on a drive with sufficient space to perform the installation.

Both silent and remote installation use the `Temp` directory as defined by a *user account* that has Administrator privileges on the target computer. So when you are running a silent or remote installation, you are more likely to run into space issues. This is because you might be unaware of the setting for the `%Temp%` environment variable on the remote computer.

If the `Temp` directory lacks the necessary space, the agent installation might fail without an error message. The only way to detect a failed agent installation is when you cannot subsequently discover it.

In this situation, you should find out where the `.msi` installers are unpacking the files:

- **Standard installation** (the `AMSetup.exe` file launches the `.msi` package): Check the System `%Temp%` environment variable on the local computer
- **Remote and silent installation**: Check the User `%Temp%` environment variable on the target computer
- **Installation by manually launching an `.msi` installer**: Check the System `%Temp%` environment variable on the local computer

Understanding Agent Reporting Capabilities

When you enable reporting capability on the agent, a default report output folder is created in the AppManager directory, for example, in `\NetIQ\AppManager\web\Report`. The setup program also installs additional files to allow the agent to perform repository queries and rendering operations.

Note If you are upgrading from AppManager version 6.0.2 to 7.0.1, the installation will reset the location where reports are stored. The reports are now stored in the `NetIQ\Common\Reports` folder on the computer where you have installed the upgraded version of AppManager.

Report agents can query AppManager repositories, NetIQ Analysis Center repositories, or Microsoft Active Directory. For AppManager repositories, the AppManager Layout engine, which is installed when you select the Reporting option, uses Microsoft ActiveX Data Objects (ADO) to connect and execute SQL stored procedures against the repository to gather data for a report.

NetIQ Corporation recommends the following to optimize system resources for generating large reports:

- Install each report-enabled agent on a dedicated report server that does not have any other core AppManager components installed.
- Use one report-enabled agent computer for each repository.

Understanding Agent Automatic Discovery

To enable AppManager to automatically discover the computer on which you are installing the agent, ensure that:

- You have already installed a management server
- You designate a primary management server for the agent.

Note NetIQ Corporation recommends that you designate the primary management server on every agent during installation. This helps avoid performance problems with the AppManager repository.

Understanding MAPI Mail Settings

Agent installation offers an option to enable MAPI mail, which allows the agent to automatically send e-mail messages in response to certain events.

If you enable MAPI mail, the agent can send e-mail automatically, using the MAPI protocol, as part of a Knowledge Script job. For example, you can set up the Action_MapiMail Knowledge Script to send an e-mail notifications to selected users when an event with a minimum severity level is raised.

When you enable MAPI Mail during agent installation, the installer does not create a mailbox/profile automatically. You should create a mailbox/profile manually in your Microsoft Exchange Server and client after agent installation is complete. Additionally, you should add the mailbox/profile information to AppManager Security Manager. You can also use Security Manager to change or update this information for any managed client. For more information, see [“Using Security Manager to Update Information” on page 167](#).

Note Because Microsoft has tightened security in the most recent versions of Microsoft Outlook 2003, the `netiqMAPImail` helper script only works with Outlook 2000 or Outlook 2003 with Service Pack 1.

Understanding Windows User Accounts

You must specify a valid Windows login account for the agent services to use if you are:

- Installing the agent on the management server.
- Monitoring SQL Server and using SQL Server Windows Authentication security.
- Enabling MAPI mail as an action on the local computer. For more information, see [“Understanding MAPI Mail Settings” on page 105](#).
- Enabling the reporting capability on the local computer. For more information, see [“Understanding Agent Reporting Capabilities” on page 104](#).

Some modules (such as Exchange Server and Active Directory) require the agent services to run using a Windows user account. For more information, see the *Management Guide* for the relevant module.

Notes The Network Service account on Windows Server 2003 is not supported for the agent. On Windows Server 2003, do not configure the agent to use the Network Service account as the agent's **Log On As** account.

If you are specifying a Windows account, ensure that the account has been configured with the **Log On As Service** privilege. Otherwise, the agent services will fail to start. You can configure this privilege after installation. In such a case, you need to start the services manually.

After an agent is installed, you can change the account it is using. NetIQ Corporation recommends that you install the agent using the Local System account if you are unsure whether the application to be monitored requires a Windows account.

Understanding Management Server Designation

When you specify management server information during agent installation, the setup program runs a validity check to verify the following aspects:

- If you install the agent and the management server on the same computer, the local management server *must* be the primary management server.
- When installing the management server and agent, specify the NETBIOS name of the computer as the display name for the agent. If you specify a fully-qualified domain name or IP address, the NETBIOS name and the specified name are displayed in the Control Center Console. To resolve this issue, delete the computer name that you had specified during agent installation.
- Agent discovery will fail if the agent cannot communicate with either the primary or secondary management server. In such a case, you should manually run the Discovery Knowledge Script after installation. Once the agent has been successfully discovered, you can use the AMAdmin_SetPrimaryMS Knowledge Script to change the primary and secondary management servers.

Note New agents in AppManager version 7.0 cannot communicate with a management server that has been upgraded from 5.0.1 to 7.0 with security level 1 (encryption) or 2 (encryption and authentication). To overcome this problem, run the NQKeyGenwindows.exe utility on the computer hosting the repository with the following command line parameters:

```
NQKeyGenWindows.exe -db db_name:user_name:sql_server_name
-agentpwd
```

Command Line Parameter	Description
db_name	The name of the AppManager Repository

Command Line Parameter	Description
user_name	The AppManager Repository can be installed using either Windows authentication or SQL authentication. In the case of Windows authentication, this field can be left blank. In the case of SQL authentication, you must provide a valid SQL server username. The utility prompts for a password if you are using SQL authentication.
sql_server_name	The SQL Server where the AppManager Repository has been installed.
agentpwd	Prompts for the agent password. This is the password which gets stored in the AppManager Repository and is used for subsequent communication between the agents and the management servers.

Example: `NQKeyGenWindows.exe -db QDB::SQLServerABC -agentpwd`

In the above example, `db_name` is `QDB` and `sql_server_name` is `SQLServerABC`. When you run the command, you need to enter the password on the command line.

Restricting Management Server Communications

During agent installation, you may see a popup asking you whether to “restrict management server communication with this agent.” This setting refers to an agent security feature that prevents unauthorized (or “anonymous”) management servers from contacting it.

Note If you select **Anonymous access** while configuring security for the Web management server, this popup will not appear.

When you upgrade an agent to AppManager version 7.0 or later, you can restrict the authorized servers to the designated primary and secondary management servers. Alternatively, you can keep the current configuration until you change the agent’s designated management servers in the Windows registry using the `AMAdmin_SetPrimaryMS` Knowledge Script.

If you do not change management server designation during the installation or upgrade, or if you click **No** in the popup dialog box and decide later that you want to add this security measure, you can use the `AMAdmin_AgentConfigMSRestrictions` Knowledge Script to restrict the authorized management servers.

Installing the Agent Locally

Before you begin the agent installation, ensure that you have either local or domain Administrator privileges on your computer.

Note If an earlier version of the agent is already installed on your computer, choose between the following:

- Upgrading the agent services, local repository, and modules, and preserving any data in the agent's local repository
- Upgrading and discarding the existing data.

For more information about upgrading the agent, see the *Upgrade and Migration Guide for AppManager*.

To install the agent:

- 1 After selecting a location to install the AppManager agent (see [“Running the AppManager Setup Program” on page 70](#)), click **Next**.
- 2 In the Reporting and Discovery Options dialog box, select:
 - **Enable reporting capability:** To allow the agent to generate and configure AppManager reports from the data it collects.
 - **Automatically attempt to discover this agent computer during setup:** To perform discovery automatically and add this managed computer to the Operator Console TreeView as part of agent installation.
- 3 Click **Next**.

- 4 In the Windows Agent Security Level dialog box select the appropriate level of security to use for all communication between the agent and its management server.

Option	Description
Cleartext communications (no security)	<p>Allow communication in clear text between the managed client and its management server.</p> <p>If you select Cleartext, no further security configuration is necessary.</p>
Encrypted communications only (medium security)	<p>Encrypt all communication between the management server and this managed client.</p> <p>If you select Encrypted Communications, you will be asked to supply an agent encryption key and password later during the installation.</p> <p>Note</p> <p>Encrypted communications and Authentication and encrypted communications require the following additional configuration after completing the installation:</p> <ul style="list-style-type: none">• Running the NQKeyGenWindows.exe utility (in the AppManager\bin directory) to generate an encryption key file and insert it into the repository database.• Running the AMAdmin_AgentConfigSecurityKey Knowledge Script to distribute the agent encryption key to the agents.
Authentication and encrypted communications (highest security)	<p>Require managed clients to authenticate the identity of the management server before sending encrypted communication.</p> <p>If you select this option, all communication between the managed client and its management server is encrypted to provide an additional layer of security. The managed client must authenticate the management server before sending any data. You cannot use authentication without encryption.</p>

Notes Ensure that the security level for the agent is the same as that you set for the repository and management server. For more information, see [“Installing the AppManager Repository” on page 83](#).

If you are upgrading from a previous release of AppManager, you are not prompted for security information. Instead, the setup program retains your existing security configuration and key file information (if applicable). If you want to change your security configuration, you must do so after upgrading all AppManager components. For more information, see the *Upgrade and Migration Guide for AppManager*.

For more information about AppManager component security options, see the *Administrator Guide for AppManager*.

- 5 If you select **Cleartext communications**, and click **Next**, the Managed Client Computer Name dialog box is displayed.

Note Steps 6-8 are applicable only if you select **Encrypted communications only** or **Authentication and encrypted communications** and click **Next**.

- 6 In the Agent Encryption Key dialog box, type a password for the encryption key, and then confirm the password by retyping it.
- 7 Click **Next**. The Managed Client Computer Name dialog box is displayed.
- 8 In the Managed Client Computer Name dialog box, enter a name for the managed client and click **Next**.

Tip Enter a name that is helpful in the context of your AppManager management site. You can also enter the IP address, DNS name, computer name, or server hostname.

- 9 In the Management Server and Ports dialog box, enter the **Management server port** and **Agent port** and click **Next**.

Note Typically, the default ports are appropriate:

- 10** In the MAPI Mail Settings dialog box, select **Enable MAPI mail** to enable the agent to send MAPI e-mails.

Field	Description
Exchange Server Name	Name of the Microsoft Exchange Server that the managed client uses to send e-mail messages.
Mailbox Alias Name	<p>Exchange mailbox alias name for the agent account.</p> <p>The e-mail alias, which identifies an e-mail account, is the portion of the e-mail address that precedes the "@" symbol. For example, yourAlias@netiq.com. Enter only a valid alias here.</p> <p>The default is netiq-computer.</p> <p>If the mailbox alias does not already exist for the service account user and profile, use Exchange Administrator to set it up. For more information, see "Configuring a Mailbox for MAPI Mail" on page 164.</p>
Exchange Client Profile Name	<p>Exchange client profile name.</p> <p>The setup program automatically creates an Exchange profile for the mailbox using the name you specify. The agent will use this profile to send test email messages to monitor Exchange connectivity.</p> <p>A mail profile instructs Exchange which e-mail account to use, including the username, display name, e-mail server name, and where to deliver e-mail for this account.</p> <p>The default is netiq-computer.</p>

If you do not enter the Exchange Server profile and mailbox alias name during installation, you can add the same using the AppManager Security Manager. You can also use Security Manager to change or update this information for any managed client. For more information, see ["Using Security Manager to Update Information"](#) on page 167.

Note By default, **Disable MAPI mail** is selected.

- 11** Click **Next**. The Windows User Account Information dialog box appears.
- 12** In the Windows User Account Information dialog box, select **Windows user account**.

- 13** Enter the required information for a valid Windows user account and click **Next**.

Field	Description
Username	The name of the Windows login account you want to designate as the service account for the NetIQmc and NetIQccm agent services. The default is netiq_nt. Note The Windows login account should not be the Local System account.
Password	Password for the Windows login account.

Note After agent installation, you can modify the account used by the agent services. Both services must always be configured to use the same account information.

- 14** In the Management Servers dialog box, select:

- **Designate management servers now:** to specify the primary and secondary management servers during installation, or
- **I will do this later:** to specify the management servers after installation.

Note During the agent installation, if you select security level 2 (authentication and encryption), the agent does not authenticate the Primary management server. To resolve this problem, you must disable the group policy to install the agent with authentication and encryption. Alternatively, you can install the agent manually.

- 15** If you select **Designate management servers now**, enter the hostname or IP address of the computer that you want to use as the **Primary(required)** management server for the agent.
- 16** Optionally, enter the hostname or IP address of the computer that you want to use as the **Secondary(optional)** management server for the agent.
- 17** Click **Next**. The Deployment Web Service dialog box appears.

18 In the Deployment Web Service dialog box, select **Designate the Web Server now**.

Note If you have not yet installed a Deployment Web Service, select **I will do this later**. You can install the Deployment Web Service when you install Control Center. Alternatively, run the `AMAdmin_SetDeploymentWebService` Knowledge Script on the agent to configure the Deployment Web Service after the agent installation is complete.

After the agent is installed, you do not get software inventory information for the agent. This also prevents subsequent modules from being installed on the managed client computer until you manually set the deployment web service using the `AMAdmin_SetDeploymentWebService`. After you run the `AMAdmin_SetDeploymentWebService` Knowledge Script, you must restart the agent or wait for six hours for the software inventory to be sent to the Deployment Web Service.

19 Enter the **Web Server** name or IP Address and click **Next**.

20 In the Installation Summary dialog box, click **Install**.

Note If prompted with the reminder that AppManager requires disk performance counters to be started, click **OK**.

21 Click **Finish** after the installation is complete.

Installing Agents Remotely

Once you have installed a repository, management server, agent, and Control Center Console, you can install more agents on remote Windows computers in your environment. For more information on installing agents on remote Windows computers, see the *Control Center User Guide for AppManager*.

Note At present, you cannot install agents remotely in a UNIX environment.

With past AppManager versions, you could use the following Knowledge Scripts to remotely install or update agents and modules:

- AMAdmin_AgentInstall
- AMAdmin_AgentInstallProxy

These Knowledge Scripts are still available in your repository, but they can only be used to install **older** versions of the AppManager agent and modules. They will **not** run on version 7.0 or later of the agent.

Post-Installation Tasks

After completing agent installation, you should be able to see the managed client in the Operator Console TreeView or in Control Center. An agent that has been discovered is called a managed client. Its resources are now available in the TreeView pane or on the **Objects** tab of the Knowledge Script Properties in Control Center so that it can be monitored with AppManager.

Manually Discovering the Agent

If you disabled automatic discovery of the agent during the installation, you must run a Discovery Knowledge Script to discover the agent computer and add it to the Operator Console TreeView or to Control Center. Run one of the operating-system Discovery Knowledge Scripts, such as Discovery_NT or Discovery_Unix, to discover the agent. Support for monitoring the operating system is installed along with the agent on both Windows and UNIX systems.

Firewall Considerations

On Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1, the built-in Windows firewall may require you to take additional post-installation steps to enable discovery. You cannot manually add the managed client to the TreeView.

To enable the managed client for AppManager discovery over Windows firewall:

- Enable the ICMP protocol in the Windows firewall.
- Manually open the relevant TCP ports to enable communications among AppManager components. For more information, see [“Reviewing AppManager Port Usage” on page 22.](#)

Note The Windows firewall is disabled by default with Windows Server 2003 SP1, but it is *enabled* by default with Windows XP SP2.

To enable the ICMP protocol on a computer where a Windows firewall is active:

- 1** Click **Start > Settings > Control Panel > Windows Firewall**. Or in the Windows **Security Center**, click the **Windows Firewall** link.
- 2** Click the **Advanced** tab.
- 3** Click the **ICMP Settings** button.
- 4** Select **Allow incoming echo request** and click **OK**.

To open TCP ports in the Windows Firewall:

- 1** Click **Start > Settings > Control Panel > Windows Firewall**.
- 2** Click the **General** tab. Make sure the **On** option is enabled. This indicates that the Windows Firewall is active.
- 3** Click the **Exceptions** tab.
- 4** Click **Add Port**.
- 5** In the Add a Port dialog box, enter a name for the port you want (for example, **netIQms**), and specify the port to open. Make sure **TCP** is selected.
- 6** Click **OK** to add the port. To add another port, repeat Steps 3 and 4.
- 7** Click **OK** after adding the ports you want.

Once you have changed the ICMP and TCP port settings in the Windows firewall, you should be able to successfully add the computer to the Operator Console TreeView or Control Center.

Changing the Default AppManager Listening Ports

You can change the listening ports that the agent services use by editing a key in the Windows registry:

- 1 Expand the **SOFTWARE\NetIQ\AppManager\4.0\NetIQmc\NetIQmsPort** registry key.
- 2 Double-click **Port** to change the port for Windows agents.
- 3 Select the **Decimal** option to display the current value in decimal format.
- 4 Type the new port number for the **DWORD** value.

You will need to make the corresponding change for the management server. For more information, see the *Administrator Guide for AppManager*.

Installing UNIX Agents

The AppManager UNIX agent is a daemon that you install on each of the UNIX servers you want to manage. An installation script guides you through the steps for installing and starting the agent. Running the installation script requires **root** user permission. However, the UNIX agent itself does not have to run under the **root** user account.

For more information about installing UNIX agents, see the *AppManager for UNIX Management Guide*, included with the installation kit.

Installing Modules

This chapter describes the steps for installing modules on agents and other AppManager components. Ensure you have the AppManager agent installed on computers you want to monitor before following the steps in this chapter. For more information about installing agents, see [Chapter 9, “Installing Agents.”](#)

This chapter contains the following sections:

- [“About AppManager Modules” on page 119](#)
- [“Introducing Module Installation” on page 120](#)
- [“Installing Modules on Managed Clients” on page 121](#)
- [“Installing Modules by Downloading From the Web” on page 122](#)
- [“Installing Modules Using the AppManager Installation Kit” on page 125](#)
- [“Installing Modules Remotely by Using Control Center” on page 125](#)
- [“Installing Modules in a VoIP Environment” on page 126](#)

About AppManager Modules

Modules are software probes that “plug into” the AppManager agent or UNIX agent. They provide application or component-specific support to the agent and allow Knowledge Script jobs to run. Modules reside on managed client computers as AppManager DLLs and provide the following functionality:

- Monitor elements and properties of applications
- Gather performance and health data

- Access data sources for running jobs






Modules are installed alongside AppManager agents on the computers you want to monitor using AppManager.





Modules are found by a Discovery process. The Discovery process also determines the specific properties of each module. Object properties must be compatible with an individual Knowledge Script so the Knowledge Script can initiate a job on that object.

Note In past releases of AppManager, managed-object installation was accomplished as part of agent installation.

Introducing Module Installation

Install AppManager modules by completing the following checklist:

	Step	Description
	1 Ensure the AppManager agent is already installed.	For more information about installing agents, see Chapter 9, “Installing Agents.”
	2 Install the module on the repository computer.	If you are installing or upgrading AppManager, you may have performed this step as part of installing or upgrading the repository. For more information about installing the AppManager repository, see Chapter 6, “Installing the Repository.”
	3 Install the module on the Console computers.	If you are installing or upgrading AppManager, you may have performed this step as part of installing or upgrading the Consoles. For more information about installing the Consoles, see Chapter 8, “Installing the Operator Console Programs” and Chapter 12, “Installing Control Center.”
	4 Install the module on managed client computers.	“Installing Modules on Managed Clients” on page 121

	Step	Description
	5 If you are installing a later version of the module, upgrade the Knowledge Script jobs.	For more information about upgrading Knowledge Script jobs, see the <i>Upgrade and Migration Guide for AppManager</i> .
	6 Discover computers to monitor.	If you are installing or upgrading AppManager, you may have performed this step as part of installing or upgrading the managed client. However, some discovery scripts require configuration before you run them. For more information, see the Help for the module Discovery Knowledge Script.
	7 Some application-specific configuration maybe required.	For more information on application-specific configuration, see the <i>Management Guide</i> and Readme for the module you are installing.

Installing Modules on Managed Clients

The steps you take to install the a module vary, depending on the environment you are monitoring. You need to have Administrator privileges to install modules on managed clients. You can install AppManager modules in the ways described below for the Windows and UNIX operating systems.

- In a Windows environment, you can:
 - Download the module setup program from the Web and install the module locally. For information, see [“Installing Modules by Downloading From the Web”](#) on page 122.
 - Use the AppManager installation kit to install the modules locally. For more information, see [“Installing Modules Using the AppManager Installation Kit”](#) on page 125.
 - Use the AppManager Control Center Console to install the module remotely. For more information, see [“Installing Modules Remotely by Using Control Center”](#) on page 125.

- In a UNIX environment, you can install the module locally:
 - By running the installation script, `netiq_component_install`, from the `unixclient` directory. This directory is extracted from the `unixclient.tar` file included with the AppManager UNIX Components installation kit.
 - By installing the module silently. For more information on silent installation, see [Appendix B, “Performing a Silent Installation.”](#)

Notes Managed-object installation is integrated with the UNIX agent installation. You can also run the `netiq_component_install` Knowledge Script directly to install or remove components on computers where you have already installed the UNIX agent. For more information on installing UNIX agents and modules, see the *AppManager for UNIX Management Guide*, available in the UNIX Components installation kit.

Modules for both Windows and UNIX are uninstalled when you uninstall the agent.

Installing Modules by Downloading From the Web

To install modules by downloading from the Web, you need to download the module you want to install, extract the files into a temporary folder, and double-click the setup program.

Note Modules with version numbers earlier than 7.0 cannot be installed on agents of version 7.0 and later.

To install an AppManager 7.0 module:

- 1 Download installation kit for the module that you want to install onto the distribution computer. For more information about the distribution computer, see [“Saving Installation Kits to a Distribution Computer”](#) on page 67. For example, if you want to install AppManager for SQL Server version 7.0:

- Use `AM70_SQL_xx_pwd.exe` to install a trial version of the module. You can obtain the package at www.netiq.com/products/am/trialcenter.asp.
- Use `AM70_SQL_xx.exe` to install a licensed version of the module. You can obtain the package at www.netiq.com/support/am/extended/modules.asp.

When you download AppManager modules, these files are copied by default to the **Program Files\NetIQ** folder on the download computer. NetIQ Corporation recommends that you copy these files to `\windows_installation\setup\Setup Files` directory on the same distribution computer on which you saved your AppManager software and documentation. By doing so, you maintain all AppManager software in one location that is easily accessible when you want to add more repositories, management servers, or agents.

2 Double-click the file to extract the following files into a temporary folder:

- `.msi` (the application module setup program)
- `ck<Module_name>.exe` (the pre-installation check used with the AppManager setup program, for example, `ckDe11.exe`)
- `.ini` (a configuration file used with the AppManager setup program)
- `.xml` (a configuration file used for deploying the module with Control Center. This is the file you check into the Control Center Web Depot.)
- `.pdf` (Management Guide)
- `.htm` (ReadMe)

3 Install the module using one of the following methods:

- Run the setup program locally on the agent, repository, and console computers.
- Run the setup program locally on the repository and console computers, and then use the Control Center to remotely install

the module on the agent computers. For more information, see the *Control Center User Guide for AppManager*.

- Run the AppManager setup program on the repository, agent, and console computers. For more information, see [Chapter 4, “Installing AppManager.”](#)

Note You can find a record of the problems encountered during the installation in files named `<modulename>_Install.log` and `AM70-App1-7.0.xx.0.msi.log`, located in the `\Netiq\Temp\NetIQ_Debug\<computer_name>` folder.

To install an AppManager 6.0.2 module:

- 1 Download the installation kit of the module that you want to install on your computer. For example, if you want to install AppManager for SQL Server version 6.0.2:
 - Use `AM60_SQL_xx_pwd.exe` to install a trial version of the module. You can obtain the package at www.netiq.com/products/am/trialcenter.asp.
 - Use `AM60_SQL_xx.exe` to install a licensed version of the module. You can obtain the package at www.netiq.com/support/am/extended/modules.asp.
- 2 Double-click the file to extract the following files into `\Program Files\NetIQ`:
 - `.exe` setup program (the application module setup program)
 - `.pdf` (Management Guide)
 - `.htm` (ReadMe)
- 3 Double-click the `.exe` file to install the module.

Note You can find a record of the problems encountered during the installation in a file named `<modulename>_Install.log`, located in the `\Netiq\Temp\NetIQ_Debug\<computer_name>` folder.

Installing Modules Using the AppManager Installation Kit

This section describes instructions to install modules using the AppManager installation kit.

To install modules using the AppManager installation kit:

- 1 Insert the AppManager CD-ROM into the drive. The AppManager Control Center Version 7.0 dialog box is displayed.
- 2 Click **Production Setup**.
- 3 Click **Begin AppManager Setup**.
- 4 Click **Run** to run the AppManager 7.0 setup program.
- 5 In the Welcome dialog box, select **Production**, and then select **Monitoring Modules**.
- 6 Click **Next**. The pre-installation check runs.
- 7 In the Monitoring Modules dialog box, select the module(s) that you want to install.
Note If the module that you want to install does not appear in the list, click **Click here to view preinstall details** to view the pre-installation check report.
- 8 Click **Next**. The Summary dialog box lists the modules you have chosen to install.
- 9 Click **Install**. The Setup Complete dialog box indicates that setup has completed.
- 10 Click **Finish** to complete the installation.

Installing Modules Remotely by Using Control Center

After you have installed the AppManager repository, management server, and at least one Control Center Console in your

environment, you can install AppManager modules remotely on Windows managed clients.

Notes At present, you cannot deploy modules remotely in a UNIX environment.

The AppManager agent version 7.0 must be installed before you can deploy any modules remotely.

For more information on remotely installing modules on Windows managed clients, see the *Control Center User Guide for AppManager*.

Installing Modules in a VoIP Environment

Deploying modules and agents in a Voice Over IP (VoIP) environment presents a few unique requirements. AppManager provides close to 20 modules that monitor VoIP hardware and software, VoIP call quality, and related network devices, such as routers and gateways. AppManager even provides monitoring support for hardware that does not allow local installation of an agent. In such cases, agents must be installed on *proxy agent* computers. With the AppManager proxy architecture, the module is installed on a proxy that is communicates with the server to be monitored. When you run a Knowledge Script job, the module runs on the agent proxy computer and sends messages to and from the servers or devices being monitored.

Because a number of VoIP modules use the proxy architecture, they can be installed on most computers running Windows 2000 or later and do not require other software. Those modules appear in the list of modules to install on a Windows computer, even if your environment lacks VoIP hardware and software.

If you are installing on servers running Cisco applications, the list of modules to install includes only those that have been verified to run on the Cisco server. Some modules, such as IIS and SQL Server, do not appear in the list, even if the corresponding application

prerequisites are met. In the case of Cisco modules, AppManager management of SQL Server and IIS resources is provided by the VoIP module and not by the SQL Server or IIS modules. Also, if you try to remotely install the SQL Server or IIS module on a computer where one of the Cisco applications was running, the Deployment task will not be created for the affected agent targets.

The ReadMe and Management Guides for the Cisco modules provide a list of the modules that are verified to run on a Cisco server.

Installing the Web Management Server

This chapter describes the steps for installing the AppManager Web management server.

The following topics are covered:

- [“Understanding Web Management Server Installation” on page 129](#)
- [“Installing the Web Management Server” on page 130](#)
- [“Configuring Web Server Security” on page 130](#)
- [“Verifying the Chart Component” on page 132](#)

Understanding Web Management Server Installation

For security reasons, NetIQ Corporation recommends installing the Web management server on the same computer as your AppManager repository. Installing the Web management server on the same computer as the SQL Server lets you use integrated security for your Operator Web Console. Otherwise, you must enable Basic authentication on the Web management server computer. In Basic authentication, the passwords used to authenticate Operator Web Console users are sent to the repository in clear text. For more information, see [“Configuring Web Server Security” on page 130](#).

We also recommend installing the report agent on the same computer as the Web management server. This configuration creates the necessary virtual directories and links for that computer’s IIS Default Web Site, and allows you to use the Operator Web Console to view reports.

Installing the Web Management Server

Before you begin the Web management server installation, ensure that you have either local or domain Administrator privileges on your computer.

To install Web management server:

- 1 After selecting a location to install the Web management server, (see [“Running the AppManager Setup Program” on page 70](#)), click **Next**.

Notes If the setup program detects that you do not have Active Server Page extensions enabled, it displays a warning and asks you to enable Active Server Page extensions before continuing.

When you are prompted to stop and restart the IIS Admin service, click **Yes**.

- 2 In the Confirmation dialog box, click **Install**.
- 3 Click **Finish** after the Web management server is successfully installed.

Configuring Web Server Security

After you install the AppManager Web management server, you need to configure some security settings for the Web server.

The Web server where you installed the Web management server needs to authenticate the users who will be logging on to the AppManager repository using the Operator Web Console. Depending on your environment and where you chose to install the Web management server, you may need to change the IIS Directory Security settings for the Web management server.

When Microsoft SQL Server is set to use Mixed or Integrated Security, some settings in IIS must be changed to enable Active

Server Pages (ASP) to connect to it using a trusted connection. The Microsoft [Knowledge Base article 176379](#) contains more information.

Note All user accounts for the Web management server must be valid user accounts for the SQL Server where the AppManager repository is installed.

To configure security for the Web management server:

- 1 Start the IIS Manager by clicking **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
- 2 Expand the list of **Default Web Sites**.
- 3 Right-click **NetIQ**, then click **Properties**.
- 4 In the NetIQ Properties dialog box, click the **Directory Security** tab.
- 5 Click **Edit** to change the settings for anonymous access and authentication method.
- 6 In the Authentication Methods dialog box, specify how IIS authenticates users who attempt to start an Operator Web Console session.

The authentication method you select for the Operator Web Console should depend on your environment and how you expect users to log in to the repository:

- If you want to allow users to log on to the Operator Web Console using any supported Web browser from either a Windows or a Linux computer, select **Enable Anonymous access**. This option allows users to log on without being separately authenticated by the IIS Web server.
- If users will only log on to the Operator Web Console using Internet Explorer from a Windows computer, select either

Basic authentication (which is not very secure) or **Integrated Windows authentication**.

Note If you select **Anonymous access** and use the SQL Server credentials to log in to the Operator Web Console, you will not be able to view any computers in the domain.

If all users who need access to the Operator Web Console use Windows computers and Internet Explorer, you should verify whether anonymous access is disabled and choose an appropriate authentication method:

Option	Description
Basic authentication	<p>Allow Windows users to authenticate themselves. For example, by using a different Windows username and password than the current Windows user.</p> <p>Basic authentication transmits the user name and password to the IIS server in unencrypted form (clear text).</p> <p>Basic authentication is useful if you want to establish a separate user account for logging on to IIS that is different from your standard Windows user accounts.</p> <p>If you want users to log on with their current Windows user name and password, you should use Integrated Windows authentication.</p>
Integrated Windows authentication	<p>Configure IIS to automatically authenticate the current Windows user account as a valid Windows account with proper domain privileges.</p> <p>If you enable Integrated Windows authentication, IIS will always verify the current Windows account.</p>

- 7 Click **OK** to close the Authentication Methods dialog box, then click **OK** again to close the NetIQ Properties dialog box.

Verifying the Chart Component

After you install the AppManager Web management server component, you can use a Web Browser to access the Web

management server. In such a case, your Web Browser becomes your Operator Web Console.

If you want to use the Operator Web Console to generate and view charts, you need to download and install the AppManager Version Checker program. The AppManager Version Checker program verifies that the correct version of the AppManager chart component is installed.

To install the AppManager chart component in the Operator Web Console:

- 1** Start the Operator Web Console and log in to an AppManager repository.
- 2** Click **Charts** in the Navigation bar.
- 3** When prompted, download and install the AppManager Version Checker program by clicking the **Chart Component** hyperlink, and then clicking **Open**.

Once the chart component installation completes, click **Charts** in the Navigation bar to view charts. For more information, see the *Operator Console User Guide for AppManager*.

Installing Control Center

This chapter describes the steps for installing Control Center.

The following topics are covered:

- [“Understanding Control Center Installation” on page 135](#)
- [“Understanding the Command Queue Service Options” on page 137](#)
- [“Understanding Optional Configuration for the Command Queue Service” on page 138](#)
- [“Understanding the SQL Server Agent Service Account” on page 140](#)
- [“Understanding the SQL Server Account for Control Center Administration” on page 140](#)
- [“Installing Control Center” on page 141](#)
- [“Installing Components for Deploying Agents Remotely” on page 145](#)
- [“Post-Installation Tasks” on page 152](#)

Understanding Control Center Installation

You can install Control Center version 7.0 as part of the overall AppManager Suite installation, or install Control Center separately. For more information about Control Center, see the *Control Center User Guide for AppManager*.

Control Center installation consists of the following components, which are listed in the following order in the setup program:

- Deployment Service
- Deployment Web Service
- AppManager Control Center Database
- Command Queue Service
- Console

You can install all Control Center components on the same host. However, NetIQ Corporation recommends distributing the components across different Windows servers to improve performance.

While larger networks require multiple AppManager repositories and management servers, a single Control Center repository can manage your entire organization. Similarly, a single Deployment Web Service will be sufficient for your entire organization. NetIQ Corporation recommends installing multiple Deployment Servers reporting to a single Deployment Web Service-Control Center repository combination. You should install a Deployment Server for every firewall-separated segment of your network. For more information, see [“Installing Components for Deploying Agents Remotely” on page 145](#).

If you install Control Center components on computers in separate network domains, the Control Center repository uses both the domain name and username for authentication purposes. Making connections between Control Center components across *untrusted* domains is not possible unless you have installed the Control Center repository on a SQL Server instance that is using SQL authentication. To allow a Control Center console to connect to a Control Center repository in a different *trusted* network domain using Windows authentication, you must add an Administrator account (in the [DOMAIN]\Administrator format) as a Control Center user in AppManager Security Manager.

Understanding the Command Queue Service Options

The Command Queue Service allows for communication between the Control Center repository and the AppManager repositories being managed with Control Center. It polls the Command Queue table in the Control Center repository at regular intervals, looking for commands to be sent to individual AppManager repositories. It then sends any commands it finds to the AppManager repositories, where they are retrieved and executed by the appropriate agents. For more information, see the *Control Center User Guide for AppManager*.

If you select the Command Queue Service for installation, you are first prompted to supply a Windows user account under which the Command Queue Service should run. The Command Queue Service Account is used for two purposes:

- To run the Command Queue Service.
- To give the Command Queue Service access to each managed repository (unless you use a SQL Server account to access the repository).

Note When you add an AppManager repository to the list of repositories to be managed by Control Center, you are given the option to use a SQL Server account to access that repository. Unless you select this option, the account you supply for the Command Queue Service must have full AppManager Administrator privileges in each managed repository. You must add this account as an AppManager user on each repository, using the AppManager Security Manager.

Supply a valid Windows user account with Administrator privileges in the Control Center repository database. The account you specify must be part of the local Administrators group. An account with Domain Admin privileges is not sufficient unless it is also a direct member of the local Administrators group. This account must also be configured as an Administrator in Control Center. You are prompted to supply the username and password associated with the selected user account.

When you install a Command Queue Service on a computer that lacks a Control Center repository, you are prompted for the name of the Control Center repository to which it should connect. Otherwise, the local Control Center repository is used automatically for this parameter.

We do not recommend connecting more than one Command Queue Service to a Control Center repository.

Understanding Optional Configuration for the Command Queue Service

A configuration file, `NQCQS.exe.config`, is installed in the `ControlCenter\bin` folder when you install the Command Queue Service (`NQCQS.exe`). The `NQCQS.exe.config` file contains XML variables with editable values. By default, the file is populated with default settings that are currently in use by the service. The Control Center options dialog can be used to modify most of these values. However, you must restart the Command Queue Service before the modified values take effect.

The following table describes the settings in the Command Queue Service configuration file:

Value	Description
"ServerName" value = "RALQEROW06A02"	Displays the AppManager Control Center Repository computer name
"DBName" value = "NQCCDB"	Displays the AppManager Control Center Repository name
"HealthcheckPoll" value = "15"	Specifies the interval at which the Command Queue Service looks for new commands in the Control Center Repository. The default is 15 seconds.
"ReconnPoll" value = "60"	Specifies the interval at which the Command Queue Service retries a failed attempt to connect to the Control Center or AppManager Repository. The default is 60 seconds.

Value	Description
"numbackups" value = "100"	Displays the maximum number of log files. The default value for the maximum number of SyncQDBLog.txt and CQSLog.txt log files are configured at installation. When the maximum numbers of log files have been created, the oldest log file is overwritten.
"filepath" value = "C:\Program Files\NetIQ\Temp\NetIQ_Debug\CC_CQSTrace\"	Displays the path on the Command Queue Service computer for the log files. The default path is: [drive]:\Program Files\NetIQ\Temp\NetIQ_Debug\CC_CQSTrace.
"FileSize" value = "500000"	Specifies the maximum size, in bytes, for the SyncQDBLog.txt and CQSLog.txt log files. The default is 50,000 bytes. If the log file exceeds this threshold, a new log file is created. The default threshold is configured at installation.
"TraceLevel" value = "Info"	Specifies the level of tracing information you want in the SyncQDBLog.txt and CQSLog.txt log files. You can set the tracing level to: <ul style="list-style-type: none"> • Off to disable logging for non-Error events. • Error to log program exceptions to the Windows Event Log and the Command Queue Service log file. All critical messages are always logged to the Windows Event Log. • Warning to logs program recoverable errors to the Command Queue Service log file. • Info to log program warnings and flow information to the Command Queue Service log file. This is the default. • Verbose to log program debug and trace information such as variable values and thread state to the Command Queue Service log file.
"NoSyncThread" value = "10"	Specifies the number of parallel sync activities that will be executed in parallel. It defines the number of parallel threads used to run sync commands. The default is 10 and maximum is 60.
CommandPoll	Specifies the interval at which the Command Queue Service looks for new commands in the Control Center repository. The default is 30 seconds.
HealthcheckPoll	Specifies the interval at which the command queue service checks the connectivity to the Control Center repository.

Understanding the SQL Server Agent Service Account

The SQL Server Agent Service is also known as the Cache Manager that runs under a Windows account. It needs Administrator privileges to access both the Control Center and the AppManager repository.

When you add an AppManager repository to the list of repositories managed by Control Center, you can use a SQL Server account to access the Control Center repository. If you do not select this option, the account you supply for the SQL Server Agent Service must have *full* AppManager Administrator permissions in each managed repository. Use AppManager Security Manager to add this account as an AppManager user on each repository.

Like the account used by the Command Queue Service (see [“Understanding the Command Queue Service Options” on page 137](#)), this account must also be a valid Windows user account, with similar privileges and Control Center access. Although you can use the Windows Local System account, NetIQ Corporation recommends that you use the same account that you specified for the Command Queue Service.

Understanding the SQL Server Account for Control Center Administration

During Control Center installation, you need to designate a SQL Server account that serves as an alternate Control Center Administrator.

After installation, this account becomes the default administrator for Control Center. It becomes the owner of the Control Center repository (NQCCDB). Although the SQL Server account is a Control Center Administrator account, you cannot use it to run the Command Queue and Cache Manager services because it is not a Windows account.

Installing Control Center

Before you begin the Control Center installation, ensure that you have either local or domain Administrator privileges on your computer.

Note A Configuration Check dialog box is displayed when the Control Center installation starts. This enables you to run the Configuration check utility to verify Microsoft DTC connectivity. For more information, see [Appendix E, “Reviewing Microsoft DTC and Control Center Installation.”](#)

To install Control Center:

- 1 After selecting a location to install the Control Center (see [“Running the AppManager Setup Program” on page 70](#)), click **Next**.
- 2 In the Select Features dialog box, select the Control Center components you want to install and click **Next**.
- 3 Select the Control Center components that you want to install, and click **Next**.

Note NetIQ Corporation recommends installing all Control Center features, including the Deployment Service and the Deployment Web Service. They are required for installing agents, modules, and upgrades on remote computers.

- 4 In the Customer Information dialog box, enter the appropriate information and click **Next**.
- 5 In the **SQL Server Security Information** dialog box, select the SQL server where you want to install the Control Center repository (NQCCDB).

Note The setup program needs a secure login account to create a database in SQL Server. The account you supply for installation and repository ownership must have **System Administrator** privileges.

- 6 Select the authentication type for the repository and click **Next**:
 - **Use Windows authentication:** The Windows user account you are currently logged in as. This is the default selection.
 - **Use SQL Server authentication:** Enter the **SQL Server account** name and **password**. This option is enabled only if you are running your SQL Server in mixed authentication mode.
- 7 In the Command Queue Service Account Information dialog box, select:
 - **Use Local System account**
 - **Use Windows account:** Enter the **Username** and **Password** for the Windows user account.

Note For more information about the accounts used by the Command Queue Service, see [“Understanding the Command Queue Service Options” on page 137.](#)

- 8 Click **Next**.
- 9 In the SQL Server Agent Service Account dialog box, select:
 - **Use the default Windows service account (LocalSystem)**
 - **Use the account the Command Queue Service is using (recommended)**
 - **Use the following Windows user account**

Note If you select Use the following Windows user account, you need to enter the **Domain**, **Username**, and **Password** for the Windows user account.

For more information about the SQL Server Agent Service Account, see [“Understanding the SQL Server Agent Service Account” on page 140.](#)

- 10 Click **Next**.

- 11** In the SQL Server Account for Control Center Administration dialog box, enter the **SQL Server account** name and **Password**. The default user name is **netiq**.

For more information, see [“Understanding the SQL Server Account for Control Center Administration”](#) on page 140.

- 12** Retype the **Password** to confirm it and click **Next**.

Note If you have already the AppManager repository, the Setup program displays a message indicating that the **netiq** user name already exists. You can change it if required.

- 13** In the Control Center Repository Options dialog box, type the following information or accept the default values, then click **Next**.

Field	Description
Data file location	The location where the Control Center repository data is stored. For example: C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data To browse for the location, click the [...] button.
Initial data file size (MB)	The size in MB for the Control Center repository data device. The default is 500 MB.
Log file location	The location where the Control Center repository log is stored. The default is c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data To browse for the location, click the [...] button
Initial log file size (MB)	The size in MB for the Control Center repository log device. The default is 200 MB.

Tip Adjust the data and log file sizes based on the number of repositories you plan to manage and the number of management groups and views you plan to create.

- 14** In the Remote Deployment Setup dialog box, select:

- Check in packages and import rules during installation or

- Check in packages and import rules later, from Control Center Console.

Note For more information about remote deployment using Control Center, see the *Control Center User Guide for AppManager*.

15 Click **Next**.

16 In the Deployment Service Account Information, select:

- **Use Local System account:** This is the default selection.
- **Use Windows account:** You need to enter the **Domain**, **Username** and **Password** for the Windows account.

For more information about the Deployment Service, see [“Installing the Deployment Service” on page 149](#).

17 Click **Next**.

18 In the Confirmation dialog box, verify your installation choices and click **Next**.

19 Click **Finish** after the Control Center is successfully installed.

Notes During the installation, you may be prompted to allow the setup program to start or stop services such as **NetIQms** and **SQLServerAgent**.

When you install the Control Center, it installs report-sharing components as a separate process. You need to manually verify that the report-sharing components are installed successfully. You can view the log file, `nqRSC.log`, in the `<InstLoc>\NetIQ\Temp\NetIQ_Debug` folder. You can also see a separate entry for Report Sharing Components in the **Add/Remove Programs** folder. You can see the report-sharing components in the registry entry at `HKLM\Software\NetIQ\Report Sharing Components\Sharing Applications`.

Installing Components for Deploying Agents Remotely

Deploying agents and modules remotely is supported on AppManager version 7.0 and later.

Control Center relies on the following components to install agents and updates on remote computers:

- **Deployment Service**—A service used to install agents and updates on remote computers.

The computer where this service is installed is called the Deployment Server. You may have multiple Deployment Servers to handle deploying agents remotely. If a firewall is active on your network between the Deployment Server and the Control Center repository, the Deployment Service can run in proxy mode, which allows it to use the Deployment Web Service to communicate with the repository.

- **Deployment Web Service**—A Web service that allows the Deployment Service to communicate with the Control Center repository and deploy agents remotely across a firewall.

The Deployment Web service also allows agents to report software inventory to the Control Center repository, and handles the check-in of deployment packages to the Web Depot. The Deployment Web Service needs access to the Control Center repository to retrieve task information required to perform deployments.

- **The Web Depot**—The computer where agent and module installation files are staged for remote deployment. Agent and module packages are checked into the Web Depot. The Web Depot is also installed when you install the Deployment Web Service.

The procedure to deploy agents and modules remotely involves the following steps:

- 1 Web Depot configuration and package check-in. For more information, see [“Creating the Web Depot” on page 146](#).
- 2 Deployment Web Service configuration. For more information, see [“Installing the Deployment Web Service” on page 147](#).
- 3 Deployment Server configuration. For more information, see [“Installing the Deployment Service” on page 149](#).

Creating the Web Depot

The first setup step in deploying remotely is to create the Web Depot computer, a staging area for installation files. You are asked whether you want to “check in” packages and default rules for use in AppManager agent and module deployment as part of the installation. All available agent and module packages, plus a set of generic deployment rules, are checked into the Web Depot during the installation by default.

“Packages” are the installation files needed to deploy agents and modules in your network. The check-in procedure for packages ensures that the installation and configuration files associated with all modules and the Windows agent are made available to the Control Center console and repository.

The default deployment rules are samples that can help you perform basic deployments of agents and modules, with modifications. The rules you check in here are disabled by default; this means that no deployment tasks will be performed until you edit and configure the rules for your environment and then enable them using the Control Center Tasks pane.

If you change the default to **Check in packages and import rules later from Control Center Console**, you will need to perform package checkin yourself as part of configuration. For more information on package check-in, see the *Control Center User Guide for AppManager*.

Installing the Deployment Web Service

The Deployment Web Service allows agents to communicate with the Control Center repository. The Deployment Web Service also needs to retrieve deployment task information for the Deployment Service if a firewall is present on the network.

Note If you do not install the repository and the Deployment Web Service at the same time, you need to specify security information for the Control Center repository.

- 1 Supply information about a **Windows user account** that is configured as an Administrator in Control Center.

Note The Windows Local System account does not have the necessary permissions. Supply the username and password associated with a valid Windows user account that has Administrator privileges in the Control Center repository and is part of the local Administrators group. An account with Domain Admin privileges is not sufficient unless it is also a *direct* member of the local Administrators group.

- 2 Supply the SQL Server name and the instance where the Control Center repository is installed. Use the format `SQL Server Name\Instance name`.

A Control Center repository should have only one Deployment Web Service communicating with it. If you already have a Deployment Web Service associated with your repository, cancel the installation.

If necessary, you can change the user account associated with the Deployment Web Service after the installation is complete. For more information, see [“Changing the User Account for the Deployment Web Service” on page 157](#).

When the Deployment Web Service is installed, three virtual directories are created under the default Web site in IIS:

- `DeploymentWebService`
- `ProxyDeploymentWebService`

- webDepot

The `ProxyDeploymentWebService` directory is only used if you run the Deployment Service in proxy mode (for cross-firewall deployments). If you run in proxy mode, you will need to enable Secure Sockets Layer security (SSL) on the IIS Web Server for the default Web site, as well as install the certificate on the Proxy Deployment Service. When you enable SSL, be sure **not** to check the option to **Require Secure Channel** under the **Edit** option for the certificate. For more information, see [“Installing SSL Certificates” on page 150](#).

Note If you want to enable anonymous authentication for the Deployment Web Service, use the Directory Security tab in the IIS Manager to configure anonymous access. In addition, you need to grant Administrator privileges for the anonymous user.

Importing Deployment Rules After Installing Deployment Web Service

If you choose not to install default deployment rules during the Deployment Web Service installation, you can import the rules later using Control Center.

To import deployment rules after installing the Deployment Web Service:

- 1 Start Control Center.
- 2 In the Navigation pane, click **Rules**.
- 3 In the Tasks pane, click **Import Rule(s)...**
- 4 Navigate to the location where the deployment rules (XML files) are stored and select the rules you want to import.

Note You can select multiple rules by selecting the CTRL or Shift buttons on your keyboard.

- 5 Click **Open** to successfully import the default deployment rules.

Installing the Deployment Service

The Deployment Service, which is used to install agents and updates on remote computers, needs to retrieve task information from the Control Center repository, either directly or in proxy mode.

If you plan to install multiple Deployment Services in your network, NetIQ Corporation recommends that you co-locate them in your remote sites. If these computers cannot access the Control Center repository directly due to firewalls, you can run the Deployment Service in proxy mode.

- If no firewall is active between these computers, you can simply supply the Control Center repository SQL Server name and instance name in the Deployment Service Configuration dialog box.
 - If a firewall is active on the network between these computers, the Deployment Server needs to use the Deployment Web Service as a proxy to reach the Control Center repository computer across the firewall.
- 1** To set up proxy mode for the Deployment Service, select **A firewall is active between the Deployment Server and the Control Center repository**.
 - 2** Supply the hostname or IP address of the Web server where you have installed the Deployment Web Service.

To run in proxy mode, the Deployment Service requires a Secure Sockets Layer (SSL) certificate to be properly installed on the Deployment Server. Otherwise, as soon as the Deployment Service attempts to start, you will see a failure message stating, “The underlying connection was closed. Could not establish trust relationship with remote server.” For more information, see Microsoft Knowledge Base article [324284](#).

The necessary steps to take to install an SSL certificate on the Deployment Server are provided below, in [“Installing SSL Certificates” on page 150](#).

Installing SSL Certificates

You can deploy agents and modules on remote computers located on the other side of a firewall. If you configured the Deployment Server to run across an active firewall during Deployment Service installation, you instructed the Deployment Web Service to run in proxy mode. For more information, see [“Installing the Deployment Service” on page 149](#).

Proxy mode requires a Secure Sockets Layer (SSL) certificate to be properly installed on both the Deployment Server and Deployment Web Service computer. Otherwise, as soon as the Deployment Service attempts to start, you will see a failure message stating, “**could not establish trust relationship with remote server.**” For more information, see Microsoft Knowledge Base article [324284](#).

When you enable SSL, be sure **not** to enable the option to **Require Secure Channel (SSL)** for the certificate. You can check this setting on the **Directory Security** tab of the Default Web Site Properties dialog box in the IIS Manager. It requires all HTTP connections to the default Web site to use HTTPS. The Web Depot and Deployment Web Service do not require SSL, so this setting will prevent connections to them. If you have enabled the secure channel requirement, you may see an error stating, “Unknown error code from BITS: 80190193.”

The steps to install an SSL certificate on the Deployment Server are outlined in that article, and the relevant ones are summarized here. You may first have to install the Windows Certificate Services using Add/Remove Programs. Then you may need to create an SSL certificate using the Web Server Certificate wizard in the IIS Manager. The Microsoft KB article mentioned above provides help. The IIS Manager Help explains how to start the Web Server Certificate wizard.

To install a Secure Sockets Layer (SSL) certificate:

- 1 In the **Open** field of the IIS Manager Web Server Certificate wizard, type `mmc`. Click **OK**.

- 2** On the File menu, click **Add/Remove Snap-in**.
- 3** Click **Add**.
- 4** Click **Certificates**, and then click **Add**.
- 5** Click **Computer Account**, and then click **Next**.
- 6** Click **Local Computer**, and then click **Finish**.
- 7** Click **Close**, and then click **OK**.

The list of certificate categories for the local computer appears in the snap-in window.

- 8** Expand **Certificates (Local Computer)**.
- 9** Expand **Trusted Root Certification Authorities**.
- 10** Right-click **Certificates**, point to **All Tasks**, and then click **Import**.
- 11** In the Certificate Import Wizard, click **Next**. Click **Browse**, and then locate the certificate.

This may be a certificate that you created using the Web Server Certificate Wizard. Microsoft Knowledge Base article [324284](#) contains more information about certificate creation.

- 12** Click the certificate file, and then click **Open**.
- 13** Click **Next**.
- 14** Click **Next** again, and then click **Finish**. Click **OK** to acknowledge the successful importation.

Deployment Service Account Information

If no firewall is active on the network between the Deployment Server and the Control Center repository, you are asked for account information to allow the Deployment Service to access the Control Center repository. For more information, see [“Installing the Deployment Web Service” on page 147](#). By default, Setup uses the

Windows account under which you are currently logged into the computer.

If a firewall is active, the credentials you supplied when you installed the Deployment Web Service are used, and the Deployment Service runs in proxy mode to access the Control Center repository.

You can change the Windows account for the Deployment Service after installation is complete. For more information, see [“Changing the User Account for the Deployment Service” on page 155](#).

Post-Installation Tasks

Your environment is unique, and your network security measures are similarly unique. AppManager and Control Center therefore offer many options for customizing your installation.

The topics that follow outline some extra configuration steps you might want to take to ensure that Control Center conforms to your security policies and to customize some associated services.

SQL Server Security

Some user accounts needed by Control Center during the installation are also used later to administer your management site. For example, the account used as an alternate Control Center Administrator, the “SQL Server Account for Control Center Administration,” assumes ownership of the Control Center repository database (**NQCCDB**) after installation. By default, a “netiq” user account, which is created during Control Center repository installation, is used. That account has System Administrator (**sa**) privileges, which are required to create a SQL Server database.

Similarly, anytime you add a normal workstation user and place him or her in the Control Center Administrators group, that user account is given **sa** privileges as well.

Having multiple accounts and/or services with **sa** privileges may violate your security policies.

One option is to use the SQL Enterprise Manager to remove the SQL Administrator privilege for selected Control Center accounts, including the netiq user account. In general, if you remove the System Administrator role for any user, that user loses the ability to add new data sources (repositories) to Control Center. You will therefore need to restore this permission to the netiq user account when you want to:

- register a new repository.
- add a new Control Center user.

NetIQ Corporation recommends that you wait to remove this privilege until after your list of repositories and users has stabilized.

Optional Configuration for the Deployment Service

A configuration file, `DeploymentService.exe.config`, is installed in the `ControlCenter\bin` folder when you install the Deployment Service (`DeploymentService.exe`). This configuration file contains XML variables with editable values. By default, the file is populated only with those settings that are currently in use by the service.

If you make changes made to the configuration file, you must restart the Deployment Service before they will go into effect.

The following table summarizes the settings in the Deployment Service configuration file, lists their defaults, and explains their usage:

Value	Description
ServerName	Machine name and instance of the Control Center repository. For example, <code>NYCTest03\INST2005</code> .
DBName	The name of the Control Center database to which the deployment service is connecting. This value should probably remain unchanged from its default. The default is <code>NQCCDB</code> (the default name for the Control Center repository).

Value	Description
ProxyWebService	<p>The hostname of the computer where the Deployment Web service with which the Deployment Service should communicate is installed. The proxy capability of the Deployment Service is only used when firewalls are active on the network. This value is set during installation and should not be changed.</p> <p>By default, this value is empty. It should be blank when the <code>serverName</code> parameter is populated.</p>
PackagePathSetting	<p>The location where Web Depot packages are copied locally. This can be an override if the packages are inaccessible for some reason from the Web Depot.</p> <p>By default, this value is empty.</p>
NumBackups	<p>The number of trace log backups that are kept in the <code>CC_ADSTrace</code> folder (see the <code>TraceLevel</code> parameter for more information on tracing).</p> <p>The default is 10.</p>
FileSize	<p>The maximum file size for the trace log files; once this file size is reached, the trace log is backed up (to the file <code>DeploymentServerZ.log</code>, where <code>z</code> is an integer from 1 to <code>NumBackups</code>—see the previous parameter).</p> <p>The default is 5,000,000 bytes.</p>
FilePath	<p>The location of the trace logs.</p> <p>The default path is <code>...\NetIQ\netiq_debug\Temp\CC_ADSTrace</code></p>
NumDeliveryThreads	<p>The number of threads that will be available for the execution of tasks; these threads will be used to deliver and install files simultaneously.</p> <p>The default is 50 threads.</p>

Value	Description
TraceLevel	<p>The level of tracing that will be logged to the deploymentService.log* files under the path selected for the FilePath variable (see above). The default level will show errors and warnings that are thrown during execution of the deployment service.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> • Error • Warning • Info • Verbose <p>During normal testing and use, the default level of Warning is sufficient. For troubleshooting of defects, however, the Info or Verbose settings are recommended.</p>
NotificationEmailFromAddress	<p>Enables you to send an email about the success or failure of a task. You need to configure the email settings in the Rule Wizard.</p> <p>The default value is "" (null or empty). The value is generated dynamically when you configure the email address in Control Center. For more information, see the <i>Control Center User Guide for AppManager</i>.</p>
BypassAuthentication	<p>Typically used in a workgroup environment to bypass security certificate (SSL) authentication errors.</p> <p>In a workgroup environment where SSL is enabled, you may encounter errors when the Deployment Service is unable to make trusted connections. Use this parameter to bypass the client SSL certificate authentication.</p> <p>The default value is "true".</p>

Changing the User Account for the Deployment Service

In the Deployment Service Account Information dialog box, you are asked for the Windows account that should be used by the Deployment Service to log in to the Control Center repository. This information is then stored in the Windows registry under HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\Control

Center\1.0\CCDB. The relevant keywords are `WindowsAuthName` and `WindowsAuthPass`.

You can change the user account information later, after the installation has completed.

To change the Windows user account for the Deployment Service to log into the Control Center repository:

- 1** In the Services area of the Windows Control Panel, stop the Deployment Service (`DeploymentService`).
- 2** At a command prompt, `cd` to the `C:\Program Files\NetIQ\AppManager\Control Center\bin` directory (or wherever your `DeploymentService.exe` configuration file is saved). Then enter the following:
`DeploymentService -setwindowsauth domain\username password`
- 3** Start the `DeploymentService`.

You will then need to add the new user account information to the list of permitted users in the Control Center database. For more information about changing the number of permitted users, see the *Control Center User Guide for AppManager*.

For more information about the Deployment Service configuration file, see [“Optional Configuration for the Deployment Service” on page 153](#).

Registering the Location of the Deployment Web Service

When you install an AppManager agent, you are prompted to enter the name of the Deployment Web Service computer if you have already installed it.

If you choose to install Control Center and the Deployment Web Service *after* agent installation, you need to edit a registry setting at the agent computer so that it can locate this service, which is used for

the agent to report its software inventory to Control Center repository.

The `AMAdmin_SetDeploymentWebService` Knowledge Script can perform this task for you. For more information, see the Help for the `AMAdmin_SetDeploymentWebService` Knowledge Script.

Changing the User Account for the Deployment Web Service

You can change the Windows user account for the Deployment Web Service later, after installation has completed, by updating the identity of the IIS application pool associated with the service. Use the IIS Manager to update the properties of the `AutoDeploymentAppPool`.

To change the user account for the Deployment Web Service:

- 1 In the IIS Manager, right-click the `AutoDeploymentAppPool` and select **Properties**.
- 2 On the **Identity** tab, click **Configurable** to update the username and password. For the username, use the format `Domain\User`.
- 3 Add the new username to the `IIS_WPG` (worker process) group.
- 4 Stop and restart the application pool.
- 5 Stop and restart the `IISAdmin` service.
- 6 Add the user account to the list of permitted users in the Control Center database. For more information, see the *Control Center User Guide for AppManager*.

Post-Installation Configuration

This chapter describes the steps to configure AppManager Security Manager to grant access to AppManager users.

The following topics are covered:

- [“Understanding Security Manager” on page 159](#)
- [“Configuring SNMP for Monitoring Hardware” on page 161](#)
- [“Configuring a Mailbox for MAPI Mail” on page 164](#)
- [“Using Security Manager to Update Information” on page 167](#)
- [“Working with AppManager Connectors” on page 168](#)

Understanding Security Manager

Security Manager enables AppManager administrators to control access to views and tasks. Depending on your access rights and your SQL Server security setting, you can use Security Manager to identify SQL Server users to use AppManager, add new SQL Server users, assign roles to AppManager users and manage user rights. For more information, see the AppManager Help.

Note You can use SQL Server Enterprise Manager to verify the authentication type and whether the account has permission to access SQL Server databases. Once you have identified at least one Windows or SQL Server account for logging in to the repository the first time, you can use Security Manager to grant other SQL Server login accounts access to AppManager.

Starting Security Manager for the First Time

To use the Security Manager for the first time, you must have at least one SQL Server login or Windows user account with permission to access SQL Server and the AppManager repository.

For more information about accounts and access permissions, see the *Administrator Guide for AppManager*.

To start Security Manager for the first time:

- 1 From the Windows desktop, click **Start > Programs > NetIQ > AppManager > Tools & Utilities > Security Manager**.
- 2 In the Security Manager Logon dialog box, enter the following information:

Field	Description
Server	The name of the Windows server where the AppManager repository is installed. After you enter the name, the repositories available on that server are displayed in the Repository list.
Repository	The database name for the AppManager repository you want to work with. The default repository name for AppManager is qdb. Note Once you have logged into the Security Manager, you can switch to another repository.
Connection Information	Use Windows authentication — Log on using your current Windows user name and password. You must use this type of connection if SQL Server uses Windows Authentication security. Use SQL Server authentication — Log on to SQL Server by typing the Login name and Password . Note <ul style="list-style-type: none">• If you are running SQL Server in Windows Authentication mode, you will not see this option.• When using a SQL user account, make sure the password for the user account is less than 32 characters. If your password exceeds 32 characters, Security Manager displays an error message.

3 Click **Logon** to open Security Manager.

For more information about configuring Security Manager, see the AppManager Help and the *Administrator Guide for AppManager*.

Configuring SNMP for Monitoring Hardware

AppManager monitors hardware statistics through integration with SNMP-based agents on the managed clients. If you are monitoring any product in the Hardware category, check that the SNMP service is installed and started and that you registered the SNMP **community name** for the server when you installed the module on the computer. Keep in mind that the community name is case-sensitive.

The products included in the Hardware category include:

- HP Insight Manager
- Dell OpenManage
- IBM Director
- Siemens ServerView

If the community name has been entered incorrectly or changed after installation, use Security Manager to update it. Security Manager does not change the actual SNMP community string or verify the information you enter. It only updates the information in the AppManager repository. For more information, see [“Using Security Manager to Update Information” on page 167](#).

Checking the SNMP Service

In some environments, the SNMP service may not be installed by default, or it may be set to run manually.

To check whether the service is installed and running:

- 1** Double-click **Services** in the Administrative Tools.
- 2** In the list of services, be sure **SNMP Service** is listed and started.

If the SNMP service is not listed:

- Close the Services program.
 - Follow the SNMP installation instructions for your computer. Completing the installation requires restarting your computer and may require re-applying a Windows service pack.
 - Start the SNMP service.
- 3** In the list of services, be sure other appropriate services are listed and started.

Application	Services to Check
HP Insight Manager	CIM agent services for your version of CIM.
Dell OpenManage	<ul style="list-style-type: none">• Dell Baseboard Agent• Win32sl <p>Note The version of the Dell OpenManage agent software must correspond to a supported version of the Dell server BIOS. For more information, see the Dell Support Web page at http://www.dell.com/support.</p>
IBM Director	Director Support Program service.
Siemens ServerView	Siemens ServerView SNMP agent.

- 4** Close the Services program.

Checking SNMP Security

If SNMP security on the managed client computer is configured to accept SNMP packets from a specified host list, the managed client must be configured to accept its own SNMP packets.

To check the SNMP security settings:

- 1** On the Windows desktop, right-click **Network Neighborhood** and then click **Properties**.
- 2** In the Network dialog box, click the **Services** tab.
- 3** Right-click **SNMP Service**, and then click **Properties**.

- 4 In the Microsoft SNMP Properties dialog box, click the **Security** tab.
- 5 If **Accept SNMP Packets from These Hosts** is selected, make sure the name of the local computer is included in the list. If it is not in the list, click **Add** and type the local computer name or IP address.
- 6 Click **OK** and then click **Close**.

If you added a hostname, stop and then re-start the SNMP service for your changes to take effect.

Using the Microsoft SNMP Utility

The Microsoft Windows resource kit includes a utility for checking SNMP, which can be useful for troubleshooting the installation of SNMP and hardware agents. This utility is called `SNMPUTIL.EXE`.

With the `SNMPUTIL.EXE`, you can verify whether basic SNMP is installed and configured correctly by using a command such as:
`snmputil getnext servername communitystring 1`

For example:

```
Q:\>snmputil getnext zebra public 1
```

If SNMP is installed and configured properly, the utility should return information similar to the following:

`SnmpTool - Simple Network Management Protocol Tool for win32`

```
ErrorStatus: 0 (No Error)
ErrorIndex: 0
```

```
varbind 1:
```

```
    Name: system.sysDescr.0
```

```
    OID: 1.3.6.1.2.1.1.1.0
```

```
    Type: OCTET STRING
```

```
    Length: 135
```

```
    Value: Hardware: x86 Family 6 Model 5 Stepping 2 AT/
AT COMPATIBLE - Software: windows NT Version 4.0 (Build
Number: 1381 Uniprocessor Free)
```

If the utility returns an error, you should reinstall or check SNMP configuration.

You can also use the utility to verify the installation of the hardware agent by specifying the proper OID for the agent. For example, you can check for the CIM agent using the following command:

```
snmputil get servername communitystring  
.1.3.6.1.4.1.232.2.2.4.2.0
```

Check the documentation for your hardware vendor to determine the appropriate OID to specify in checking the hardware agent.

Configuring a Mailbox for MAPI Mail

Agent installation provides you with an option to configure a MAPI mailbox for the agent to use when sending e-mail in response to events generated by Knowledge Scripts.

Make sure the following prerequisites are met before you install the agent:

- Install an Exchange client (Microsoft Outlook) on the computer.
- Set up a Windows account for the AppManager agent services to use.
- Set up an Exchange mailbox for the agent service account.

You can then enter the Windows account information and Exchange Server, profile, and mailbox alias names during agent installation.

Note Because Microsoft has tightened security in the most recent versions of Outlook 2003, the **NetiqMAPImail** helper script only works with Outlook 2000 or Outlook 2003 with Service Pack 1. The agent cannot perform the Action of sending e-mail on Outlook 2003 without service packs or Outlook 2003 with Service Pack 2.

If the managed client is also an Exchange Server that you plan to monitor, you may want to use the same Windows login account and Exchange mailbox. For more information, see the *AppManager for*

Exchange Management Guide in the \Documentation folder of the AppManager installation kit.

Note If you are setting up your management server to send MAPI mail as an Action and you are working in a cluster environment, you must use the same user account and Exchange profile information on each cluster node.

Installing an Exchange Client

If the computer is not an Exchange Server or an Exchange Client, a MAPI client must be installed in order to set up the Exchange profile and mailbox alias for sending MAPI mail. For installation instructions, see your Exchange documentation.

Creating an Account for the Agent

The user account is required to create an Exchange profile and mailbox alias. To create a Windows user account, you must have **Administrator** privileges.

The following steps provide an example of user account creation using Windows 2000.

To create a local Windows user account:

- 1** Open **Computer Management** in the Windows Administrative Tools.
- 2** Expand **Local Users and Groups**.
- 3** Click **Users**. Right-click and select **New User**.
- 4** Type a username and password for the account, then retype the account password to confirm the entry.

You can use any name for this account. The default username for the agent service account is **netiq_nt**. The user account is unique in each Windows security domain.

Note Both agent services (**NetIQmc** and **NetIQccm**) must use the same account information. You are prompted to provide this information when you run the setup program or the AgentInstall Knowledge Script. It is automatically applied for both services. If you change the service account after installation, however, be sure to change the account information for both services.

5 Type a full name and description for the account, if desired.

6 Check **Password Never Expires**.

7 Click **Create**, then click **Close**.

After you create the user account, you can click **Groups** to add the account to the **Domain Admins** or a similar administrative group and use the Local Security Settings to define specific rights for the account. At a minimum, you should authorize the service account to **Log on as a Service** and **Log on locally**. For more information about setting up user accounts, groups, and security policies, see the appropriate Windows documentation for the version of Windows you are using.

Creating an Exchange Mailbox

The steps to take when creating an Exchange mailbox depend on the version of Exchange you are using. In most cases, you must be logged on to an Exchange Server with a user account that has an Exchange Administrator permission to create a mailbox. Follow the instructions appropriate for the version of Exchange Server you are using to create a mailbox for the user account the AppManager agent services are using.

Note If you are using Exchange 2000, you can create a mailbox when you create the user account with Active Directory Users and Computers.

Using Security Manager to Update Information

Some AppManager modules require user names, passwords, or other secure information to run certain Knowledge Scripts. Typically, you provide this information during the installation. In some cases, however, you may need to enter or update this information manually after completing the installation.

Identifying Modules that Require Secure Information

With this release, the following AppManager modules require secure information to run some or all Knowledge Scripts in the relevant categories:

- AppManager for BlackBerry Enterprise Server (BES)
- AppManager for Call Data Analysis
- AppManager for Cisco CallManager Express
- AppManager for Cisco Unity Express
- AppManager for HP Insight Manager
- AppManager for Dell OpenManage
- AppManager for Exchange 2000 Server and Exchange 2003
- AppManager for Nortel Contact Center
- AppManager for Oracle RDBMS on Windows
- AppManager for Siemens ServerView
- AppManager for SQL Server
- AppManager for VoIP Quality

If you are monitoring applications with any of these modules, you need to provide secure information such as user names and passwords, either through the setup program (when you install the module), or after installation, using Security Manager.

Additional AppManager modules may be available that require you to provide user names, passwords, or other secure information. For

more information about module-specific security information, see the *Management Guide* for each module.

Note If you did not enter secure information during installation, enter the information manually in Security Manager after you have installed and discovered the agent and resource objects.

Entering Secure Information

To enter or update secure information after installation, you must use AppManager Security Manager. Security Manager stores secure information in the AppManager repository and makes it available for the Knowledge Script jobs that need it.

For more information, see the AppManager Help and the *Administration Guide for AppManager*.

Working with AppManager Connectors

Once you have installed AppManager, you must run the AppManager Connector setup program for any framework products with which you want to integrate. Each Connector has its own setup program and documentation. In most cases, you run the setup program on the computer where the AppManager management server is installed.

For specific information on how to install and use AppManager Connectors, see the appropriate Connector documentation. You can find the documentation for Connectors in the AppManager installation kit that you downloaded and unpacked.

Staging the Deployment

This chapter provides an overview of typical deployment stages and describes the recommended deployment process.

The following topics are covered.

- [“Installing in a Lab Environment” on page 169](#)
- [“Preparing to Install the Pilot Group” on page 170](#)
- [“Running the Recommended Core Knowledge Scripts” on page 172](#)
- [“Adjusting Thresholds and Intervals” on page 179](#)
- [“The Next Stage of Deployment” on page 179](#)
- [“Expanding the Scope of Your Deployment” on page 180](#)
- [“Reviewing and Refining the Deployment” on page 183](#)
- [“Extending AppManager” on page 184](#)
- [“Roadmap for a Staged Deployment” on page 185](#)

Installing in a Lab Environment

It is not always necessary or practical to take the time for a test deployment. However, having the project team install AppManager in a lab environment before deploying it on a production network is useful. A test deployment may be part of an evaluation prior to purchase.

Installing in a lab environment before any actual deployment can point out specific aspects of the organization that the project team may need to address to ensure a successful pilot deployment. In

addition, the test installation gives the project team experience in installing AppManager components and learning what to expect in the installation process. Therefore, NetIQ Corporation recommends installing AppManager in a lab environment initially if possible, especially if the project team has no previous experience installing AppManager components.

When you install AppManager in a lab environment, you should focus on the following key goals:

- Uncovering potential conflicts between AppManager and other applications, such as firewalls. For example, you may find you have special port requirements or restrictive account policies that may cause problems. If you uncover any problems, consult the AppManager Knowledge Base on the NetIQ Web site for information about resolving the problem. Or contact NetIQ Technical Support for help.
- Quantifying the resource usage requirements of AppManager components. This allows you to test your assumptions in a safe but meaningful way and verify that the computers where you intend to install components during the actual deployment meet the requirements.
- Documenting network utilization between components. Even when deploying in a test environment, setting up a realistic sample of scripts and distribution of components lets you assess your bandwidth and latency assumptions.
- Testing the distribution of AppManager agents to ensure you have reliable account information and permissions (for example, usable passwords and domain account names).

Preparing to Install the Pilot Group

Depending on your organization's size, the importance of your monitoring needs, the expertise of your deployment team, and the resources available to you, the pilot deployment may involve a small but representative number of computers or all of the servers you

intend to monitor. NetIQ Corporation recommends installing on enough computers to get a realistic view of the full-scale deployment.

Identify and contact the owners of the computers that are going to be part of the initial deployment. In meeting with key individuals, provide a realistic estimate of the time it takes to install components. Although installation itself takes very little time, your estimate should provide enough buffer time to troubleshoot any failures.

Tip The AppManager setup program does not require rebooting servers. Therefore, it is not necessary to schedule installation for off-hours. However, for servers running business-critical applications, it is best to schedule the installation for a time that will cause the least disruption of service. This advice applies when installing any new software on a server that runs business-critical applications.

The most common sources of installation failure stem from problems with account privileges and permissions to access the servers. Even if you have researched and documented this information, allow some time to resolve these kinds of issues.

- Identify dates and times the computers are available. Access may be strictly controlled.
- Gather all the necessary information, such as passwords or user accounts. You may need information for both the operating system and the application to be monitored.
- Start the AppManager setup program to see the results of a pre-installation check. For more information, see [“Understanding The AppManager Pre-Installation Check”](#) on page 68.
- Then run Setup again to install core components (the AppManager repository, management server and agent, console programs) on selected computers.
- Install Control Center.
- Install the AppManager agents and modules remotely on selected computers.

Running the Recommended Core Knowledge Scripts

Once you have installed AppManager on a number of computers in your environment, you need to make specific decisions about what to monitor. During the planning stage, you should have determined a list of the key Knowledge Scripts to run. If you have done thorough planning, the list may include many Knowledge Scripts and cover a large number of applications. At this stage, however, NetIQ Corporation recommends starting with a **core set** of Knowledge Scripts to monitor server health and availability.

In most environments, each monitored computer runs approximately 15 to 20 Knowledge Script jobs at regular intervals to ensure basic operational health and availability. Additional jobs are then run less frequently to diagnose problems or take corrective action. Although running 15 to 20 jobs is typical, your initial core set may include fewer jobs.

To help you get started, AppManager provides a core set of **recommended** General and NT Knowledge Scripts that are applicable in most organizations, including the following:

Knowledge Script	Guidelines for Running this Knowledge Script
General_EventLog	Monitors the Event Log for events based on virtually any criterion. Initially, NetIQ Corporation recommends monitoring all logs for any Error ("Stop") type of event. You can further filter the log entries to include or exclude specific IDs, descriptions, user names, computer names, or other criteria.

Knowledge Script	Guidelines for Running this Knowledge Script
General_MachineDown	<p>Checks communication between the computer where you drop it on and selected computers.</p> <p>Special requirements: The agent services must run as a service account with Administrator privileges on the server where the job is running and on the servers to which the script is testing the connection.</p> <p>Where to run this script: On a computer in the same subnet as the management server. When specifying the properties for that job, for the Machine List, you should specify a limited number of computers that represent different subnets in your network. You can then drop additional MachineDown jobs on each computer specified in the first job to monitor them in their own subnets.</p> <p>This approach provides coverage without stressing network bandwidth. It also ensures that, if a router or subnet is down, you only receive one event for the server being monitored from the agent on the management server's subnet. The other servers in that subnet will not post duplicate "Machine Down" events.</p> <p>Do not run this Knowledge Script on a management server. Instead, include it in the Machine List.</p>
NT_MemUtil	<p>Physical memory is the most critical statistic you should monitor with this Knowledge Script, which is often used in conjunction with other Knowledge Scripts, such as NT_PagingHigh.</p> <p>Handling spikes: Because memory usage is often subject to temporary spikes, NetIQ Corporation recommends setting a short interval (2 to 5 minutes), but raising an event only after thresholds are exceeded in 3 to 5 consecutive periods.</p>
NT_LogicalDiskSpace	<p>Monitors disk space used and free space available for all logical disks. This Knowledge Script is strongly recommended, especially on computers with Exchange Server or SQL Server. On computers with applications like Exchange Server or SQL Server that take available disk space as needed, NetIQ Corporation recommends setting a lower than normal threshold (for example, 80%) to keep unplanned changes in disk usage from overloading the system.</p> <p>If you see events, add disk or remove unnecessary files.</p>

Knowledge Script	Guidelines for Running this Knowledge Script
NT_CpuLoaded	<p>This script monitors both the percentage of CPU used and processor queue length. By itself, high CPU usage may not indicate a problem. Instead, consider several factors:</p> <ul style="list-style-type: none"> • queue length • how you are using the computers being monitored • your overall strategy for the environment <p>For example, in a transactional environment, you may have a computer with CPU usage consistently at 90%. The computer has no room for growth, but if the queue length remains low and stable (never more than 2 or 3 processes waiting), it may be sized perfectly for maximum efficiency. If the queue length increases and processes are waiting, it may be a problem you need to address. In a batch environment, however, you may want an event if CPU usage exceeds 50% and any process is waiting (queue length at 0) to ensure the computer has enough CPU headroom when batch jobs are running. Also consider the number of users you expect to support, for how long, and how much room for growth you need.</p> <p>Monitor load for each CPU individually. For example, if you monitor overall load and see CPU usage is 100%, the information is not as useful as seeing that CPU 0 is running at 90% and CPU 1 is running at 10%.</p> <p>Handling spikes: Because CPU and queue length are often subject to temporary spikes, NetIQ Corporation recommends setting a short interval (2 to 5 minutes), but raising an event only after thresholds are exceeded in 3 consecutive periods.</p> <p>Collecting data: Enable data collection to identify server usage trends. For example, if CPU usage is increasing steadily, it can help you plan for growth. For this type of analysis, run a second job less frequently.</p>

Knowledge Script	Guidelines for Running this Knowledge Script
NT_LogicalDiskBusy or NT_PhysicalDiskBusy	<p>Monitor disk operation and queue length.</p> <ul style="list-style-type: none"> • In a RAID array environment, use LogicalDiskBusy. • In a non-RAID array environment, use PhysicalDiskBusy. <p>Events may indicate a slow disk controller, a bad physical disk, or an application that needs to be tuned (for example, a poorly tuned database application that is causing excessive swapping).</p> <p>Use these scripts in conjunction with NT_PagingHigh to help you determine the root of an event.</p>
NT_ServiceDown	<p>Checks whether required services are running and automatically restarts down services.</p> <p>Although you can specify services individually, NetIQ Corporation recommends you use an asterisk (*) to check all automatically started services—unless you are collecting data. If you are collecting data, specify the services for which to collect data (for example, you may want to exclude services such as Messenger and Spooler).</p>
NT_TrustRelationship	<p>Checks whether a computer in a certain domain trusts a specified domain.</p> <p>Special requirements: The AppManager agent services must run under a service account with Domain Admin privileges. Do not run this Knowledge Script on the PDC.</p>

Beyond this basic group of Knowledge Scripts that are universally applicable, each additional server type or application you are monitoring has its own set of recommended Knowledge Scripts.

Tip For more recommendations and suggestions about selecting the Knowledge Scripts to run and implementing monitoring policies with Knowledge Script groups, see the *Administrator Guide for AppManager*. You may also want to poll other AppManager users about their practices and recommendations. Subscribe to the AppManager mailing list through the NetIQ Support Web site.

Setting Thresholds for Recommended Scripts

There are three approaches to setting Knowledge Script properties during the first stage of deployment:

- Use the default threshold values or your own experience and understanding of your environment to begin monitoring right away.
- Set all Knowledge Scripts only to collect data (that is, not to raise events) for a week or more to identify normal baseline operating values before setting thresholds for events. At the end of the data-collection period, you should evaluate the information collected to determine a baseline for a normal operating environment and set thresholds accordingly. For housekeeping purposes, you should then delete all of the data collected during this stage from the database. For information about removing data from the database, see the *Administrator Guide for AppManager*.
- Set only those Knowledge Scripts that address critical issues in your environment to raise events, and set the remaining Knowledge Scripts to collect data. This approach can be employed enterprise-wide or only on the servers that you have identified as needing immediate attention.

If you have not been doing any type of monitoring and are deploying a large number of Knowledge Scripts (particularly for applications such as Exchange or SQL Server), the second or third approach is recommended. The first approach, however, allows you to begin actually monitoring right away.

If you decide to start raising events right away, keep in mind that all AppManager Knowledge Scripts provide default thresholds and intervals. These defaults are based on research, testing, and field expertise. If you have not already selected thresholds, use the default values at this stage.

In addition, at this stage you should track the frequency of events, or the number of data points collected. This data will help you tune your system at a later stage.

What You Should See

The initial, testing stage of your deployment should last from two to four weeks. One goal at this stage is to keep things simple, so NetIQ Corporation recommends that you not run additional Knowledge Scripts, or that you strictly limit any additional scripts beyond the recommended core set. You should also strictly limit access to the console and restrict the number of users allowed to perform various activities, such as acknowledging and closing events or starting and stopping jobs.

The purpose of this initial stage is to undergo a “shake-out” period that reveals:

- Serious problems that need immediate attention, for example, computers that are dangerously low on disk space or that have pegged CPU.
- Any environmental issues you need to address, for example, problems with insufficient privileges, instability, or services, such as SNMP, that need to be installed.
- The current state of your environment and how closely the computers you want to monitor conform to your expectations.

Running only a core set of Knowledge Scripts also helps you prevent your staff from being overwhelmed by a sudden barrage of events. By focusing on a limited number of key Knowledge Scripts early in the deployment, you can develop an understanding of the events generated, begin to develop your methodology for responding to them, and effectively troubleshoot any issues that arise.

During this initial deployment stage, you should also evaluate the threshold settings and intervals you have set for your Knowledge Script jobs. If you are seeing too many events, the thresholds may be set too low for your environment, the interval may be too short, or critical resource issues may need to be addressed.

Tip Controlling the number of events early in the deployment is essential. If the operations or administrative staff becomes overwhelmed by events they are not prepared to handle, they may

become frustrated or, worse, may ignore events as redundant or meaningless. With any monitoring system, the key to success is how the team reacts to an alarm.

Using the Data Collected

NetIQ Corporation recommends enabling data collection on core Knowledge Scripts during the initial stage of deployment and then running reports. From the reports, you can review the high, low, and average values for core statistics in hourly, daily, weekly, or monthly time periods. Several basic report Knowledge Scripts are easily configured to access and evaluate this information.

To create reports about your environment:

- 1 Install at least one report-enabled agent. For more information about enabling reporting capability for an agent, see [“Understanding Agent Reporting Capabilities” on page 104](#).
- 2 Run the `Discovery_ReportAgent` Knowledge Script on the computer with the report-enabled agent.
- 3 In the Report view, click through tabs in the Knowledge Script pane to select the reports to run.

Based on the information you find in reports, you can begin to adjust threshold settings to more accurately reflect the specific characteristics of your environment.

Basic AppManager reporting provides detailed information about the computers in a single management site. Once you have expanded your deployment to multiple management sites with multiple repositories, you may want the more sophisticated reporting available in NetIQ Analysis Center.

The AppManager Help provides information about configuring and viewing reports and about using Analysis Center.

Adjusting Thresholds and Intervals

Throughout the first phase of your deployment, review the data collected by the core set of Knowledge Scripts. Initially, you may see quite a few events as you adjust settings and stabilize your environment, but as you solve the serious problems that the core set of Knowledge Scripts are intended to point out, you should begin to develop a sense of your normal operating environment and begin adjusting thresholds and intervals to reflect that environment and the event load you can reasonably handle.

Use the information in the reports and your own experience to modify the thresholds for the core scripts. Keep in mind that this is likely to be an ongoing process: as you gain experience or as the organization changes, you need to periodically review your settings.

Tip Some performance statistics are volatile. Many AppManager Knowledge Scripts let you raise events only after multiple samples find a particular condition. You can, for example, raise an event only after several consecutive threshold crossings.

The Next Stage of Deployment

After running the core set of recommended Knowledge Scripts for two to four weeks and making some adjustments, you should have a stable environment that is not generating a large number of events. At the end of this stage:

- You should have identified and resolved any AppManager installation issues, such as problems with domains or account permissions.
- You should have identified and resolved basic problems in your system, such as low disk space or available memory.
- You should have a clearer understanding of the health and operation of the computers you are monitoring, the number of events to expect, and the appropriateness of the default thresholds and intervals for your organization.

The time it will take to achieve these goals can be influenced by several factors, including the distribution of servers and staff, the condition of your environment before deploying AppManager, and the resources available to you. When you feel comfortable with the core set of Knowledge Scripts you are running and the stability of the operating environment, you are ready to move to the next stage of deployment.

Expanding the Scope of Your Deployment

The second stage of deployment extends AppManager monitoring to additional servers.

Very large or widely distributed organizations typically phase in a full deployment of AppManager over a period of several weeks or even months. For example, if your organization is going to monitor a group of servers in the United States, Germany, and Spain, you may decide to deploy the system first in Germany, stabilize the environment there, and then expand the deployment to include servers in Spain and the United States. Or you might decide to expand the deployment to include the servers in Spain, allow time to uncover problems and stabilize that environment, and deploy to the servers in the United States at a later time.

Deploying Additional Knowledge Scripts

Regardless of the timetable you use to expand the deployment, in the second stage, you should also expand the scope of your management policy to include some or all of the AppManager **recommended** Knowledge Scripts.

The set of recommended Knowledge Scripts varies according to the applications you are monitoring and your organization's goals, but as a baseline, consider running all or some of the following:

Knowledge Script	Description
General_AsciiLog	Monitors any text file for a search string. For example, find error or failure messages. This script is suggested because of the flexibility it provides and because in most environments there are log or text files that should be monitored.
General_Counter	Monitors any Performance Monitor counter. Provides flexibility; most organizations are interested in specific counters that may not already be monitored by other AppManager Knowledge Scripts.
NT_NetworkBusy	Monitors the percentage of bandwidth being used.
NT_PagingHigh	Monitors paging activity per second—a good indicator of actual system performance.
NT_PrinterHealth	Monitors status of printers and print jobs. Recommended for file and print servers; may be useful for some application servers.
NT_PrinterQueue	Monitors printer queue length. Recommended for file and print servers; may be useful for some application servers.
NT_RunAwayProcesses	Finds and, optionally, kills runaway processes based on sustained high CPU usage.
NT_SystemUpTime	Monitors the number of hours that a computer has been operational since last rebooted.

Tip You may find it useful to hear from other AppManager users about their practices. Subscribe to the AppManager mailing list through the NetIQ Support Web site.

Once you have selected a set of Knowledge Scripts for monitoring basic server health and key application resources, you can begin planning for and implementing policy-based monitoring. For more information about implementing monitoring policies, see the *Administrator Guide for AppManager*.

Identifying Your Reporting Requirements

During this stage of the deployment, you should also focus on your reporting needs. You need to identify:

- The standard AppManager reports to generate and the Knowledge Scripts required to generate those reports.
- Who should receive the reports and how frequently.
- How reports will be generated. For example, you may want to generate reports automatically on a scheduled basis or manually on demand.
- Who should be responsible for generating the reports, For example, you may want to restrict who can use the Report view or you may want to assign Exchange reports to an Exchange administrator and SQL Server reports to your DBA group.
- The format to use for reports. For example, you need to decide whether data should be displayed in table format, in charts, or both.
- How reports should be delivered. For example, you may choose to deliver reports through e-mail, post them on a Web site, view them with the Report Viewer, or print them.

There is no “core” set of reports to run. Reports you should probably run at this stage include ReportAM_EventSummary, ReportAM_SystemUpTime, ReportAM_CompDeploy, ReportAM_WatchList, NT_Report_CPULoadSummary, and NT_Report_LogicalDiskUsageSummary.

Deploying Actions and Notification Policies

As you expand the deployment and gain experience in using AppManager, start looking for ways to add responsive and corrective actions to your Knowledge Scripts.

AppManager Knowledge Scripts can automatically perform corrective actions and notify selected people in response to certain events. You can also set up automatic acknowledgment of events. For

more information, see the *Operator Console User Guide for AppManager*.

At this stage of AppManager deployment, your system should be tuned sufficiently for effective Knowledge Script automation. However, you may need to install additional components. For example, you may need an agent that is capable of sending e-mail responses to events. For more information, see [“Understanding MAPI Mail Settings”](#) on page 105.

Reviewing and Refining the Deployment

As you deploy AppManager across your organization, you will continue to refine your management policies and uncover new requirements. Typically, once basic monitoring is underway, it becomes easier to fine-tune thresholds and job intervals, articulate and automate event-response policies, and tailor event notification, data collection, and the user interface to suit the needs of a particular organization.

At this stage, the tasks to focus on include:

- Managing events and event notification.
- Handling data-collection and the archiving of data.
- Controlling communication between managed clients and the management server.
- Managing security and security roles within AppManager.
- Adding management servers and configuring primary and secondary management servers for all managed clients.
- Organizing the computers in your network into meaningful groups.
- Identifying and establishing Knowledge Script Groups, dynamic views, and monitoring policies for the computers in your environment.

Note Before you implement any policy-based monitoring in your production environment, you should mimic your implementation in a test environment and be sure you understand the difference between standard ad hoc jobs and policy-based jobs. In addition, you should keep the initial implementation of policy-based monitoring as straightforward and simple as possible until you are comfortable working with policy-based jobs. By design, it is more difficult to make changes to policy-based jobs than to standard ad hoc jobs.

Extending AppManager

Even after you have deployed AppManager to all or most of the servers in your environment, you will probably continue to improve and streamline your management process. This is an ongoing process that does not end when AppManager is fully deployed. Instead, over time, organizations tend to focus more on extending and customizing AppManager to suit specific needs and on developing more sophisticated monitoring and notification strategies.

In addition, it will become increasingly important for you to manage key aspects of the AppManager environment itself to ensure reliability and optimal performance. For example, you need to develop a consistent backup strategy, and a plan for when and how to perform routine database maintenance. For information and recommendations concerning database maintenance, see the *Administrator Guide for AppManager*.

At this stage and beyond, you will typically concentrate on the following types of tasks:

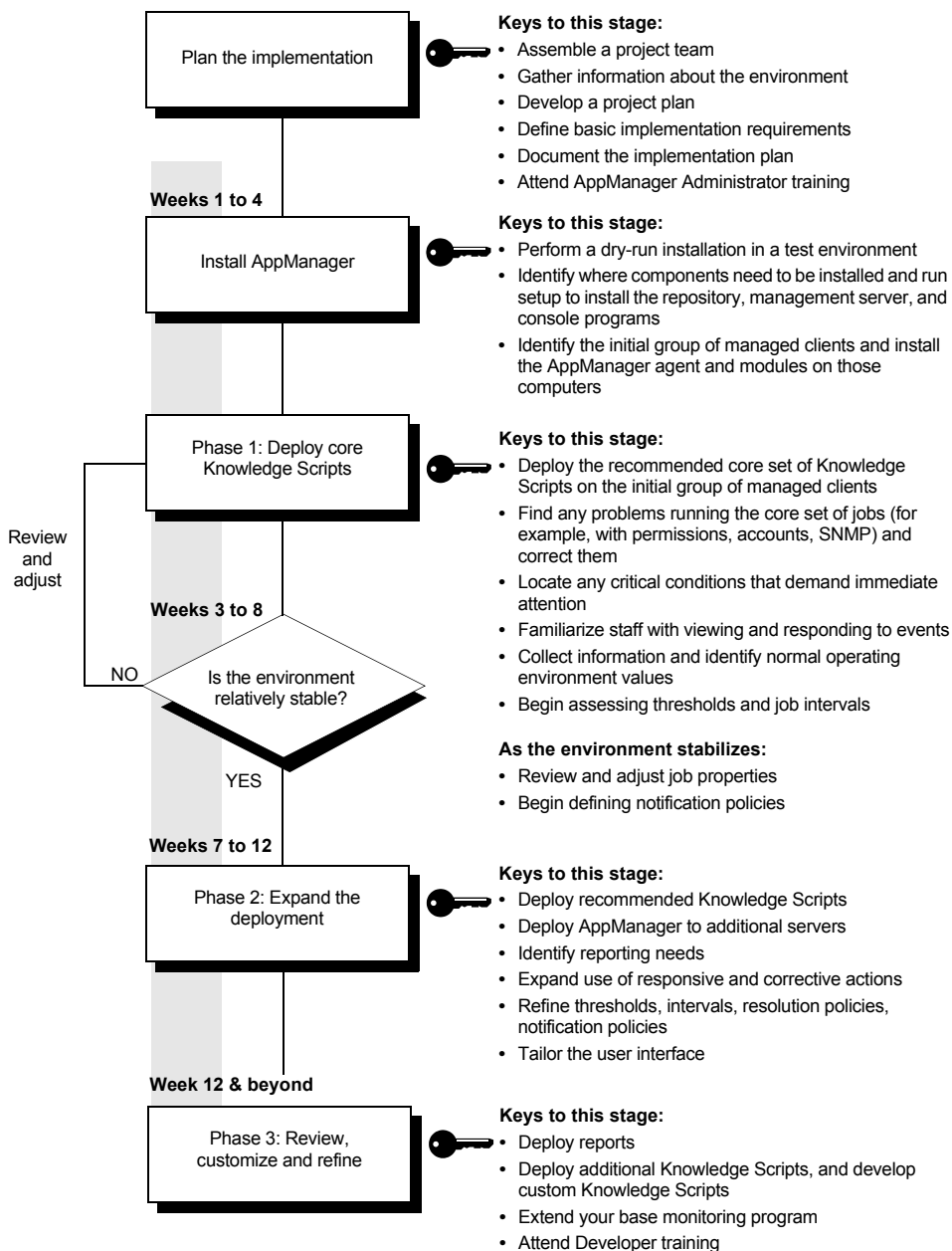
- Deploying reports automatically and designing requirements for any customized reporting (for example, to produce custom reports focused on Service-Level Agreements).
- Running additional Knowledge Scripts that are uniquely useful for your environment or for troubleshooting specific problems.

- Identifying any extensions to your base monitoring program: for example, adding new applications; correlating additional monitoring tasks; setting up responsive actions.
- Developing custom Knowledge Scripts.
- Designing more complex notification or resolution rules.
- Integrating AppManager with other products.
- Documenting your extensions to AppManager and your management and resolution policies.
- Maintaining the AppManager repository.
- Periodically reviewing and, if necessary, updating the AppManager environment; for example, adding or modifying users and roles, or redistributing components.

Roadmap for a Staged Deployment

The diagram on the next page summarizes a typical deployment scenario, including the main focus of each phase. Remember that the phases may overlap, and that the process of refinement is ongoing. In addition, a key to success for all phases is to document your policies and processes, to communicate policies and processes to others in the organization, and to make the documentation widely available.

Many of the tasks described generally in this chapter and diagram are expanded or illustrated through examples in either the *Operator Console User Guide for AppManager* or *Administrator Guide for AppManager*.



Updating License Information

This appendix describes the procedure to view and update AppManager license information.

The following topics are covered:

- [“Understanding AppManager License Keys” on page 187](#)
- [“Managing AppManager Licenses” on page 188](#)
- [“Requesting a License Key” on page 189](#)
- [“Starting License Manager” on page 190](#)
- [“Updating an Expired License” on page 191](#)
- [“Adding and Deleting a License Key” on page 191](#)
- [“Requesting License Information” on page 192](#)
- [“Importing License Keys from a File” on page 193](#)
- [“Running a License Report” on page 193](#)

Understanding AppManager License Keys

AppManager licenses are classified as evaluation and production. An evaluation license enables you to install all AppManager components but with limited functionality. An evaluation license is valid for 30 days from the date of installing AppManager. For more information, see [Chapter 5, “Installing AppManager for Evaluation Purposes.”](#)

When you purchase AppManager, you receive a permanent license key that replaces the evaluation key and identifies the specific component or components you have purchased.

Because license keys are typically associated with individual AppManager modules, you will receive multiple license keys. You need to enter the license keys during AppManager installation. For example, if you purchase the base AppManager product and a 50-server license for monitoring Windows, you receive two license keys: one for the Operator Console and one for the Windows module.

Although NetIQ Corporation recommends that you supply a permanent license key when you install the repository, you can use the default evaluation key during installation and update the license information after you complete the installation process.

Note If you use the default evaluation key during installation, or if you purchase additional AppManager components after installation, you need to update the license information using the AppManager License Manager. For more information, see [“Adding and Deleting a License Key” on page 191](#).

Managing AppManager Licenses

You can easily manage multiple AppManager licenses by requesting NetIQ Corporation for a text file that contains the license keys you have purchased. You can import these licenses during installation. This process ensures that each time you install any AppManager component, your license information automatically appears in the License Manager. For more information, see [“Importing License Keys from a File” on page 193](#).

To select or enter a license key during AppManager repository installation:

- 1 Make sure you have followed Steps 1–9 in [“Running the AppManager Setup Program” on page 70](#).
- 2 In the License Manager dialog box, add the license keys you have purchased, or accept the default evaluation key, and click **Next**

Note The following table describes the difference between the information you need to enter for different types of license.

Type of Installation	Steps to Take
A copy of AppManager that you purchased (permanent license)	Type the 15-digit license key number you received when you purchased AppManager. Use the format nnnnn- nnnnn- nnnnn- nnnnn, then click Add .
An evaluation copy of AppManager (time-limited license)	The default key is automatically registered. It allows you to use all AppManager components for a 30-day evaluation period from the date you install the repository component. Note Once you convert the evaluation copy to a licensed version of AppManager, you must update the license information.

Requesting a License Key

You can request permanent license keys using the License Manager.

To request a permanent license key for AppManager, provide the following information:

- Your company name and address
- The name, telephone number, and e-mail address of a contact person
- A list of the AppManager components for which you need license key information

Note To purchase AppManager components, contact an authorized NetIQ representative.

For more information, see [“Requesting License Information” on page 192](#).

Starting License Manager

The License Manager enables you to view, add, import, delete, or request AppManager licenses. You can open License Manager in one of the following ways:

- From the Operator Console or Security Manager, click **Help > License Manager** to view or add license information.
- From Control Center, you can only view license information. Click **Help > Manage Licenses**.
- On computers where the AppManager console, repository, or Web management server components have been installed, you can open AppManager License Manager from the Windows Desktop.

If the License Manager displays an expiration date for any component, you have installed that component using an evaluation license key. The component will not be accessible after the evaluation period expires until you update License Manager with the permanent license key for the component.

To start License Manager, log on to the AppManager repository with a SQL Server login account that has permission to access AppManager. For information about granting access to AppManager to SQL Server login accounts, see [“Understanding Security Manager” on page 159](#).

To start License Manager:

- 1** Click **Start > Programs > NetIQ > AppManager > Tools & Utilities > License Manager**.
- 2** In the License Manager dialog box, type the name of the **Server** and select the **Repository**.

If you are using SQL Server authentication, type the SQL Server **Login name** and **Password** to connect to the repository.

- 3** Click **Logon**.

Updating an Expired License

If you have installed an evaluation copy of AppManager, you should note the expiration date. After the expiration date, none of the console programs will run.

Note The expiration date of the Operator Web Console license might be different from that of the Operator Console or Control Center license. All Console programs are authorized with a single license.

If the AppManager evaluation period has expired, the next time you log into the Operator Console you are prompted to update your license. Click **Update license**, and type a new permanent license key number.

Adding and Deleting a License Key

When you convert from an evaluation copy or purchase additional AppManager components, you need to update the AppManager license information.

You do not need to re-install AppManager to add a new license key for a component that has already been installed. For example, if you purchase AppManager after the evaluation period, you only need to add the new permanent license key.

To add a new permanent license key:

- 1 Click **Start > Programs > NetIQ > AppManager > Tools & Utilities > License Manager**.
- 2 Type your 15-digit license key.
- 3 Click **Add** to add the component license key.
- 4 To add additional keys, repeat Step 2 and Step 3.
- 5 When you have finished adding license keys, click **Close**.

To delete a new permanent license key:

- 1 Select the license key by clicking on it.
- 2 Click **Delete**.
- 3 Click **Yes** to delete the license key.

Notes If you are updating license information for an AppManager Connector, you must also stop and restart the NetIQ AppManager Management Service (**NetIQms**) to enable the Connector.

For more information about AppManager Connectors, see the relevant Connector documentation, available in the AppManager Connectors installation kit.

Requesting License Information

You can request licenses by calling the NetIQ toll-free number or by sending an e-mail request. For more information, see [“Contacting NetIQ Corporation” on page xviii](#).

To request licenses by e-mail:

- 1 Click **Start > Programs > NetIQ > AppManager > Tools & Utilities > License Manager**.
- 2 Click **Request**.
- 3 In the Request Licenses dialog box, select **Send NetIQ licensing information from your repository** to include information about your current licenses with your request.
- 4 Type your contact information.

Field	Description
Your name	Your first and last name.
Your email address	The e-mail address to which licenses should be sent.

Field	Description
Your phone number	A telephone number where you can be reached in case there is a problem fulfilling your request.
SMTP computer name	The name of your SMTP server. Enter the hostname or the IP address for the server.

- 5 Click **Request Licenses**. The License Manager sends your request to NetIQ support. You will receive an e-mail response to your request.

Importing License Keys from a File

If you have more than one or two license keys, or if you need to update multiple license keys, you may want to import the information from a file rather than type the keys manually. When you purchase AppManager or request new licenses, you also receive a text file that contains all of the license keys.

To import the license keys from a text file:

- 1 Start the License Manager.
- 2 Click **Import**.
- 3 Locate the `license.txt` file you received from NetIQ.
- 4 Click **Open**. The license key information is imported and displayed in the License Manager.

Running a License Report

If you have installed and discovered at least one report-enabled agent, there are two reports that you can run to provide information about the number of AppManager components you have licensed and installed in your environment. These reports are available from the Master or Report view in the Operator Console when you click the **ReportAM** tab in the Knowledge Script pane:

- **CompLic** generates the AppManager Component License report.

- **CompDeploy** generates the AppManager Component Deployment report.

These report scripts collect information about the licensed components associated with a specific AppManager repository, such as the number of permanent and evaluation licenses deployed in your environment and which application management modules you have licensed and installed.

If the number of deployed components exceeds the number of licensed components, you are reminded to purchase additional licenses.

Note Evaluation copies of AppManager are included in the number of deployed components but are not reflected in the number of licensed components.

For more information about configuring and running reports, see the AppManager Help.

Performing a Silent Installation

This appendix explains the steps for installing AppManager components silently over a network from a command prompt.

The following topics are covered.

- [“Understanding Silent Installation” on page 195](#)
- [“Understanding Silent Installation on Windows Vista” on page 196](#)
- [“Repository Installation” on page 197](#)
- [“Sample Repository Installation File” on page 200](#)
- [“Management Server Installation” on page 200](#)
- [“Operator Console Programs Installation” on page 203](#)
- [“AppManager Agent Installation” on page 204](#)
- [“Module Installation” on page 210](#)
- [“Web Management Server Installation” on page 212](#)
- [“Control Center Installation” on page 213](#)
- [“Control Center Log File Options” on page 216](#)
- [“Silent Installation on UNIX” on page 217](#)
- [“Executing UNIX Agent Silent Installation” on page 217](#)
- [“Performing an Evaluation Installation Silently” on page 218](#)

Understanding Silent Installation

Performing a silent installation allows you to install an AppManager component without user intervention. From a command prompt,

you instruct the setup program associated with a selected AppManager or Control Center component to perform the installation. The command you enter can contain all of the installation options you have selected, or it can allow the installation to use the default options.

In past versions of AppManager, silent installations were performed using an initialization (.ini) file containing all your instructions. But because AppManager version 7.0 installation has been split into separate component installers, you must now perform silent installation as a separate step for each component you want to install.

In most cases, silent installation involves the invocation of a .MSI installer with parameters to specify a silent installation and to supply optional installation parameters. However, the AppManager repository and Control Center use a different type of installation package and require slightly different procedures.

Understanding Silent Installation on Windows Vista

If you want to silently install any AppManager component on Windows Vista, you must run the component as an Administrator. In addition, you must run the Windows Command Prompt itself as an Administrator. These restrictions are applicable even if you have logged on to your computer with Administrator privileges.

To silently install an AppManager component on Windows Vista:

- 1 On your Windows (Vista) Desktop, click **Start>Programs>Accessories**.
- 2 Right-click **Command Prompt**, and click **Run As Administrator** to open the Command Prompt as an Administrator.
- 3 Type the silent installation parameters for the AppManager component you want to install.

Repository Installation

Silent installation of the AppManager repository differs slightly from the procedure involved in installing other components.

Take the following steps to install a repository silently:

- 1** On the AppManager distribution computer (where you have saved the AppManager installation kit), change directories to the `\Setup\Setup Files` directory.
- 2** Find the configuration file named `qdbinstall.iss`. Copy it to a writeable directory on the computer where you want to install a repository.
- 3** In the directory where you have copied `qdbinstall.iss`, create a writeable response file named `silent.ini`.
- 4** Write the following line to the `silent.ini` file, and save it:
`NQ_INSTALLPATH=<Install Directory>`
- 5** Run the following installation command:
`"<Setup Files Directory>\NetIQ AppManager Repository Installation.exe" /s /f1"<full path to .iss file>" - silentinstall"<full path to .ini file>"`

This command installs the repository with the default settings. At minimum, you would need to supply values for the parameters shown in brackets `< >`. To supply your own responses to the options

that are described in [“Installing the Repository” on page 81](#), add the following parameters to your `silent.ini` response file:

Parameter	Description and Values
RP_CLUSTER_INSTALL	1 or 0. 1 = Installation is on a clustered server. 0 = Installation is on a non-clustered server.
RP_WINDOWSAUTH	1 or 0. 1 = Use your current Windows account and password to log in to SQL Server. For more information about this account, see “Installing the AppManager Repository” on page 83 . 0 = Use SQL Server authentication. See the following parameter.
RP_SQLUSER	The username associated with a user account for this SQL Server. For more information about this account, see “Installing the AppManager Repository” on page 83 .
RP_SQLPWD	Password for the SQL Server user account specified above.
RP_SQLSERVER	Name of the SQL Server computer and instance (if any) where repository should be installed.
RP_NETIQPWD	Password for the “netiq” user account. For more information, see “Installing the AppManager Repository” on page 83 .
RP_NAME	Name of the new repository. Default is “qdb”.
RP_DATANAME	Name for the repository data file. Default name is <i>DBNameData</i> .
RP_DATASIZE	Initial size of the data file. Default is 100 MB.
RP_DATAPATH	Data device path: the location of the folder where AppManager database data is stored. Default is <code>C:\Program Files\Microsoft SQL Server\MSSQL\Data</code> . Note If you specify a non-default path, the installer still installs the data file in the default path. If you want to use non-default data installation folders, you must configure SQL Server after installation.
RP_LOGNAME	Name of the repository log file. Default is <i>DBNameLog</i> .

Parameter	Description and Values
RP_LOGSIZE	Initial size of the repository log file. Default is 50 MB.
RP_LOGPATH	<p>Location of the folder where the repository database log is stored. Default is c:\Program Files\Microsoft SQL Server\MSSQL\LOG.</p> <p>Note If you specify a non-default path, the installer still installs the log file in the default path. If you want to use non-default log installation folders, you must configure SQL Server after installation.</p>
RP_ENC_CONFIG	<p>Whether to configure security options for Windows and/or UNIX agents. Use 1, 2, or 3, where:</p> <p>1 = Windows agents only 2 = UNIX agents only 3 = Windows and UNIX agents</p> <p>For more information, see “Installing the AppManager Repository” on page 83.</p>
RP_ENC_LEVEL	<p>Whether to configure a security level for agent-to-management server communications. Use 1, 2, or 3, where:</p> <p>1 = no security (use clear text) 2 = encrypt communications 3 = encrypt and authenticate communications</p> <p>For more information, see “Installing the AppManager Repository” on page 83.</p>
RP_SSLWINUNIX_PWD_QDB	Password for the encryption key stored in the repository.
RP_SSLWINUNIX_IMPORTKEY	<p>1 or 0. Whether to export agent encryption key information to a file.</p> <p>1 = Export key to a file. 0 = Do not export key to a file.</p> <p>Note: This setting does not apply to UNIX agents.</p>
RP_SSLWINUNIX_KEYPATH	Path and filename where the key should be exported. Default is c:\Program Files\NetIQ\AppManager\nqwindowsPublic0.key.

Parameter	Description and Values
RP_SSLWINUNIX_PWD_AGENT	Password for the agent to access its portion of the repository encryption key.
RP_UPGRADE_OPTION	TRUE or FALSE. Whether to upgrade an existing AppManager repository. TRUE = Upgrade and preserve management data. FALSE = Discard management data and overwrite or replace existing repository. Do not include this parameter if no repository is currently installed on the computer.

Sample Repository Installation File

The silent installation response file `silent.ini` contains the instructions for installing the AppManager repository on the local computer. The following sample response file illustrates what the file might look like after you have edited it to include your responses:

```
RP_CLUSTER_INSTALL=False
RP_WINDOWSAUTH=True
RP_SQLServerName=NYC_Ralphie\Instance01
RP_NetiqPassword=@9PX>(Pf35A92$d<c0Pd&!D(b515
RP_QDBName=QDB
RP_DataName=QDBData
RP_DataSize=400
RP_DataPath=C:\Program Files\Microsoft SQL Server\MSSQL\Data
RP_LogName=QDBLog
RP_LogSize=100
RP_LogPath=C:\Program Files\Microsoft SQL Server\MSSQL\Data
RP_SSLWINUNIX_Config=3
RP_SSLWINUNIX_Encrypt_Level=3
RP_SSLWIN_Pwd_QDB=@&E)@bRf35A92$d<c0Pd&!D(b5151$504
RP_SSLWIN_Key_Path=C:\Program Files\NetIQ\AppManager
RP_SSLWIN_Pwd_MC=@bb9X(4YC5A92$d<c0Pd&!D(b5151$5044!
```

Management Server Installation

Unlike the repository installation, management server installation invokes an `.msi` installer, with filename `NetIQ AppManager management server.msi`. This file is located in the `\Setup\Setup Files` directory of the AppManager installation kit.

To install the AppManager management server silently on the local computer, run the following command in that directory:

```
msiexec.exe /i "<Setup Files Directory>\NetIQ AppManager  
management server.msi" /qn INSTALLDIR="<Install Directory>"  
MS_NETIQPWD="<netiq pwd>" MS_B_WINUSER=1  
MS_WINDOMAINUSER="<domain\user info>" MS_WINPWD="<user pwd>"
```

This command installs a management server silently, using default settings. At minimum, you need to supply values for the parameters shown in brackets (< >).

You can supply values for additional parameters on the command line. These parameters are all described in detail in [“Installing the Management Server” on page 91](#). The following table summarizes the relevant parameters for silent installation of an AppManager management server:

Parameter	Description and Values
/i	Install.
/qn	Run silently.
INSTALLDIR	Directory where the management server should be installed. Default is C:\Program Files\NetIQ.
MS_DSN	Data Source Name for connecting to the repository. If you do not include this entry, the default (NetIQms) is used.
MS_RPNAME	Name of the AppManager repository. Default is “QDB”.
MS_RPSERVERNAME	Name of the AppManager repository server.
MS_NETIQPWD	Password for the netiq database user.
MS_WINDOMAINUSER	Specifies that the management server should run using a Windows domain user account.
MS_WINDOMAIN	Domain for the service account under which the management server will run.
MS_WINUSER	Username associated with the service account.
MS_WINPWD	Password associated with the service account.

Parameter	Description and Values
MS_UPGRADE	Whether to upgrade the existing management server registry keys. Do not include this parameter unless you are upgrading an existing management server.
MS_PORT	RPC port number where management server listens for communications from agents. Default is 9998.
MC_PORT	The RPC port number where managed clients listen for communications from management server. Default is 9999.
MS_PORTUNIX	Enables UNIX agent support and specifies the port number for the management server to listen on for communication from UNIX agents. Default is 9001.
MS_B_INSTALL	Whether the management server is being installed. 1 = Management server is an upgrade and not default. 0 = The default is being used.
MS_B_UPGRADE	Whether the management server installation is new install or upgrade. 1 = Upgrade of an already installed management server. 0 = A new installation of the management server.
MS_RPUSER	Name of the AppManager repository user. The default is netiq.
MS_NETIQPWDE	Encrypted password for the netiq database user.
MS_PORTUNIX	Enables UNIX agent support and specifies the port number for the management server to communicate with UNIX agents. The default is 9001. To change the MS_PORTUNIX parameter, a value of 1 must be specified for the MS_B_PORTUNIX parameter.
MS_B_PORTUNIX	Whether to change the default port number for the management server to communicate with UNIX agents. 1 = Value of 1 indicates a change in the port number. 0 = Default port number.
MS_B_WINUSER	Whether the management server should run using the Windows domain user service account. 1 = Using a Windows user account. 0 = Using the Windows Local System account.

Parameter	Description and Values
MS_B_WINUSER_VALID	Whether windows user is validated. 1 = Using Windows user account. 0 = Using Windows Local System account.
MS_WINPWDE	Encrypted password associated with the Windows service account under which the management server services will run.
MS_B_ISCLUSTER	Whether machine has a cluster environment. 1 = Machine has cluster environment. 0 = Machine does not have cluster environment.
MS_B_CLUSTER	Whether the management server installation is on a clustered server - shared or local drive. 1 = Management server is installed in the shared drive of cluster server nodes. 0 = Management server is installed in the local drive of cluster server.
MS_SHAREDDISK	The drive shared by the two nodes of cluster in a clustered server. Only one node can use this shared drive at a time. Management server might be installed in a shared drive or local drive.

Operator Console Programs Installation

Installation of the Operator Console and associated user interface programs invokes an .msi installer, with filename **NetIQ AppManager Console Installation.msi**. This file is located in the \Setup\Setup Files directory of the AppManager installation kit.

To install the AppManager console programs silently on the local computer, run the following command in that directory:

```
msiexec.exe /i "<Setup Files Directory>\NetIQ AppManager  
Console Installation.msi" /qn INSTALLDIR="<Install  
Directory>"
```

This command installs the AppManager Operator Console using default settings. At minimum, you need to supply values for the parameters shown in brackets (< >).

You can supply values for additional parameters on the command line. Console installation is described in detail in [“Installing the Operator Console Programs” on page 95](#). The following table summarizes the relevant parameters for silent installation of AppManager console programs, such as the Operator Console and Security Manager. (Control Center is not included. For more information about installing Control Center components silently, see [“Control Center Installation” on page 213](#).)

Parameter	Description
UI_SDK	The SDK files and help files. If the value is 1, all the files in this group will be installed.
UI_WIN32	The Win32 files and shared files group. If the value is 1, all the files in this group will be installed.
UI_SECMGR	The Security Manager file group. If the value is 1, all the files in this group will be installed.
INSTALLDIR	The install location of the Operator Console. If you want to install Operator Console to a different location, You can give a different directory location.
USERNAME	The user name specified for the install to use while registering the product.
COMPANYNAME	The company name specified for the install to use while registering the product.

AppManager Agent Installation

Once you configure the agent remotely using Control Center, the deployment service internally invokes an `.msi` installer, with filename `NetIQ AppManager agent.msi`. This Windows installer uses the parameters in the silent configuration file to install the Windows Agent. This file is located in the `\Setup\Setup Files` directory of the AppManager installation kit.

For information about silent installation of the UNIX agent, see the *AppManager for UNIX Management Guide*, included in the \Documentation folder of the AppManager UNIX Components installation kit.

To install an AppManager agent silently on the local computer, run the following command in the Setup Files directory:

```
msiexec.exe /i "<Setup Files Directory>\NetIQ AppManager  
agent.msi" /qn INSTALLDIR="<Install Directory>"  
MC_B_REPORTAGENT=1 MC_B_WINUSER=1  
MC_WINDOMAINUSER="<domain\user info>" MC_WINPWD="<user pwd>"
```

This command installs the AppManager agent services (NetIQmc and NetIQccm) and the local agent repository using default settings. At minimum, you need to supply values for the parameters shown in brackets (< >).

You can supply values for additional parameters on the command line. Options for installing agents on Windows are described in detail in [“Installing Agents” on page 99](#). The following table summarizes the relevant parameters for silent installation of the AppManager agent on Windows:

Option	Description
/i	Install.
/qn	Run silently.
INSTALLDIR	Directory where the agent should be installed. Default is C:\Program Files\NetIQ.
MCUPGRADE	Upgrades an existing local repository, preserving any existing data. Supply one of the following values: <ul style="list-style-type: none">• 1 = Upgrade the local agent repository and preserve data.• 0 = Overwrite the local agent repository; do not preserve data.
MC_B_REPORT_AGENT	Whether to install the reporting capability for the agent. Supply one of the following values: <ul style="list-style-type: none">• 1 = Install the agent with reporting capability.• 0 = Do not install the reporting capability.

Option	Description
MC_AUTODISCOVERY	<p>Whether to attempt to perform automatic agent discovery. Supply one of the following values:</p> <ul style="list-style-type: none"> • 0 = You plan to discover the agent later, using a Discovery Knowledge Script. • 1 = Agent should be discovered during installation.
MC_MSPRISEC	<p>Whether to set the primary and, optionally, the secondary management server during installation. Supply one of the following values:</p> <ul style="list-style-type: none"> • 0 = You plan to set the primary and secondary management server later, using the SetPrimaryMS Knowledge Script. Or you want to leave an existing setting (upgrade only). • 1 = You want to set the primary and, optionally, the secondary management server during installation. <p>Note NetIQ Corporation recommends setting at least a primary management server during installation.</p>
MC_MSPRIMARY	Name of the primary management server.
MC_MSSECONDARY	Name of the secondary management server.
MC_B_MSPRISEC_REMOVEALLOWMSSTAR	<p>Whether to remove the authorization for all management servers to communicate with the computer during installation. The AllowMS registry key stores the list of management servers that are allowed to communicate with a managed client. The key uses an asterisk (*) to allow all management servers to communicate with a managed client when no primary management server is designated.</p> <p>If you are setting the primary management server during installation or upgrade, the MC_B_MSPRISEC_REMOVEALLOWMSSTAR parameter removes the asterisk from the AllowMS registry key.</p> <p>If you are not setting the primary management server during the installation or upgrade, this parameter indicates that the AllowMS registry key should be left unchanged until you run the SetPrimaryMS Knowledge Script.</p>
MC_B_PROXY	<p>Whether to install the agent as a proxy. Supply one of the following values:</p> <ul style="list-style-type: none"> • 1 = Install as proxy agent. • 0 = Do not install as proxy agent.

Option	Description
MC_B_WINUSER	Whether the agent should run using a Windows domain user account. Supply one of the following values: <ul style="list-style-type: none"> • 1 = Use a Windows user account. • 0 = Use the Windows Local System account.
MC_WINDOMAINUSER	Domain and username for the service account under which the agent services will run. Use the format domain\username.
MC_WINPWD	Password for the service account under which the agent services will run.
MC_MAPI	Enables the MAPI mail option. For more information, see “Understanding MAPI Mail Settings” on page 105 .
MC_MAILBOX	Name of the mailbox to enable MAPI mail as an action.
MC_PROFILE	Name of the Exchange profile to enable MAPI mail as an action.
MC_EXCHSVR	Name of the Exchange Server to enable MAPI mail as an action.
MC_B_PORT	Whether to change the default RPC ports where the management server and agents listen for communications from each other. Supply one of the following values: <ul style="list-style-type: none"> 1 = I will change the ports 0 = Use the default ports. Defaults are: <ul style="list-style-type: none"> • 9999 (management server listens for agent communications) • 9998 (agents listen for management server communications)
MS_PORT	RPC port number where the management server listens for agent communications. A value of 1 must be specified for MC_B_PORT, above.
MC_PORT	RPC port number where the agent listens for management server communications. A value of 1 must be specified for MC_B_PORT, above.

Option	Description
MC_SECLEVEL	Specifies the security level to use. The valid values are: <ul style="list-style-type: none"> • 0 = No security (clear text) • 1 = Encryption only • 2 = Management server authentication and encryption
MC_SECPWD	If using encryption or authentication and encryption security, this option specifies the password for the agent key file. A value of 1 or 2 must be specified for MC_SEVLEVEL, above.
MC_B_AUTODISCOVERY	Whether to attempt automatic agent discovery. 1 = Agent will be discovered during installation. 0 = Agent will be discovered later by using a Discovery Knowledge Script.
MC_B_DISPLAYNAME	Whether to change agent computer display name. 1 = Change display name of the computer on which the agent is being installed. 0 = Use the default tree view name of the computer on which the agent is being installed.
MC_B_MAPI	If enabled the agent can send e-mail automatically, using the MAPI protocol, as part of a Knowledge Script job. 1 = MAPI mail option enabled. 0 = MAPI mail option not enabled.
MC_B_MSPRIMARY_EXIST	Whether primary MS is available. 1 = Primary Management Server is available. 0 = Primary Management Server is not available.
MC_B_MSSECONDARY_EXIST	Whether secondary MS is available. 1 = Secondary management server is available. 0 = Secondary management server is not available.
MC_B_MSPRISEC	Whether the management server has passed the primary/secondary check. 1 = Primary/secondary check passed. 0 = Primary/secondary check failed.

Option	Description
MC_B_MSPRISEC_REMOVESERVER	Whether to allow the anonymous management server to exchange report with the agent. 1 = Do not allow the anonymous management server to exchange report with the agent. 0 = Allow the anonymous management server to exchange report with agent.
MC_B_REPORTAGENT	Whether to enable reporting capabilities of the agent. 1 = Reporting capabilities for the agent enabled. 0 = Reporting capabilities for the agent not enabled.
MC_B_UPGRADE	Whether agent is being upgraded. 1 = Agent is being upgraded. 0 = Agent is being installed.
MC_B_ONMS	Whether the management server is present on the machine where the agent is being installed. 1 = The management server is present on the machine where the agent is being installed. 0 = The management server is not present on the machine where the agent is being installed.
MC_ALLOWMS	There are two scenarios for this parameter. 1 Manual/AMSetup Installation where the value depends on the MC_B_MSPRISEC parameter: <ul style="list-style-type: none"> • MC_ALLOWMS = *; Allow anonymous management server • MC_ALLOWMS = Primary management server, Secondary management server; Allow only Primary management server/Secondary management server to communicate. 2 Remote installation, which has four cases: <ul style="list-style-type: none"> • MC_ALLOWMS = *; Allow anonymous management server • MC_ALLOWMS = ; Do not allow anonymous management server • MC_ALLOWMS = *; Allow anonymous management server until primary/secondary for this agent is set • MC_ALLOWMS = ; Never allow anonymous management server

Option	Description
MC_DISPLAYNAME	Tree view name of computer on which the agent is being installed.
MC_MDBPATH	Default local repository path - location of local MDB folder.
MC_MSPRIMARY	Name of primary management server.
MC_MSSECONDARY	Name of secondary management server.
MC_SECPWDE	If using authentication or encryption security, this option specifies the encrypted password for the agent key file. A value of 1 or 2 must be specified in the MC_SECLEVEL parameter.
MC_WINUSER	Username associated with the service account.
MC_WINDOMAIN	Domain for the service account number under which the agent will run.
MC_WINPWDE	Encrypted password associated with the Windows service account under which the management server services will run.
MC_INPUTXML	XML input file for remote installation
MC_B_WEBSERVER	Whether to specify web server name to be used by the agent. 1 = Specify web server name to be used by the agent. 0 = Use default, which is domain name.
MC_WEBSERVER	Deployment web server name to be used by the agent. A TRUE value must be specified for MC_B_WEBSERVER to change this parameter.
MC_B_PRE60UPGRADE	Whether install is an upgrade from pre-6.0. 1 = Upgrade of AppManager from pre-6.0. 0 = New install.
MC_B_60TO65UPGRADE	Whether install is upgrade from 6.0 to 6.5. 1 = Upgrade of AppManager from 6.0 to 6.5. 0 = New install.

Module Installation

Once you configure the AppManager modules remotely using Control Center, the deployment service internally invokes an `.msi`

installer, with a filename conforming to the following convention: **AM70-[knowledgeScriptCategoryName]-7.0.xx.x.msi**. This Windows installer uses the parameters in the silent configuration file to install the module.

The relevant file is located in the **\Setup\Setup Files** directory of the AppManager installation kit.

To install a module silently on the local computer, run the following command in the **Setup Files** directory:

```
msiexec.exe /i "AM70-<ModuleName>-7.0.msi" /qn  
MO_CONFIGOUTINI=<CONFIG WIZARD OUTPUT XML  
FILE>
```

This command installs the selected module using default settings. At minimum, you need to supply values for the items shown in brackets (< >).

A few modules require extra configuration. For example, the setup program for the AppManager for Microsoft SQL Server module asks you for a SQL Server or Windows user account and password to access the SQL Server. The following table provides a summary of the flags you will need to supply for the modules that require extra information:

Keyword or Parameter	Description
MO_CommunityString= <i>public</i>	Community string for monitoring hardware (for example, CIM, Dell, Siemens, IBM Director, or Cisco devices).
MO_CONFIGOUTINI	For the Microsoft Exchange module, enables AppManager to automatically create the required Exchange mailbox.
MO_STARTEXCH	Enables AppManager to automatically start the Exchange Directory service.
MO_NOTES_CONFIG	Enables AppManager to configure parameters for monitoring Lotus Domino (Notes) automatically.

Keyword or Parameter	Description
<code>MO_Oracle_User=<i>user</i></code>	Username for discovering Oracle databases. This authentication information is used to connect to an Oracle instance. One username and password will be used for all instances. Thus, this user account should be known by all Oracle databases on the computer.
<code>MO_Oracle_Password=<i>password</i></code>	Password for discovering Oracle databases.
<code>MO_SQL_USER=<i>user</i></code>	SQL Server login for monitoring SQL Server. This flag also specifies the type of authentication to use for connecting to a SQL Server instance. If it is not included, AppManager uses Windows authentication for SQL Server monitoring. Note If you select SQL authentication, the username and password you supply are used for all instances.
<code>MO_SQL_Password=<i>password</i></code>	Password for the SQL Server user to use for monitoring Microsoft SQL Server.

Web Management Server Installation

Installation of the AppManager Web management server invokes an `.msi` installer, with filename `NetIQ AppManager web Installation.msi`. This file is located in the `\Setup\Setup Files` directory of the AppManager installation kit.

To install a Web management server silently on the local computer, run the following command in the `Setup Files` directory:

```
msiexec.exe /i "<Setup Files Directory>\NetIQ AppManager web
Installation.msi" /qn INSTALLDIR="<Install Directory>"
```

This command installs the AppManager Web management server using default settings. You need to supply values for the parameters shown in brackets (< >).

The Web management server is described in more detail in [“Installing the Web Management Server” on page 129](#). The following

table summarizes the relevant parameters for silent installation of the AppManager Web management server.

Parameter	Description
/i	Install.
/qn	Run silently.
INSTALLDIR	Directory where the Web management server components should be installed. Default is c:\Program Files\NetIQ\AppManager.

Control Center Installation

Installation of NetIQ Control Center invokes an InstallShield executable file, with filename **NetIQCCSetup.exe**. This file is located in the **\Setup\Setup Files** directory of the AppManager installation kit.

To install Control Center silently on the local computer, run the following command in the **Setup Files** directory:

```
"NetIQCCSetup.exe" /s /v"/L<Log file options>  
CC_AD_SERVICE=1 CC_AD_WEBSERVICE=1 CC_CCDB=1 CC_CQS=1  
CC_CONSOLE=1  
CCDB_SQLSERVERINSTANCE=<serverName\instanceName>  
CCDB_WINSECMODE=1 CCDB_SQLUSER=netiq CCDB_SQLUSERPWD=pwd  
INSTALL_MO_HELP=FALSE CHECKIN_AD_PACKAGES_NOW=1  
CQS_DOMAIN=<windowsDomain> CQS_USER=<UserName> CQS_PWD=pwd
```

Note You must mention the full path of **NetIQCCSetup.exe** in the command.

This command installs the Control Center repository, Command Queue Service, console, and both Deployment services using default settings. You can disable some components for installation using the parameters shown above. At minimum, you need to supply values for the parameters shown in brackets (< >).

Notes The Control Center Command Queue Service installation fails in silent install when the repository name (CC_CCDB=1) is entered incorrectly.

The Control Center User Interface silent installation fails if you use a space in the INSTALLDIR parameter, and no information is added in the log file.

You can supply values for additional parameters on the command line. Options for installing Control Center components are described in detail in [“Installing Control Center” on page 135](#). The following table summarizes the relevant parameters for silent installation of Control Center components:

Parameter	Description
/s	Run in silent mode.
/v	Include Microsoft installer command-line options.
/L	Specify a path to the log file.
<Log file options>	Options for specifying what information is included in the installation log file. For more information, see the table of log file options below.
INSTALLDIR	Directory where the components should be installed. Default is C:\Program Files\NetIQ.
CC_AD_SERVICE	Whether to install the Control Center Deployment Service, used to enable deploying agents and modules remotely. Supply one of the following values: <ul style="list-style-type: none">• 1 = Install the Deployment Service.• 0 = Do not install the Deployment Service.
CC_AD_WEBSERVICE	Whether to install the Control Center Deployment Web Service, used to enable deploying agents and modules remotely. Supply one of the following values: <ul style="list-style-type: none">• 1 = Install the Deployment Web Service.• 0 = Do not install the Deployment Web Service.
CC_CCDB	Whether to install the Control Center repository. Supply one of the following values: <ul style="list-style-type: none">• 1 = Install the Control Center repository.• 0 = Do not install the Control Center repository.

Parameter	Description
CC_CQS	Whether to install the Control Center Command Queue Service. Supply one of the following values: <ul style="list-style-type: none"> • 1 = Install the Command Queue Service. • 0 = Do not install the Command Queue Service.
CC_CONSOLE	Whether to install the Control Center console program. Supply one of the following values: <ul style="list-style-type: none"> • 1 = Install the Control Center console. • 0 = Do not install the Control Center console.
CCDB_SQLSERVERINSTANCE	Name of SQL Server computer and instance (if any) where Control Center repository should be installed. Use the format <code>serverName\instanceName</code> .
CCDB_WINSECMODE=1	Whether to use the Windows user account you are currently logged in as to create the Control Center repository. Supply one of the following values: <ul style="list-style-type: none"> • 1 = Use the Windows user account of the user who is currently logged in to the computer. • 0 = Use a SQL Server account (with SQL authentication).
CCDB_SQLUSER	The username of the login account used to create a database in SQL Server. Default is <code>netiq</code> . For more information, see “SQL Server Security” on page 152 .
CCDB_SQLUSERPWD	The password associated with the login account used to create a database in SQL Server.
INSTALL_MO_HELP=FALSE	Whether to install the AppManager Help files. These files provide Help for the Operator Console and Knowledge Scripts. <p>Supply one of the following values:</p> <ul style="list-style-type: none"> • 1 = Install the Help files. • 0 = Do not install the Help files. <p>Note This setting does not affect Control Center-specific Help files, which are always installed along with the Control Center console.</p>
CHECKIN_AD_PACKAGES_NOW	Whether to check in module and agent packages for deploying remotely. For more information, see “Creating the Web Depot” on page 146 . <p>Supply one of the following values:</p> <ul style="list-style-type: none"> • 1 = Check in packages. • 0 = Do not check in packages. <p>Default is 1.</p>

Parameter	Description
CQS_DOMAIN	Windows domain where the Command Queue Service should run. For more information, see “Understanding the Command Queue Service Options” on page 137 .
CQS_USER	Username associated with the Windows user account under which the Command Queue Service should run. For more information about this account, see “Understanding the Command Queue Service Options” on page 137 .
CQS_PWD	Password associated with the Windows user account under which the Command Queue Service should run.

Control Center Log File Options

For the <Log file options> shown in the command-line example above, you can pass in other flags to control logging. The /L flag allows you to specify a path to the log file.

Here is an example of the syntax:

```
NetIQCCSetup.exe" /s /v"/Liwear \"C:\Program Files\NetIQ\Temp\NetIQ_Debug\AM-INSTALL-DEV\nqCC_MSI.log\""
```

The following flags can be used to control logging:

Flag	Description
i	Logs status messages
w	Logs non-fatal warning messages
e	Logs any error messages
a	Logs the commencement of action sequences
r	Logs action-specific records
u	Logs user requests
c	Logs initial user interface parameters
m	Logs out-of-memory messages
p	Logs terminal settings

Flag	Description
v	Logs the verbose output setting
+	Appends data to an existing file
*	Wildcard character; allows you to log all information (excluding the verbose output setting)

Silent Installation on UNIX

Performing a silent installation allows you to install AppManager UNIX agents and modules without interactively running the installation script. The silent installation option is particularly useful for UNIX components because deploying agents remotely is not possible for UNIX.

Like the silent installation of other AppManager components, the silent installation of the UNIX agent and UNIX modules uses an installation file that records the information required for completing the installation. Each line in the file is a *name=value* pair that provides the required information—for example, `HOME=/opt/netiq`.

You may want to manually create a silent installation file to install the UNIX agent, but a file you can use for this purpose is automatically created for you as soon as you complete UNIX agent installation. Look for it in the following directory: `$nqmagt_home/log/silentinstall.ini`.

The *AppManager for UNIX Management Guide*, which is included in the AppManager UNIX Components installation kit, contains a complete set of instructions for creating and running a silent installation file for the UNIX agent and UNIX application management modules.

Executing UNIX Agent Silent Installation

Once you have created the installation file, you can execute the silent installation either from the command line or in a script by using the

command-line option `-s` and the installation file name. For example:

```
./netiq_agent_install -s Sample_SilentInstall.ini.
```

Note The installation filename must be specified as an absolute path.

The script will then extract information from the installation file and install the agent according to the values you have specified.

Performing an Evaluation Installation Silently

When AppManager runs in Evaluation mode, it uses default settings for all components. The following commands let you install AppManager and Control Center components silently, using default settings.

Repository Database:

```
"NetIQ AppManager Repository Installation.exe" /s /
f1"qdbinstall.iss" -silentinstall"silent.ini"
```

The `silent.ini` file must contain the following line:

```
NQ_INSTALLPATH=[install path]
```

Management Server:

```
msiexec /i "NetIQ AppManager management server.msi" /
qn"INSTALLDIR=[install path] MS_NETIQPWDE=netiq
MS_B_WINUSER=1 MS_WINDOMAINUSER=[domain_name\user_name]
MS_WINPWDE=[password]"
```

Agent (Windows):

```
msiexec /i "NetIQ AppManager agent.msi" /
qn"INSTALLDIR=[install path] MC_B_REPORTAGENT=1
MC_B_WINUSER=1 MC_WINDOMAINUSER=[domain_name\user_name]
MC_WINPWDE=[password]"
```

Modules:

```
msiexec /i [module msi file] /qn"MO_B_MOINSTALL=1
MO_B_CCDBINSTALL=0 MO_B_CCUIINSTALL=0 MO_B_MSINSTALL=0
MO_B_QDBINSTALL=0 MO_B_UIINSTALL=1
AM_B_CALLED_FRM_AMSETUP=1"
```

Operator Console:

```
msiexec /i "NetIQ AppManager Console Installation.msi" /qn  
INSTALLDIR=[install path]
```

Control Center and Deployment Service:

```
NetIQCCSetup.exe /s /v\"/Liwear nqCC_MSI.log  
CC_AD_WEBSERVICEPROXY=0 CC_CCDB=1 CC_CQS=1 CC_CONSOLE=1  
CCDB_SQLSERVERINSTANCE=[local computer name]  
CCDB_WINSECMODE=1 CCDB_SQLUSER=netiq CCDB_SQLUSERPWD=netiq  
INSTALL_MO_HELP=FALSE CQS_DOMAIN=[domain name]  
CQS_USER=[username] CQS_PWD=[user password]"
```


Uninstalling AppManager

This appendix explains your options for uninstalling AppManager.

The following topics are covered:

- [“Understanding AppManager Uninstallation” on page 221](#)
- [“Understanding the Uninstallation Sequence” on page 222](#)
- [“Uninstalling AppManager” on page 223](#)
- [“Uninstalling AppManager from a Remote Computer” on page 224](#)
- [“Uninstalling the Control Center Console” on page 225](#)
- [“Uninstalling Agents and Modules Remotely” on page 225](#)

Understanding AppManager Uninstallation

With AppManager version 7.0 and later, you can select individual components to uninstall. For example, if a computer has the management server, AppManager repository, and Operator Console installed, you can uninstall just the management server.

Notes Do not to uninstall a repository containing data that you still need. Uninstalling AppManager permanently deletes the repository, including all stored data and jobs. However, you can *upgrade* the repository and retain management data.

When you uninstall the agent, all modules are uninstalled along with it. However, the software inventory information of the agent is maintained.

Starting with AppManager version 7.0, you can also remotely uninstall agents and modules. For more information, see [“Uninstalling AppManager from a Remote Computer” on page 224](#).

Typically, AppManager components are installed on various computers in your environment. When AppManager components reside on multiple computers, before running the uninstallation program, you need to manually:

- Stop the NetIQ AppManager Management Service (**NetIQms**).
- Disconnect any users and applications that are accessing the AppManager repository.

Understanding the Uninstallation Sequence

NetIQ Corporation recommends uninstalling AppManager in the following order:

1 AppManager modules.

The order in which you uninstall individual modules is not significant. NetIQ Corporation recommends that you use Control Center to remotely uninstall modules.

2 Web management server

3 Operator Console or Operator Web Console

4 Management server

5 AppManager agent or UNIX agent

6 All Control Center components

7 AppManager repository (all instances)

Note During the uninstallation of Control Center, SQL Server services are stopped on the target machine. This may cause some other data links to fail if they are connected to the Control Center Repository.

Before you start to uninstall the AppManager repository, you must first stop any services that make connections to the repository. The WorldWide Web Publishing Service (**w3svc**), which is running on any computer where you have installed the Control Center Deployment Web Service, has a connection to the repository. This service must be stopped before you start the uninstallation. You can stop it in the Services Control Panel, or you can enter the following at a command prompt in the **WINDOWS\System32** directory:

```
net stop w3svc
```

To restart the service, use the command **net start w3svc**.

If you have installed the Deployment Web Service on the same computer as the Control Center repository, the **w3svc** service is stopped automatically as part of Control Center uninstallation.

Note If the setup program detects any open connections to the repository, it prompts you to close each of them before continuing with uninstallation.

Uninstalling AppManager

Use the Add/Remove Programs feature in the Windows Control Panel to uninstall AppManager.

You have several options for uninstalling AppManager components:

- You can uninstall **manually** from a local computer.
All AppManager and Control Center components must be uninstalled manually except agents and modules running on Windows.
- You can uninstall **remotely** across a network. For more information, see [“Uninstalling Agents and Modules Remotely” on page 225](#)
- You can run a Knowledge Script job to uninstall backlevel agents and modules (pre-AppManager version 7.0) from remote

computers. For more information, see [“Uninstalling AppManager from a Remote Computer” on page 224](#).

To uninstall AppManager manually:

- 1** From the Windows Desktop, click **Start > Settings > Control Panel**.
- 2** Open **Add/Remove Programs**.
- 3** Select **NetIQ AppManager** from the list of installed programs.
- 4** Click **Yes** in the confirmation message box.

Note The AppManager ResponseTime for Networks application management module installs a NetIQ endpoint that is a separate component. Uninstalling AppManager does not remove the endpoint. If you have installed AppManager ResponseTime for Networks and want to remove it, you need to uninstall the endpoint separately.

Uninstalling AppManager from a Remote Computer

Uninstalling AppManager from a remote computer involves the following aspects:

- Using Control Center for AppManager version 7.0 or later.
- For older components (older than AppManager version 7.0), run the AMAdmin_AppManagerUninstall Knowledge Script on the remote computer.

Uninstallation Knowledge Scripts only run on backlevel agents.

- For older components (older than AppManager version 7.0) on managed clients where you have enabled remote installation, run the AMAdmin_AppManagerUninstallProxy Knowledge Script.

Note Remote uninstallation is not yet available for UNIX components, or for any AppManager components other than agents and modules.

For more information about these Knowledge Scripts, see the AppManager Help.

Uninstalling Agents and Modules Remotely

Use Control Center to uninstall agents and modules on remote computers.

- 1 Using the Deployment Rule Wizard, create a deployment rule to uninstall the selected components.
- 2 While creating a deployment rule, select the **Uninstall all selected packages** check box in the Packages tab.
- 3 Set up a schedule for rule execution.
- 4 Approve the uninstallation task to begin the uninstallation.

Note If an outstanding deployment task to uninstall the agent is waiting for approval, you cannot create additional uninstallation tasks for modules. For more information, see the *Control Center User Guide for AppManager*.

Uninstalling the Control Center Console

The procedure to uninstall the Control Center Console slightly varies from other AppManager components.

To uninstall the Control Center Console:

- 1 From the Windows Desktop, click **Start > Settings > Control Panel**.
- 2 Open **Add/Remove Programs**.
- 3 Select **NetIQ AppManager Control Center** from the list of installed programs.
- 4 Click **Change/Remove**.

- 5 In the Welcome screen, select **Modify** and click **Next**.
- 6 In the Configuration Check screen, click **Next**.
- 7 In the Select Features screen, select all features except **Console** and click **Next**.
- 8 Click **Yes** in the message box.
- 9 In the Confirmation screen, click **Next** to begin uninstalling the Control Center Console.
- 10 Click **Finish** once the Control Center Console is uninstalled.

Uninstalling the UNIX Agent

If you need to uninstall the AppManager UNIX agent, run the `netiq_agent_uninstall` script. The `netiq_agent_uninstall` script is located in the `bin` directory under the home directory for the UNIX agent. For example, if you installed in the default location for Sun Solaris, you would find the `netiq_agent_uninstall` script in `/opt/netiq/UnixAgent/bin`.

To run the uninstall script, log in as `root`. Change to the UNIX agent `bin` directory, and then run the following command:

```
# ./netiq_agent_uninstall
```

Using SMS to Install AppManager Agents

This appendix describes the procedures to work with components over a network using Microsoft Systems Management Server (SMS) distribution functions. The procedures in this chapter apply only if you have installed Microsoft Systems Management Server (SMS) 2003 version 2.5 with Service Pack 2.

The following topic is covered:

- [“Working with Packages” on page 227](#)

Working with Packages

This section describes procedures to create packages (that SMS uses for distribution) and advertisements. This section also describes procedures to uninstall a component using SMS.

To create a package that SMS uses for distribution:

- 1 In the Systems Management Server (SMS) console, right-click **Packages**, and then select **New > Package**.
- 2 In the General tab, specify a name for the package (the name should not exceed 50 characters) and enter the following information:
 - Version number of the software package (the version number should not exceed 32 characters)
 - Name of the software publisher (the publisher’s name should not exceed 32 characters)
 - Language version (the version should not exceed 32 characters)

- Description of the package (the description should not exceed 127 characters)
- 3** In the Data Source tab, select **This Package Contains Source Files**.
 - 4** For Source Directory, select the type of connection for the source files, and then click **Apply**.
 - 5** In the Distribution Settings tab, select **High** from the Sending Priority menu, and click **OK**. The package is displayed under the **Packages** node of the Site Database tree in the SMS console.
 - 6** Expand the package under the **Packages** node, and then right-click **Distribution Points**.
 - 7** In the New Distribution Points Wizard dialog box, select the servers that you want to designate as the distribution points, and then click **Finish**.
 - 8** Under the **Packages** node, right-click **Programs**, and then select **New > Program**.
 - 9** In the Command Line panel of the Program Properties dialog box, click **Browse** to locate the install folder.
 - 10** To run the installer using the `msiexec` program, enter:


```
msiexec.exe /i "<full path to the .msi file>.msi" /qn
```

or

```
msiexec.exe /i "<full path to the .msi file>.msi" /qn  
<PARAMETERS>="<values>"
```

Note Use this option only if all the client computers have the MSI 2.0 (or later) engine installed. Ensure that you provide field details that contain up to 255 characters only.
 - 11** In the Environment tab, clear **User Input Required**, and click **Run with Administrative Rights**.
 - 12** Click **OK** to display the SMS package.

To create an advertisement:

- 1** On the Site Database tree, expand **Collections**, and then right-click the collection that receives the package.
- 2** Select **All Task > Distribute Software**. The Distribute Software wizard starts.
- 3** Click **Next**.
- 4** In the Package dialog box, select **Distribute an Existing Package**, and click **Next**.
- 5** In the Distribution Points dialog box, ensure that the distribution point is selected, and click **Next**.
- 6** In the **Select a Program to Advertise**, select a program, and click **Next**.
- 7** In the Advertisement Name dialog box, ensure that the correct package and collection names is displayed, and click **Next**.
- 8** In the Advertise To Subcollections dialog box, specify any subcollections that should receive the advertisement, and click **Next**.
- 9** In the Advertisement Schedule dialog box, confirm or change the time that the advertisement is offered.
- 10** Enter the advertisement expiration details.
- 11** In the Assign Program dialog box, click **Yes** to assign the program, and click **Next**.
- 12** In the Completing The Distribute Software Wizard dialog box, review the settings, and click **Finish**.

To uninstall a component using SMS:

- 1** Follow steps 1 through 9 in [Working with Packages](#) to create a package.

- 2** Follow steps 1 through 10 in [To create an advertisement:](#) to create an advertisement.
- 3** In the General tab of the Program Properties dialog box, type the following:

```
msiexec /x "<full path to the .msi file>.msi" /qn
```


Reviewing Microsoft DTC and Control Center Installation

AppManager Control Center uses the Microsoft Distributed Transaction Coordinator (DTC) to connect to every AppManager repository it manages. The Control Center repository database requires DTC to be running as a service on the computer where you install it.

If you install Control Center components on Windows Server 2003 with Service Pack 1, you will have to do some extra configuration to make sure Control Center can find and use the DTC service.

This appendix contains the following sections:

- [“Verifying DTC Connectivity before Installation” on page 231](#)
- [“Reconfiguring DTC in Microsoft Windows Server 2003 SP1 for a Non-Clustered System” on page 233](#)
- [“Reconfiguring DTC in Microsoft Windows Server 2003 SP1 for a Clustered System” on page 234](#)
- [“Reconfiguring MSDTC Through a Firewall” on page 236](#)
- [“Troubleshooting DTC Connectivity” on page 236](#)

Verifying DTC Connectivity before Installation

The Configuration Checker utility is an optional but recommended part of Control Center installation. It tests DTC connectivity between the Control Center database host and all of the hosts of the AppManager repositories managed by Control Center.

To check DTC connectivity:

1 On the computer that will host the Control Center repository database, click **Start > Programs > NetIQ > AppManager > AppManager Control Center Configuration Checker**.

2 Click **Run**.

Note If the **Run** button is disabled, you do not have the Microsoft .NET Framework, version 1.1 or later installed on your system. The Microsoft .NET Framework installer is located in the AppManager installation kit.

3 In the Database Servers dialog box:

- **Enter SQL server name\instance where CCDB is or will be:**
The SQL server (or an instance) will access the Control Center repository when it is installed.
- **Enter SQL server name\instance where QDB is or will be:**
The SQL server (or an instance) will access the AppManager repository when it is installed.

The Configuration Checker runs the **Preinstall** category of tests automatically to verify that DTC connectivity exists between the Control Center database and the AppManager repository.

4 In the Configuration Checker dialog box, click **Tasks > Server Setup** to reopen the **Database Servers** dialog box.

5 Each time Configuration Checker runs, it checks DTC connectivity to a single AppManager repository. Run it once for each repository you plan to manage with Control Center. Repeat Steps 3 through 5 for each repository.

In addition to DTC service status and version, the Configuration Checker utility also checks the validity of the SQL Server names you enter. For more information on DTC connectivity, see [“Troubleshooting DTC Connectivity” on page 236](#).

Reconfiguring DTC in Microsoft Windows Server 2003 SP1 for a Non-Clustered System

This section describes the procedure to reconfigure DTC for each Microsoft Windows Server 2003 SP1 system that hosts a component of Control Center.

- 1 Click **Start > Administrative Tools > Component Services**.
- 2 In the Component Services dialog box, expand **Component Services**, and then expand **Computers**.
- 3 Right-click **My Computer** and select **Properties**.
- 4 Click the MSDTC tab.

Note In a non-cluster environment, the **Take Ownership** button is not displayed.

- 5 Click **Security Configuration**. The Security Configuration dialog box is displayed.
- 6 Accept the defaults, but select the following:
 - **Allow Remote Clients**
 - **Allow Remote Administration**
 - **Allow Inbound**
 - **Allow Outbound**
- 7 Select **No Authentication Required**.
- 8 Click **OK**, and then click **Apply**.
- 9 Click **OK** in the My Computer Properties dialog box.
- 10 Restart the computer.

Reconfiguring DTC in Microsoft Windows Server 2003 SP1 for a Clustered System

If you use clustered servers for the Control Center database, you must run the following procedure on *each* node in the cluster.

In a cluster environment, the following additional information is available in the My Computer Properties dialog box:

- The **Take Ownership** button
- The **Security Configuration** button is disabled.

Case 1. Security Configuration button is enabled (not grayed out)

- 1 Click **Start > Administrative Tools > Component Services**.
- 2 In the Component Services dialog box, expand **Component Services**, and then expand **Computers**.
- 3 Right-click **My Computer** and select **Properties**.
- 4 Click the **MSDTC** tab.
- 5 Click the **Security Configuration** button.
- 6 Make sure the following options are selected:
 - **Allow Remote Clients**
 - **Allow Remote Administration**
 - **Allow Inbound**
 - **Allow Outbound**
- 7 Click the **No Authentication Required** button.
- 8 Click **OK** and then click **Apply**.
- 9 Click **OK** in the My Computer Properties dialog box.
- 10 Restart the computer.
- 11 Repeat Steps 1 through 9 for each node in the cluster.

Case 2. Security Configuration button is not enabled

When configuring a cluster node, the **Security Configuration** button may be disabled.

To enable the Security Configuration button:

- Click the **Take Ownership** button.
 - Click **OK** to close the My Computer Properties dialog box to enable the **Security Configuration** button.
- 1** Click **Start > Administrative Tools > Component Services**.
 - 2** In the Component Services dialog box, expand **Component Services** and then expand **Computers**.
 - 3** Right-click **My Computer** and select **Properties**.
 - 4** Select the **MSDTC** tab.
 - 5** Click the **Security Configuration** button.
 - 6** Make sure the following options are selected:
 - **Allow Remote Clients**
 - **Allow Remote Administration**
 - **Allow Inbound**
 - **Allow Outbound**
 - 7** Select **No Authentication Required**.
 - 8** Click **OK** and then click **Apply**.
 - 9** Click **OK** in the My Computer Properties dialog box.
 - 10** Restart the computer.
 - 11** Repeat Steps 1 through 9 for each node in the cluster.

Reconfiguring MSDTC Through a Firewall

If DTC communications must pass through a firewall, and you reconfigure DTC by following the procedures described in the previous sections, you have several options:

- Reconfigure DTC to work through the firewall. For more information, see the Microsoft Knowledge Base Article: <http://support.microsoft.com/kb/311846> (INFO: Description of names and IP addresses that an MSDTC client in a cluster environment must have). This will require opening some ports.
- If you do not want to open new ports in your firewall, you can disable the firewall.
- If you do not want to open new ports in your firewall, you can set up a VPN connection between the Control Center repository and AppManager repositories so that they can communicate with each other across the firewall. For more information, see the white paper on VPN connections located in the \Documentation folder of the AppManager installation kit.

Troubleshooting DTC Connectivity

DTC-related problems reported by Control Center users include the following.

- [Server Name Resolution Failure.](#)
- [DTC Fails To Communicate In Windows Server 2003.](#)
- [The SID Of One Of The DTCS Is Not Unique.](#)
- [SQL Server System Variable @@servername Is Incorrect Or Null.](#)
- [Double Hop Error With Kerberos Credentials](#)
- [Delay In Syncing Of Data From The Appmanager Repository To The Control Center Repository](#)

If the DTC problem you encountered does not resemble one of the types described above, you may want to perform a more thorough

diagnosis using the steps described in the following Microsoft Knowledge Base Articles:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;306843>
(HOWTO: Troubleshoot MS DTC Firewall Issues).

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;306212>
(HOWTO: Troubleshoot error 7391 that occurs when you use a linked server in SQL Server).

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;293799>
(HOWTO: Use DTC Tester Tool).

Server Name Resolution Failure

Symptom

Error number 7391. Look in the Control Center database SQL Agent job history for an error message like the following:

Executed as user: NETIQUUS\liul. The operation could not be performed because the OLE DB provider 'SQLOLEDB' was unable to begin a distributed transaction. [SQLSTATE 42000] (Error 7391)

Cause

The DTC services cannot find each other by server name.

Resolution

To resolve this problem, verify that the servers can communicate with one another by name, not just by IP address. Check in both directions to make sure both machines can ping each other.

For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;169790> (How to Troubleshoot Basic TCP/IP Problems).

DTC Fails To Communicate In Windows Server 2003

Symptom

Either the Control Center database computer or the AppManager repository computer runs on Windows Server 2003, Enterprise Edition, and you see Error number 7391. In the SQL Agent job history, you see an error message similar to the following:

Executed as user: NETIQUUS\liul. The operation could not be performed because the OLE DB provider 'SQLOLEDB' was unable to begin a distributed transaction. [SQLSTATE 42000] (Error 7391)

Causes

There are two likely causes.

- 1 DTC is not network-access enabled. By default, the network access of MSDTC is disabled on new installations of SQL Server 2000 on Windows Server 2003. For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;329332> (PRB: You Receive Error 7391 When You Run a Distributed Transaction Against a Linked Server) or <http://support.microsoft.com/default.aspx?scid=kb;EN-US;817064> (HOWTO: Enable Network DTC Access in Windows Server 2003).
- 2 The DTC proxy in Windows Server 2003 may not correctly authenticate MSDTC when both computers are not in the same domain.

Resolution

For Cause 1, DTC is not network-enabled. For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;329332> (PRB: You Receive Error 7391 When You Run a Distributed Transaction Against a Linked Server).

- 1 Click **Start > All Programs > Administrative Tools > Component Services**.

- 2 In the Component Services Wizard, expand **Component Services**, and then double-click **Computers**.
- 3 Right-click **My Computer**, and select **Properties**.
- 4 Click the MSDTC tab, and then click **Security Configuration**.
- 5 In the Security Configuration dialog box, click to select the **Network DTC Access** check box.
- 6 Under Network DTC Access, click **Network Transactions**.
- 7 Make sure that DTC Logon Account is set to **NT Authority\NetworkService**.
- 8 Click **OK**.
- 9 In the message box, click **Yes** to continue.
- 10 In the DTC Console Message dialog box, click **OK**.
- 11 In the System Properties dialog box, click **OK**.
- 12 Restart the computer.

Note In some cases, you must start the DTC service before you start the computer that is running SQL Server so that the linked server distributed queries work well.

For Cause 2, where the DTC proxy in Windows Server 2003 may not correctly authenticate DTC when the computers are not in the same domain. For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;827805> (BUG: MSDTC Fails to Mutually Authenticate When Computers Do Not Run in the Same Domain). In this article, Microsoft confirms that this is a bug in its product.

- 1 In the registry editor, locate the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC

- 2 On the Edit menu, click **Add Value**. Add the key `TurnOffRpcSecurity` to the registry as a `REG_DWORD` with value = 1.
- 3 Close the Registry Editor.

The SID Of One Of The DTCS Is Not Unique

Symptom

You see an error message similar to the following:

New transaction cannot enlist in specified transaction coordinator.

Cause

The problem often occurs because one of the database computers is duplicated or cloned (a disk image) from another server, for example, by using VMware or Ghost. As a result, the DTC security ID (SID) is not unique, and the DTC instance cannot be uniquely identified. For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;162001> (Do Not Disk Duplicate Installed Versions of Windows).

Resolution

To resolve this problem, re-install MSDTC. For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;279786> (HOWTO: Reinstall MS DTC for a non-clustered Windows 2000 Server).

- 1 In the Control Panel, stop all services.
- 2 Change the Startup Type for all services to “Manual” except for the following services:

- Alert
- COM+ Event System
- Computer Browser
- Distributed File System

Distributed Link Tracking Client
Distributed Link Tracking Server
DNS Client
Event Log
IPSEC Policy Agent
License Logging Service
Logical Disk Manager
Messenger
Net Logon
NT LM Security Support Provider
Network Connectors
Plug and Play
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Removable Storage
Security Accounts Manager
Server
System Event Notification
Task Scheduler
TCP/IP NetBIOS Helper Services
Windows Management Instrumentation
Windows Management Instrumentation Driver Extensions
Windows Time
Workstation

The key point here is to set the startup type for the Distributed Transaction Coordinator, MSSQLSERVER, SQLSERVER AGENT, and any NetIQ services to “Manual”.

3 Restart your computer.

Note If you do not restart the computer, this entire process will fail on all versions of Windows.

4 At a command prompt, type the following command:

```
msdtc -uninstall
```

- 5** In the registry, remove the following keys, if they exist:

```
HKEY_CLASSES_ROOT\CID  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MS  
DTC  
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MSDTC  
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MSDTC  
HKEY_LOCAL_MACHINE\Software\Microsoft\MSDTC
```

- 6** From the %WINDIR%\System32 folder, run the file `Dtcsetup.exe`.

On Windows Server 2003, this file does not exist. Instead use the following command to reinstall DTC:

```
msdtc -install
```

- 7** In the Installation Success message box, click **OK**.

- 8** Restore the startup type for all Windows services to their original values, and restart your computer.

- 9** At a command prompt, enter the following command:

```
msdtc -resetlog
```

- 10** On Windows Server 2003, enable Network Access. For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;329332> (PRB: You Receive Error 7391 When You Run a Distributed Transaction Against a Linked Server).

You can also use GuidGen to create a new SID and update the DTC registry with the new SID. For more information, see the Knowledge Base Article: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;306843> (HOWTO: Troubleshoot MS DTC Firewall Issues).

SQL Server System Variable @@servername Is Incorrect Or Null

Symptom

Error number: 7391. In the SQL Agent job history, you see an error message similar to the following:

Server: Msg 7391, Level 16, State 1, <ObjectName>, Line xx
The operation could not be performed because the OLE DB
provider '%ls' was unable to begin a distributed transaction.

In some instances, you see an error message similar to the following:

Distributed transaction aborted by MSDTC.

Causes

Here are a few reasons why the SQL Server system variable @@SERVERNAME may be NULL or not match the current SQL Server (instance) name:

- The computer was renamed.
- An image was taken of the SQL Server computer, and then copied onto another computer.
- The `sp_dropserver` stored procedure was run for the local SERVERNAME.

Resolution

- 1 On the SQL Server, execute (on Query Analyzer, for example) “`SELECT @@servername`”.
- 2 If the result is NULL, skip to Step 4. If the result is different from the SQL Server (instance) name, execute “`sp_dropserver ‘xxx’`”, where xxx is the incorrect server name.
- 3 Execute “`sp_addserver ‘yyy’, ‘local’`”, where yyy is the correct server name.
- 4 Restart the SQL Server service and SQL Agent service.

- 5 Verify that “SELECT @@servername” returns the correct server name.

Double Hop Error With Kerberos Credentials

Symptom

If you move the NetIQ AppManager Control Center Command Queue Service to a computer where the Control Center Repository is not present, the following error message shows up in the Cache Manager status pane:

Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'

Causes

This error occurs when there is a double hop problem with Kerberos credentials.

Resolution

To resolve this issue, you must enable Kerberos delegation from the NetIQ AppManager Control Center Command Queue Service machine to the Control Center Repository machine. This allows the Repository machine to impersonate the user under whose credentials the NetIQ AppManager Control Center Command Queue Service is running.

Refer to the following link on Microsoft's Web site for information on configuring Kerberos delegation: www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerbdel.mspx

Delay In Syncing Of Data From The Appmanager Repository To The Control Center Repository

Symptom

There is a delay in syncing of data from the AppManager Repository to the Control Center Repository.

Causes

- Microsoft Distributed Transaction Coordinator (DTC) is not enabled on both the machines.
- AppManager Repository and Control Center Repository are not in the same domain.

Resolution

To resolve this issue, you must enable Microsoft Distributed Transaction Coordinator (DTC) on both the machines, and ensure that the AppManager Repository and Control Center Repository are in the same domain.

VMware Support

This appendix contains support information on VMware. The following sections describe AppManager Suite support for VMware:

- [“AppManager Suite” on page 247](#)
- [“AppManager 7.0” on page 248](#)
- [“AppManager Performance Profiler \(AMPP\)” on page 250](#)
- [“AppManager Analysis Center” on page 250](#)
- [“VMware Versions Supported” on page 251](#)
- [“Additional Limitations” on page 251](#)

AppManager Suite

Equivalent Requirements Must Be Met—NetIQ's product documentation details the minimum hardware, software and configuration requirements needed for real (i.e. non-virtualized) environments to properly run AppManager components. When any AppManager component is run within or connected to a virtual environment, the virtual environment must satisfy the equivalent requirements for the applicable components as detailed in the product documentation. If adequate resources are not configured, the component cannot be guaranteed to operate satisfactorily in the virtual environment. Specifically, the configuration of the component must meet the requirements specified in System requirements for AppManager components.

AppManager 7.0

Windows Agents—AppManager agents for Windows are supported on (a) VMware guest operating systems running within a VMware ESX or GSX virtual environment, (b) VMware host operating system of a GSX virtual environment and (c) VMware Workstation.

Report Agents—AppManager Report agents are supported on VMware guest operating systems running within a VMware ESX or GSX virtual environment and on VMware Workstation.

Application Modules Running on Windows Agents—When an AppManager application module is run within a Windows guest operating system, the application module is supported with some limitations as described below. As long as the source of instrumentation (for example, PerfMon) returns accurate and valid data, the functionality of the knowledge scripts utilizing that data is expected to work normally and the associated application module feature is supported. To the extent that the source data is not generated or provided properly to the NetIQ application module, the associated feature is not supported.

UNIX and Linux Agents—AppManager agents for Red Hat Linux and SUSE Linux are supported on guest operating systems running within a VMware ESX environment.

Application Modules Running on Linux Agents—When an AppManager application module is run within a Linux guest operating system, the application module is supported with some limitations as described below. As long as the source of instrumentation returns correct data, the functionality of the knowledge scripts utilizing that data is expected to work normally and the associated application module feature is supported. However, there may be issues with instrumentation returning data values that are not valid in a virtual environment, and to the extent that the source data is not generated or provided properly to the NetIQ application module, the associated feature is not supported by NetIQ.

Management Server—AppManager management servers are supported on VMware guest operating systems running within a VMware ESX virtual environment. AppManager management servers are not supported as a failover cluster (MSCS cluster) within a virtual environment. In such cases, multiple management servers should be configured as an alternative.

Web Management Server—AppManager web management servers are supported on VMware guest operating systems running within a VMware ESX virtual environment.

Repository—AppManager repositories (QDB) are supported on VMware guest operating systems running within a VMware ESX virtual environment. At release time AppManager repositories are not supported in conjunction with a SQL Server failover cluster (MSCS cluster) within a virtual environment; contact NetIQ Solutions Support for updated status on support of this configuration.

Operator Console—The AppManager Operator console is supported on VMware Workstation.

Web Console—The AppManager web console is supported on VMware Workstation.

Diagnostic Console—The user interface portion of AppManager Diagnostics Console is supported on VMware workstation.

Control Queue Service (CQS)—The AppManager Control Center CQS is supported on VMware guest operating systems running within a VMware ESX virtual environment. At release time the CQS is not supported on a failover cluster (MSCS cluster) within a virtual environment; contact NetIQ Technical Support for updated status on support of this configuration.

Control Center Repository—AppManager Control Center repositories (NQCCDB) are supported on VMware guest operating systems running within a VMware ESX virtual environment. At release time AppManager Control Center repositories are not supported in conjunction with a SQL Server failover cluster (MSCS

cluster) within a virtual environment; contact NetIQ Technical Support for updated status on support of this configuration.

Control Center Console—The AppManager Control Center console is supported on VMware Workstation.

AppManager Performance Profiler (AMPP)

AMPP Templates—Current AMPP templates are supported in virtualized environments. In such an environment, AMPP will profile a server or application based on the virtual environment's view of resources.

AMPP Services—AMPP Services (including Alarm Export, Analytics, Data Collection, Tomcat and Watchdog) are supported on VMware guest operating systems running within a VMware ESX virtual environment.

AMPP Repositories—The AMPP repository (**AMPPDB**) is supported on VMware guest operating systems running within a VMware ESX virtual environment. At release time AMPP repositories are not supported in conjunction with a SQL Server failover cluster (MSCS cluster) within a virtual environment; contact NetIQ Technical Support for updated status on support of this configuration.

AMPP Console—The AMPP console is supported on VMware Workstation.

AppManager Analysis Center

Services—AppManager Analysis Center services (including Data Extension and Web Service) are supported on VMware guest operating systems running within a VMware ESX virtual environment.

Repositories—AppManager Analysis Center repositories (Data Mart, Data Warehouse SQL, and Data Warehouse OLAP) are supported on VMware guest operating systems running within a VMware ESX

virtual environment. At release time AppManager Analysis Center repositories are not supported in conjunction with a SQL Server failover cluster (MSCS cluster) within a virtual environment; contact NetIQ Technical Support for updated status on support of this configuration.

Analysis Center Console—The AppManager Analysis Center console is supported on VMware Workstation.

VMware Versions Supported

The following VMware versions are supported.

VMware Name	Versions Supported
VMware ESX Server	2.5 and 3.0
VMware Server	3.2
VMware Workstation	5.0 and 5.5

Additional Limitations

Configurations Not Covered—If a configuration is not explicitly declared above, it is not supported by NetIQ. In this case, NetIQ reserves the right to decide what level of support will be provided the customer on a case by case basis.

Installing in a Clustered Environment

This appendix describes the procedure to install AppManager components in a clustered environment. You can install AppManager components only on Microsoft Cluster Server. If you install AppManager components on another clustering product, such as Veritas Cluster Server, it may result in unexpected behavior.

The following topics are covered:

- [“Installing the Repository on a Cluster” on page 253](#)
- [“Installing the Management Server on a Cluster” on page 257](#)
- [“Installing Agents on a Cluster” on page 262](#)
- [“Installing Modules on a Cluster” on page 263](#)

Installing the Repository on a Cluster

AppManager supports installation of the repository on a cluster. Installing the AppManager repository and management server on a Microsoft Cluster Service (MSCS) server can help ensure that the management and monitoring of your network environment continues uninterrupted. MSCS provides fault tolerance and uninterrupted service by detecting the failure of applications and servers and automatically recovering resources and workload.

Understanding MSCS Terminology

A **cluster** is a collection of two or more Windows servers that work together. Each Windows server that is part of the cluster is called a **cluster node**. Nodes share one or more SCSI disks, which are called **shared cluster disks**, and they manage cluster resources.

A **cluster resource** is a basic system entity (for example, a physical disk, process, service, network address, or network name). A **cluster group** is a collection of one or more cluster resources related either logically or physically by dependencies.

When a node provides resources and executes processes belonging to a cluster group, the node is said to own the cluster group and all of its resources. A node in a cluster may own different shared cluster disks at different times; however, each shared physical disk and all logical disks on the physical disk are owned by only one cluster node at a time.

A **failover** happens when one or more cluster resources in a cluster group fail and MSCS migrates the troubled group from one node to another. Ownership of the group is transferred to the new node at the time the failover takes place.

When installing MSCS, you specify the **network name** of the cluster. This name is important because it becomes the name of the virtual servers you install on the cluster.

A **virtual server** is an application server within a cluster group. Executables and other dependent files of a virtual server are installed on a shared cluster disk so that each node in the cluster can execute the programs. Clients connect to the virtual server through a cluster resource **network name**. The network name—which is part of the cluster group—provides transparent access to the virtual server regardless of which cluster node currently owns the group. If a failover takes place, ownership of the group—including the network name—is transferred to a new cluster node. The node restarts all member processes of the virtual servers in the group. Because the client uses the network name to connect to the virtual server, it does not matter that a different node now owns the group.

There are various **execution modes** for a virtual server, including:

- **Active/passive** (also referred to as active/inactive): In this mode, there can be only one active instance of the virtual server among all nodes in the cluster. When a failover happens and MSCS

migrates the virtual server from one node to another, the virtual server becomes passive on the old node and active on the new node.

- **Active/active:** In this mode, there can be active instances of the virtual server on more than one node in the cluster. To distribute the workload evenly among all cluster nodes, each instance of an active/active virtual server is usually configured to run on a different cluster node. When a cluster node is brought down or fails, the virtual server instance is migrated to another cluster node, along with the rest of the cluster group.

The AppManager repository can be installed on a virtual SQL Server instance running in either **active/passive** or **active/active** execution mode.

In active/passive mode, there can only be one AppManager repository with the same name on each instance of the virtual SQL Server. In other words, you can have multiple repositories on the same instance of a virtual server if the repository names are unique. If the virtual SQL Server is running in active/active execution mode, each active instance of a virtual server can have a repository with the same name.

Note The virtual server where you install the repository should be part of the resource group owned by the node carrying out the installation.

Reviewing Account Requirements to Install the Repository on a Cluster

The AppManager setup program requires the following account information to install the repository on a cluster:

- A valid Windows login account with either Local or Domain Administrator privileges
- Network name for the virtual SQL Server
- The password for the SQL Server **sa** login account

Note The password for the SQL server **sa** login account is needed only when the repository is to be installed with SQL authentication. The repository installation on a cluster is also permitted with Windows authentication.

Installing the Repository on a Virtual Server

During repository installation, the AppManager setup program prompts you to identify the repository server name. For more information, see [“Installing the AppManager Repository” on page 83](#). If you type the local server name for the cluster node, the repository is installed as a stand-alone server on the cluster node. When installed as a stand-alone server, the AppManager repository is not cluster-enabled, and you do not get the benefits of MSCS, such as availability. Instead, you install the repository on a virtual server.

To install the repository on a virtual SQL Server in the cluster:

- 1** Follow the typical steps to start the setup program with the **Repository Database** component selected in the Welcome dialog box.
- 2** In the Choose Installation Folder dialog box, click **Next** to accept the default installation folder, or click **Browse** to navigate to the folder where you want to install the repository. To enable cluster support, the repository files must be installed on a shared cluster disk and not on a disk on the local cluster node.
- 3** In the SQL Server Login dialog box, select the network name from the **SQL Server Name** list. The network name is the virtual server name or computer name that the SQL Client uses to connect to the clustered SQL Server.

For example, if the repository were being installed on a SQL Server 2000 computer with the local hostname **SQL**, to install your AppManager repository on a cluster, you would want to select a virtual server name from the **SQL Server Name** list.

- 4 Select the type of SQL Server security to use, just as you would for any repository installation. For more information, see [“Installing the AppManager Repository” on page 83](#). Click **Next**.
- 5 In the AppManager Repository Database Name dialog box, enter a name for the repository you are installing, or accept the default name (**QDB**). Click **Next**.

If the virtual server is installed for example, on drive **F:** of a shared cluster disk, the repository database data and log files would also be installed on the same drive.

To take advantage of MSCS clustering support, the AppManager repository data and log files should be installed on a shared cluster disk. By default, they are installed on the same disk drive as the virtual SQL Server.

- 6 Click **Next** and continue with the installation as described in [“Installing the AppManager Repository” on page 83](#).

AppManager Knowledge Script files are installed on the cluster shared disk in the *shared drive*:`\Program Files\NetIQ\AppManager\qdb` directory.

Installing the Management Server on a Cluster

The AppManager management server can be installed on Microsoft Cluster Service (MSCS) to help ensure that the management and monitoring of your network environment continues uninterrupted in the event of a server outage. If you install it with the cluster support options selected, the management server runs as a *virtual server* on MSCS.

A virtual server is an application server within a cluster group. Executable and other dependent files of a virtual server should be installed on a **shared cluster disk** so that each node in the cluster can execute the program. Clients then connect to the virtual server through a cluster resource **network name**. The network name

provides transparent access to the virtual server, regardless of which cluster node currently owns the group.

The repository and management server can be installed on the same cluster or on different clusters, as needed. For more information, see [“Understanding MSCS Terminology” on page 253](#).

Preparing to Install on a Cluster

Before you run the AppManager Setup program to install the management server on a cluster, you should verify that your environment meets the following requirements:

- The cluster node where you want to install the management server is the **active** node.
- There is at least one cluster group configured with **IP Address**, **Network Name**, and **Shared Disk** resources. If a cluster group does not exist with these resources, you must create a group with these resources before you run the AppManager Setup program.
- A valid Windows login account with either Local or Domain Administrator privileges for running the Setup program has been configured on the cluster node.
- You have identified an account for the NetIQ AppManager management server service to run under—either the Local System account or a valid Windows user account.

Running Setup on a Cluster Node

To install the management server on a Microsoft cluster, run the AppManager Setup program on the cluster node that currently has ownership of the shared disk where you want to install the AppManager management server. Use the Cluster Administrator to change ownership of a shared disk to the cluster node you want.

When installing the AppManager management server on a cluster node, the AppManager Setup program asks whether you want to

install the management server on a cluster node or on a local computer.

- 1 In the Cluster Management Server Options dialog box, select **Shared cluster disk** to install the management server on a cluster.

If you select **Local cluster node as a stand-alone server**, the management server is installed on the local cluster node acting as a stand-alone server (the management server is not cluster-enabled and you do not get the benefits of MSCS, such as availability).

- 2 In the Shared Cluster Disk Selection dialog box, select the shared disk where you want to install the management server.
- 3 Click **Next**. The new destination is displayed for confirmation.

Note The setup program only lists shared disk resources that belong to a cluster group that is also configured with an **IP Address** and a **Network Name** resource. The setup program creates a **netiqms.exe** resource in the corresponding cluster group.

- 4 Click **Next**. The Repository Information dialog box appears. The installation process from this point forward is the same as that described in [“Installing the AppManager Repository” on page 83](#).

If the AppManager repository is installed on a clustered virtual SQL Server, be sure to enter the **network name** of the virtual server (not the local computer name) when prompted for the repository server name.

When you install the AppManager management server on one cluster node, the setup program automatically installs the management server on the other nodes in the cluster. A **NetIQms cluster resource** is created and is added to the same cluster group as the shared disk. If other cluster resources are required in this group, you should manually add those resources to the cluster group.

Note When you install the Management Server on a cluster shared disk, it gets installed on every node of the cluster, but runs only on the

owner node. During agent installation, the physical nodes might not be written to the AllowMS list in the registry (`Software\NetIQ\AppManager\4.0\NetiqMC\Security`). This could happen because there is no network connectivity between the agent machine and the physical node, or if one of the nodes is down during installation. When the Management Server sends the job to the agent machine, it sends the physical IP address of the owner node. If the physical IP address is not present in the AllowMS list, the job is not executed on the agent machine and two events are raised - "Job <jobid> from ms <ms_ip> not authorized to run" and "Communication is not authorized. See detailed error message". In such a case, you need to manually modify the AllowMS list on the agent machine to include the Management Server machine IP address for which the communication was not authorized.

The cluster group is then migrated to the other nodes in the cluster. To minimize the amount of time it takes to migrate the cluster group, NetIQ Corporation recommends installing the management server on a shared physical disk on which other cluster resources are not dependent. After you install the AppManager management server on a cluster node, move the Quorum Disk for the cluster to the **NetIQms cluster resource**. Moving the Quorum Disk ensures proper failover operation.

Operating in Active/Passive Mode on a Cluster

After you install the management server on a cluster node, the AppManager management server operates in an **active/passive** execution mode. In this mode, there can be only one active instance of the virtual server among all nodes in the cluster. When a failover happens and MSCS migrates the virtual server from one node to another, the virtual server becomes passive on the old node and active on the new node.

Installing AppManager Agents on Each Cluster Node

When the management server is installed on a cluster node, the AppManager agent and the Windows module are automatically installed on that node only. You **must** install the agent on each of the other nodes in the cluster.

Note When you install the AppManager agent and are asked to provide the name of the AppManager management server, the name of the clustered management server is the **network name** of the cluster, which is specified when you install MSCS.

Configuring Communication with Managed Clients

It is important that the AppManager agent on the managed client communicates with the clustered AppManager management server using the network name of the management server, not the IP address.

After installing the management server on a cluster, take the following steps:

- 1** Install the AppManager agent on the computers the management server communicates with.
- 2** Install an Operator Console or Control Center Console. For more information about installing the:
 - Operator Console, see [Chapter 8, “Installing the Operator Console Programs.”](#)
 - Control Center Console, see [Chapter 12, “Installing Control Center.”](#)
- 3** Start an AMAdmin_ConfigSiteCommType Knowledge Script job on all managed clients that are monitored by the management server.
- 4** In the Properties dialog box, click the **Values** tab and set the **Use IP address to communicate with management server?** parameter

to **n**. This setting changes the communication method from IP address to host name.

5 Click **OK** to run the job.

For more information about this Knowledge Script, refer to the Help for Knowledge Scripts.

Installing Agents on a Cluster

The AppManager agent does not run as a virtual application; therefore, it must be installed on the local (not shared) disk of each physical node in a cluster.

Besides installing the agent on each node in the cluster, you should also install the same set of modules on each node of the cluster.

After you install the agent and modules, you can run a combination of application-specific, MSCS, and NT Knowledge Scripts to monitor a virtual server. For more information, see the *Administrator Guide for AppManager*.

Installing on an Active Cluster Node

Before you install the AppManager agent and the application-specific or Microsoft Cluster Service module, check whether the virtual server is active on the cluster node where you are performing the installation.

If the virtual server is not active on the computer where you are installing the agent, some resource objects will not be discovered. Move the active virtual server to each node before you install the agent. Or install on an inactive node and clear the option to **Automatically attempt to discover this agent during setup**. After installation, you can then move the virtual server to the appropriate node and run the discovery script manually.

To install the agent locally on each cluster node, follow the instructions in [“Installing Agents in a Windows Environment”](#) on

[page 102](#). You can remotely deploy agents to the nodes of a cluster. However, the same rule applies: agents must be deployed to physical nodes, not to the virtual server.

Note Be sure you have a Windows domain, account name, and password for the agent to use. The agent on each node of a cluster must run using a Windows login account (not the Local System account, which is the default option). For more information, see [“Understanding Windows User Accounts”](#) on [page 106](#).

Communicating with a Clustered Management Server

To be sure all of the managed clients in the cluster are properly monitored by the AppManager management server, run the AMAdmin_ConfigSiteCommType Knowledge Script on each cluster node and disable the **Communication via IP address** parameter.

The AppManager agent on the managed client will then communicate with the clustered management server using the network name, not the IP address.

For more information about the AMAdmin_ConfigSiteCommType Knowledge Script, see the Help.

Installing Modules on a Cluster

The AppManager agent can run in a cluster and provide support for monitoring clustered applications. However, you must install the agent on the local (not shared) disk of each physical node in a cluster. Similarly, you must install the modules on physical cluster nodes. To ensure that you are monitoring the clustering behavior of your servers, install the same modules on each node of the cluster.

For more information about installing the agent on a cluster, see [Chapter 9, “Installing Agents”](#). As a general rule, the same information applies to the installation of modules on clustered servers. For more information about installing the module locally on

each cluster node, see [“Installing Modules by Downloading From the Web” on page 122](#).

Note The agent on each node of a cluster must run using a Windows user account and not the Local System account. The Local System account is the default option. For more information, see [“Understanding Windows User Accounts” on page 106](#).

After installing modules on each physical node of the cluster, you must run the module-specific Discovery Knowledge Script on each physical node of the cluster.

For more information on module-specific support for clusters, see the *Management Guide* for that module.