Trial Guide

NetIQ® AppManager®

June 2008



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.

© 1995-2008 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, Aegis, AppAnalyzer, AppManager, the cube logo design, Change Administrator, Change Guardian, Compliance Suite, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowing is Everything, Knowledge Scripts, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, the NetIQ Partner Network design, Patch Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Risk and Compliance Center, Secure Configuration Manager, Security Administration Suite, Security Analyzer, Security Manager, Server Consolidator, VigilEnt, Vivinet, Vulnerability Manager, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Contents

About This Guide

Intended Audience vii

Conventions viii

Using Online Help viii

Other Information in the Library ix

About NetIQ Corporation x

Contacting NetIQ Corporation xi

Chapter 1 Introducing AppManager

What is AppManager? 3

What is Unique about AppManager? 4

How Does AppManager Work? 5

AppManager Architecture and Components 5

Control Center Architecture and Components 8

How Does Deployment Work? 10

Rule-based Deployment 10

Approval-based Deployment Tasks 11

Agent Deployment Architecture and Components 11

Does AppManager Provide Reporting Capabilities? . . . 12

Can AppManager Manage and Predict the Behavior of My IT Environment? 14

Does AppManager Provide a VoIP Management Solution? 17

How Do I Evaluate AppManager Support for a Particular Application? 18
Whom Do I Contact for Technical Assistance and Sales Information? 18

Chapter 2 Installing AppManager

System Requirements for Evaluating AppManager 19
Configuring Windows Application Services 22
Starting the Installation 24
Installing the AppManager Repository 27
Installing the Management Server 36
Installing the AppManager Agent and Modules 41
Installing the Web Management Server 52
Installing Control Center 54
Installing the AppManager Console Applications 67

Chapter 3 Exploring AppManager

Starting the Control Center Console 74
Understanding Management Groups 77
About Control Center Console Views 77
Creating a Rule-based Management Group 78
Creating a Server View 84
Understanding Agent Deployment 86
About the Administration Pane 86
Before You Begin 87
Configuring a Rule to Deploy the Agent 87
Enabling the Rule 103
Approving Deployment Tasks 105

Understanding Monitoring Policies 106
Creating a Knowledge Script Group 108
Enabling the Monitoring Policy 122
Working with Server Views 124
Looking at Jobs 125
Viewing the Properties of a Job 125
Looking at Events 127
Working with Event Views 128
Looking at Events 129
About Filtering Events 129
Filtering the Event View 130
Acknowledging an Event 136
Organizing and Managing Groups of Events 138
Working with Job Views 141
About Filtering Jobs 141
Filtering the Job View 142
Understanding Service Map Views 146
Understanding Charts 148

Index

About This Guide

The NetIQ AppManager product (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 step-by-step instructions to help you evaluate the main features of the product, letting you discover for yourself the benefits that AppManager provides to those who need to centrally manage and monitor the performance, availability, and server health for a broad spectrum of operating environments, applications, and server hardware.

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

Conventions

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

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and installation kit titles • Variable names and values • Emphasized words
`Fixed Font`	• 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**.

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**.
- In the Knowledge Script pane of the Operator Console, highlight a Knowledge Script and press **F1**.

Other Information in the Library

The library provides the following information resources:

- *Installation Guide for AppManager*: Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.
- *Control Center User Guide for AppManager*: 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 for AppManager*: Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.
- *Upgrade and Migration Guide for AppManager*: Provides complete information about how to upgrade from a previous version of AppManager.
- Management guides: Provide information about installing and monitoring specific applications with AppManager.

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

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

- Downloads, including hotfixes, service packs, and product upgrades.
- Documentation, including white papers and the most current information about version support for the systems and applications monitored by AppManager.

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

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

About 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 IT Process Automation, 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

Chapter 1

Introducing AppManager

AppManager delivers the productivity and visibility enterprises demand of their systems management solutions while providing the critical foundation needed for safely adopting and exploiting next-generation technologies, such as:

- VMware ESX Server
- Microsoft SharePoint and Exchange Server 2007
- BlackBerry Enterprise Server
- Oracle Grid Computing
- Avaya, Cisco or Nortel IP Telephony (VoIP) solutions

AppManager is an efficient approach to systems management. The extensible, flexible nature of AppManager allows customers to achieve greater time to value with AppManager than other competitive solutions.

From a central console, administrators configure monitoring functions called **Knowledge Scripts** that collect performance data and monitor for simple or complex events. For example, you can configure Knowledge Scripts to monitor a particular Microsoft Exchange Server resource, such as queue length, and monitor the response time to send and receive an e-mail message from the end-user perspective.

If an event condition is detected, the Knowledge Script raises an event and can take a corrective action such as restarting a service that has gone down or sending an e-mail notification. The result is a powerful and automated "closed-loop" solution that proactively detects and resolves problems across a broad spectrum of operating environments, applications, and server hardware.

AppManager delivers comprehensive systems management, including monitoring, reporting and analysis, and diagnostics and resolution. AppManager is designed to manage a variety of components, from physical hardware to server applications to end-user response time.

This chapter is presented as a series of frequently asked questions and answers. As you read this chapter, you will become acquainted with the business problems that AppManager solves, as well as the product's features and architecture.

What is AppManager?

AppManager is an integrated enterprise systems management solution that lets you effectively manage your applications and infrastructure within today's tight resource constraints and growing workloads.

AppManager provides enterprises with the ability to:

- **Gain Greater Control over the IT Environment:** AppManager establishes control through features such as automated detection and deployment, policy exception management, secure delegation, and self-maintaining service maps. These features help establish a solid systems management foundation so that enterprises safely adopt and exploit next-generation technologies.
- **Improve IT Management Productivity and Visibility:** AppManager gives IT automation that adapts to dynamic business environments. End-to-end service visibility vastly reduces and pre-empts business service downtime and improves event impact assessment through visually represented service maps.
- **Maximize Return on IT Investment:** AppManager's extensive out-of-the-box functionality, flexible integration with existing IT infrastructure, extensible platform, and easy customization ensure that enterprises benefit from maximum functionality with the shortest time to value.

What is Unique about AppManager?

AppManager is the right choice for systems management:

- **End-to-End visibility from a single pane of glass.** With the AppManager Control Center Console, you can take advantage of a visual representation of IT resources mapped to business applications or services, enabling you to prioritize problem response. By mapping services to elements, you can visually recognize all elements the service depends upon and understand how element failure impacts the service.
- **The perfect balance between simplicity and flexibility.** AppManager's out-of-the-box knowledge provides rapid time-to-value and the level of customization that large, heterogeneous enterprises require.
- **Self-maintaining service maps.** Service maps built using rule-based management groups will automatically be updated as components enter or are withdrawn from the environment, ensuring operations is working with current information.
- **Highly-granular secure delegation model.** AppManager allows for the broadest access and interaction across your operations team through its highly-granular secure delegation model. Subject matter experts can access data the way they want and value is derived from AppManager at all levels of your organization.
- **Adapt to your unique infrastructure.** Extend AppManager to perform additional tasks without learning proprietary languages or technologies. AppManager's use of industry-standard scripting languages, such as VBA and Perl, minimizes training costs by using the technologies with which your staff is most familiar.

How Does AppManager Work?

AppManager uses an advanced multi-tier architecture that scales along with the growth of your organization's IT infrastructure.

AppManager Architecture and Components

The AppManager architecture provides the best combination of efficiency, scalability, and flexibility in distributing process load across multiple components and allows for efficient communication between components.

The AppManager architecture consists of the following components:

- **AppManager consoles:** A collection of programs for managing various aspects of your environment:
  - The **Operator Console** allows you to make advanced configuration changes to the AppManager repository database.
  - The **Operator Web Console** allows you to check the status of jobs and events, create and view charts, run Knowledge Scripts, view details about the computers you are monitoring, and view reports from a Microsoft Windows server with Microsoft Internet Explorer.
  - The **Chart Console** allows you to generate and view charts of AppManager repository data. The Chart Console is also available from the Operator Web Console.
  - The **Security Manager** console allows you to manage security information for an AppManager repository.

- **AppManager agent:** Windows services or a UNIX daemon that runs on a computer and receives requests from the management server to run or stop a Knowledge Script job. The agent communicates back to the management server, on an exception-basis, any relevant output from a Knowledge Script.

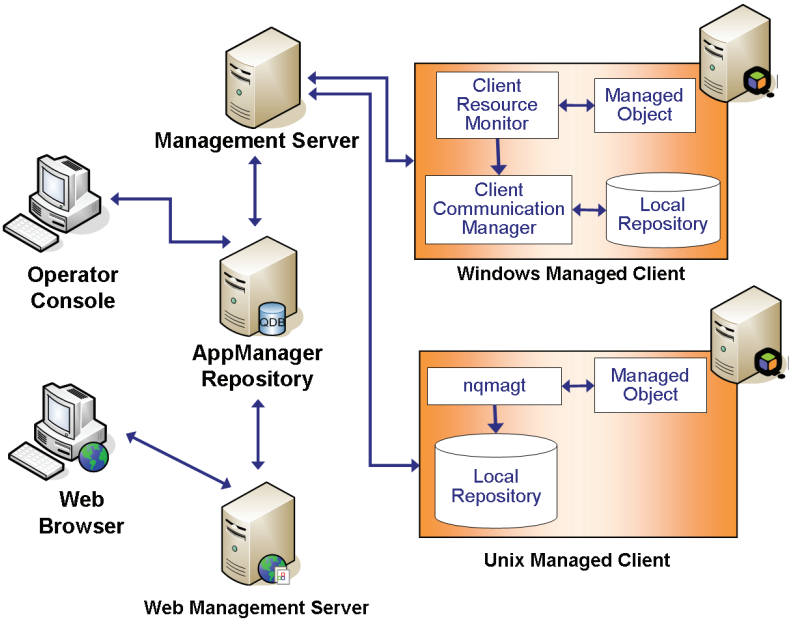
  For Windows computers, the agent consists of two Windows services, the NetIQ Client Resource Monitor and the NetIQ Client Communication Manager, a local repository database, and at least one managed object. A **managed object** enables the agent to monitor a particular application, for example, Microsoft SQL Server.

  For UNIX and Linux computers, the agent consists of a single daemon, `nqmagt`, and the supporting files and directories that provide:

  - Data persistence, which is equivalent to the local repository.
  - Access to system statistics, which is equivalent to managed objects.
- **AppManager management server:** A Windows service, NetIQ AppManager Management Service, that manages event-driven communication between the AppManager repository, AppManager console programs such as the Operator Console, and agents.
- **AppManager repository:** A SQL Server database in which management data is stored. The Operator Console connects to the AppManager repository.
- **AppManager Web management server:** A set of Active Server Pages that communicate with one or more AppManager repositories. These pages make up the Operator Web Console.

  From a Microsoft Windows server with Microsoft Internet Explorer, the Operator Web Console allows you to check the status of jobs and events, create and view charts and reports, run Knowledge Scripts, and view details about the computers you are monitoring.

The following figure provides a simplified view of the AppManager architecture:

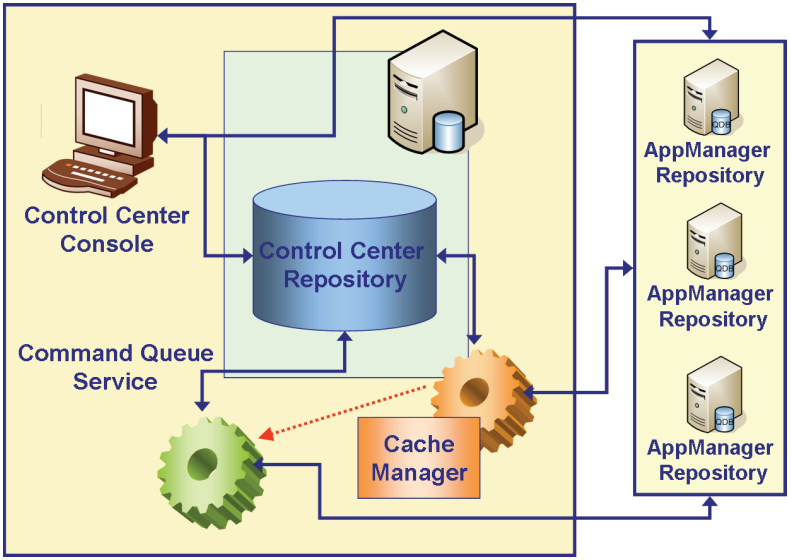


Control Center Architecture and Components

The AppManager Control Center architecture extends the AppManager architecture and consists of the following components:

- **Control Center Console:** The Control Center Console connects to the Control Center repository and allows you to run jobs on the systems and applications you manage across multiple AppManager repositories.
- **Control Center repository:** A SQL Server database for AppManager Control Center that contains:
  - Cache tables to store view information collected from each AppManager repository managed by Control Center.
  - A Command Queue table to store queries that collect view information based on the view criteria defined in the Control Center Console.
  - Tables to store other information, such as user preferences specified during installation or from the Control Center Console, definitions of management groups, and security settings.
- **Control Center Command Queue Service:** A Windows service, NetIQ AppManager Control Center Command Queue Service, that polls the Command Queue table for queries to run on a repository. The **Cache Manager**, NQSyncQDB.exe, is a child process of the Command Queue Service that runs on each AppManager repository computer. The Cache Manager runs the Control Center queries on the AppManager repository to retrieve view information for a Control Center management group.
- **Primary AppManager Repository:** The primary AppManager repository stores the Knowledge Scripts and Knowledge Script Groups that you run from the Control Center Console. If Control Center manages more than one AppManager repository, when you create a job, Control Center automatically replicates the Knowledge Script in the primary AppManager repository to the other AppManager repositories.

The following figure provides a simplified view of the AppManager Control Center architecture:



How Does Deployment Work?

The Control Center Console allows you to quickly and easily install deployment packages for the agent, module updates, and hotfixes to the remote Windows computers in your environment.

Tip An AppManager **module** is a downloadable package that provides updated monitoring support for an application. A module includes a managed object, Knowledge Scripts, and Help. For the most current information about module updates, see: http://www.netiq.com/support/am/extended/modules.asp.

Deployment provides:

- Automated detection of new computers and applications
- Automated remote installation of agents and modules
- Rapid response to changing environments
- Multiple, firewall-friendly deployment servers
- Customized deployment schedules to meet corporate maintenance windows

Rule-based Deployment

The Control Center Console provides an easy-to-use wizard to help you create deployment rules. A **deployment rule** allows you to select computers and install the agent and appropriate modules based upon a variety of criteria, including:

- Organization units in Active Directory
- Remote registry check
- Management groups in the Control Center Console
- IP address ranges
- Operating system or applications installed

Approval-based Deployment Tasks

When a target computer meets the conditions for a deployment rule, Control Center generates a deployment task. A **deployment task** delivers a specific deployment package to a particular computer at a scheduled time.

In the Control Center Console, you approve a deployment task *before* the deployment service can install the agent or module on the target computer.

Each deployment task includes the required credentials to run on the target computer.

To avoid monitoring interruptions during business hours, you can schedule deployment tasks to run outside business hours.

Agent Deployment Architecture and Components

The **deployment service** communicates with the Control Center repository to process deployment rules and deployment tasks. Deployment tasks run on the target computer using credentials provided in the deployment rule.

The computer where the deployment service is installed is the **deployment server**. If you have configured more than one deployment service, when you configure a deployment rule, you can choose the deployment service you want.

To deploy the agent to computers behind a firewall, configure a deployment service on a computer that is also behind the firewall.

The **deployment web service** consists of two Web services that are installed on a Microsoft Internet Information Services (IIS) server. This server is called the **web depot**. The deployment web service:

- Checks deployment packages into the web depot.
- Distributes deployment packages to the deployment services. The deployment web service uses Microsoft Background Intelligent Transfer Service (BITS) server extensions to distribute deployment packages to the deployment service.
- Receives software inventory information and application detection results from the agent and forwards this information to the Control Center repository.
- Provides a communication proxy for deployment services that are across a firewall.

Once you install the Control Center deployment components, you use the Control Center Console to configure a deployment rule.

At this time, you cannot deploy the agent to remote UNIX computers.

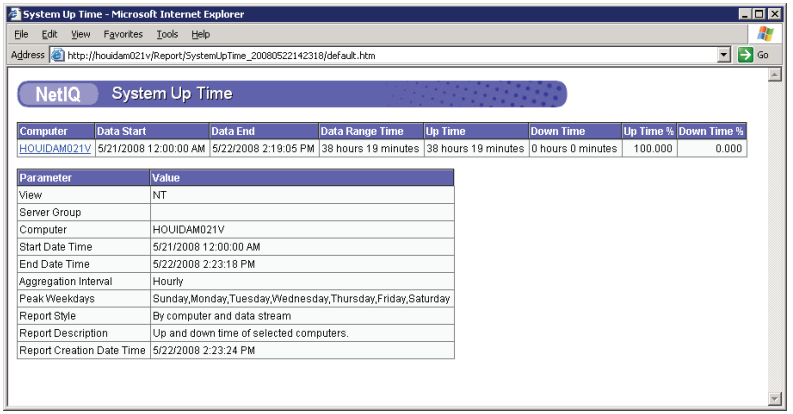
Does AppManager Provide Reporting Capabilities?

Whether you need to report on service-level conformance, historical trends, or ad hoc performance results, AppManager delivers a powerful and flexible reporting infrastructure, including:

- **Performance-related reports** to help you understand the performance of your applications and systems.
- **Trend analysis reports** to help you plan for system or application upgrades.
- **Service level agreement reports** to quantify the availability of services and service response time.

- **Event summary reports** to provide an overview of the events being created by AppManager. Use this information to develop a plan of action.
- **Configuration reports,** to provide an overview of the system details being monitored and configuration details, such as event threshold settings.

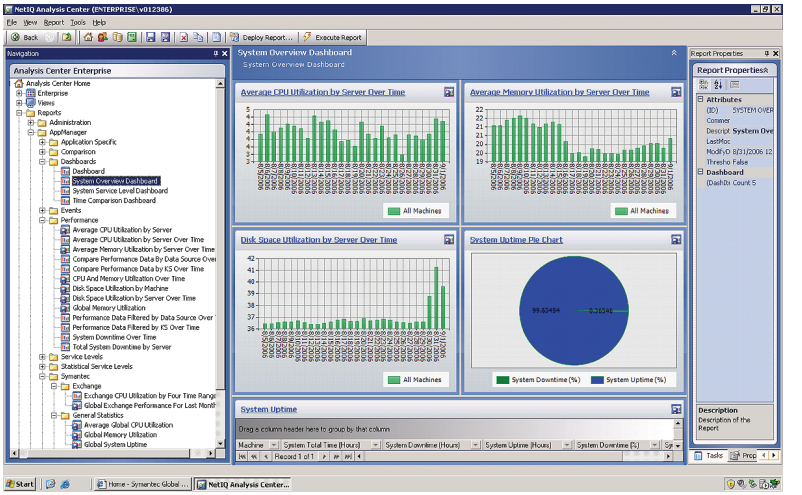
AppManager reports use the same Knowledge Script-based mechanism that you use to run jobs that collect data and raise events.



An AppManager report queries data from a single AppManager repository. At this time you cannot report on data from more than one AppManager repository in the same report.

To report on AppManager data from more than one AppManager repository in the same report, use the NetIQ Analysis Center product (Analysis Center).

Analysis Center enhances the reporting capabilities of the Service and Security Management solutions from NetIQ Corporation, helping IT organizations communicate service levels and security compliance. By offering quick time-to-value without sacrificing functionality or flexibility, Analysis Center rises above the level of individual metrics. The product provides vital information, such as overall system utilization, security incident interpretation, root-cause analysis and historical trending, and critical trends and conditions.



AppManager reporting and Analysis Center are not featured in the product tour. Please discuss your AppManager reporting needs with your NetIQ Sales Representative or NetIQ Partner.

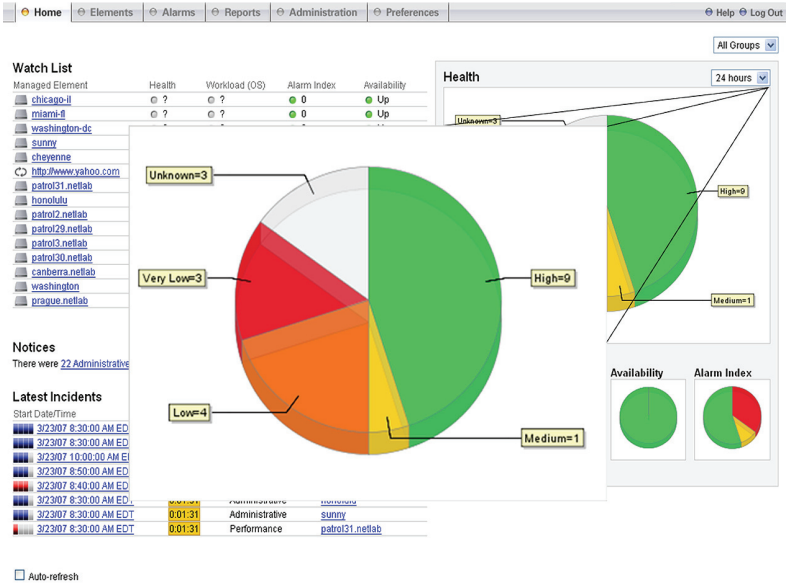
Can AppManager Manage and Predict the Behavior of My IT Environment?

The NetIQ AppManager Performance Profiler product (AMPP) enhances the capabilities of NetIQ AppManager to help IT organizations address the challenge of improving service levels, while also maximizing staff efficiency and reducing operational costs.

As a result, you can manage your systems in a dynamic environment, rapidly adjusting and managing monitoring policies and system availability, while proactively anticipating future resource issues. AMPP provides you with the following benefits:

- **Improves IT service levels** through proactive problem identification and resolution. AMPP learns a system's performance, configures dynamic thresholds automatically, and adapts over time or as usage patterns change. AMPP raises trusted alerts for abnormal conditions before they become critical.
- **Enhances IT operational efficiency** by reducing time spent manually updating and managing thresholds. AMPP reduces false positive alerts that generate trouble tickets, allowing administrators to investigate the most critical issues first.
- **Reduces IT operational costs** by maximizing server utilization, deferring the need for future server hardware purchases. Enterprise workload management reports also help identify servers that may be candidates for consolidation or virtualization.

Powered by Netuitive, AMPP is a self-learning, self-configuring and continuously adaptive tool that takes performance availability and dynamic thresholding to a new level. While continuously profiling your environment's changing characteristics, AMPP raises Trusted Alarms when it detects abnormal system behavior.



For information about including AMPP with your AppManager solution, contact your NetIQ Sales Representative or NetIQ Partner.

Does AppManager Provide a VoIP Management Solution?

AppManager provides a comprehensive solution for managing, securing, diagnosing, and analyzing the performance and availability of VoIP solutions. AppManager:

- **Simplifies VoIP management**. With AppManager you can manage VoIP solutions, including IP phones, call servers, voice mail and IP contact center applications, as well as the underlying IT infrastructure—all from a single integrated console.
- **Maximizes performance and availability**. Proactive 24x7 monitoring of the health and performance of the network, servers and VoIP applications ensures that you are immediately alerted to problems or potential problems in your VoIP environment.
- **Extends VoIP expertise**. Knowledge built into AppManager designed specifically for VoIP applications provides immediate insight into VoIP application health and availability, dramatically decreasing the time needed to manage converged VoIP technologies and applications.
- **Provides powerful reporting capabilities**. AppManager delivers a powerful and flexible reporting infrastructure. Extensive reports allow for monitoring service levels, call quality, overall performance, usage trends and capacity planning.
- **Automates Troubleshooting**. AppManager integrates with the Vivinet Diagnostics tool from NetIQ Corporation to automatically pinpoint the issues on the underlying data network that are impacting voice quality.

How Do I Evaluate AppManager Support for a Particular Application?

AppManager provides the broadest and deepest management view of your cross-platform infrastructure. AppManager centrally manages the health, performance and availability of more than 65 applications and services across Windows, UNIX, and Linux, plus VoIP applications and network devices.

AppManager **modules** provides monitoring support for an application. For more information about the monitoring support for an application, see the corresponding AppManager module **management guide** provided in AppManager installation kit under: `\windows_installation\Documentation\Management Guides`

For the most current information about supported products, including version support, see: http://www.netiq.com/support/am/supportedproducts.asp.

NetIQ Corporation is constantly adding to the list of applications and systems supported by AppManager, so check back often.

For more information, contact your NetIQ Sales Representative or NetIQ Partner.

Whom Do I Contact for Technical Assistance and Sales Information?

If you have any technical questions about how AppManager works or its product features, free technical support during your evaluation and review of AppManager is available. For more information, see "Contacting NetIQ Corporation" on page xi.

Or, use the Evaluation Support page at: http://www.netiq.com/support/am/supportrequest.asp.

Chapter 2

Installing AppManager

Before installing AppManager, review the release notes for the latest product information. The release notes, `releasenotes.htm`, are provided in the `\windows_installation\Release Notes` folder of the AppManager installation kit.

System Requirements for Evaluating AppManager

The following table describes the requirements to install and evaluate AppManager.

Requirement	Configuration for evaluation purposes
Processor	32-bit Intel Xeon processor: • Minimum: 2 GHz or higher • Recommended: Dual-core, 2.4 GHz or higher
Memory	Minimum: 2 GB Recommended: 3 GB or more

Storage	Recommended:
	• RAID 10 or SAN attached with 3 separate physical drives for:
	  • Operating system
	  • SQL Server data files
	  • SQL Server log files
	• Disk speed: 15,000 RPM

Requirement	Configuration for evaluation purposes
Operating System	32-bit version Microsoft Windows Server 2003 with Service Pack 2, which includes the following required components: • Microsoft Data Access Components (MDAC) 2.8 • Microsoft ActiveX Data Objects, which is included with MDAC • ODBC SQL Server driver, which is included with MDAC • Microsoft XML Parser 6.0 • Microsoft Jet 4.0 database • Microsoft Windows Installer 3.1 • Microsoft Background Intelligent Transfer Service (BITS) Client Extensions
Database Server	32-bit version of Microsoft SQL Server 2005 Service Pack 2, which includes the following required components: • Microsoft .NET Framework 2.0 • Microsoft XML Parser 6.0 You cannot install AppManager 7.0.1 on the 64-bit version of Microsoft SQL Server 2005.

Requirement	Configuration for evaluation purposes

Windows Application Server	From Add/Remove Windows Components, install the following Application Server options:
	• **Enable network DTC access**. By default, network DTC access is disabled on Windows Server 2003. For trial purposes, you do not need to authenticate network DTC access. Configure the credentials for DTC service to use the NTAUTHORITY\NetworkService account.
	• **ASP.NET**.
	Note that if you did not install IIS when you installed the operating system, when you install ASP.NET, the 2.x version required by AppManager may not be enabled. To fix this problem, manually register ASP.NET 2.x. For more information, see "Configuring Windows Application Services" on page 22.
	• **Internet Information Services (IIS) 6.0** with the following sub-components:
	  • **Background Intelligent Transfer Service (BITS) Server Extensions**. By default, BITS Server Extensions are not installed when you install IIS.
	  • **World Wide Web Service** with the **Active Server Pages** sub-component. By default, ASP is not installed when you install the World Wide Web Service.
	Note that if you installed Windows Server 2003, then separately installed Service Pack 2, and then install the required application services, reapply Service Pack 2 for Windows Server 2003 to update the application services.
	If you installed Windows Server 2003 R2 or installed Windows Server 2003 Service Pack 2 directly, and then you install the required Windows application services, you do not need to reapply Service Pack 2.

Web browser	• Minimum: Microsoft Internet Explorer 6.0.

Configuring Windows Application Services

If you did not install the Windows Application Services, including IIS and ASP.NET, when you installed Windows Server 2003, install and configure these services.

To install and configure Windows application services:

1. In **Add/Remove Programs**, click **Add/Remove Windows Programs** to install the required Windows Application Server components and sub-components:
   - Network DTC Access. Note that DTC is disabled by default on Windows Server 2003.
   - ASP.NET
   - IIS, along with the following sub-components:
     - ASP
     - BITS Server Extensions
2. ***If you installed a version of Windows Server 2003 that did not include Service Pack 2***, reapply Service Pack 2 for Windows Server 2003 to update the application services you just installed.
3. Verify that the **2.x** version of ASP.NET is enabled by performing the following steps:
   a. In IIS Manager, click **Web Service Extensions**.
   b. In the list of Web Service Extensions, verify that **ASP.NET 2.0.50727** is **Allowed**.

4 ***If the 1.x version of ASP.NET is the only available version***, manually register the 2.x version by completing the following steps:

a. Open a Command Prompt.

b. Change directories to location where ASP.NET 2.x is installed. By default, `ASP.NET 2.x` is installed under `C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727`.

c. Enter the following command:
`aspnet_regiis.exe -i -enable`

d. Press the Enter key.

The program displays the following:

```
Start installing ASP.NET (2.0.50727).
.....................................
Finished installing ASP.NET (2.0.50727).
```

e. When the program completes, verify in IIS Manager that ASP.NET 2.x is enabled. For more information, see Step 3.

Starting the Installation

This guide provides information about installing and evaluating AppManager 7.0.1. You can download AppManager 7.0.1 from the AppManager Support Resources area of the NetIQ web site: http://www.netiq.com/support/am.

For trial purposes, install all AppManager and Control Center components on the same computer. After you complete the installation, you can use the agent on the trial computer to monitor Microsoft SQL Server and Microsoft IIS Server.

As part of the product tour, you can install the agent to monitor additional computers. For more information about installing the agent on remote computers, see "Understanding Agent Deployment" on page 86.

To verify that the computer on which you are about to install AppManager passes all system requirements, the setup program runs a pre-installation check. Before you can install the product, the computer must pass the pre-installation check.

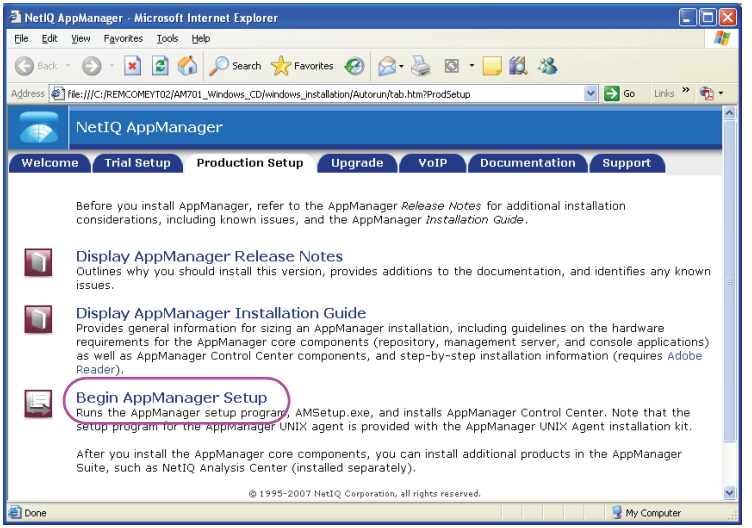
Before you install AppManager, log in using a Local or Domain Windows account with the following credentials:

- Windows Administrator permissions.
- SQL Server sysadmin fixed server role. By default, all members of the Windows BUILTIN\Administrators group, the local administrator's group, are members of the **sysadmin** fixed server role.

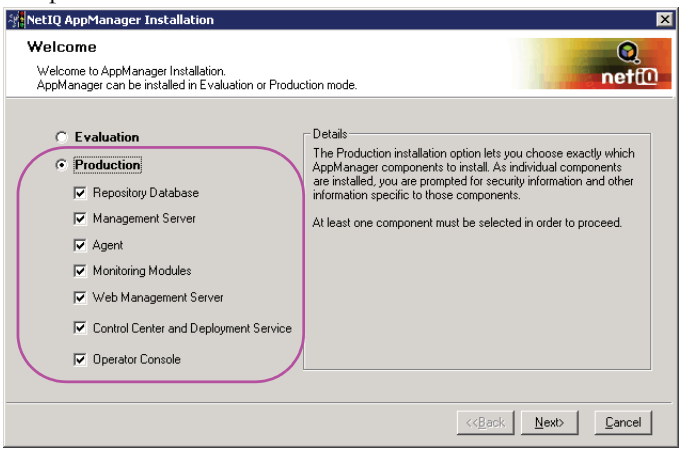
To install AppManager:

1. On the computer where you want to install AppManager, extract the contents of the AppManager installation kit.
2. In the `\windows_installation` folder, double-click `setup.exe` to start the default Web browser and open the **Welcome** startup page.

3 In the **Production Setup** page, click **Begin AppManager Setup**.

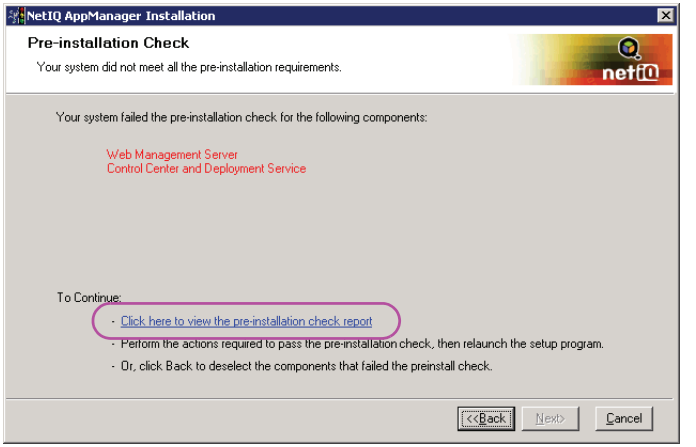


4 In the Welcome dialog box of the AppManager setup program, click the **Production** option and select the check box for each AppManager component. The **Production** option allows you to configure the installation options for each AppManager component.

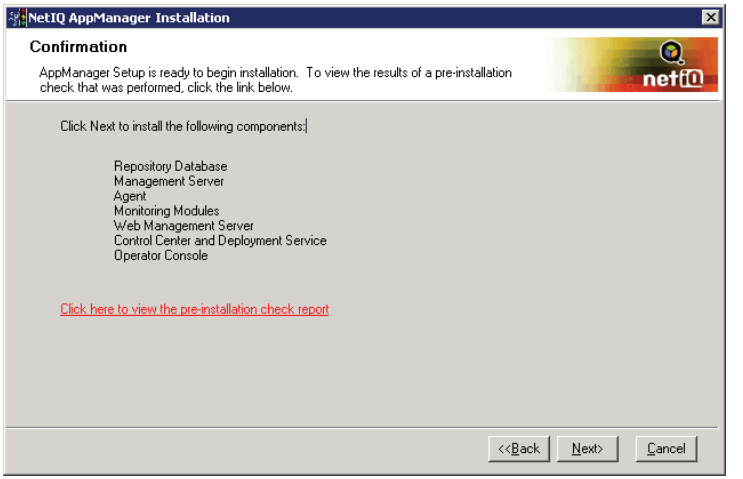


5 Click **Next** to proceed and run the pre-installation check.

6 ***If the pre-installation check report indicates there are requirement failures for a particular component,*** resolve the failures for that component. Click the link to view the results and detailed information about how to resolve the problem.



7 ***If the pre-installation check is successful,*** you are ready to install AppManager.



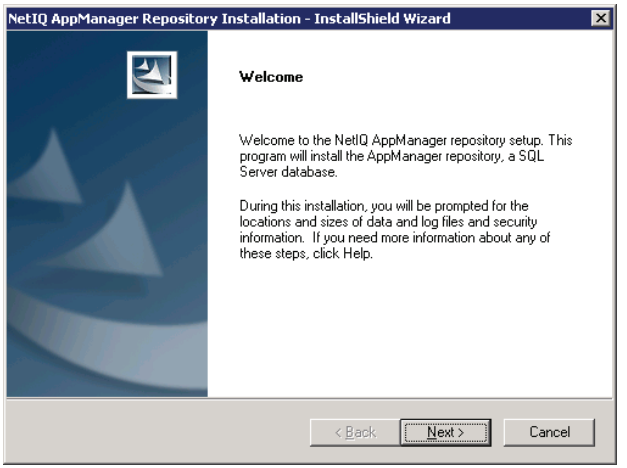
8 Click **Next** to proceed with the installation and install the AppManager repository. For more information, see "Installing the AppManager Repository" on page 27.

Installing the AppManager Repository

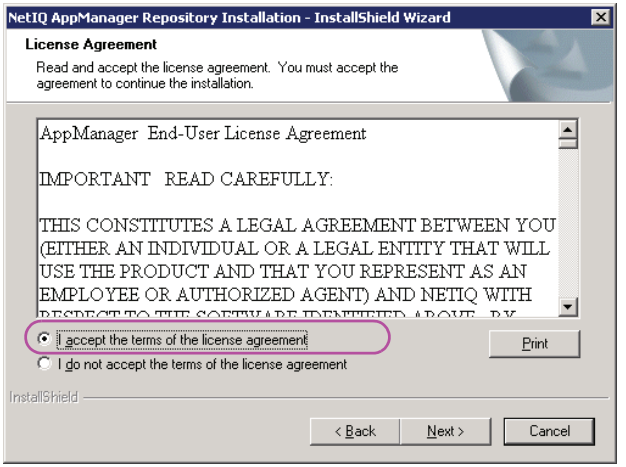
After your computer passes the pre-installation check, the setup program begins by installing the AppManager repository.

To install the AppManager repository:

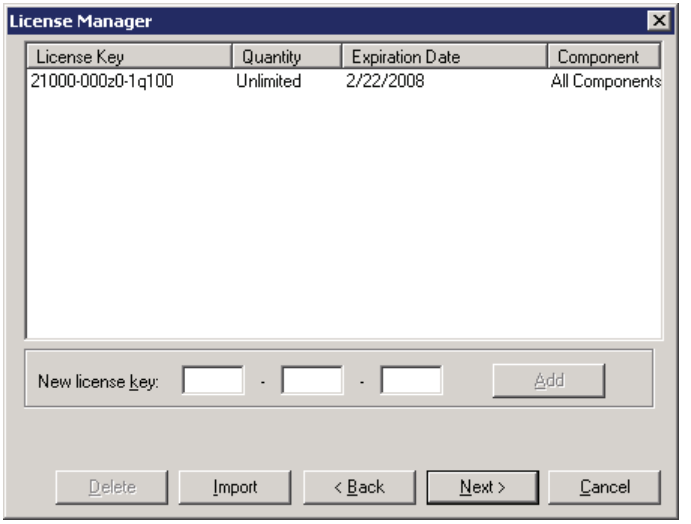
1 At the Welcome dialog box, click **Next**.



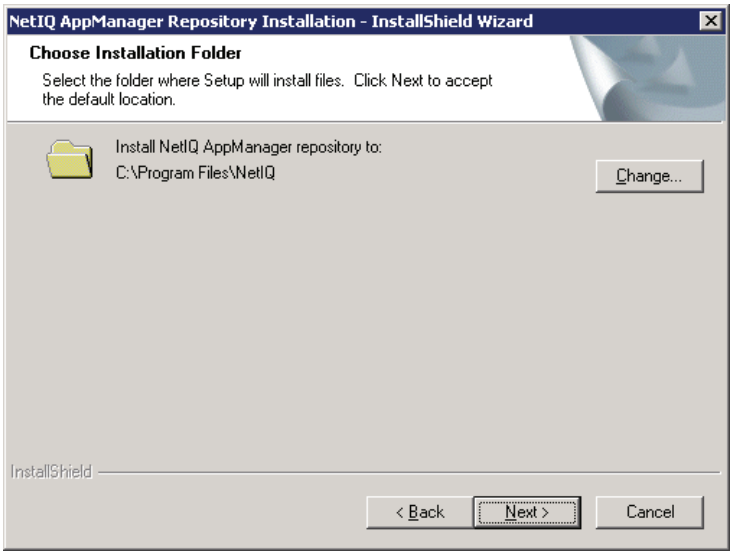
2 At the License Agreement dialog box, accept the license agreement and click **Next**.



3 At the License Manager dialog box, click **Next** to accept the default license key which allows you to evaluate AppManager for 30 days.

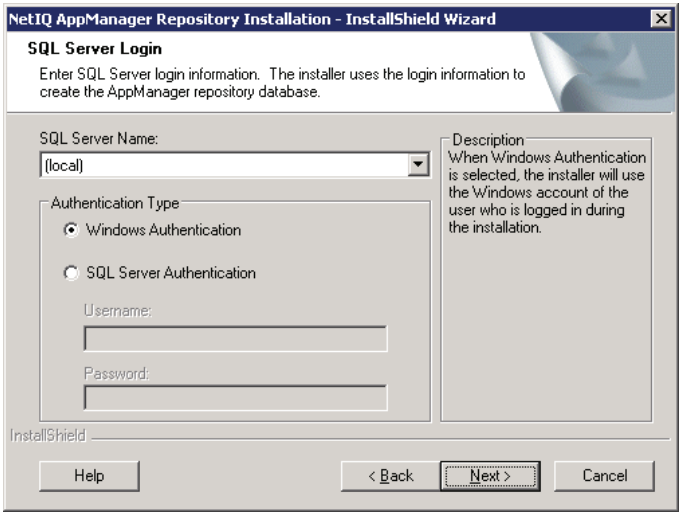


4 At the Installation Folder dialog box, select the folder where you plan to install AppManager. Except for Control Center, all AppManager components are installed to the specified location.

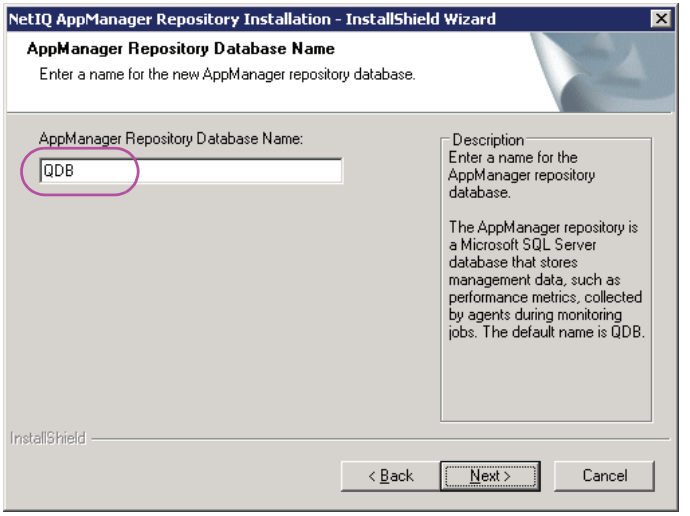


5 Click **Next**.

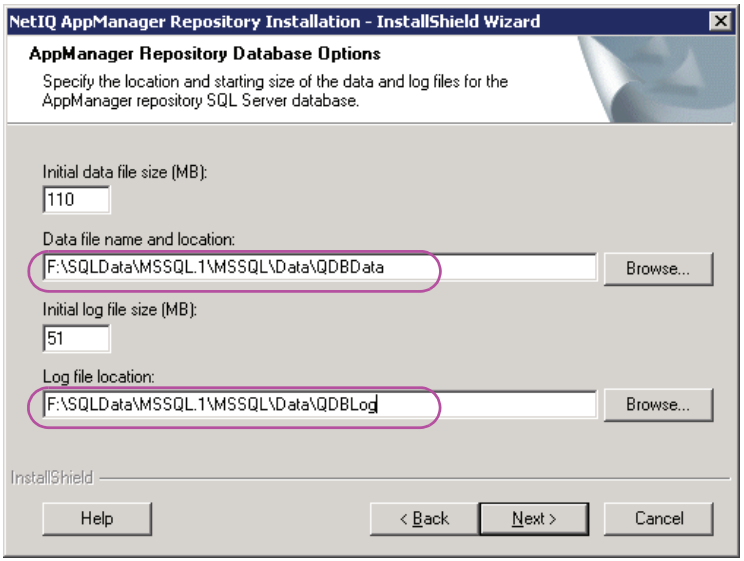
6 At the SQL Server Login dialog box, select the instance of SQL Server where you want to install the AppManager repository and click **Next** to use your current Windows credentials to log into SQL Server. You can install the AppManager repository on a default instance or a named instance of Microsoft SQL Server.



7 At the AppManager Repository Database Name dialog box, click **Next** to accept the default repository name, `QDB`.

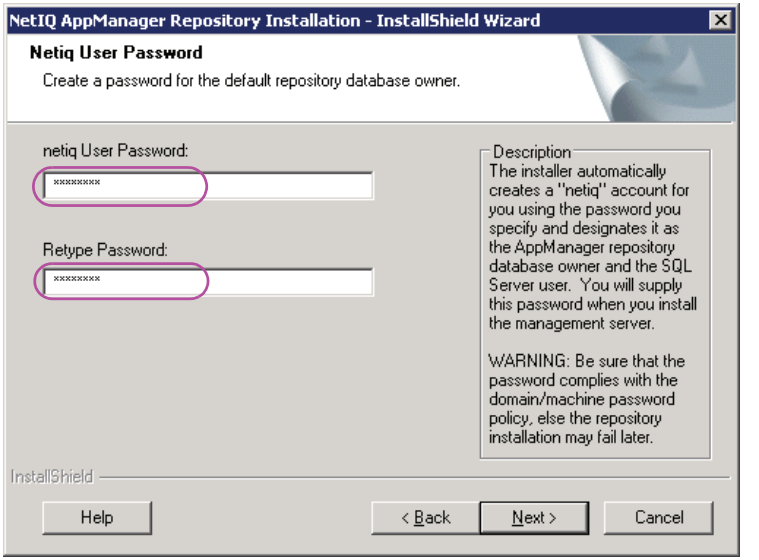


8 At the AppManager Repository Database Options dialog box, specify a location for the data and log files. NetIQ Corporation recommends that you install the data and log files on a *different* physical drive than the drive where the operating system is installed. For trial purposes, accept the default file sizes.



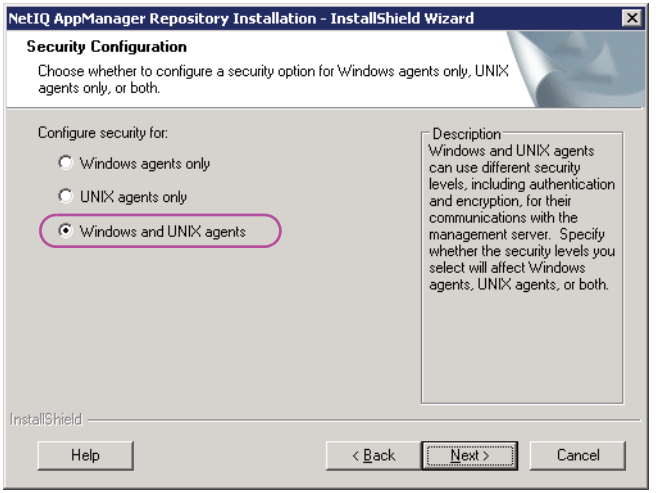
9 Click **Next**.

10 At the Netiq User Password dialog box, type a password for the netiq SQL login account that meets your Windows Password Security Policy. The netiq account is the AppManager administrator account. Keep the password for the netiq account nearby. Later in the installation, you will need to provide this password information again.

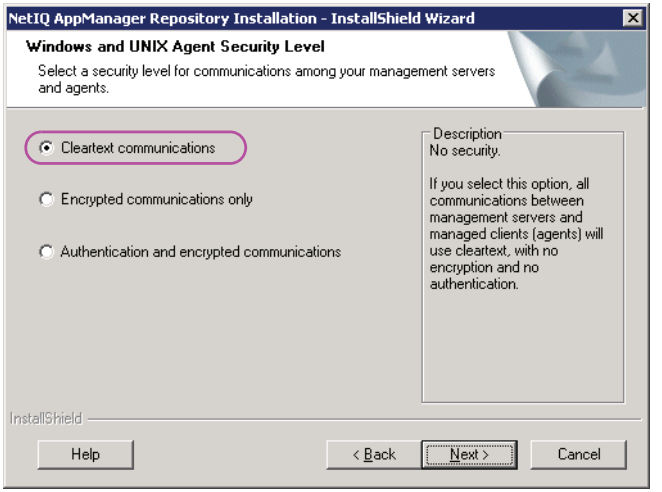


11 Click **Next**.

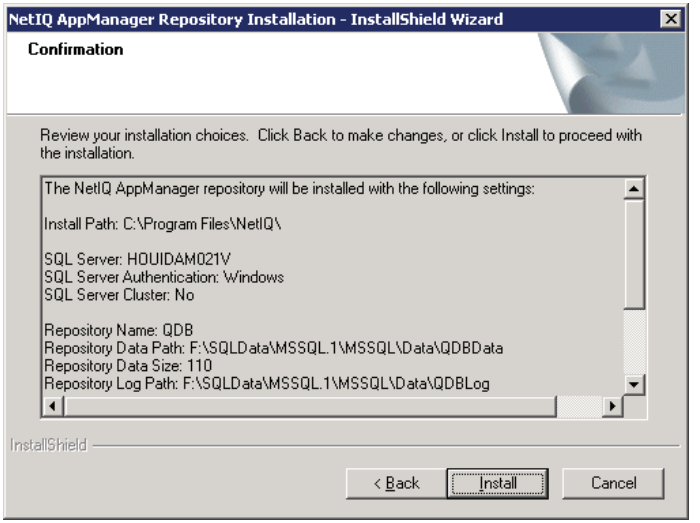
12 At the Security Configuration dialog box, click **Next** to accept the default value and configure the same communication level for agents on both Windows and UNIX computers.



13 At the Windows and UNIX Agent Security Level dialog box, click **Next** to accept the default option, **Cleartext communications**. Although cleartext communications between the agent and management server are not encrypted, **AppManager encrypts password information required by some Knowledge Scripts.**

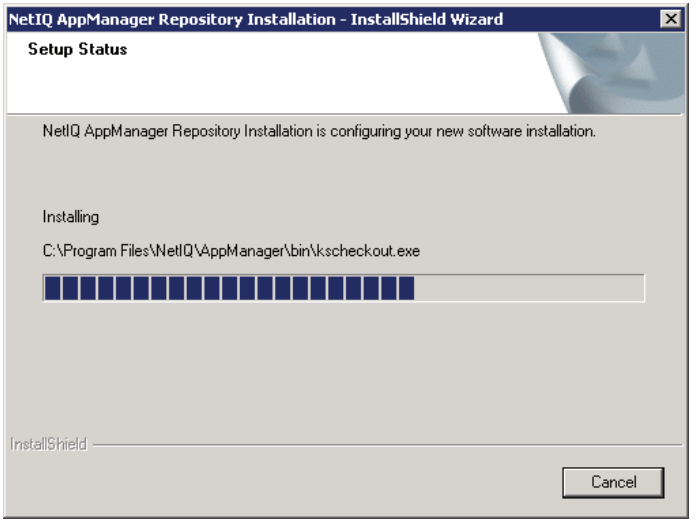


14 At the Confirmation dialog box, review the summary of the AppManager repository installation options.

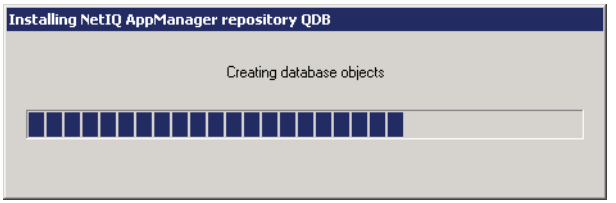


15 Click **Install**.

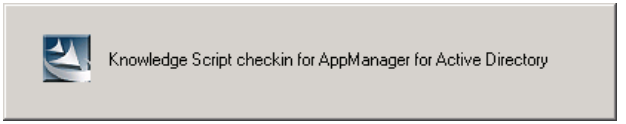
The Setup Status dialog box displays the installation progress as files are installed in the specified folder location.



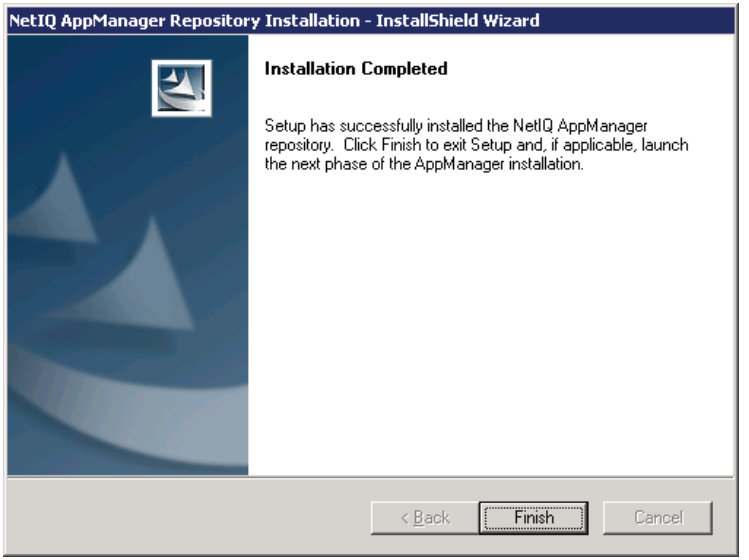
The progress meter displays the status of the database creation process.



The status updates as each Knowledge Script category is checked into the database. This process may take 30 to 90 minutes.



16 At the Completed dialog box, click **Finish**.



The installation process continues with the installation of the AppManager management server. For more information, see the "Installing the Management Server" on page 36.

Installing the Management Server

After the AppManager repository setup is finished, the setup process continues by installing the AppManager management server.

The **management server** manages event-driven communication between the AppManager repository, AppManager console programs such as the Operator Console, and agents.

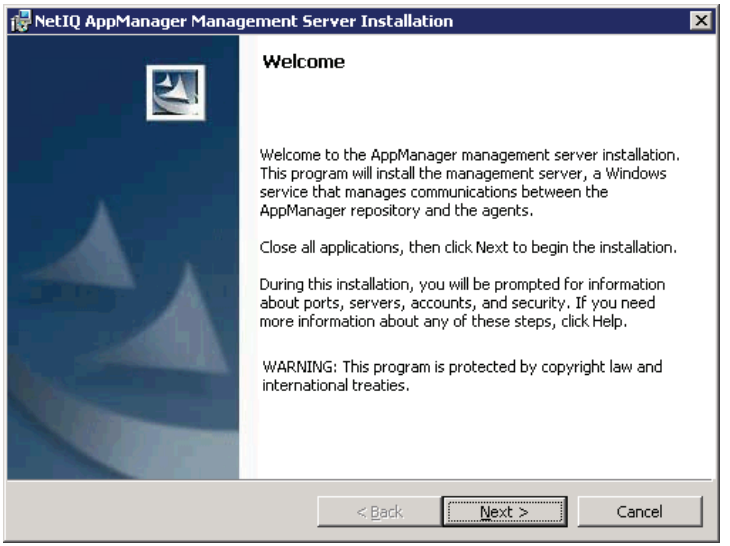
The agent is always installed with the management server.

For evaluation purposes:

- The management server is installed on the same computer as the AppManager repository. However, you typically install the management server on a dedicated computer to maximize the performance of the management server.
- Enable reporting capabilities for the agent on the management server computer. NetIQ Corporation recommends that in a production environment, you should run reports on a dedicated report agent to maximize resources available to the AppManager management server.

To install the AppManager management server:

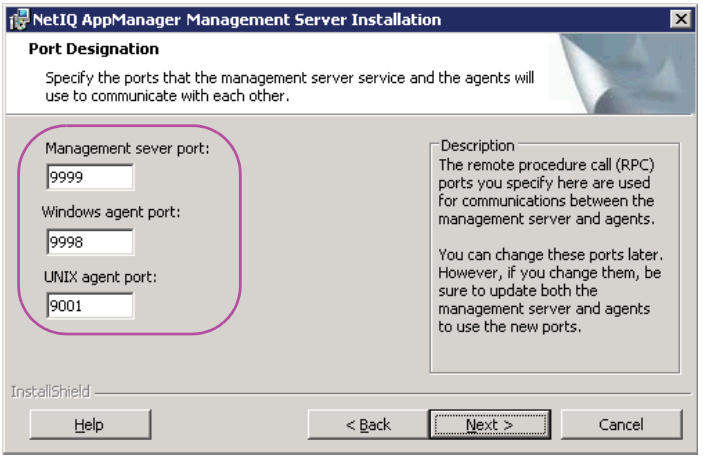
1 At the Welcome dialog box, click **Next**.



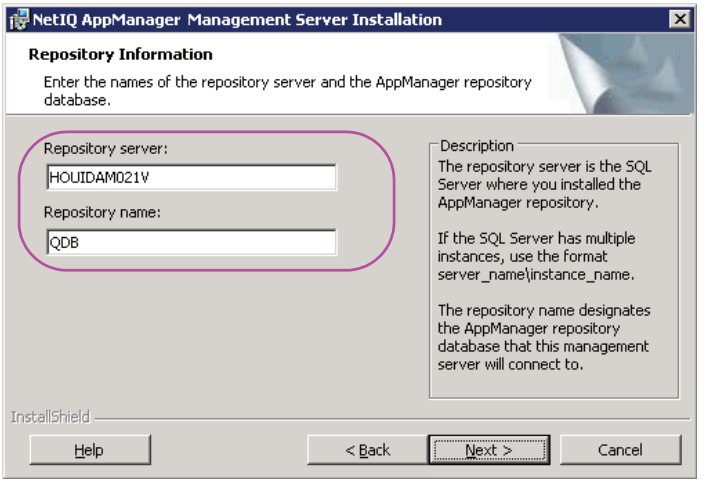
2 At the License Agreement dialog box, accept the license agreement and click **Next**.



3 At the Port Designation dialog box, click **Next** to accept the default RPC ports for the management server. To enable communication between the management server and agents, the agents require the same communication ports that you specify here.

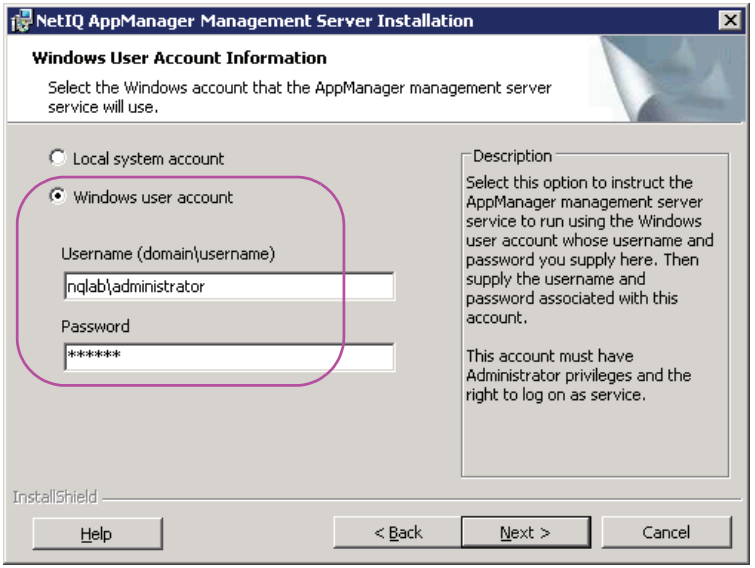


4 At the Repository Information dialog box, specify the name of the computer where you just installed the AppManager repository, and the name of the repository database. The management server communicates information from the agents to the specified repository database.



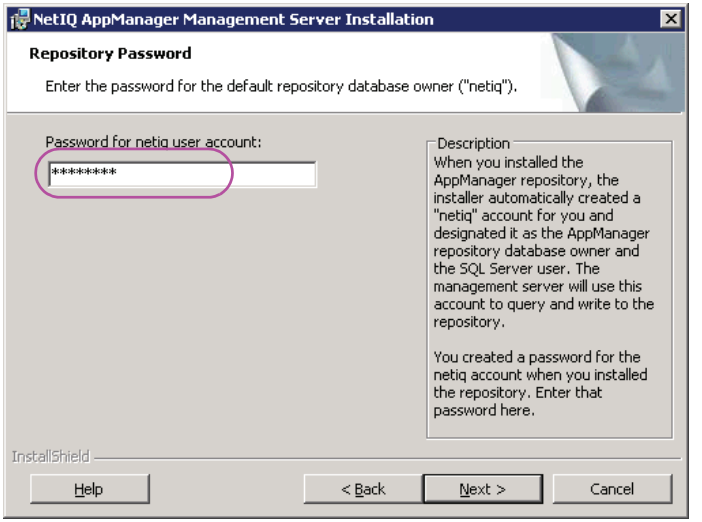
5 Click **Next**.

6 At the Windows User Account Information dialog box, select the **Windows user account** option and specify the Windows credentials you are using to install AppManager to run the NetIQ AppManager Management Service service.



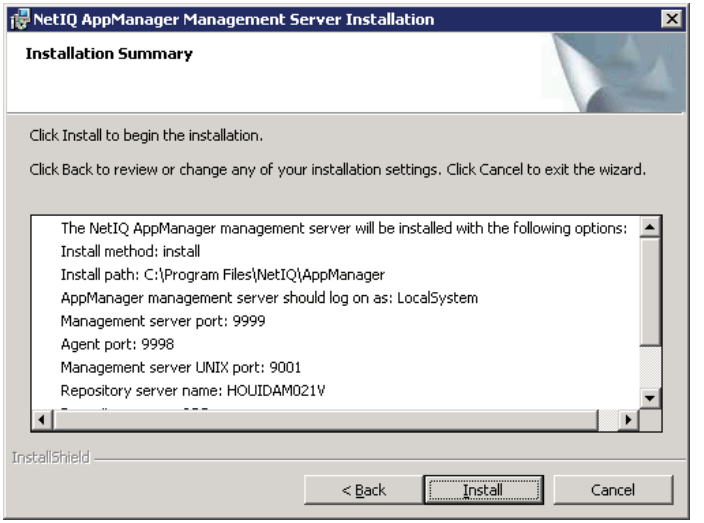
7 Click **Next**.

8 At the Repository Password dialog box, specify the administrator password you defined for the netiq account on Step 10 on page 32.



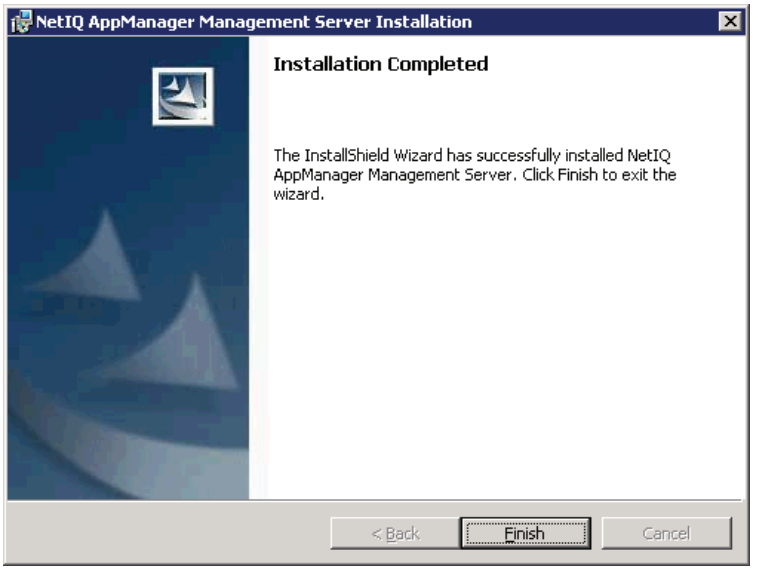
9 Click **Next**.

10 At the Installation Summary dialog box, review the summary of the management server installation options.



11 Click **Install**.

12 At the Installation Completed dialog box, click **Finish**.



The installation process continues with the installation of the agent. For more information, see the "Installing the AppManager Agent and Modules" on page 41.

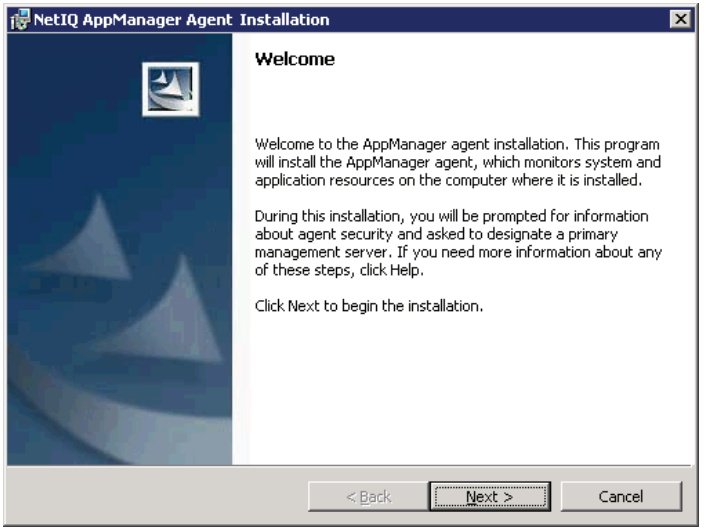
Installing the AppManager Agent and Modules

After the management server installation is finished, the setup program continues the process to install the agent and modules on the trial computer.

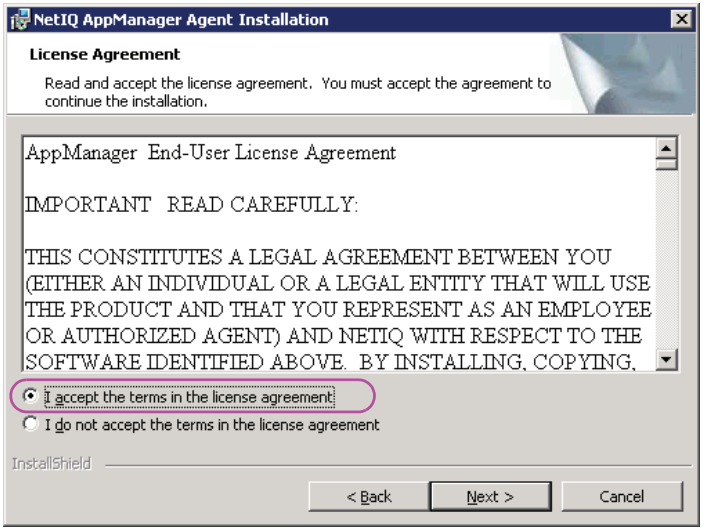
After you complete the trial installation, you can install agents and modules on the remote computers you want to monitor. For more information, see "Understanding Agent Deployment" on page 86 in the product tour.

To install the agent and modules:

1 At the Welcome dialog box, click **Next**.

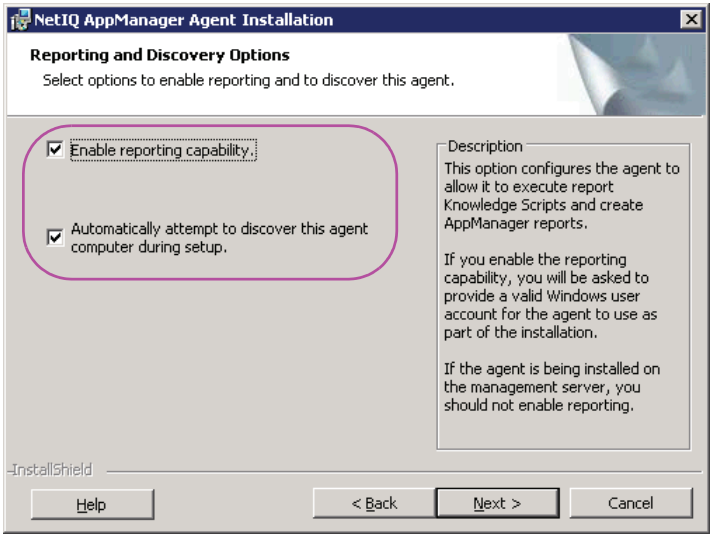


2 At the License Agreement dialog box, accept the license agreement and click **Next**.



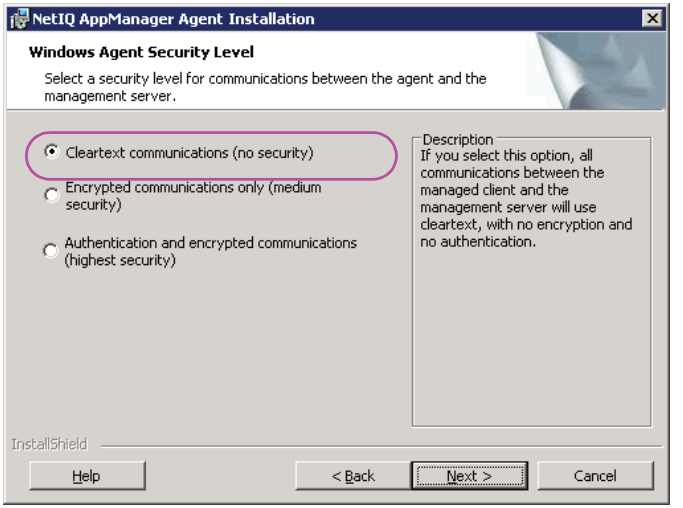
3 At the Reporting and Discovery Options dialog box:

- Select **Enable reporting capability**. The report agent functionality is required to run standard reports. For information about evaluating AppManager reports, contact your NetIQ Sales Representative or NetIQ Partner.
- Make sure **Automatically attempt to discover this agent** is selected. You must discover the agent to run jobs on the agent.

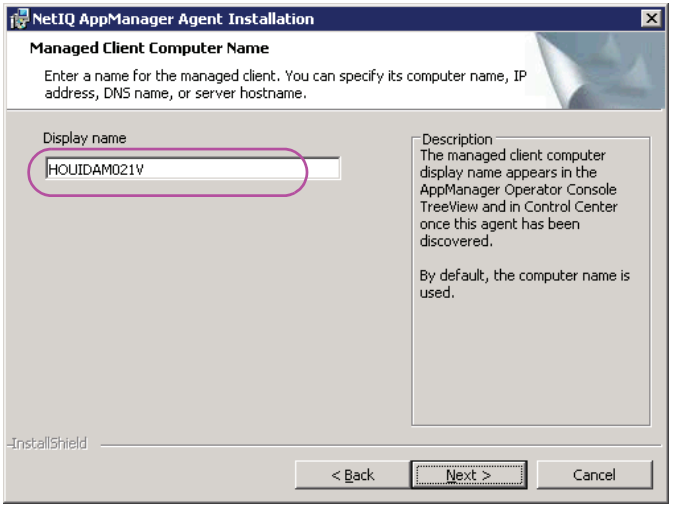


4 Click **Next**.

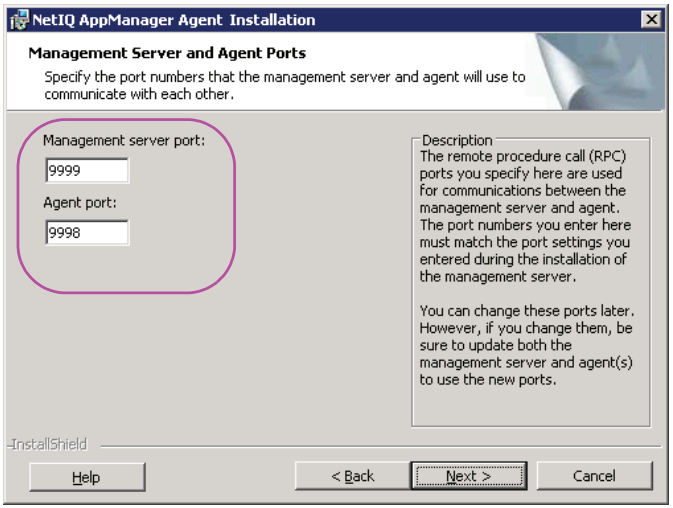
5 At the Windows Agent Security Level dialog box, click **Next** to accept the default value to configure the agent to use the same cleartext communication method that you configured for the management server in Step 13 on page 33.



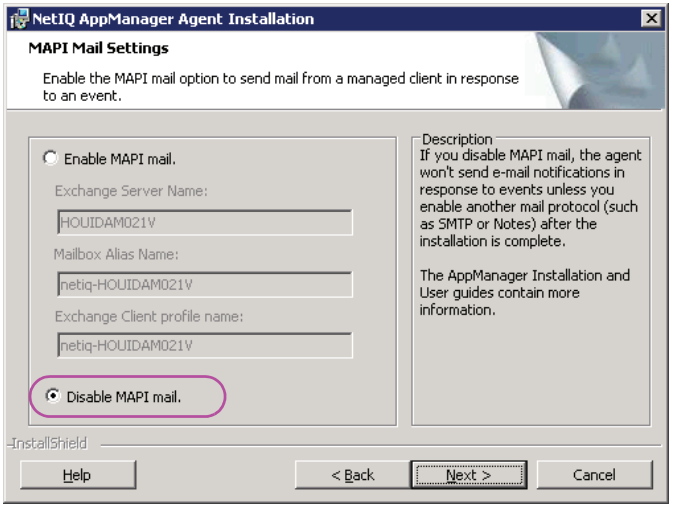
6 At the Managed Client Computer Name dialog box, click **Next** to accept the default value and display the DNS name of the computer in the Control Center Console.



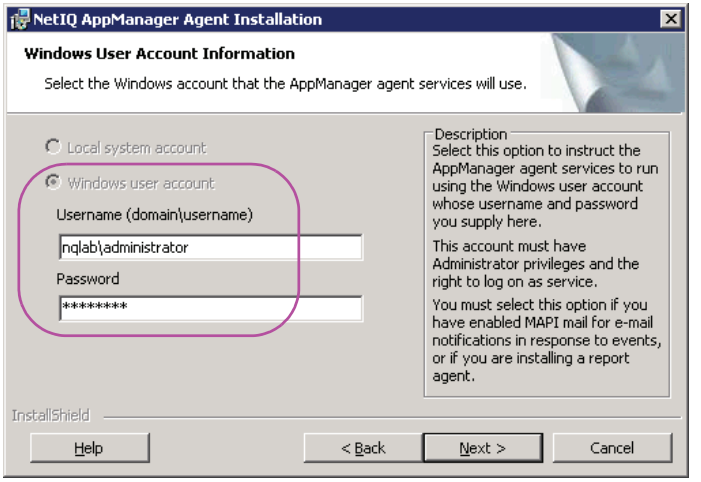
7 At the Management Server and Agent Ports dialog box, click **Next** to accept the default values and configure the agent to use the same communication ports that you configured for the management server in Step 3 on page 38.



8 At the MAPI Mail Settings dialog box, you can enable the agent to send an e-mail message as a responsive action for a job. For trial purposes, accept the default value and click **Next**.

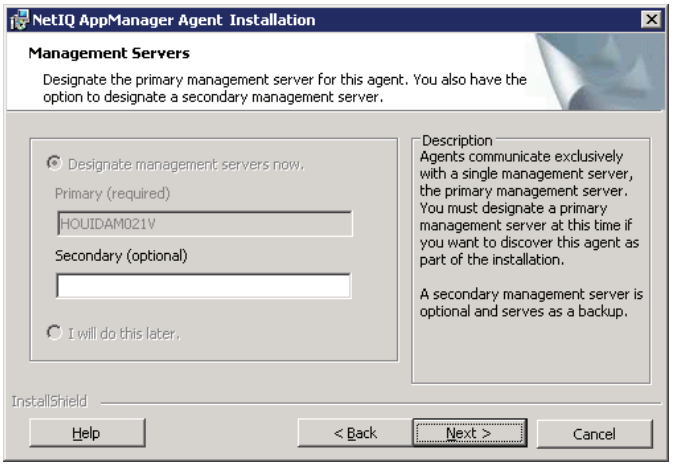


9 At the Windows User Account Information dialog box, specify the Windows credentials you are using to install AppManager to run the the agent services.

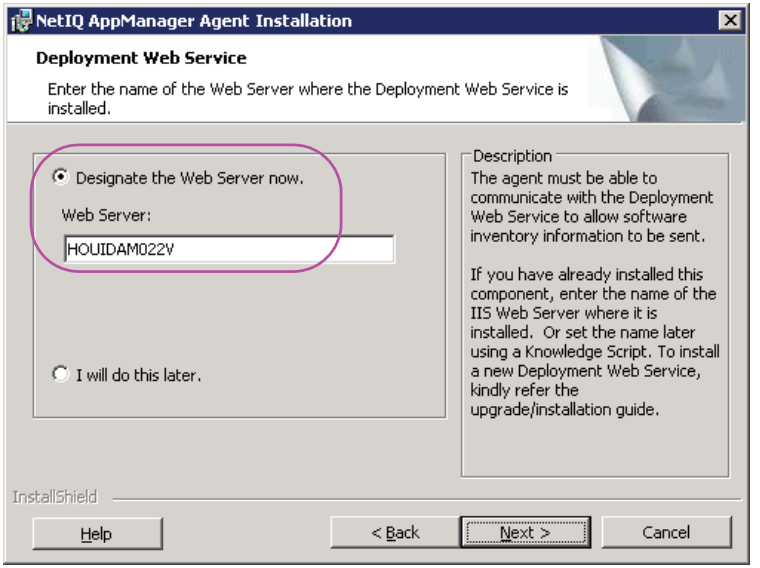


10 Click **Next**.

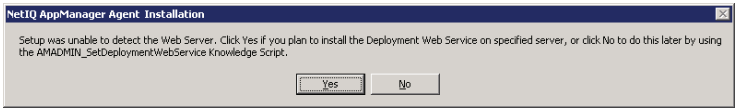
11 At the Management Servers dialog box, click **Next** to designate the management server on the local computer as the agent's **primary management server**. The agent only accepts communication from its designated primary management server.



12 At the Deployment Web Service dialog box, click **Next** to accept the default and configure the agent to report its software inventory information, such as its agent version and any installed modules, to the deployment web server on the local computer. Later, when you install Control Center, you will install the deployment web server on the local computer.

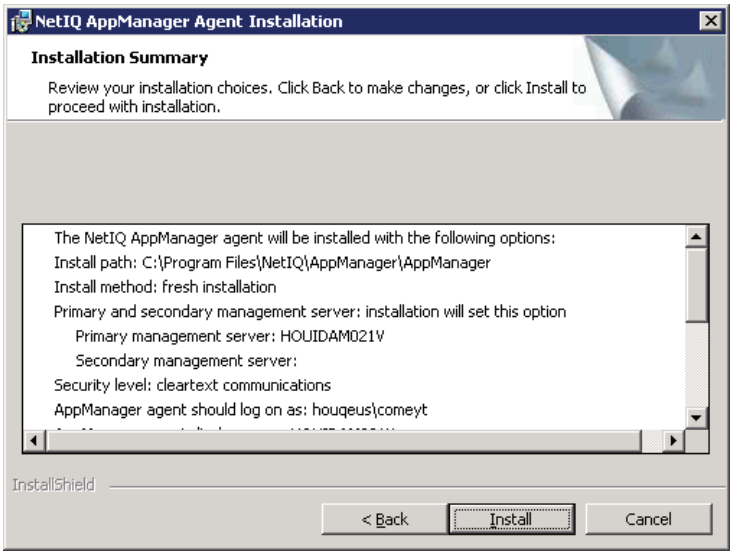


13 The installation program prompts you to continue because the deployment web service is not installed on the local computer. Because you will install the deployment web service later, click **Yes** to proceed.



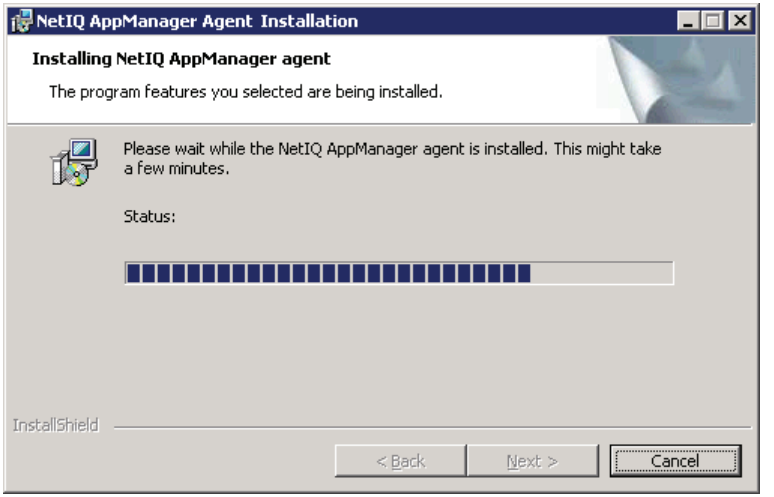
Tip The deployment web server is installed later as part of the Control Center installation.

14 At the Installation Summary dialog box, review the summary of the agent installation options.

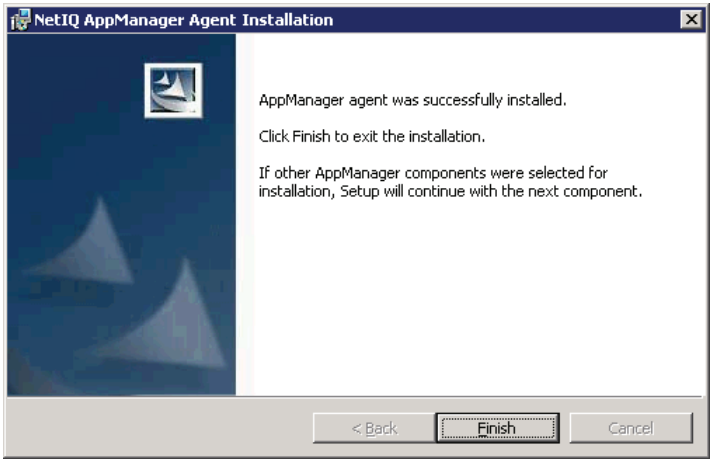


15 Click **Install**.

The Installing NetIQ AppManager Agent dialog box displays the installation progress.



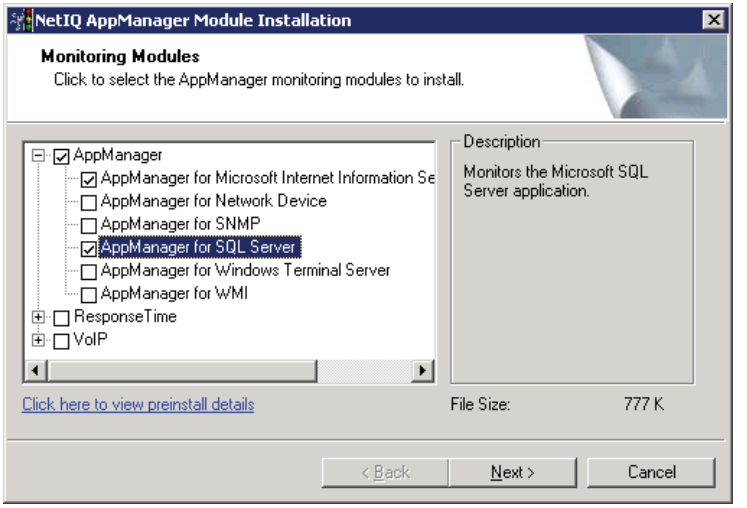
16 At the Completed dialog box, click **Finish**.



17 The installation process continues with the installation of the AppManager modules. A **module** provides monitoring support for an application.

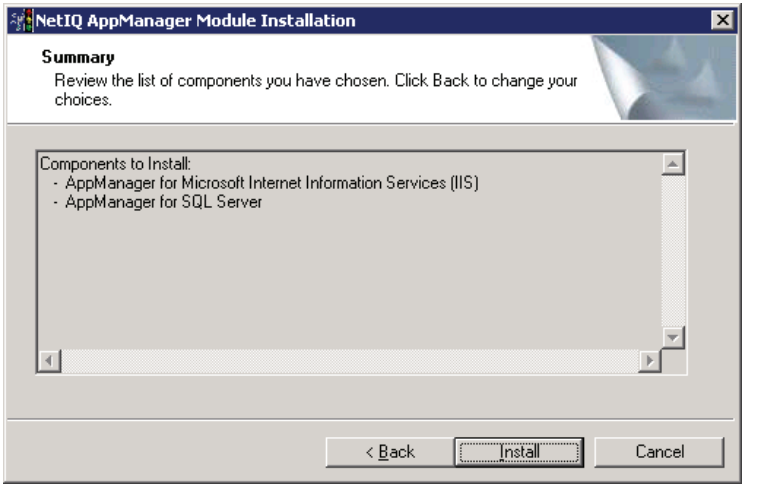
In the Monitoring Modules dialog box, select the check boxes for:

- AppManager for Microsoft Internet Information Service
- AppManager for Microsoft SQL Server.



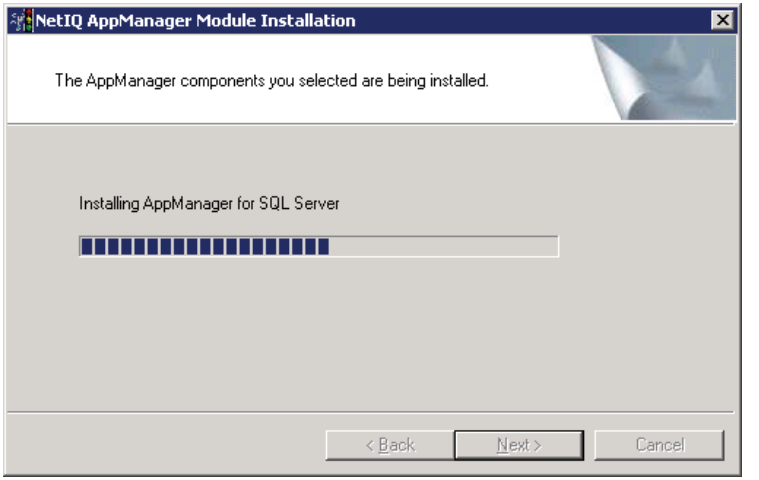
18 Click **Next**.

19 At the Summary dialog box, review the summary of the modules that will be installed.

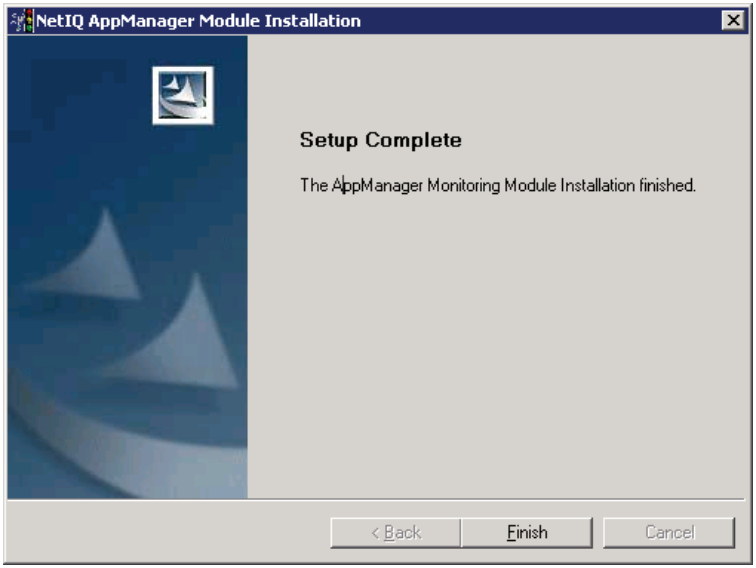


20 Click **Install**.

The Setup Status dialog box displays the progress of the module installation.



21 At the Setup Complete dialog box, click **Finish**.



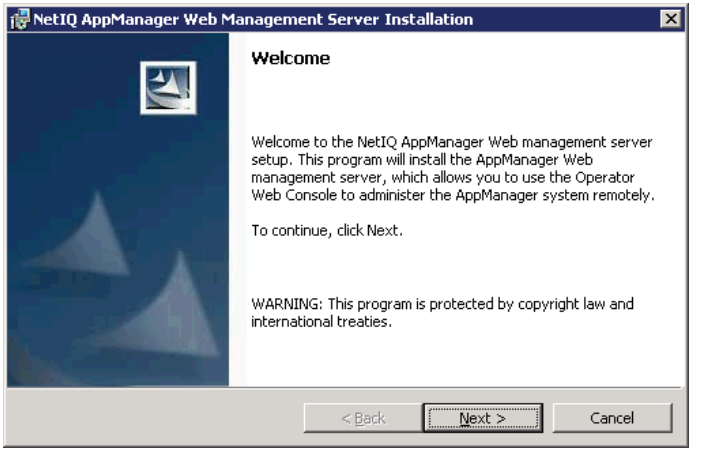
The installation process continues with the installation of the AppManager Web management server. For more information, see "Installing the Web Management Server" on page 52.

Installing the Web Management Server

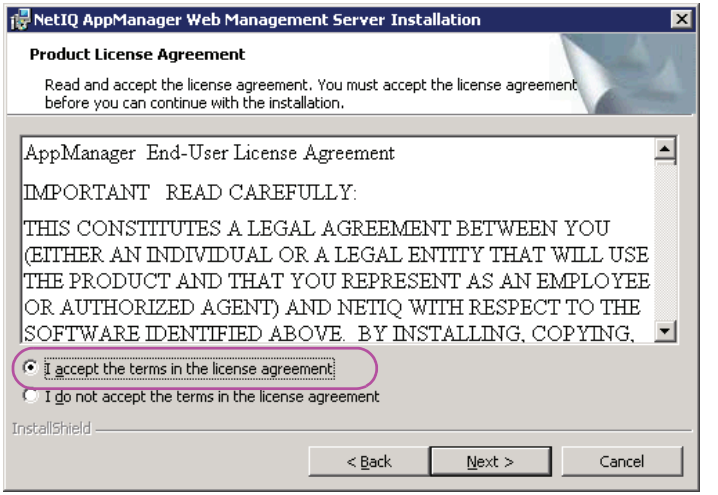
After the agent setup is finished, the setup process continues by installing the AppManager Web management server.

To install the AppManager Web management server:

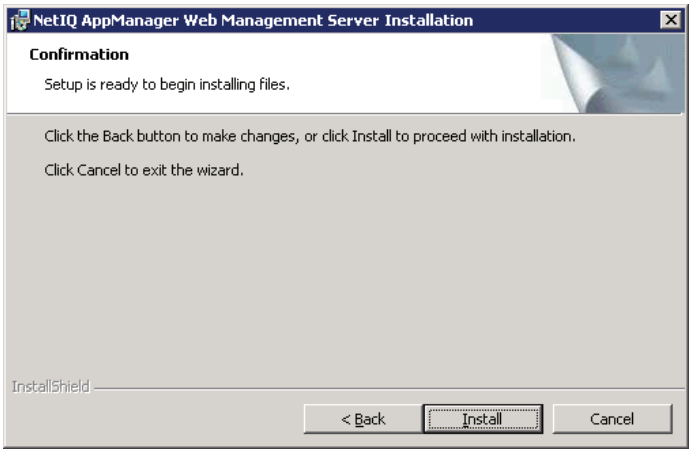
1 At the Welcome dialog box, click **Next**.



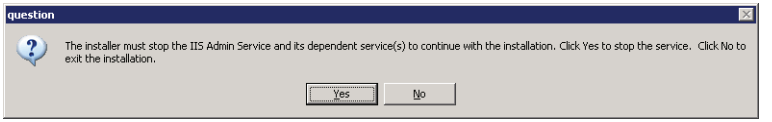
2 At the Product License Agreement dialog box, accept the license agreement and click **Next**.



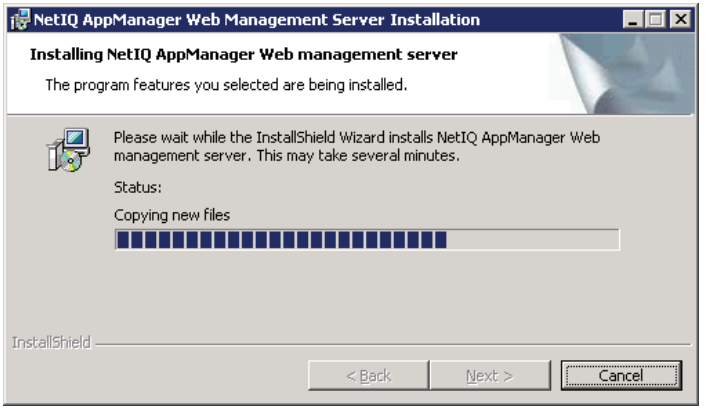
3 At the Confirmation dialog box, click **Install**.



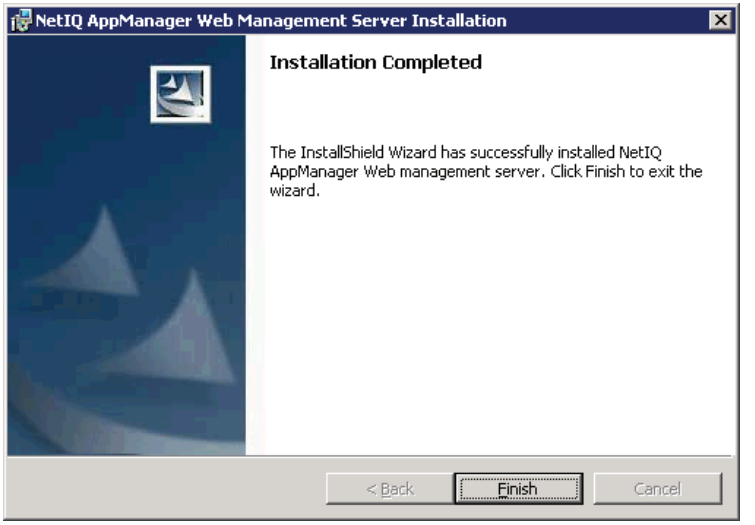
4 ***If the Control Center Console displays the following dialog box***, click **Yes** to allow the setup program to stop the IIS-related services. When the setup program finishes, the setup program automatically restarts the services.



The Installing NetIQ AppManager Web Management Server dialog box displays the installation progress.



5 At the Installation Completed dialog box, click **Finish**.



The installation process continues with the installation of Control Center. For more information, see "Installing Control Center" on page 54.

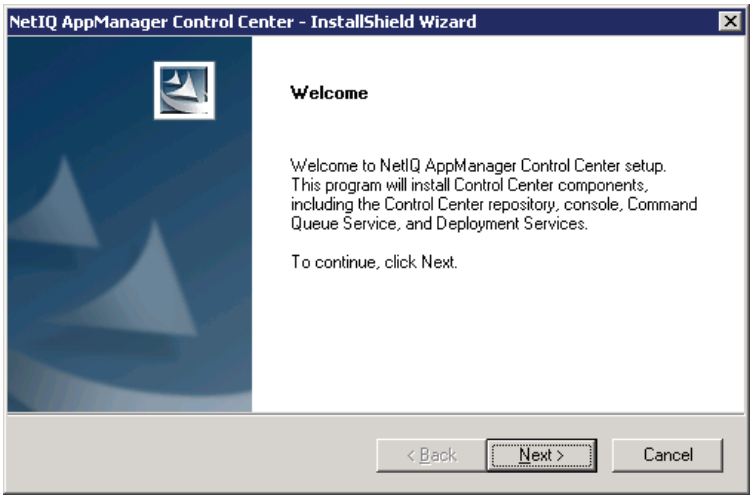
Installing Control Center

After the AppManager Web management server setup is finished, the setup process continues by installing Control Center, which includes the:

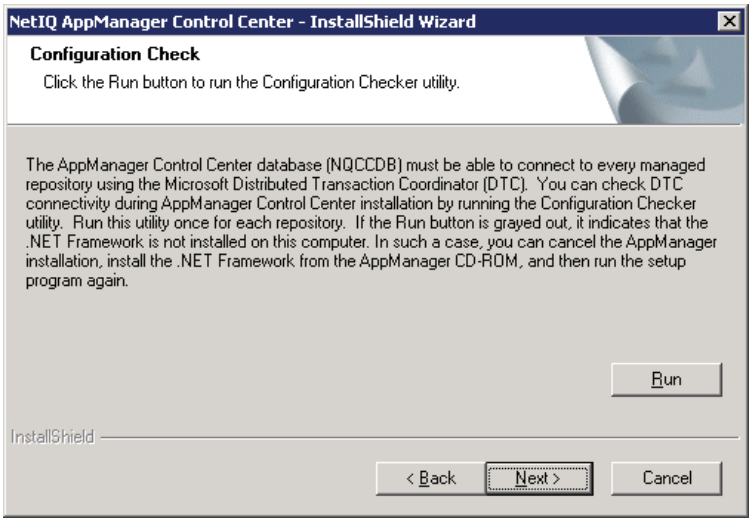
- Control Center repository database
- Control Center Command Queue Service
- Control Center Deployment Web Service
- Control Center Deployment Service
- Control Center Console

To install Control Center:

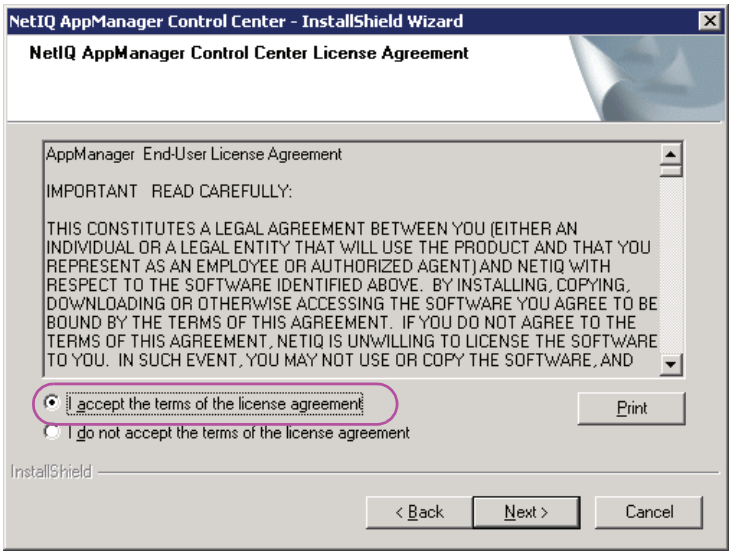
1 At the Welcome dialog box, click **Next**.



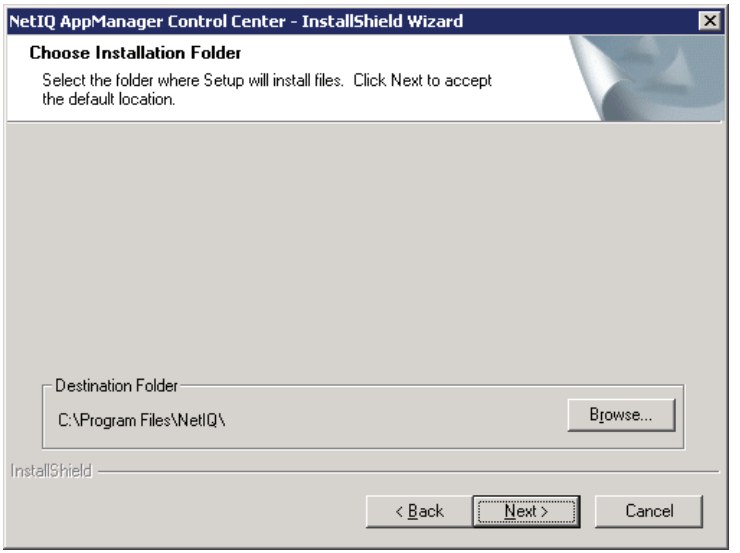
2 At the Configuration Check dialog box, click **Next** to skip the configuration check. This check is not needed when all AppManager components are on the same computer.



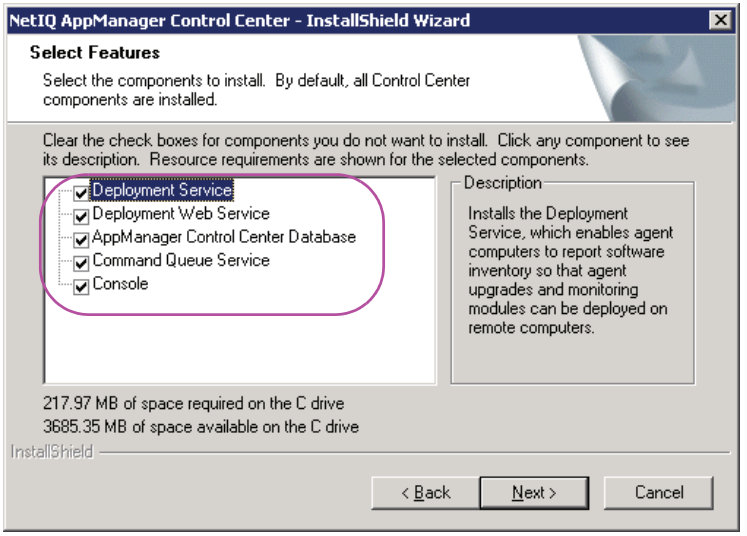
3 At the NetIQ AppManager Control Center License Agreement dialog box, accept the license agreement and click **Next**.



4 At the Choose Installation Folder dialog box, click **Next** to install Control Center in the default folder location.

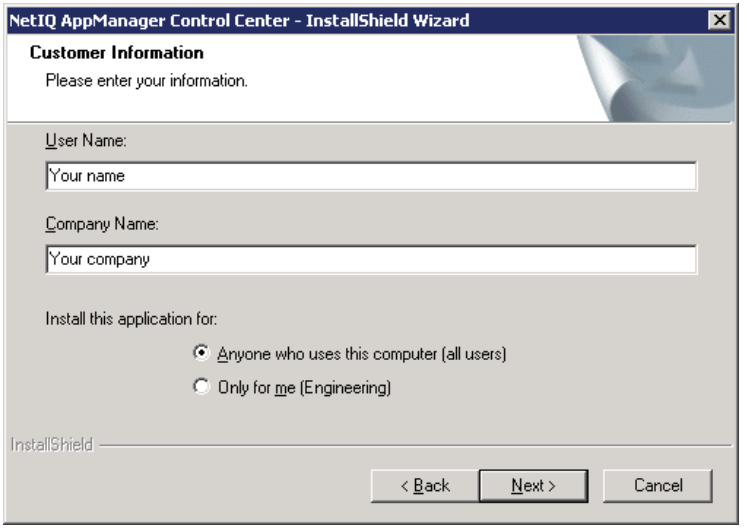


5 At the Select Features dialog box, select *all* of the components.



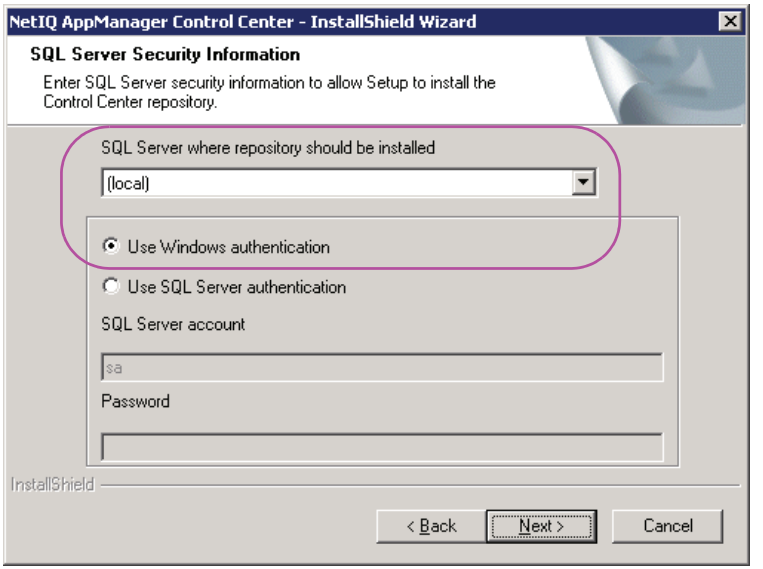
6 Click **Next**.

7 At the Customer Information dialog box, type your name and company information.

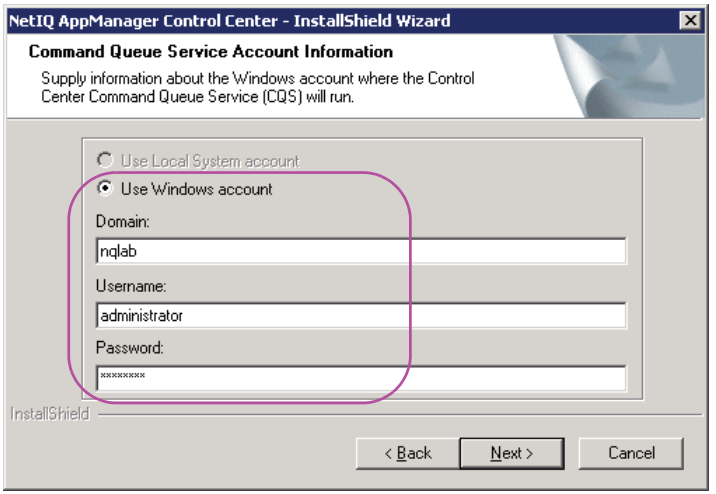


8 Click **Next**.

9 At the SQL Server Security Information dialog box, select the instance of SQL Server where you want to install the Control Center repository and click **Next** to use your current Windows credentials to log into SQL Server. You can install the Control Center repository on a default instance or a named instance of Microsoft SQL Server.

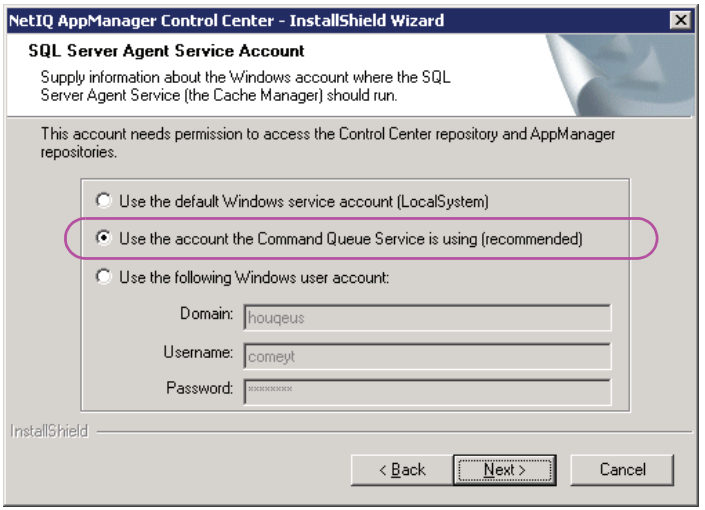


10 At the Command Queue Service Account Information dialog box, specify the Windows credentials you are using to install AppManager to run the **Command Queue Service**.

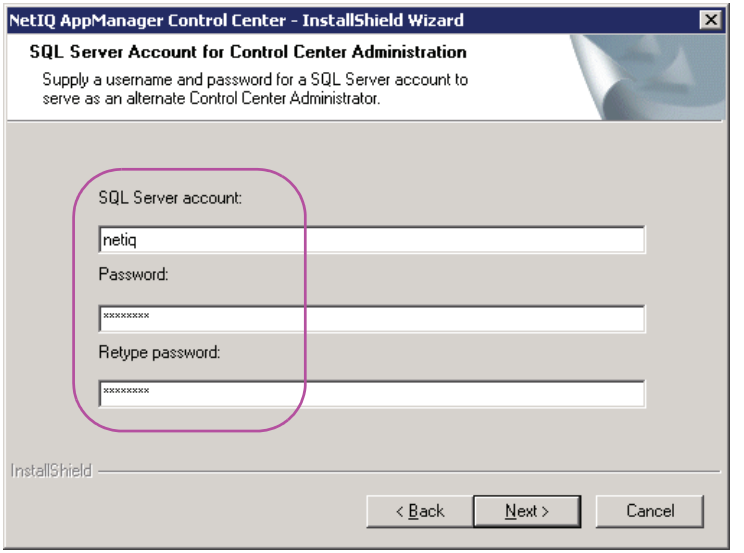


11 Click **Next**.

12 At the SQL Server Agent Service Account dialog box, click **Next** to configure the Control Center Cache Manager, `nqsyncqdb.exe`, to use the same credentials as the Control Center Command Queue Service.

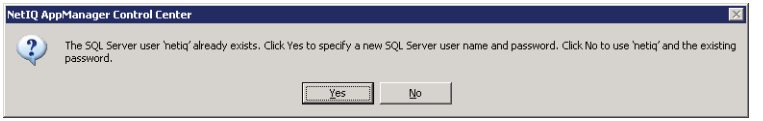


13 At the SQL Server Account for Control Center Administration dialog box, specify the netiq account as the alternate administrator account for Control Center and specify the password you defined for the netiq account on Step 10 on page 32.

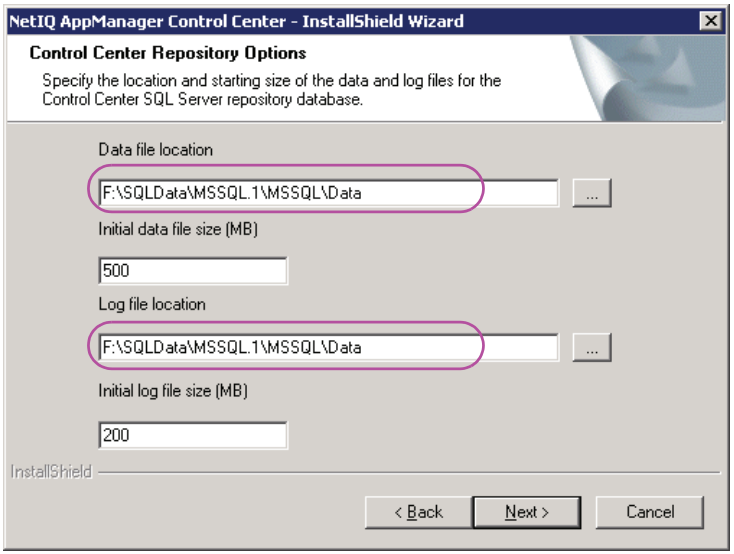


14 Click **Next**.

15 The dialog box indicates the netiq account already exists and prompts you to create a new account. Do *not* create a new account. Click **No** to use the existing netiq account.

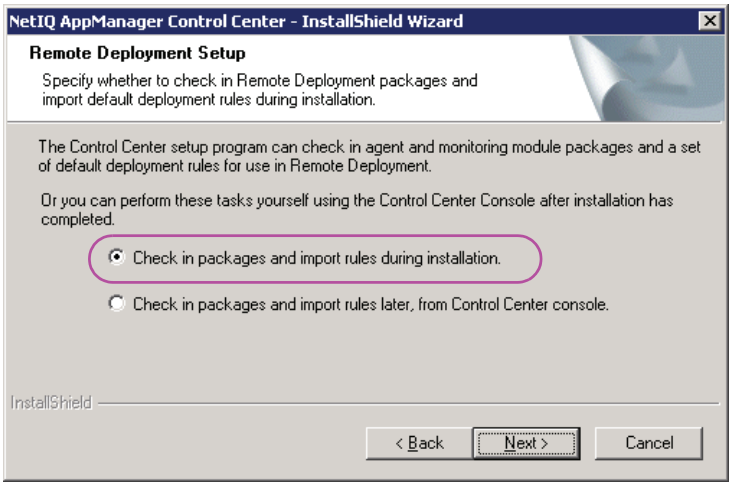


16 At the Control Center Repository Options dialog box, specify a location for the data and log files. NetIQ Corporation recommends that you install the data and log files on a *different* physical drive than the drive where the operating system is installed. For trial purposes, accept the default file sizes.

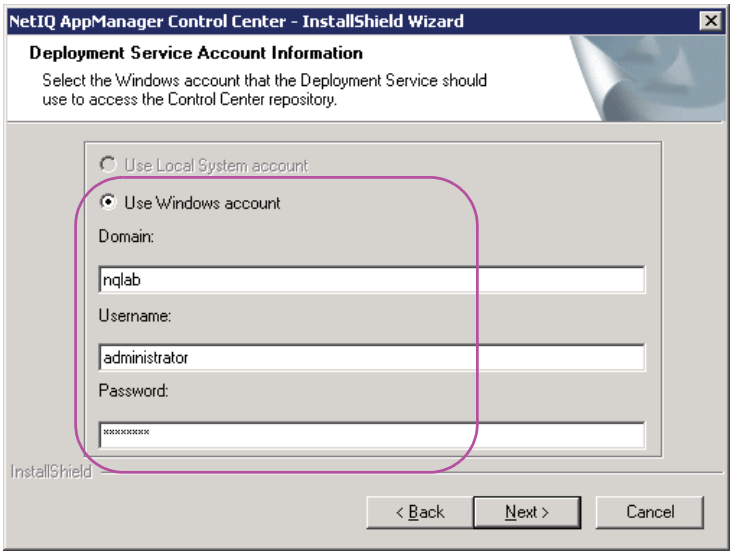


17 Click **Next**.

18 At the Remote Deployment Setup dialog box, click **Next** to accept the default option to check the agent- and module-related deployment packages and rules into the Control Center web depot.

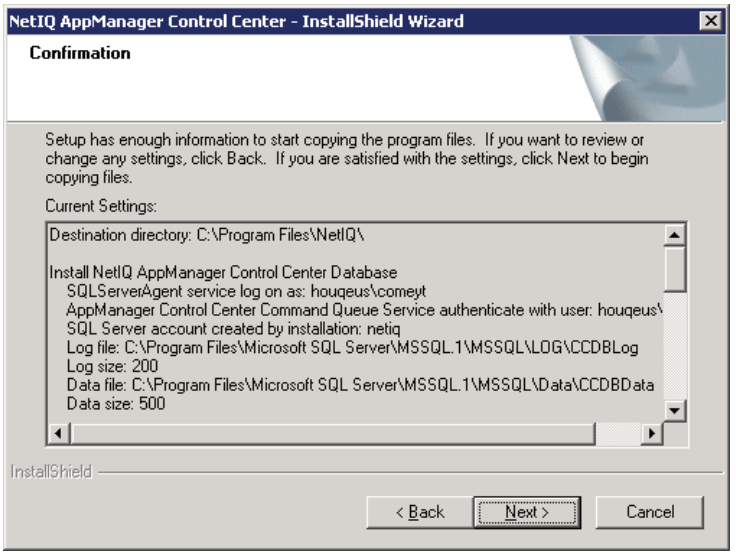


19 At the Deployment Service Account Information dialog box, specify the Windows credentials you are using to install AppManager to run the Control Center Deployment Service.



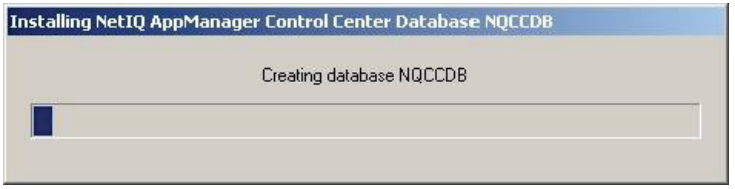
20 Click **Next**.

21 At the Confirmation dialog box, review the summary of the Control Center installation options.

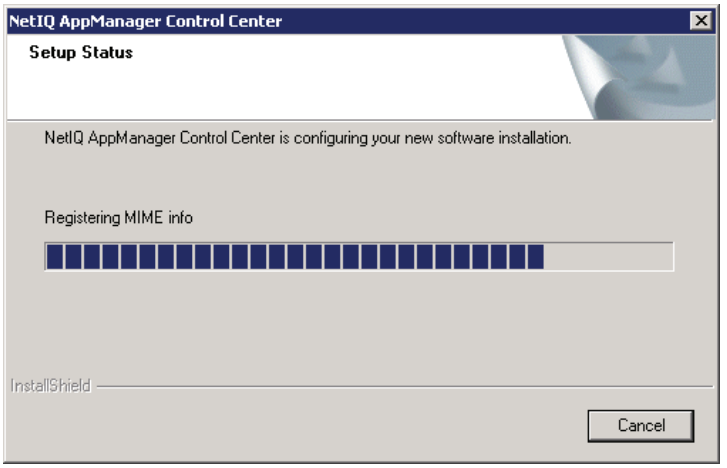


22 Click **Install**.

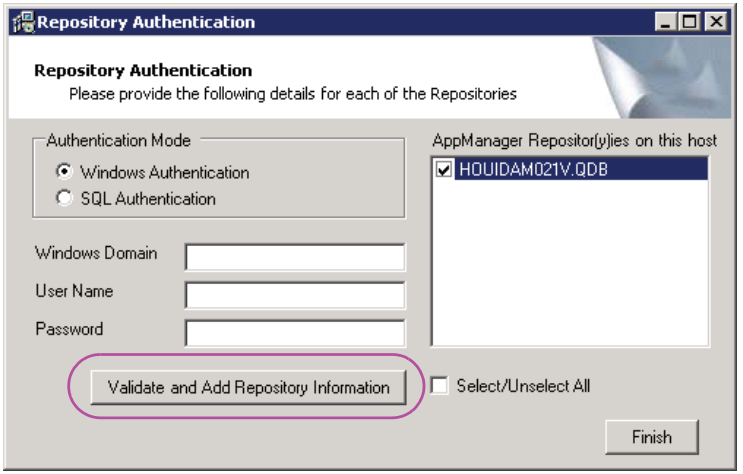
The dialog box displays the installation status of the Control Center repository database.



After the database is created, the Setup Status dialog box displays the installation progress.



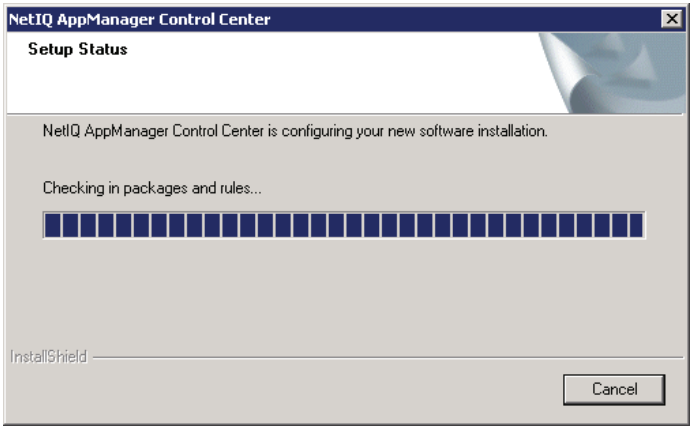
23 At the Repository Authentication dialog box, click **Validate and Add Repository Information** to add the AppManager repository to Control Center.



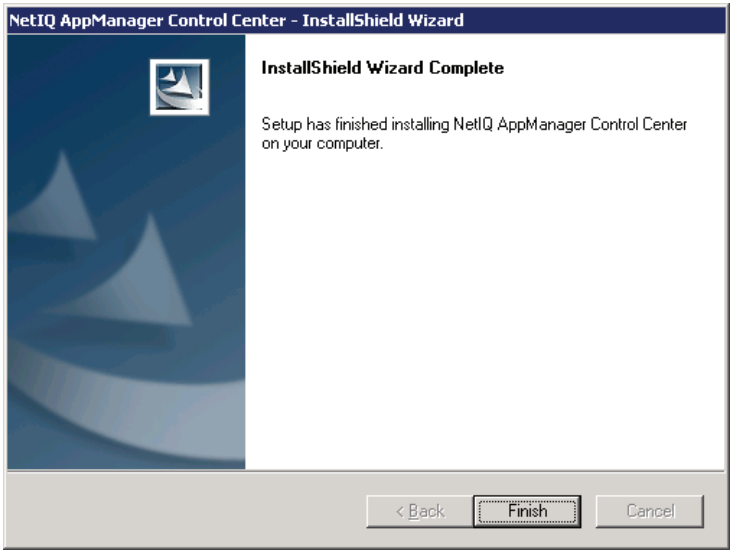
Tip If you skip this step, you can add the repository to Control Center after you have completed the installation. For more information, see Step 5 on page 75.

24 Click **Finish**.

The Setup Status dialog box displays the progress of adding the AppManager repository to Control Center.



25 At the InstallShield Wizard Complete dialog box, click **Finish**.



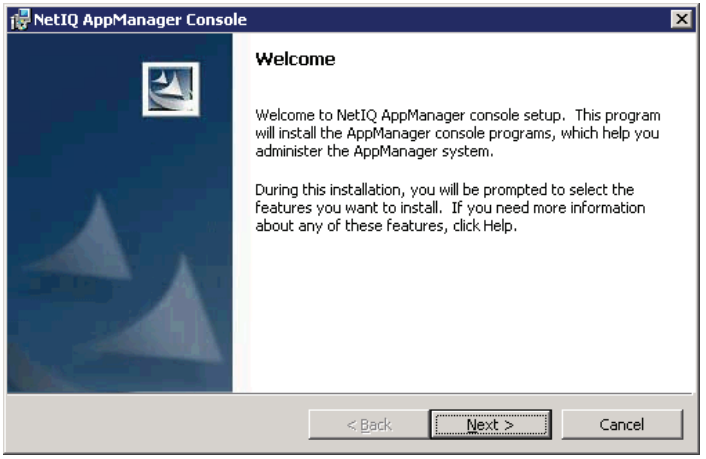
The installation process continues with the installation of the AppManager console applications. For more information, see "Installing the AppManager Console Applications" on page 67.

Installing the AppManager Console Applications

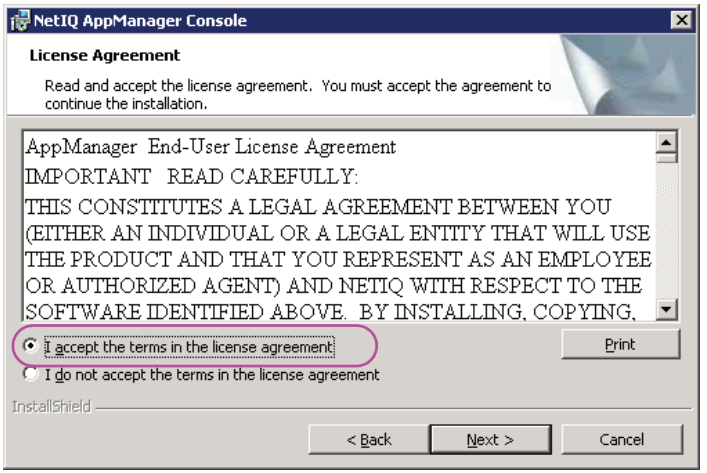
After the Control Center setup is finished, the setup process continues by installing the AppManager console applications, such as the AppManager Operator Console.

To install the AppManager console applications:

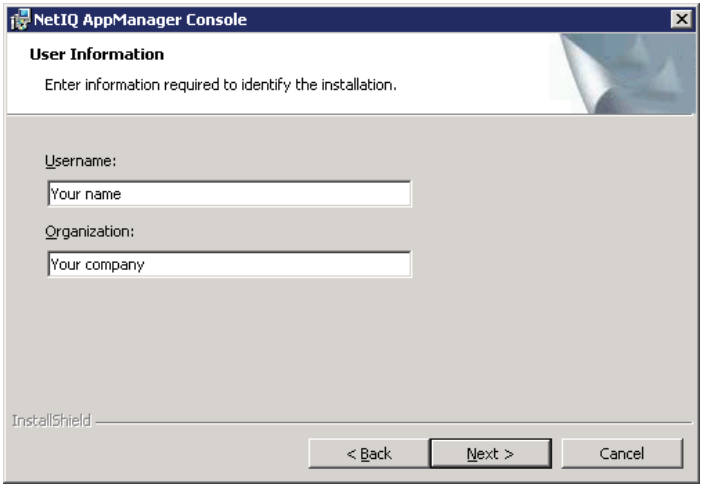
1 At the Welcome dialog box, click **Next**.



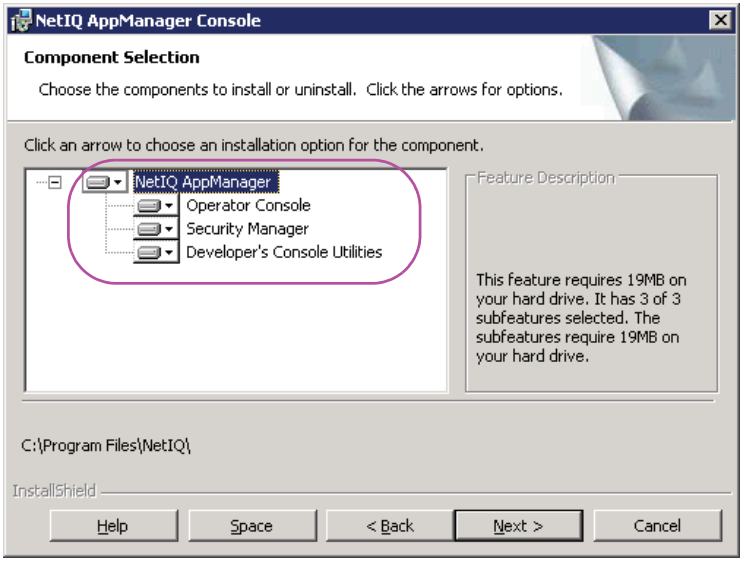
2 At the License Agreement dialog box, accept the license agreement and click **Next**.



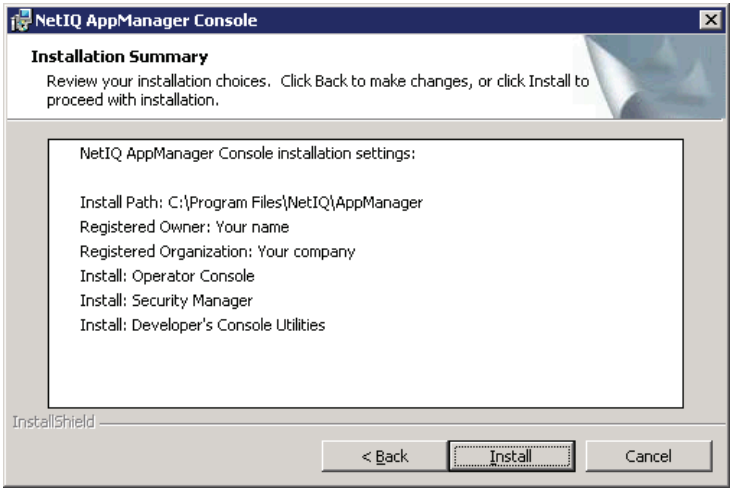
3 At the User Information dialog box, type your name and company information, then click **Next**.



4 At the Component Selection dialog box, click **Next** to select all AppManager console applications.

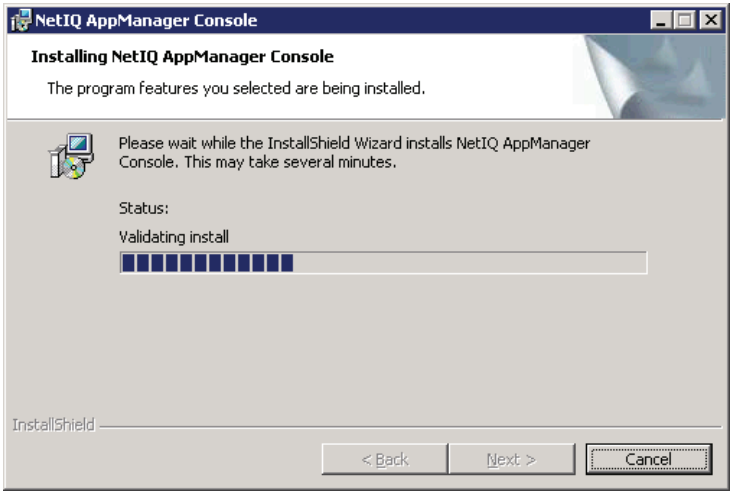


5 At the Installation Summary dialog box, review the summary of AppManager console applications and verify the Operator Console, Security Manager, and Developer's Console Utilities will be installed.

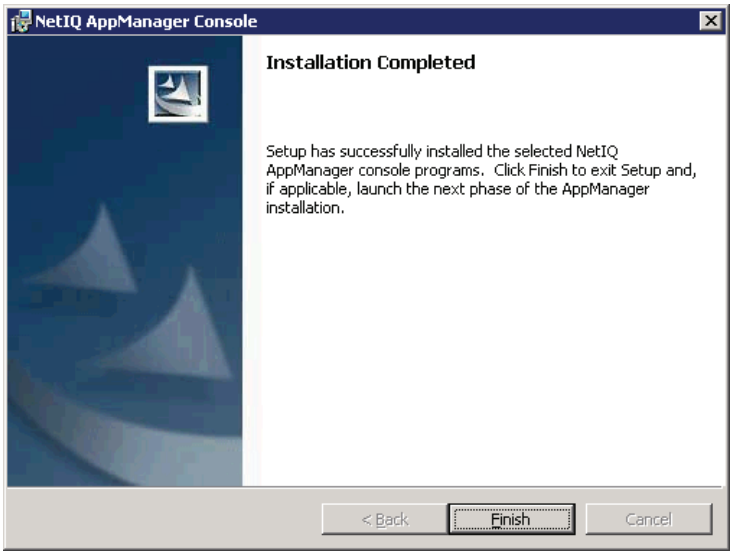


6 Click **Install**.

The Installing NetIQ AppManager Console dialog box displays the installation progress.



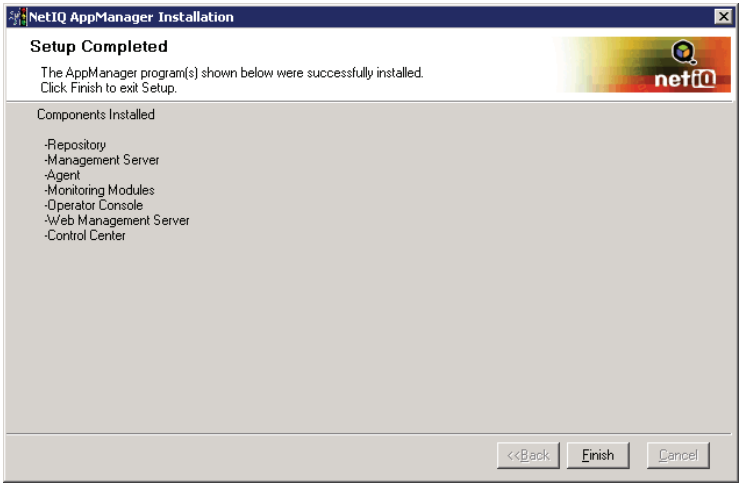
7 At the Installation Completed dialog box, click **Finish**.



The status dialog box displays the installation activity of the online help. The installation of the help can take from 5 to 60 minutes to complete.



8 At the Setup Completed dialog box, click **Finish**.



You are now ready to begin the product tour. For more information, see Chapter 3, "Exploring AppManager."

Chapter 3

Exploring AppManager

This chapter describes the Control Center Console and guides you through some of the key features of AppManager. Follow the tasks in each section in order. If you skip between sections, you may need to perform some prerequisite tasks.

After you complete the product tour in this chapter, continue to explore other areas of AppManager:

- Creating service maps
- Running AppManager reports
- Developing smarter monitoring rules through Performance Profiler
- AppManager for UNIX solutions
- AppManager for VoIP solutions

For more information about these features, contact your NetIQ Sales Representative or NetIQ Partner.

Before you begin, make sure you have properly installed and configured AppManager. For more information, see Chapter 2, "Installing AppManager."

Starting the Control Center Console

As a Control Center Console administrator, you have permission to start the Control Center Console and access all management groups. To enable other users to access the Control Center Console and its management groups, configure Control Center Console security. For information about configuring user access to Control Center Console, see the *Control Center User Guide for AppManager*.

On the computer where you installed all AppManager components, make sure you are logged in with the same credentials you used to install AppManager.

To start the Control Center Console:

1. Start the **AppManager Control Center** in the **NetIQ > AppManager** program group.
2. At the AppManager Control Center Console Logon dialog box, type the name of the trial computer. If you installed the Control Center repository on a named instance of SQL Server, specify the server name using the *computer_name**instance_name* format. For example:



3 Click **Logon**.

4 ***If you cannot log in using your Windows credentials***, clear the **Use Windows authentication** check box and specify the **netiq** SQL account you created during the installation, and then click **Logon**.

5 ***If the Getting Started pane indicates that*** `No Repositories` ***exist***, you did not designate the repository as described in Step 23 on page 65.

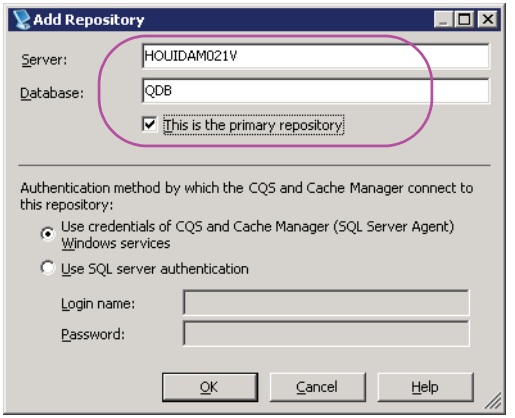


To resolve this problem, add the AppManager repository to Control Center by completing the following steps:

a. In the Control Center Console, click **File > Manage Repositories**.

b. In the Manage Repositories dialog box, click **Add**.

c. In the Add Repository dialog box, specify the AppManager repository details.



For	Do this
Server	Type the name of the computer where you installed all of the AppManager components. When specifying a computer name, specify the NETBIOS name. For example, to specify a named instance, specify `TXAM01\INST1`.
Database	Type the name of the AppManager repository database. The default database name is `QDB`.
This is the primary repository	Select this check box to designate the specified AppManager repository as the primary AppManager repository for Control Center. Control Center requires you to designate one AppManager repository as the primary AppManager repository.
Authentication method	Accept the default option, **Use credentials of CQS and Cache Manager (SQL Server Agent) Windows services**. This option specifies that SQL Server uses the credentials of the **Control Center Command Queue Service** and the **SQL Server Agent** service to access the repository database.

d. Click **OK**.

You are now ready to explore the Control Center Console. For more information, see "Understanding Management Groups" on page 77.

Understanding Management Groups

The Control Center Console uses management groups to organize and manage the computers in your AppManager environment. You can configure a management group to include managed client computers based on:

- AppManager repository views such as NT or SQL
- Rules that select computers based on their properties, such as the name of the computer or discovered resources

Rule-based management groups allow administrators to define criteria for grouping servers. Computers that match the criteria are automatically displayed in the management group.

Tip The Control Center administrator gives users access to each management group in the Control Center Console. By default, a Control Center Console user does not have permission to access any management groups. As the administrator for Control Center, you have full permissions on all management groups.

About Control Center Console Views

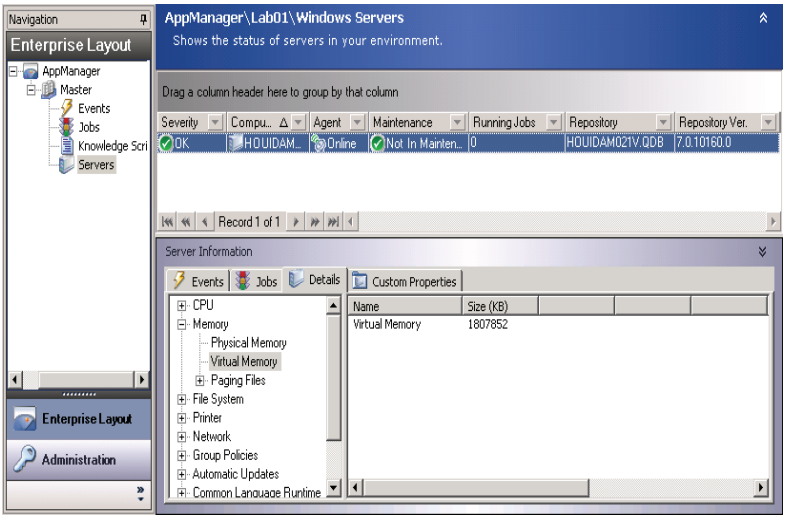
To help you manage the computers in a management group, the Control Center Console includes **views**. The standard views in a management group are:

- **Server view** Displays a list of servers in the management group. Select a server from the grid list to display server information and perform common tasks like responding to events, managing jobs and custom properties, and viewing discovery details.
- **Job view** Displays a list of jobs on the computers in the management group.

- **Event view** Displays a list of events in the management group. Use the grid to group events, for example, by computer, and respond to events.
- **Knowledge Script view** Displays a list of Knowledge Scripts. Use the grid to browse Knowledge Scripts and create groups of Knowledge Scripts.

Service Map views manage events and display the overall health of a business process. For more information, see "Understanding Service Map Views" on page 146.

For example, in the `Master` management group below, the Servers view displays server information for the selected server:



Creating a Rule-based Management Group

For trial purposes, create a rule-based management group to select the computers you want to manage. A **management group rule** consists of one or more expressions that select the computers you want, for example, SQL Server computers with more than 2 GB of memory.

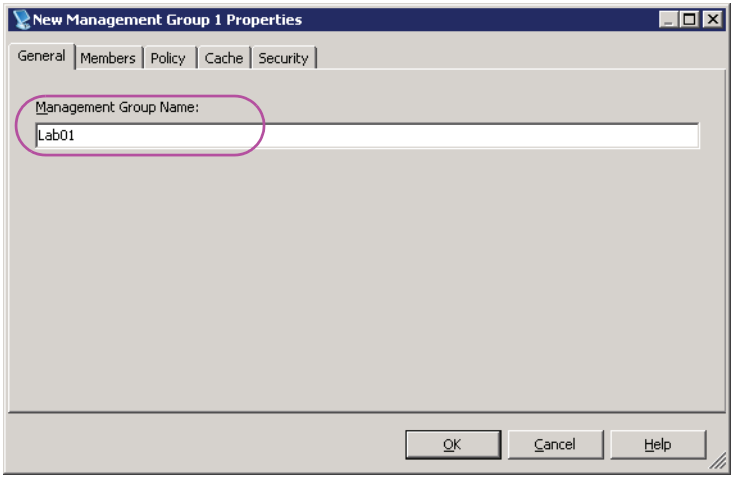
When you create a management group, you have the option to create the standard views which include Events, Jobs, Knowledge Scripts, and Servers. For trial purposes, do not create the standard views when you create the management group.

In addition to standard views, create Service Map views to illustrate and manage the business processes in your environment. For more information, see "Understanding Service Map Views" on page 146.

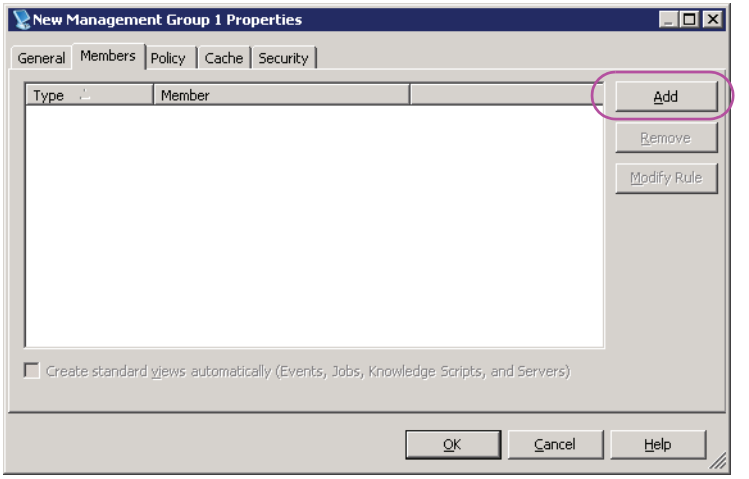
To create a rule-based management group:

1. Right-click the top-most AppManager icon in the Enterprise Layout pane, or an existing management group and click **New > Management Group**.

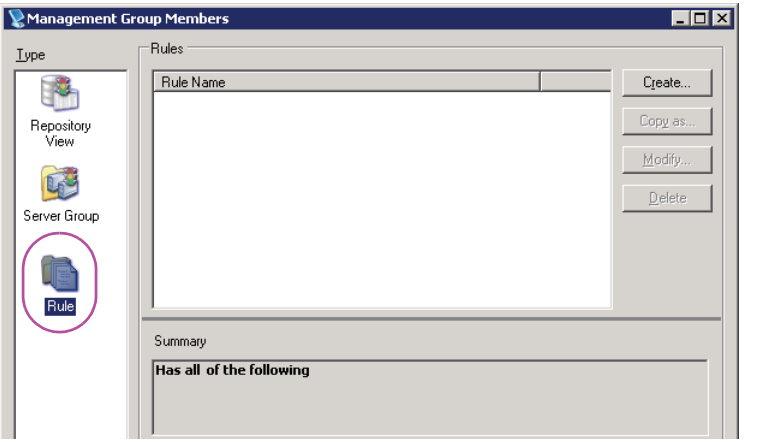
2. On the General tab of the New Management Group Properties dialog box, type a name for the management group. For trial purposes, name the management group `Lab01`.



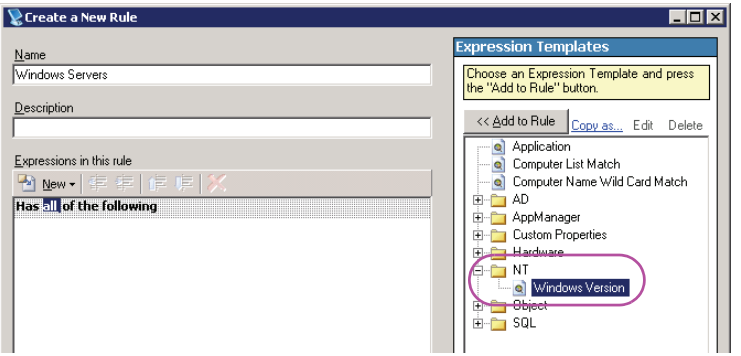
3 On the Members tab, click **Add**.



4 In the Management Group Members dialog box, click the **Rule** button to add a management group rule, then click **Create**.

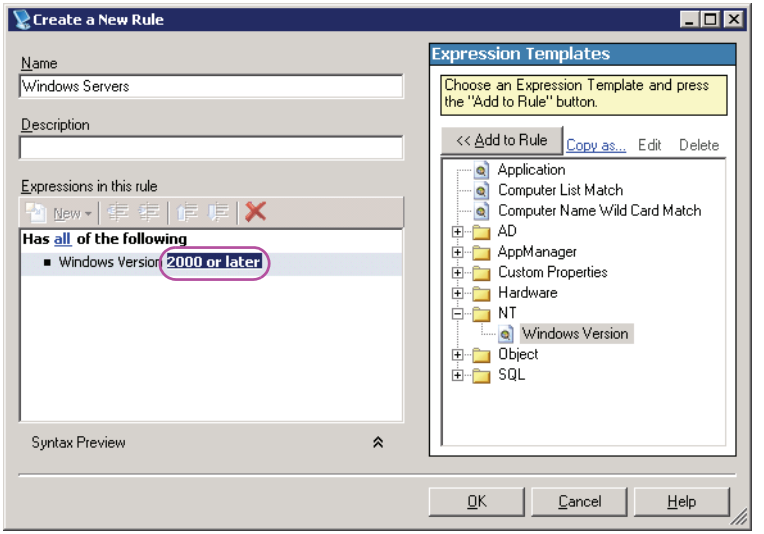


5 In the Create a New Rule dialog box, configure an expression template to select the computers you want based on operating system version.



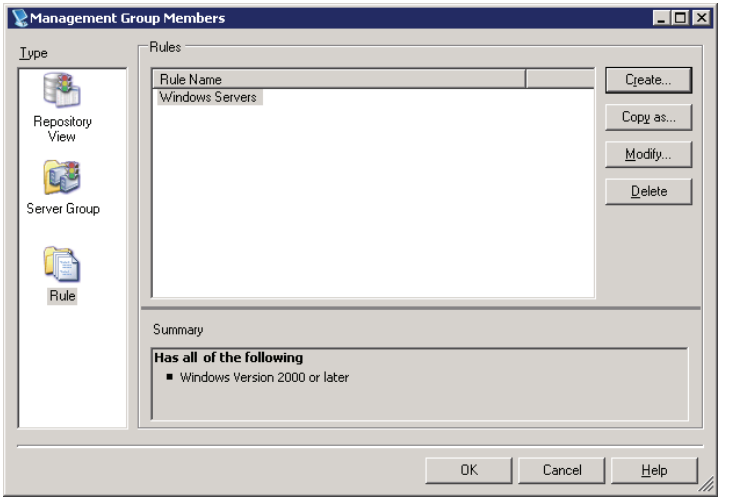
For	Do this
Name	Type a name for the management group rule, for example, `Windows Servers`.
Description	Provide a description. This parameter is optional.
Expression Templates list	Expand the **NT** folder and click the **Windows Version** template. Click the **Add to Rule** button TWICE to add the template to the management group rule.

6 In the expression editor, accept the default, **2000 or later**, to enable the management group rule to select Windows computers with an operating system version of Windows 2000 or later.



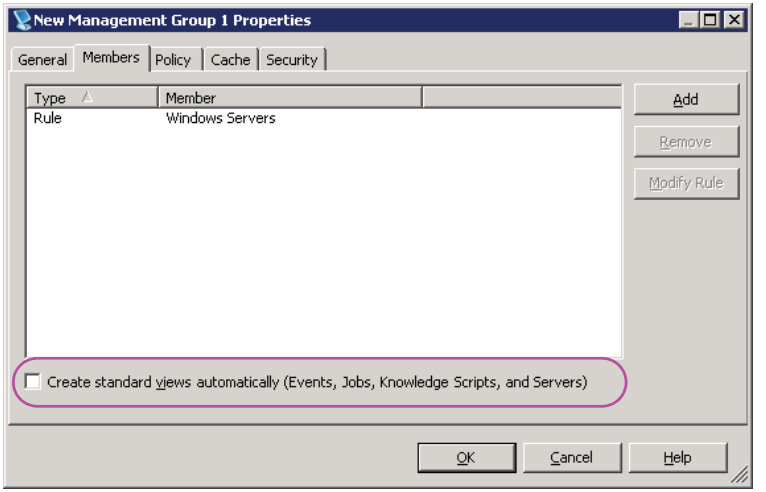
7 Click **OK**.

8 In the Management Group Members dialog box, the Windows Servers management group rule is displayed.



9 Click **OK**.

10 On the Members tab of the Properties dialog box, clear the **Create standard views automatically** check box. For trial purposes, you can create the views later.



11 Click **OK**.

After you create the management group, in the Control Center Console, the green arrows on the views indicate that Control Center is synchronizing information for the computers that match the management group rule. In the example below, the green checkmark indicates the Management Group status is synchronized.



Creating a Server View

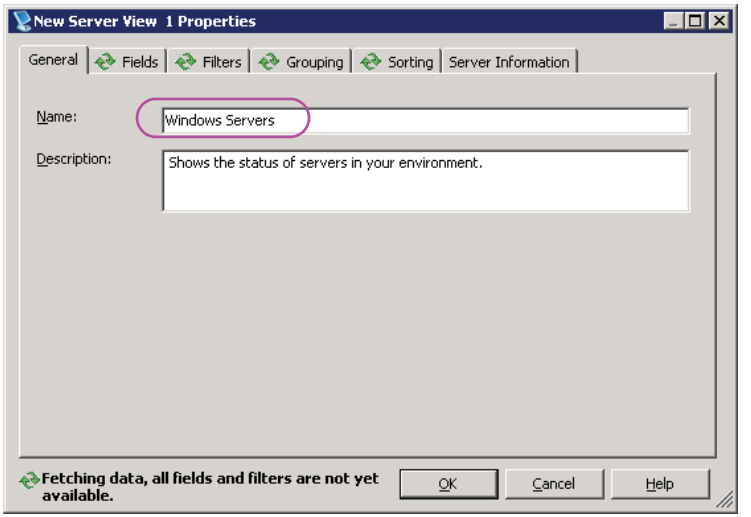
Create a Server view to display the server information for the computers in the management group you just created.

A Server view allows you to perform several tasks, such as managing events and creating jobs, from a single view.

To create a Server view:

1 Right-click the **Lab01** management group and click **New > Server View**.

2 On the General tab of the Properties dialog box, specify a name for the Server view.

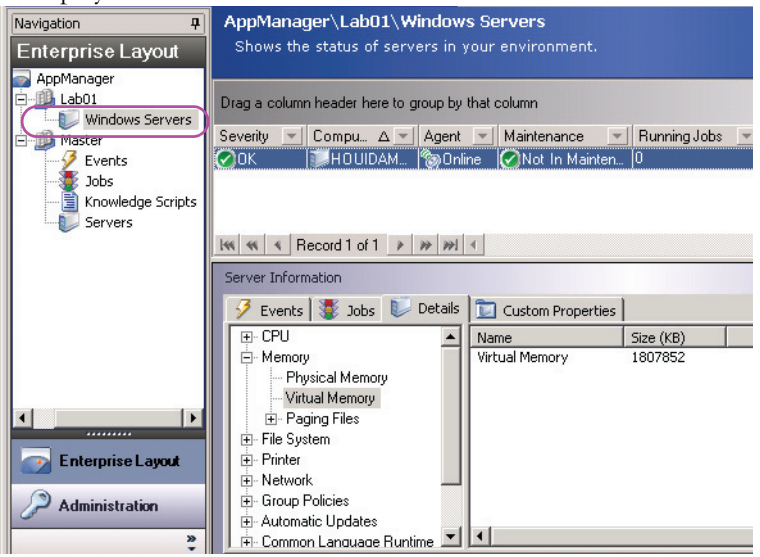


For	Do this
Name	Type `Windows Servers`
Description	No action required.

Tip Note that the green arrows on the tabs indicate that Control Center is synchronizing information for the computers that match the management group rule.

3 Click **OK**.

4 In the `Lab01` management group, click the **Windows Servers** view to display its contents.



5 Click the **Details** tab in the lower pane to view the AppManager discovery information for the selected server. In the example above, the discovery information for virtual memory is displayed.

Tip The process by which AppManager is made aware of the computers and applications you want to monitor is called **discovery**. Discovery occurs when you install the agent or modules, and when you run Discovery Knowledge Scripts.

You are now ready to deploy the agent to a remote computer. For more information, see "Understanding Agent Deployment" on page 86.

Understanding Agent Deployment

AppManager provides a rule-based solution to automatically monitor computers you add to your network. AppManager uses agents and modules to monitor computers. The Control Center Console includes the Deployment Rule Wizard to help you configure deployment rules to install and update the agent and modules on the Windows computers in your environment.

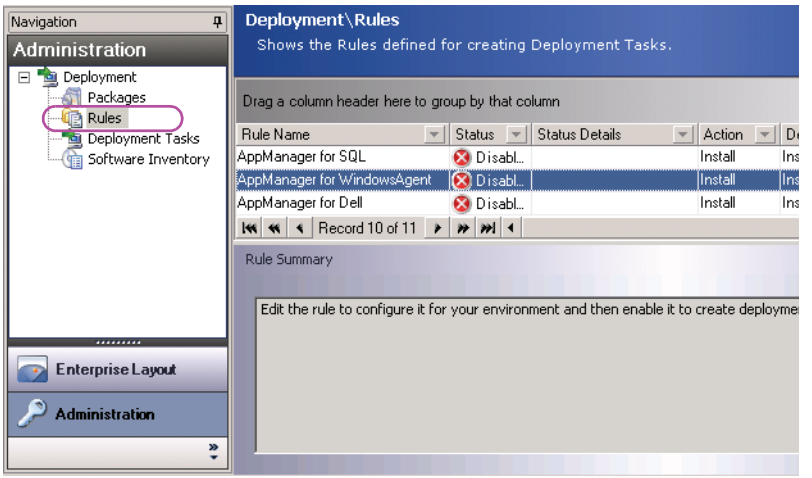
AppManager periodically checks for new computers and, pending your approval, installs agents or modules that match criteria you specify with the Deployment Rule Wizard.

For trial purposes, you can deploy the agent to Windows computers. At this time, you cannot deploy the agent to remote UNIX computers.

About the Administration Pane

The Administration pane allows you to access deployment packages, deployment rules, and deployment tasks, and the Deployment Rule Wizard.

Use the Rules view in the Administration pane to configure deployment rules.



A **deployment rule** describes the computers where you want to install one or more deployment packages. A **deployment package** is an MSI-based installer program to install the agent or a module. For your convenience, the Control Center Console includes a default deployment rule to install the agent.

Once you enable a deployment rule, the Deployment Tasks view lists the resulting deployment tasks. A **deployment task** installs a deployment package on a target computer. You must approve a deployment task before the deployment task can run on the target computer.

Before You Begin

Before you configure a deployment rule to install the agent, make sure the domain user account you plan to use as the credentials for the deployment rule is also a member of the local Administrators group on the computer where you want to deploy the agent.

Configuring a Rule to Deploy the Agent

Configure a deployment rule to install the agent on one or more computers. For your convenience, the Control Center Console provides an out-of-the-box rule to install the agent.

To configure a deployment rule:

1. In the **Administration** pane, click **Rules** to display the list of rules.
2. Double-click the **NetIQ AppManager Windows Agent** rule to configure its properties in the Deployment Rule Wizard.

3 In some cases, you can simply accept the default values.

For information about	See
Rule Name	"Specifying the Rule Name" on page 89
Packages	"Selecting and Configuring the Agent Deployment Package" on page 89
Credentials	"Specifying the Deployment Credentials" on page 97
Target Computers	"Specifying the Target Computers" on page 99 and "Specifying an Inclusion Filter" on page 100
Deployment Service	No action is required. For trial purposes, accept the default deployment service.
Deployment Schedule	No action is required. For trial purposes, accept the default deployment schedule, which requires you to approve a deployment task before the deployment task can be run on the target computer.
Notification	No action is required. For trial purposes, do not configure e-mail notification.
Rule summary information	"Viewing Summary Information for a Rule" on page 102

4 To allow the deployment service to begin the process of generating a deployment task for each target computer, enable the deployment rule. For more information, see "Enabling the Rule" on page 103.

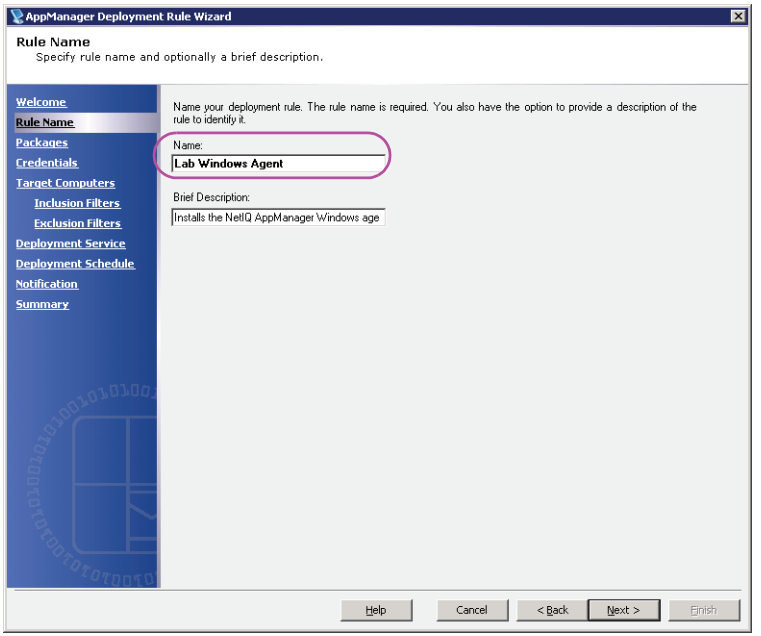
5 After Control Center generates a deployment task, you must approve the deployment task to allow Control Center to install the deployment package. For more information, see "Approving Deployment Tasks" on page 105.

Specifying the Rule Name

For trial purposes, rename the NetIQ AppManager Agent rule.

To change the rule name:

1 In the **Rule Name** section of the Deployment Rule Wizard, change the rule name. For trial purposes, in the Name field, type `Lab Windows Agent`.



2 Click **Next**.

You are now ready to configure the deployment package to install the agent. For more information, see "Selecting and Configuring the Agent Deployment Package" on page 89.

Selecting and Configuring the Agent Deployment Package

For trial purposes, configure the rule to include the deployment package for the agent. The agent does not require any additional modules to monitor the Windows operating system.

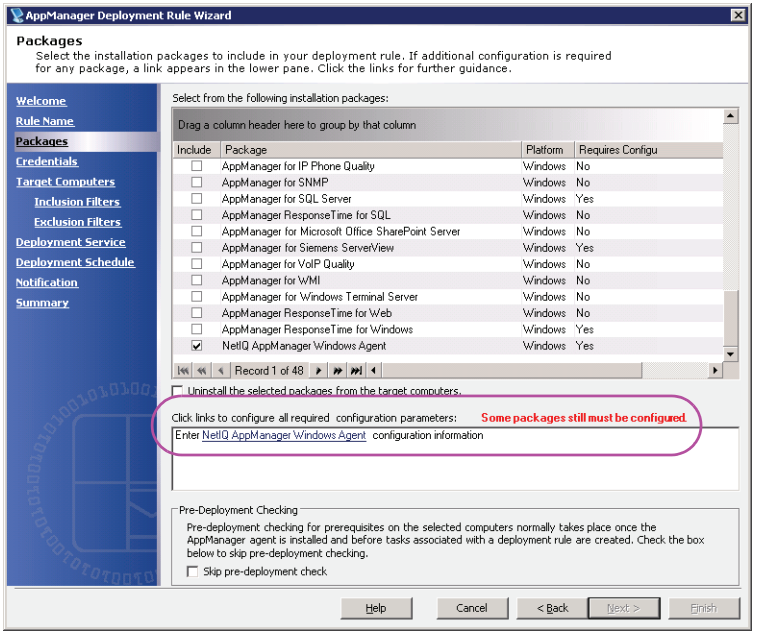
The deployment package requires you to specify configuration information, such as the folder location to install the agent.

To select and configure the deployment package for the agent:

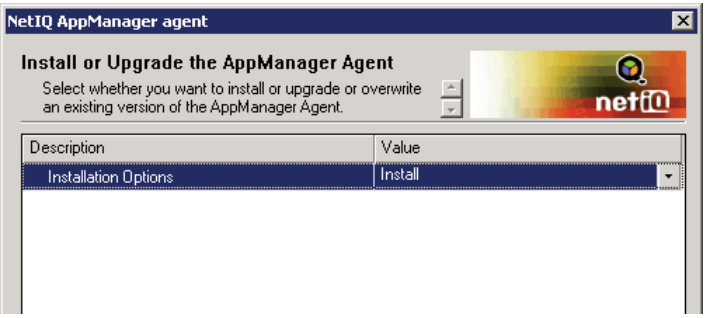
1. In the **Packages** section of the Deployment Rule Wizard, select the check box for the `NetIQ AppManager Windows Agent` deployment package.

2. After you select the check box, the Deployment Rule Wizard indicates you must configure the `NetIQ AppManager Windows Agent` deployment package.

   To configure the package, click **NetIQ AppManager Windows Agent** in the Configuration Parameters list.

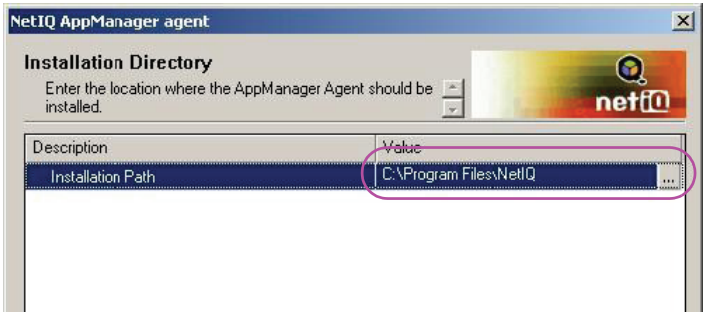


3 At the Install or Upgrade the AppManager Agent dialog box, accept the default **Install** option to install the agent.



4 Click **Next**.

5 At the Installation Directory dialog box, click the **...** button to choose a folder location to install the agent on the target computer.

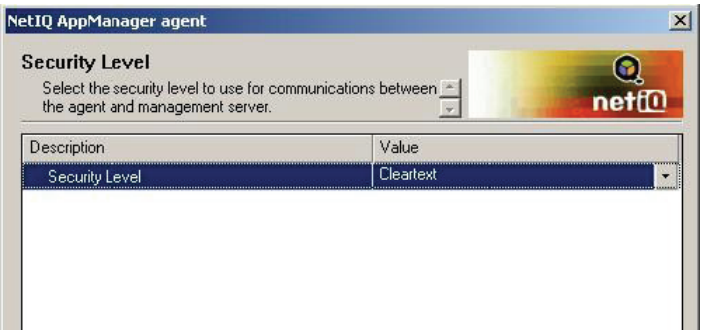


6 Click **Next**.

7 At the Reporting Capability and Service Account dialog box, click **Next** to accept the default values and configure the agent to run as the LocalSystem account.

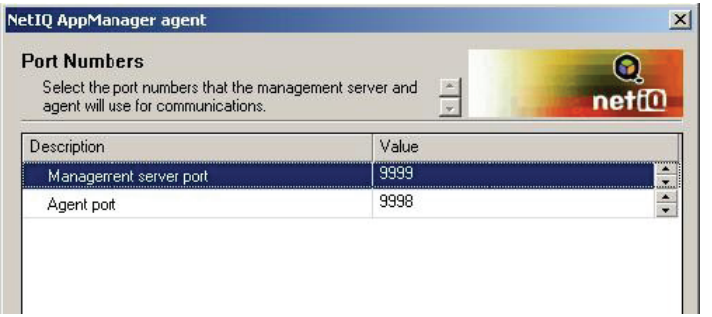


8 At the Security Level dialog box, accept the default value to configure the agent to communicate with the management server using cleartext. Because the management server uses cleartext, the agent must also use cleartext.



9 Click **Next**.

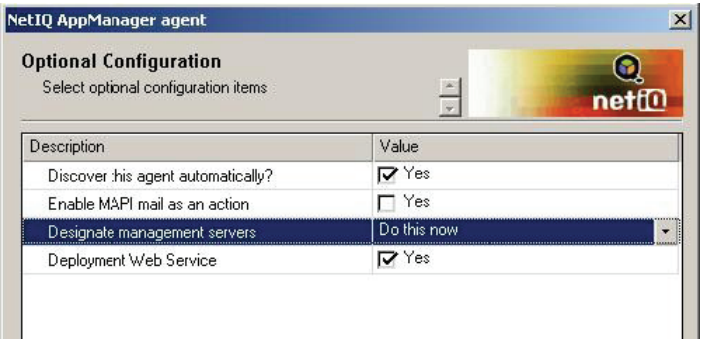
10 At the Port Numbers dialog box, accept the default RPC port values for the agent to communicate with the management server. The agent and management server must communicate with each other using the same ports.



11 Click **Next**.

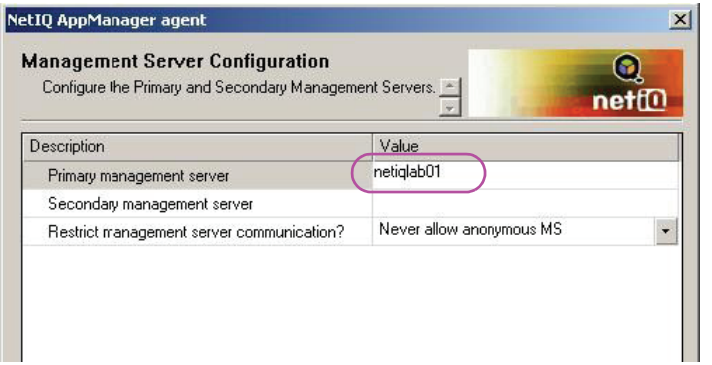
12 At the Optional Configuration dialog box, accept the default values to:

- Configure the agent installation to automatically discover Windows resources and send the discovery information to the management server.
- Enable you to configure the agent with the location of the deployment web service. To install additional deployment packages on the agent, the agent must be able to communicate with the deployment web server.



13 Click **Next**.

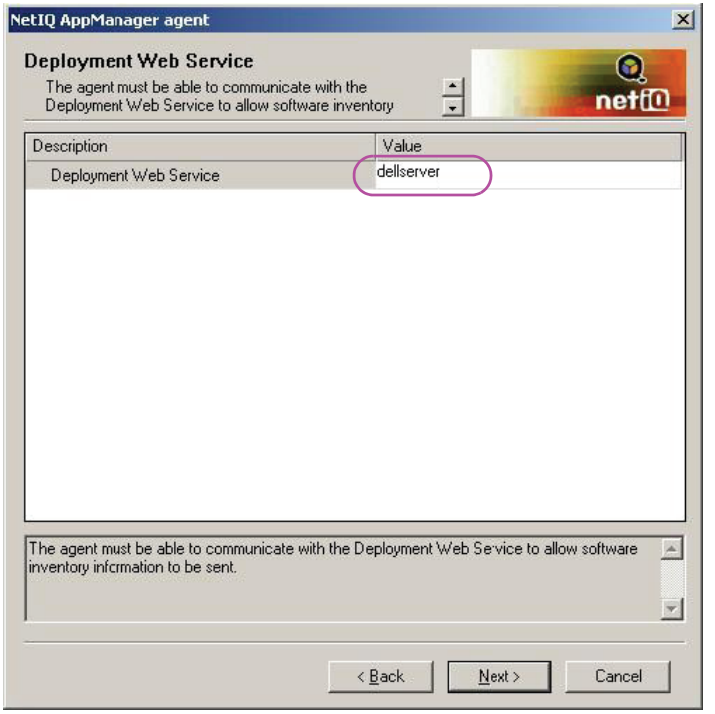
14 At the Management Server Configuration dialog box, designate the primary management server with which the agent communicates. For trial purposes, the agent will only communicate with its primary management server.



For	Do this
Primary management server	Type the name of the local computer where you installed all of the AppManager components, including the management server.
Secondary management server	Accept the default value to not configure the agent to communicate with secondary, or backup, management server.
Restrict management server communication	Accept the default value to configure the agent to only communicate with its primary management server.

15 Click **Next**.

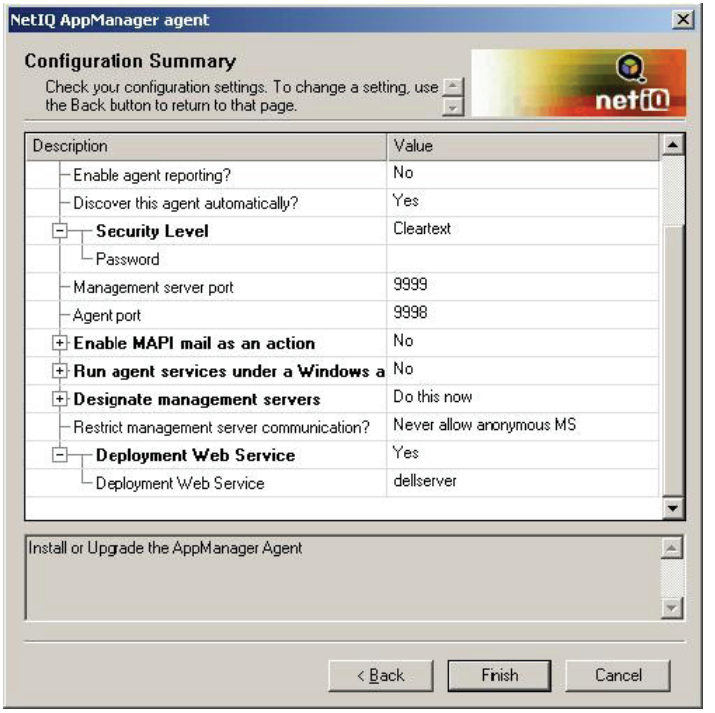
16 At the Deployment Web Service dialog box, specify the agent's deployment web server. To install additional deployment packages on the agent, the agent must be able to communicate with the deployment web server.



For	Do this
Deployment Web Service	Type the name of the computer where you installed all of the AppManager components.

17 Click **Next**.

18 At the Configuration Summary dialog box, review the summary of the agent installation options.



19 Click **Finish**.

You are now ready to configure the credentials used to install the deployment package. For more information, see "Specifying the Deployment Credentials" on page 97.

Specifying the Deployment Credentials

In the Deployment Rule Wizard, use the **Credentials** section to specify a user account with the credentials required to run the deployment package on the target computer.

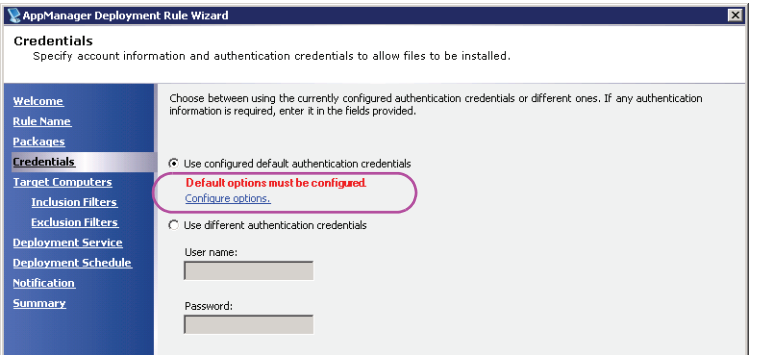
The credentials required to run the deployment package are not related to the permissions required by the agent to run particular Knowledge Scripts.

To install a deployment package on a target computer, for example, to install the agent, provide a domain user account that is member of the **Administrators** group on the target computer. When configuring a rule, use the Windows user account that is currently configured as the default for deployment, or provide different login information.

To specify the credentials that are used to install the package on the target computer:

1 In the **Credentials** section of the Deployment Rule Wizard, click **Next** to accept the default credentials.

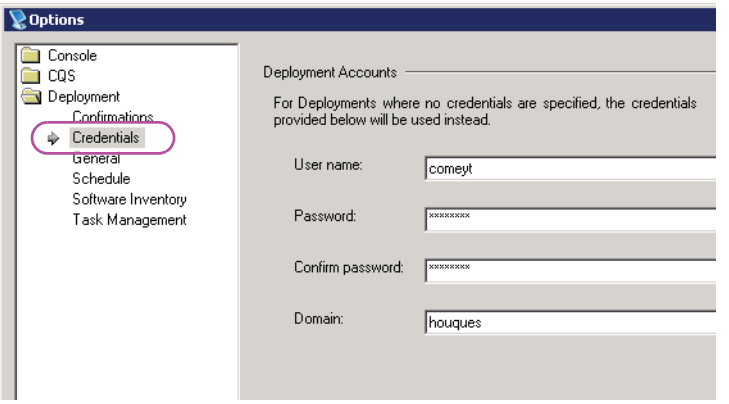
If you have not yet configured the default credentials, you must configure them now.



To configure the default credentials:

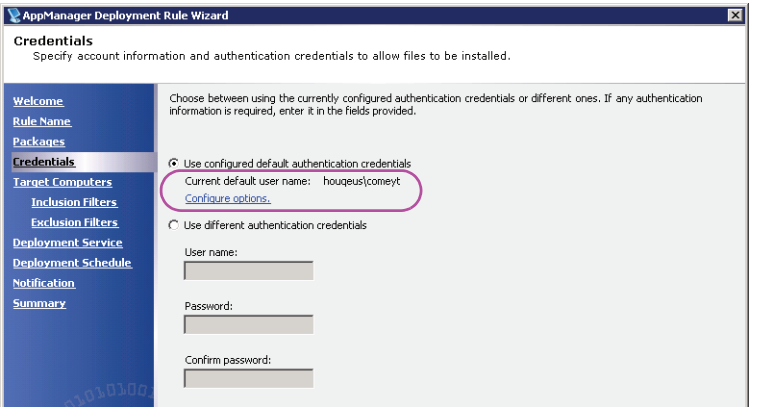
a. Click **Configure Options**.

b. In the Options dialog box, specify the credentials of a domain user account that is member of the **Administrators** group on the target computer.



c. Click **OK**.

2 In the Deployment Rule Wizard, click **Next** to accept the default credentials you specified in the previous step.



Tip If you specify invalid credentials, the Control Center Console does not raise a warning until *after* you enable the deployment rule. In the Rules view of the Administration pane, the Status Details column displays information about any problems with the configuration of the rule.

You are now ready to specify the target computers where you want to install the agent deployment package. For more information, see "Specifying the Target Computers" on page 99.

Specifying the Target Computers

In the Deployment Rule Wizard, use the **Target Computers** section to select the computers where you want to install the agent.

Configure a **target computer selection method** to specify how you want the deployment service to select the computers where you want to install the agent.

To further refine the list of selected computers, configure inclusion and exclusion filters:

- An **inclusion filter** refines the list of computers that match the target computer selection method. Only computers that match the target computer selection method and the inclusion filter are included.
- An **exclusion filter** refines the list of computers that match the target computer selection method and the inclusion filter. Computers that match the exclusion filter are not included.

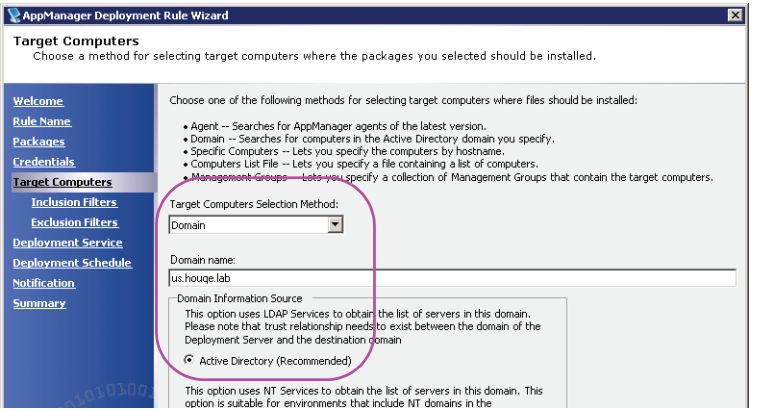
The deployment service processes all computers that match the target computer selection method before applying the inclusion and exclusion filters. For example, after you enable a deployment rule that is configured to select target computers from an Active Directory domain, the deployment service queries every computer in the domain before it generates deployment tasks for computers that match the inclusion and exclusion filter criteria.

To specify the target computer selection method:

1 In the **Target Computers** section of the Deployment Rule Wizard, configure the target computer selection method to select the computers you want from an Active Directory domain.

   For a large network, it can take several minutes after you enable a deployment rule for the deployment service to query every

computer in the Active Directory domain and then generate deployment tasks for computers that match the inclusion and exclusion filter criteria.



For	Do this
Target Computers Selection Method list	Choose **Domain**.
Domain name	Type the name of the Active Directory domain you want.
Domain Information Source	Use the default Active Directory option.

2 Click **Next**.

You are now ready to specify an inclusion filter to select the target computers. For more information, see "Specifying an Inclusion Filter" on page 100.

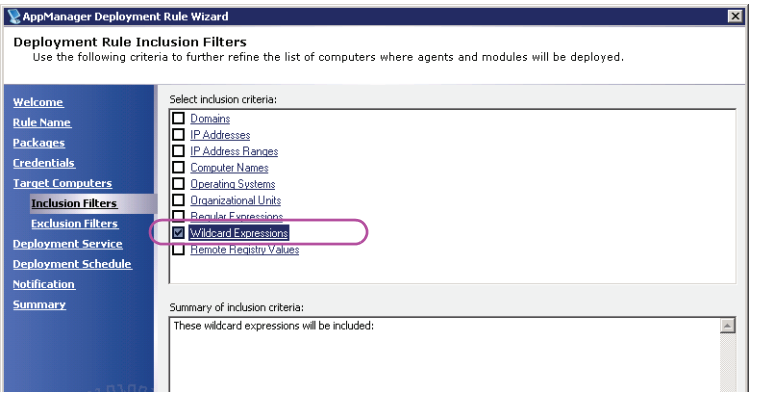
Specifying an Inclusion Filter

In the Deployment Rule Wizard, use the **Inclusion Filters** section to select the computers you want from the list of target computers.

To generate a deployment task for a computer, the computer must match both the target computer selection method and the inclusion filter.

To specify the inclusion filter:

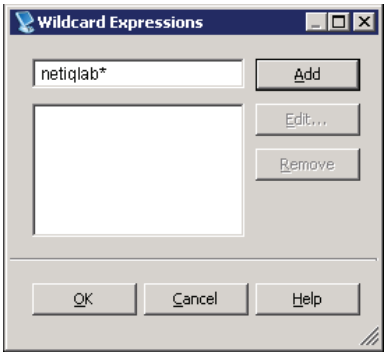
1 In the **Inclusion Filter** section of the Deployment Rule Wizard, select the **Wildcard Expression** check box.



2 Click **Wildcard Expression** to specify a wildcard expression.

3 In the Wildcard Expression dialog box, type a pattern-matching expression that selects the computers you want. Use the following pattern-matching characters:

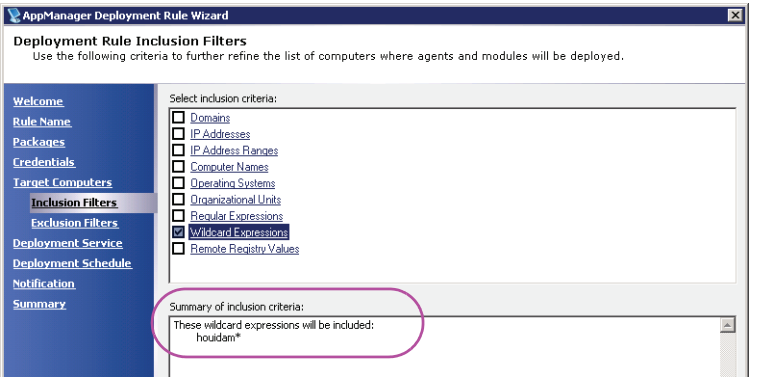
- % matches any single character.
- * matches more than one character.



4 Click **Add**.

5 Click **OK**.

The wildcard expression is displayed in the summary field.



You are now ready to review the configuration of the rule. For more information, see "Viewing Summary Information for a Rule" on page 102.

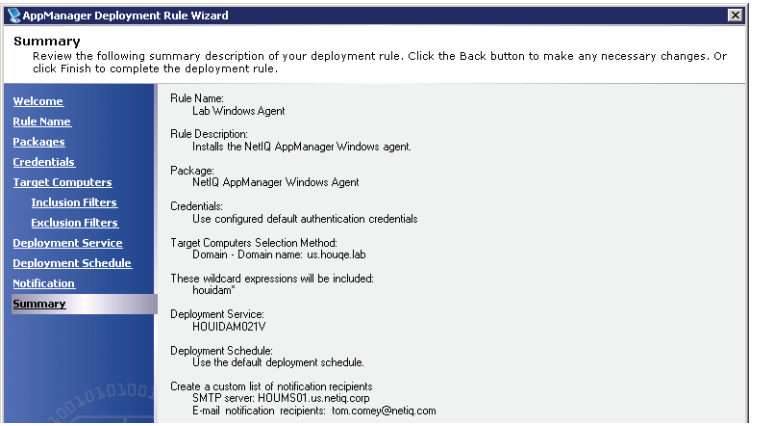
Viewing Summary Information for a Rule

Before you finish configuring the rule, view the rule's summary information, and if necessary, make any changes.

To view a summary of the rule configuration:

1 In the **Summary** section of the Deployment Rule Wizard, view a summary of how the rule is configured.

2 View the summary description for the deployment rule.



3 Click **Finish**.

You are now ready to enable the rule. For more information, see "Enabling the Rule" on page 103.

Enabling the Rule

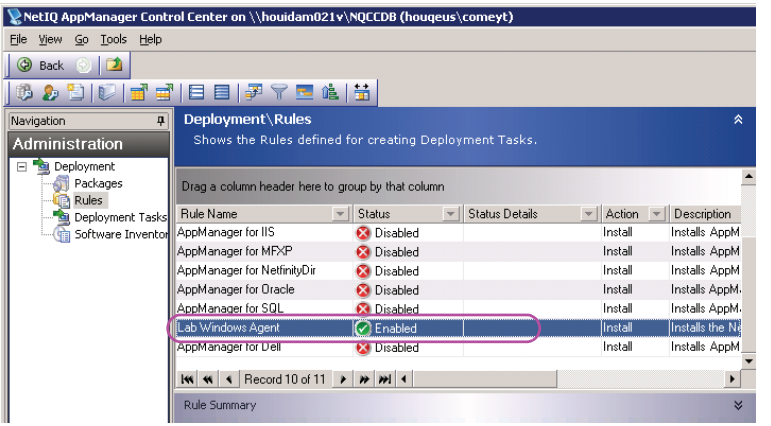
You must enable a rule to allow Control Center to begin the process of generating a deployment task for each computer that matches the rule's selection criteria.

To enable the rule:

1 In the Rules view, right-click the **NetIQ AppManager Windows Agent** rule and click **Enable Rule**. Control Center may take a few minutes to generate a deployment task for each target computer.

2 In the Status column, the rule status should change to `Enabled`.

3 ***If the rule status does not change to*** `Enabled`, manually refresh the list of rules by clicking the **Enterprise Layout** button on the bottom left and then clicking the **Administration** button.



You are now ready to approve the deployment tasks generated by Control Center. For more information, see "Approving Deployment Tasks" on page 105.

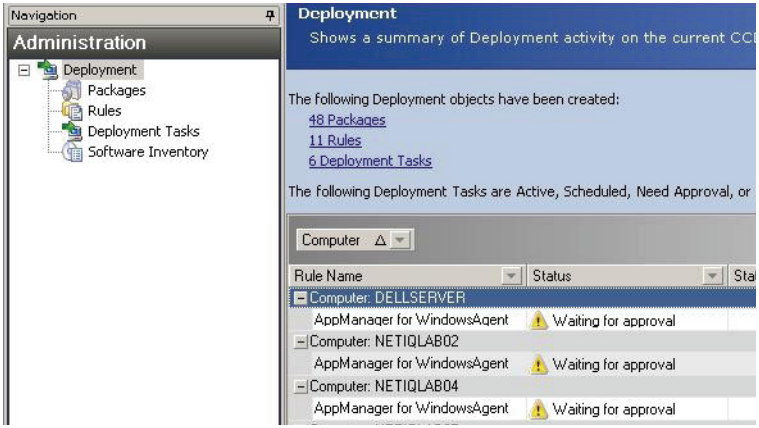
Approving Deployment Tasks

A **deployment task** delivers a specific deployment package to a particular computer. When a target computer meets the conditions for a deployment rule, the deployment service generates a deployment task.

Control Center may take a few minutes to generate a deployment task for each target computer. If you do not see any deployment tasks in the Tasks view of the Control Center Console, you can approve the deployment tasks later and proceed to "Understanding Monitoring Policies" on page 106.

To approve a deployment task:

1 In the Deployment view, browse the list to find the deployment task you want.



2 Right-click the deployment task and click **Approve Task(s)**. Press Shift+Click or Ctlr+Click to select multiple deployment tasks.

After you approve a deployment task, the deployment task status is `Active` or `Scheduled`. An `Active` deployment task takes a few minutes to install, depending on the network and hardware. A `Scheduled` deployment task runs at the deployment task's scheduled time. When the agent installation completes, the deployment task status changes to `Completed` and the Control Center Console automatically displays the managed client in any

management groups that match the grouping criteria.

3 ***If you have deployment tasks that you do not want to approve***, reject them by right-clicking a deployment task and clicking **Reject Task(s)**. Press Shift+Click or Ctlr+Click to select multiple deployment tasks.

Tip While the deployment task status is **Rejected**, the deployment rule does not generate another deployment task for the same target computer. To prevent AppManager from generating a new task, do not delete the Rejected deployment task until after you disable the deployment rule.

While the deployment tasks run, proceed to "Understanding Monitoring Policies," to configure the `Lab01` management group to automatically monitor servers that match its target selection criteria.

Understanding Monitoring Policies

AppManager performs all management and monitoring tasks by using Knowledge Scripts, which are programs that run on the AppManager agent. Knowledge Scripts can collect data, raise events, and perform specific actions in response to events. Each script is designed to perform a certain task or set of tasks, and to work on specific types of resources.

A **job** is an instance of a Knowledge Script running on a managed client. That is, when you run a Knowledge Script you are creating a job.

AppManager allows you to create jobs to monitor a particular resource, for example, the C: drive, on a particular computer. If you want to monitor another physical drive, you must update the job properties. If a new computer is added to the management group, you must create a new job on the computer to monitor its physical drives.

To automatically monitor resources as they change, configure a monitoring policy. A **monitoring policy** uses a set of pre-configured Knowledge Scripts called a **Knowledge Script Group** to automatically monitor resources in the management group.

For example, you can create a Knowledge Script Group that monitors physical disk resources and apply this Knowledge Script Group to a management group as a monitoring policy.

The monitoring policy monitors each computer in the management group using the same set of pre-configured Knowledge Scripts. If the disk configuration for a managed computer changes, for example, if you add or remove a physical disk, the next time that the Discovery_NT job runs, the discovery job updates the discovery information for physical disk resources and the monitoring policy automatically monitors the discovered physical disk resources.

If you have a computer that is temporarily outside the threshold levels permitted by the policy you have created, the Control Center Console allows you to stop and restart a policy-based job on a particular computer, or override the monitoring values for the job.

This product tour does not demonstrate how to stop and restart policy-based jobs or override the monitoring values for a policy-based job. For more information about these features, see the Control Center Console Help or contact your NetIQ Sales Representative or NetIQ Partner.

Creating a Knowledge Script Group

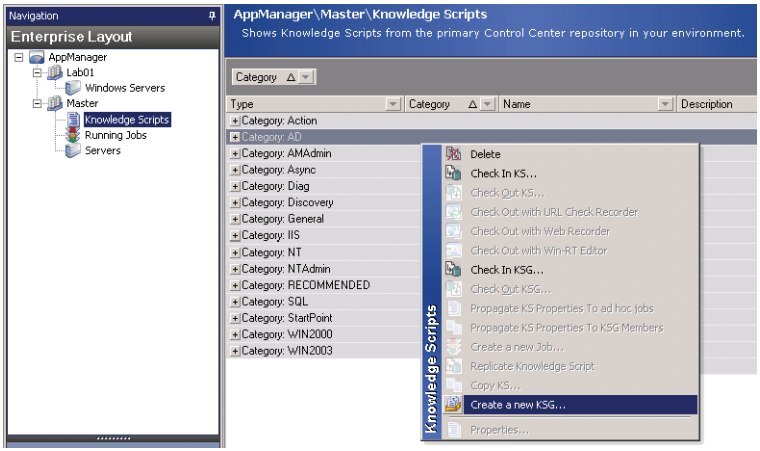
For trial purposes, create a Knowledge Script Group that includes the following **NT** Knowledge Scripts:

- **CpuLoaded** monitors total CPU usage and queue length to determine whether the CPU is overloaded.
- **LogicalDiskSpace** monitors logical disk space usage.
- **MemUtil** monitors the utilization of physical memory, virtual memory, and the paging files.
- **ServiceDown** monitors the `Stopped` and `Started` status of Windows services and, optionally, starts services that are stopped.
- **SystemUpTime** tracks the number of hours a computer has been operational since the computer was last rebooted.

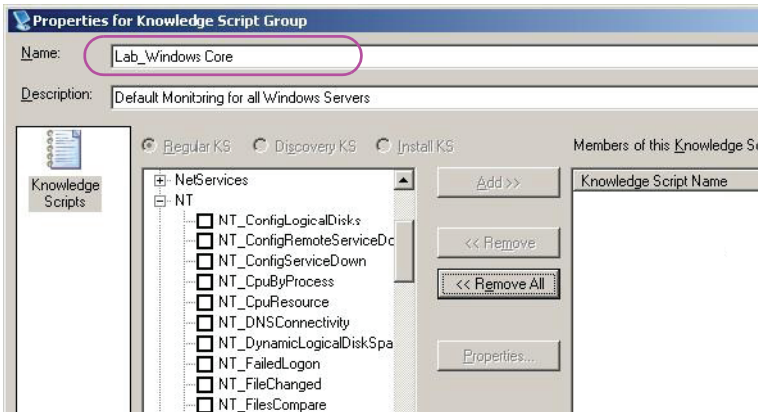
Configure these Knowledge Scripts to run on a particular schedule, collect data, and raise events.

To create a Knowledge Script Group:

1 In the Knowledge Script view of the Master management group, right-click the grid and click **Create a new KSG**.



2 In the Name field of the Properties for Knowledge Script Group dialog box, type `Lab_Windows Core` to create a new Knowledge Script category called **Lab**, and to create a new Knowledge Script Group under the **Lab** category called **Windows Core**.

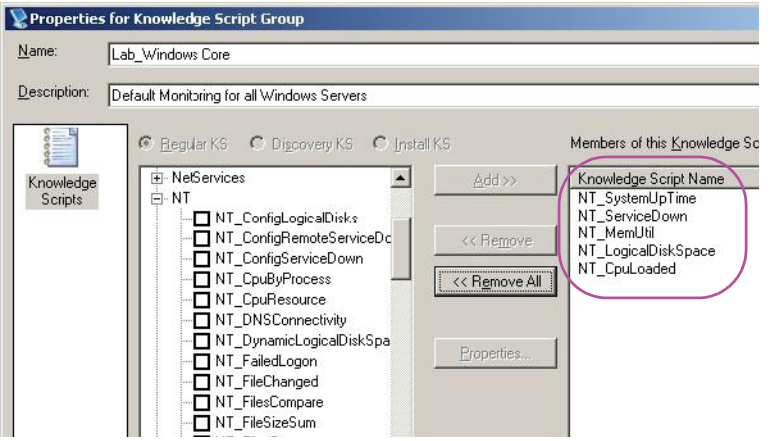


Note By default, the Knowledge Script Group name is prefixed with `KSG_` which means the Control Center Console displays the Knowledge Script Group in the `KSG` category of the Knowledge

Script view. To create the Knowledge Script Group in another category, prefix the name of the Knowledge Script Group using *category*_, where *category* is the name of the Knowledge Script Group category. For example, to create a Knowledge Script Group named NT Basics in the NT category, specify `NT_NT Basics`.

3 Expand the list of NT Knowledge Scripts and select the check box for each of the following Knowledge Scripts, then click **Add**:

- CpuLoaded
- LogicalDiskSpace
- MemUtil
- ServiceDown
- SystemUpTime



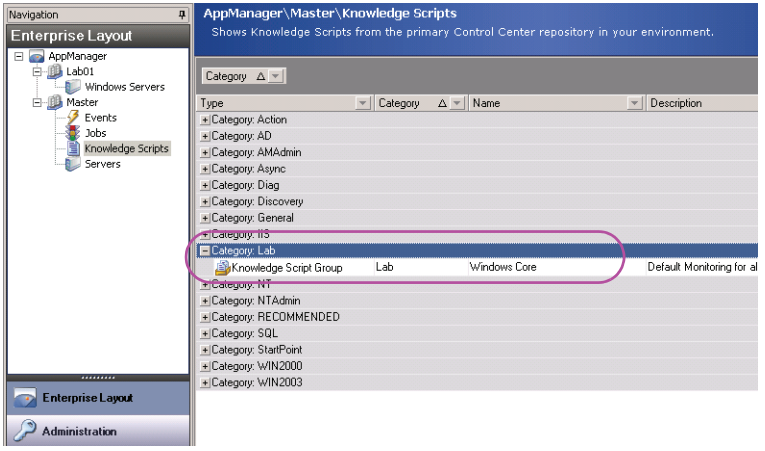
4 Configure the properties of each Knowledge Script Group member.

For information about	See
NT_SystemUptime	“Configuring NT_SystemUptime” on page 111
NT_ServiceDown	“Configuring NT_ServiceDown” on page 114
NT_MemUtil	“Configuring NT_MemUtil” on page 116

For information about	See
NT_LogicalDiskSpace	"Configuring NT_LogicalDiskSpace" on page 117
NT_CpuLoaded	"Configuring NT_CpuLoaded" on page 121

5 When you finish configuring each member, click **OK**.

6 In the Knowledge Script view, press the F5 key to refresh the screen and display the `Lab` category. Expand the `Lab` category to display the `Windows Core` Knowledge Script Group.



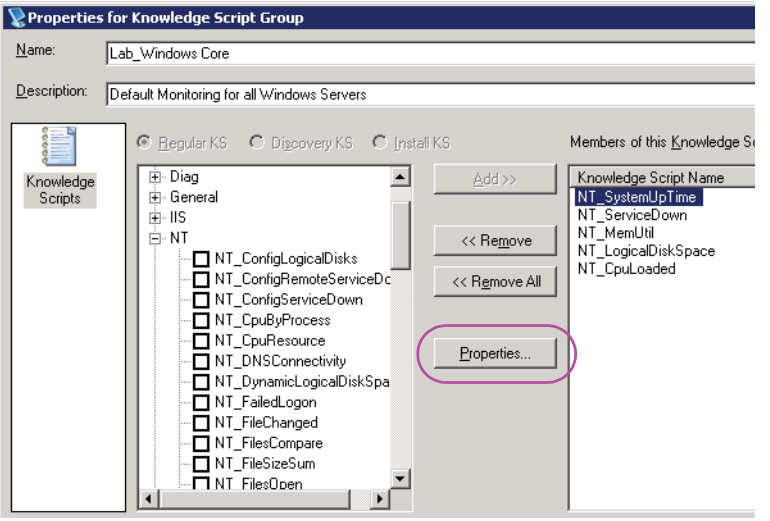
You are now ready to add the Knowledge Script Group to the monitoring policy for your management group. For more information, see "Enabling the Monitoring Policy" on page 122.

Configuring NT_SystemUptime

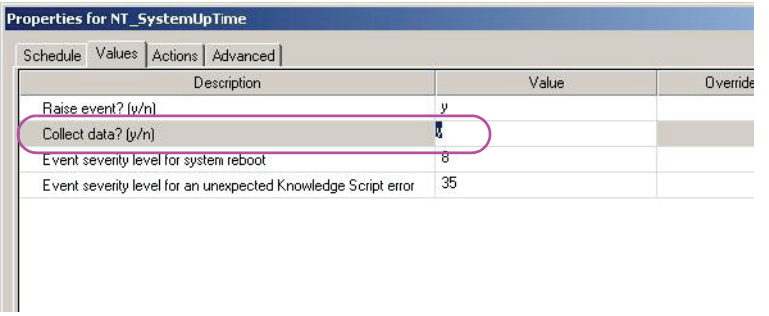
Configure NT_SystemUptime to collect data and raise events, and send an e-mail message as a responsive action if an event is raised.

To configure NT_SystemUptime:

1 In the Knowledge Script Group Properties dialog box, click **NT_SystemUptime** in the Member column and click **Properties**.



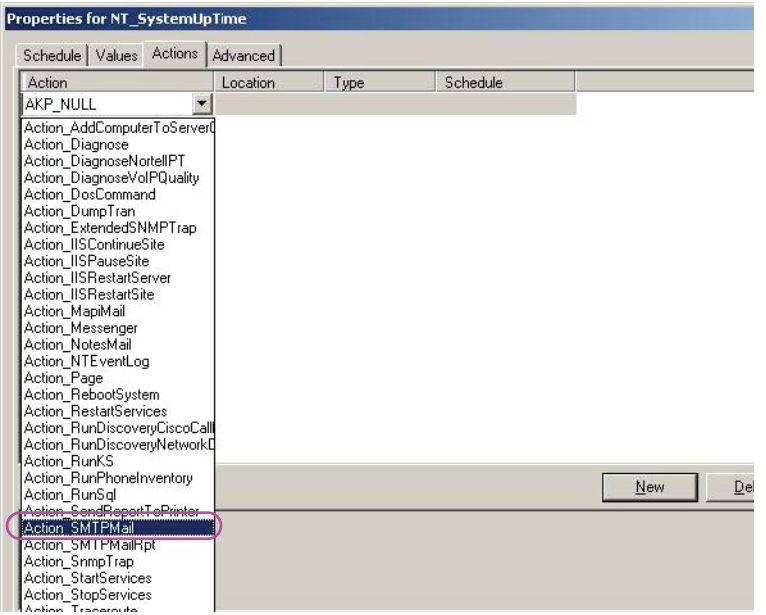
2 On the Values tab of the Properties dialog box, configure the following data collection options.



For	Do this
Collect data?	Type Y to collect data for charts and reports. If enabled, returns the number of hours the operating system has been up since the computer was last rebooted.

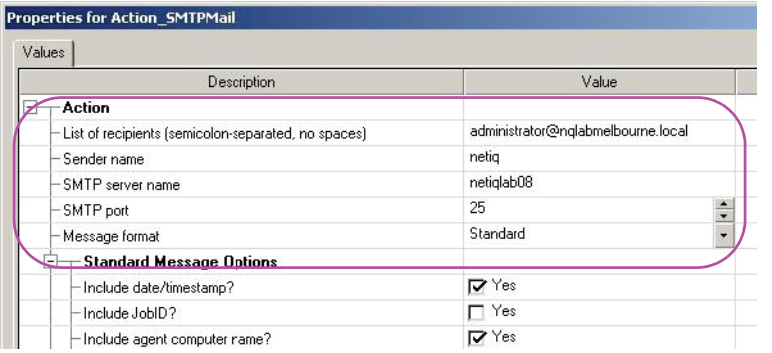
3 On the Actions tab of the Properties dialog box, click **New** to configure the **SMTPMail** Action Knowledge Script. This Action Knowledge Script sends an e-mail message as a responsive action when an event is raised. If you do not know the name of your SMTP mail server, click **OK** to finishing configuring this Knowledge Script Group member.

4 In the Action column, select `Action_SMTPMail` from the list.



5 Click **Properties**.

6 On the Values tab of the Properties dialog box, specify your SMTP server and e-mail recipients.



For	Do this
List of recipients	Specify an e-mail recipient, for example: `administrator@nqlab`
SMTP server name	Specify the host name or IP address of the server.
SMTP port	Accept the default SMTP port, `25`, or specify the port number for your SMTP server.
Standard message options	Select the following options: • `Include date/timestamp?` • `Include agent computer name?` • `Include Knowledge Script name?` • `Include event detail message?`

7 Click **OK**.

Configuring NT_ServiceDown

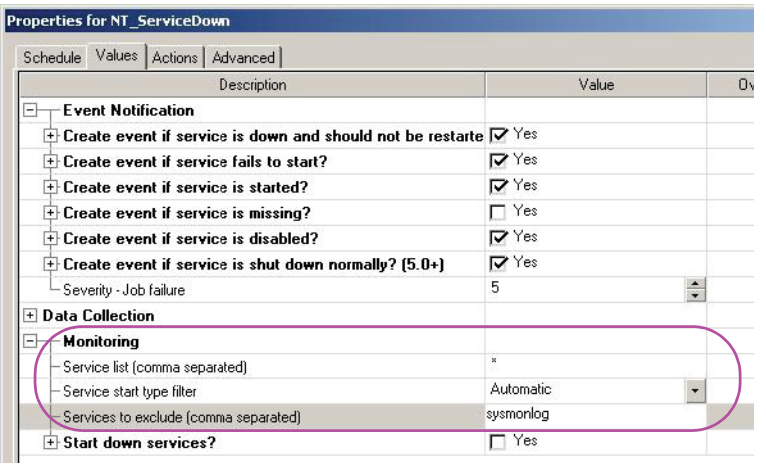
Configure NT_ServiceDown to monitor Windows services and raise an event if they stop. This Knowledge Script optionally restarts a service that is down.

Tip Typically you investigate why a service stopped rather than restart the service.

To configure NT_ServiceDown:

1 In the Knowledge Script Group Properties dialog box, click **NT_ServiceDown** in the Member column and click **Properties**.

2 On the Values tab of the Properties dialog box, configure the following monitoring options:



For	Do this
Service list	Specify * (asterisk). Specifying this wildcard character configures the Knowledge Script to monitor all services on the computer.
Services to exclude	Specify `sysmonlog`. This service is excluded from the list of services.
Start down services?	For trial purposes, clear this check box.

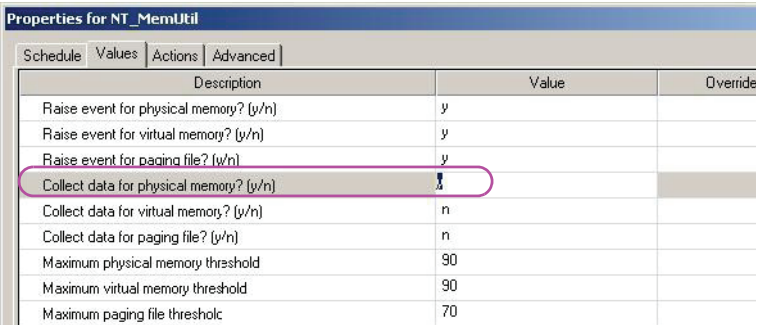
3 Click **OK**.

Configuring NT_MemUtil

Configure NT_MemUtil to collect data for physical memory usage. To ensure that temporary spikes in memory utilization do not raise a false-positive event, configure the event options to only raise an event if the threshold is exceeded every time the job runs during any 30-minute interval.

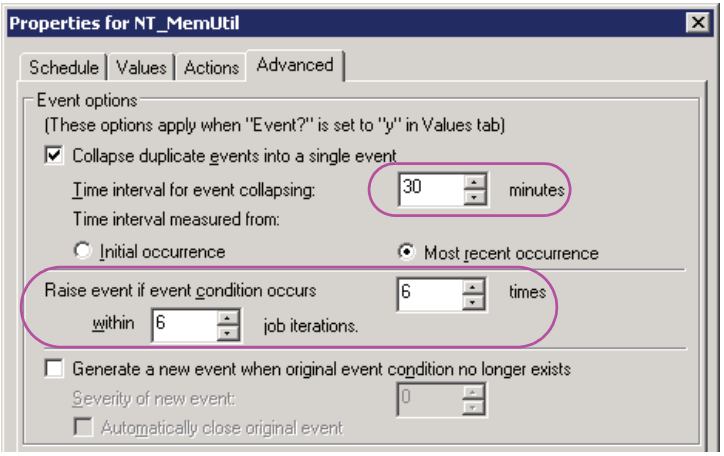
To configure NT_MemUtil:

1. In the Knowledge Script Group Properties dialog box, click **NT_MemUtil** in the Member column and click **Properties**.
2. On the Values tab of the Properties dialog box, configure the following monitoring options:



For	Do this
Collect data for physical memory?	Set to Y to collect data for charts and reports. If enabled, returns the percentage of physical memory used.

3 On the Advanced tab of the Properties dialog box, configure the event options to only raise an event if the threshold is exceeded every time the job runs during any 30-minute interval. Keep in mind that the job is scheduled to run every 5 minutes:



For	Do this
Time interval for event collapsing	Specify an event collapsing window of 30 minutes.
Raise event if event condition occurs N times within M iterations	Specify 6 times within 6 job iterations.

4 Click **OK**.

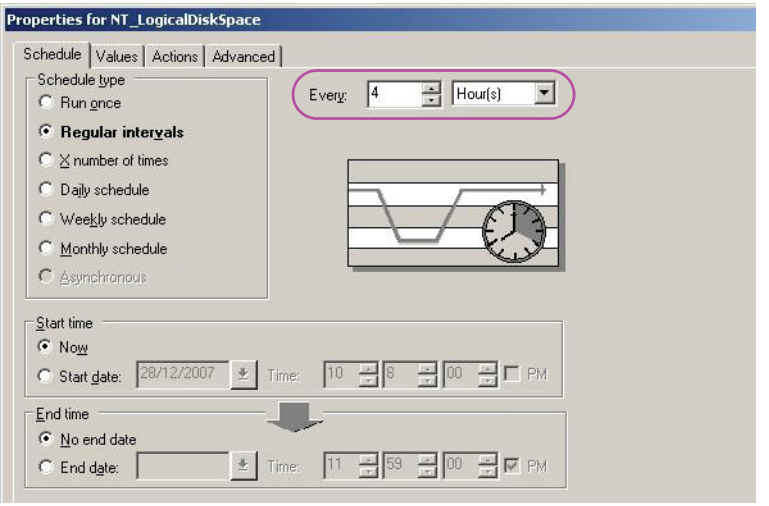
Configuring NT_LogicalDiskSpace

Configure the schedule for NT_LogicalDiskSpace to run 6 times per day, or every 4 hours, instead of once per day. To ensure that temporary spikes in logical disk space usage do not raise a false-positive event, configure the event options to only raise a new event if the threshold is exceeded twice in 2 consecutive job iterations.

To configure NT_LogicalDiskSpace:

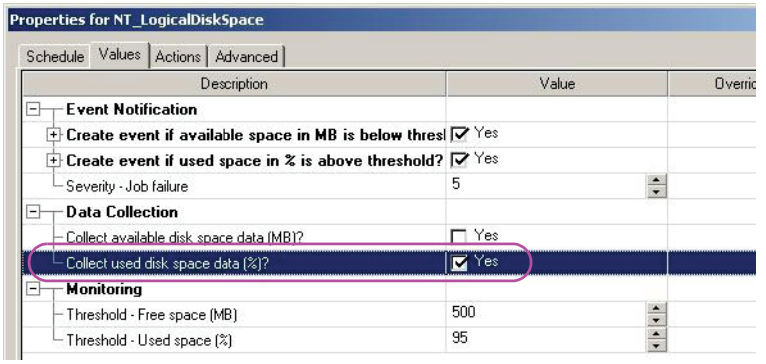
1 In the Knowledge Script Group Properties dialog box, click **NT_LogicalDiskSpace** in the Member column and click **Properties**.

2 On the Schedule tab of the Properties dialog box, configure the job interval to every 4 hours:



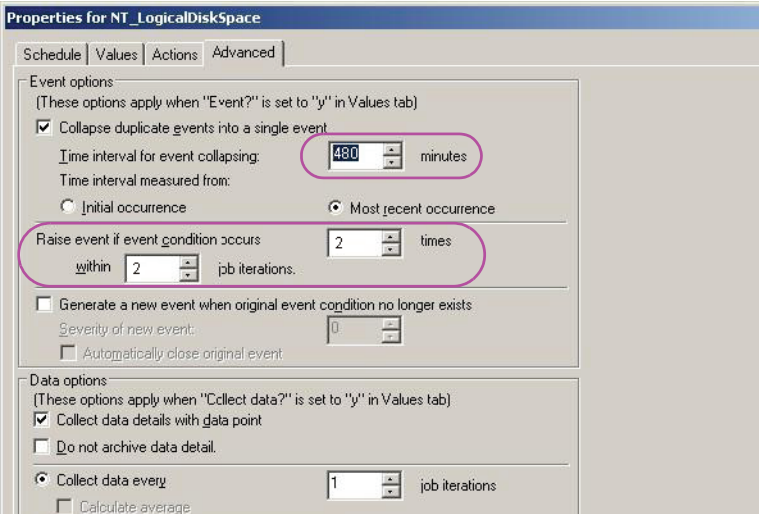
For	Do this
Schedule type	Change the regular interval to every 4 hours.

3 On the Values tab of the Properties dialog box, configure the following data collection options:



For	Do this
Collect used disk space data (%)	Select the check box to collect data for charts and reports. If selected, returns logical disk space utilization details by MB, including logical disk, free space in MB, threshold in MB, total space in MB, and used space as a percentage.

4 On the Advanced tab of the Properties dialog box, configure the event options to only raise an event if the threshold is exceeded more than once during any 480-minute, or 8-hour interval. Keep in mind that the job is scheduled to run every 240 minutes, or 4 hours:



For	Do this
Time interval for event collapsing	Specify an event collapsing window of 480 minutes.
Raise event if event condition occurs N times within M iterations	Specify 2 times within 2 job iterations.

5 Click **OK**.

Configuring NT_CpuLoaded

Configure NT_LogicalDiskSpace to collect data on the overall percentage of CPU time used. The detail data contains information about:

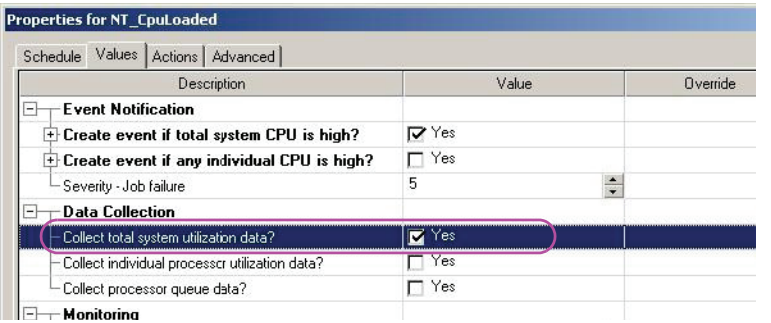
- The percentage of CPU time used
- The processor queue length
- The threshold for percentage of CPU time used
- The threshold for processor queue length

To ensure that temporary spikes in CPU utilization do not raise a false-positive event, configure the event options to raise an event if the threshold is exceeded every time the job runs during any 30-minute interval.

To configure NT_CpuLoaded:

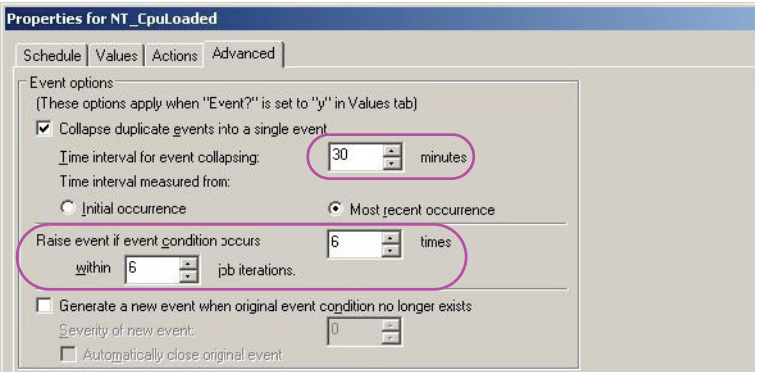
1. In the Knowledge Script Group Properties dialog box, click **NT_CpuLoaded** in the Member column and click **Properties**.

2. On the Values tab of the Properties dialog box, configure the following data collection options:



For	Do this
Collect total system utilization data?	Select the check box to collect data on the overall percentage of CPU time used.

3 On the Advanced tab of the Properties dialog box, configure the event options to only raise an event if the threshold is exceeded every time the job runs during any 30-minute interval. Keep in mind that the job is scheduled to run every 5 minutes:



For	Do this
Time interval for event collapsing	Specify an event collapsing window of 30 minutes.
Raise event if event condition occurs N times within M iterations	Specify 6 times within 6 job iterations.

4 Click **OK**.

You are now ready to add the **Windows Core** Knowledge Script Group to the monitoring policy on your `Lab01` management group. For more information, see "Enabling the Monitoring Policy."

Enabling the Monitoring Policy

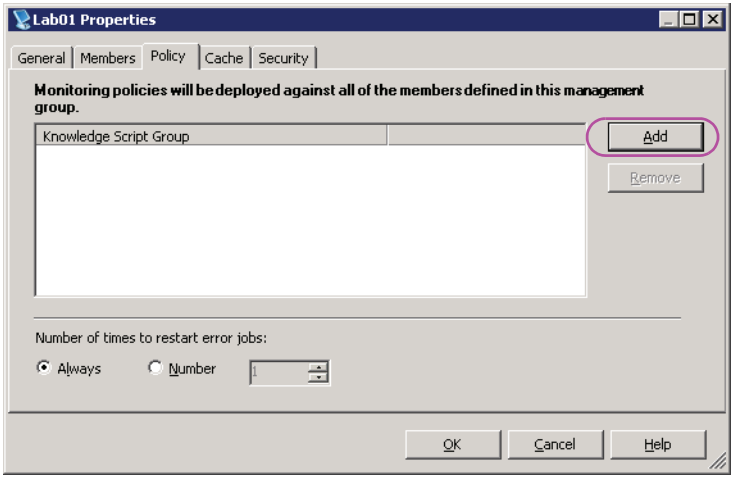
Configure the monitoring policy for the `Lab01` management group to use the `Windows Core` Knowledge Script Group. Any computers in the `Lab01` management group are automatically monitored by the members of the `Windows Core` Knowledge Script Group.

To enable a monitoring policy for the `Lab01` management group:

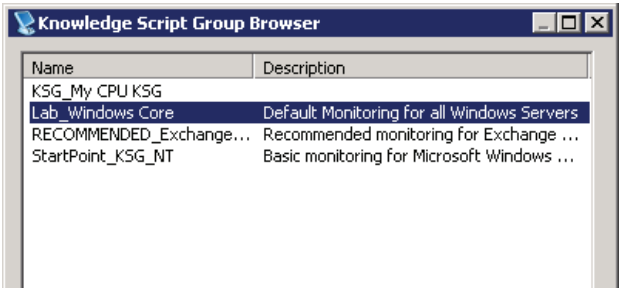
1 In the Enterprise Layout pane, right-click the **Lab01** management group and click **Properties**.



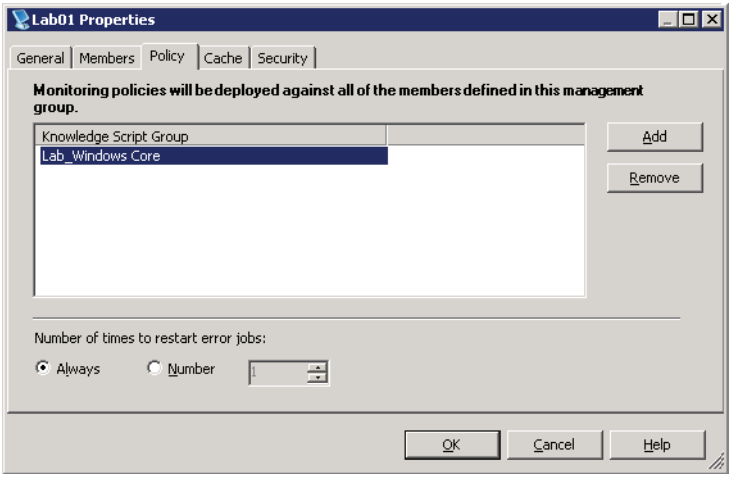
2 On the Policy tab of the Properties dialog box, click **Add**.



3 In the Knowledge Script Group Browser dialog box, click the **Lab_Windows Core** Knowledge Script Group and then click **OK**.



4 On the Policy tab of the Properties dialog box, click **OK** to enable the monitoring policy and create policy-based jobs to monitor matching resources.



For more information about viewing the resulting policy-based jobs, see "Working with Server Views."

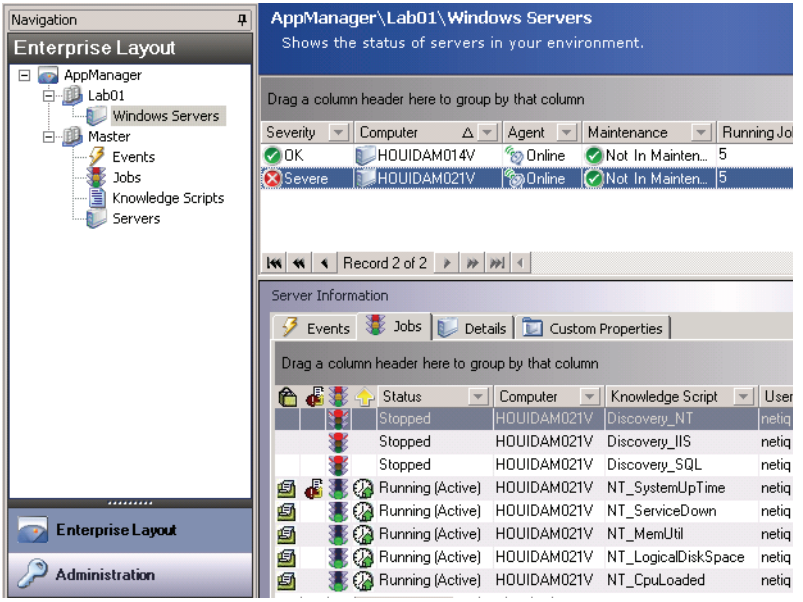
Working with Server Views

Use a Server view manage the associated events and jobs on one or more selected computers. From a Server view, you can also create jobs. Most Knowledge Script jobs run on a regular basis to keep continuous or periodic watch over system resources. In some cases, you need to run a combination of scripts to pinpoint a problem.

For example, assume the monitoring policy on the management group detects a CPU-related event condition. If the Knowledge Script sends you an alert indicating the server is overloaded, you may need to run additional Knowledge Scripts, using the Run Once schedule, to find the cause of the problem.

Looking at Jobs

In the Window Servers view, the Jobs tab displays job information for the selected computer. Because you configured a monitoring policy for the `Lab01` management group, AppManager automatically monitors the computers in the management group.



The policy-based jobs use a special icon to indicate that they are part of the management group's monitoring policy and have a status of `Running`.

Viewing the Properties of a Job

The properties of a job include, for example, the schedule to run the job and thresholds for raising events.

To view the properties of a job:

1. In the Windows Servers view of the `Lab01` management group, select a computer from the list.
2. In the Jobs tab, double-click a job to view its properties.
3. In the Job Properties dialog box, the properties are organized into tabs, such as the Schedule tab. For more information about the properties of the currently selected tab, click **Help**.
4. When you finish, click **Cancel**.

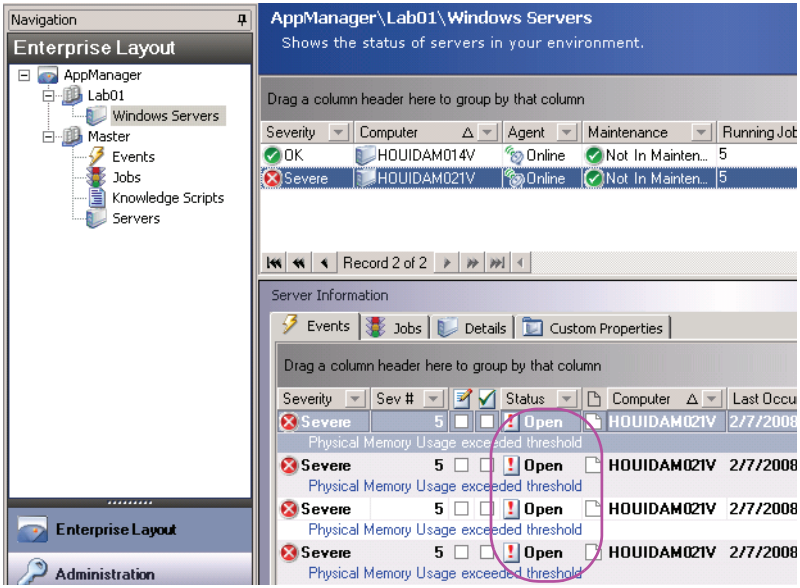
Looking at Events

As a Knowledge Script job runs, the job checks whether the condition you have defined exists, for example, whether a threshold value has been exceeded or a particular process is down.

If a Knowledge Script job detects a problem and is configured to raise an event, the event is:

- Stored in the AppManager repository.
- Displayed in the form of an event alert in an Event view of the Control Center Console.

In this state, the event is considered **Open**, requiring your attention.



To respond to an event and turn off the event indicator, you need to either acknowledge or close the event. How you use the Acknowledged or Closed status depends on your system management policies.

In general, acknowledge an event to indicate you are aware of the problem or that the problem is being addressed. Then, close the event when the problem has been resolved.

Because some jobs check for problems that severely impact your business while other jobs simply provide informational feedback, events range in severity. The event indicators displayed in the Control Center Console reflect at-a-glance the relative severity of the problem.

In the Control Center Console, events are classified as follows:

Default severity level	Indicator	Description
Severe Levels 1 to 10	 - Red	There is a very serious problem that requires your attention, for example, a computer or service is down. The Severe event indicator flashes on the event entry in the Event view.
Warning Levels 11 to 20	 - Yellow	There is unexpected behavior or minor problems that may require your attention, but they are not affecting network up time or preventing users from doing their work, for example, a counter you want to monitor or an application you want to discover is not found on the selected computer.
Informational Levels 21 to 30	 - Blue	A task was successfully completed, for example, a service is successfully started or a discovery is completed.
Diagnostic Levels 31 to 40	 - Magenta	Diagnostic information is returned, for example, when debugging problems.

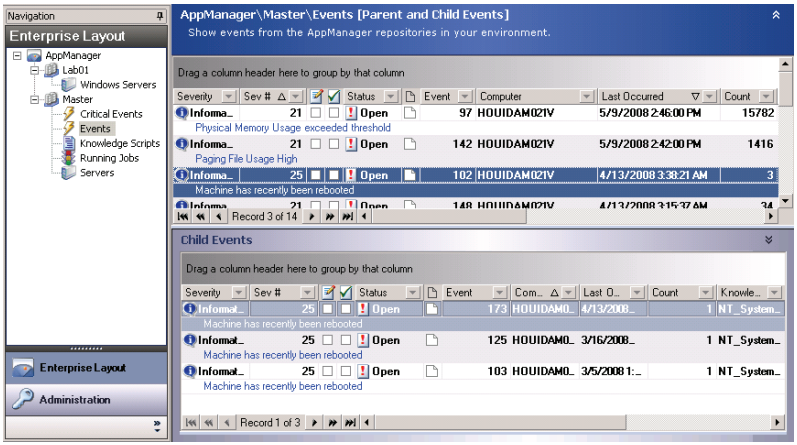
Working with Event Views

Event views provide an easy way to view and manage a subset of the events in a management group. An Event view works like the Events tab in the Server view discussed in "Looking at Events" on page 127.

Looking at Events

Events for each job are organized in a parent-child relationship under the Events view. The first event generated by a particular job creates both a parent and a child event entry. Subsequent events from the same job are then listed under the same parent event, and an event count keeps track of how many event occurrences are generated.

In the Events view, select a parent event from the top pane to view its child events. In the example below, the NT_SystemUptime job has raised 3 events on the HOUIDAM021V computer to indicate the computer has been rebooted 3 times since the NT_SystemUptime job started.



About Filtering Events

By default, the Control Center Console displays all of the events in your management group in list form, with each event as a separate entry. As AppManager detects event conditions across all of the computers in your enterprise, you may want to filter the list of events to make events easier to manage. For example, you may want to organize events by Status or Severity Level.

There are two ways to filter events:

- Filter the Event view to improve the overall performance of the Control Center Console. View filters allow you to reduce the amount of information that is available for display in the Control Center Console.
- Filter the list of events in the Event view to only display the events you want. The event information is still available from the Control Center Console and there is no reduction in the amount of information managed by the Control Center Console.

Filtering the Event View

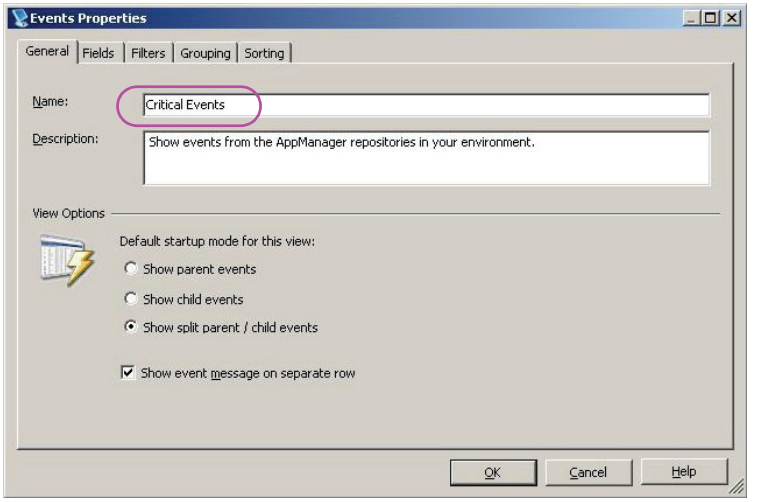
The monitoring policy you configured for the management group raises events with different event severity levels. For trial purposes, filter the standard, out-of-the-box Events view provided with the Master management group to only display events with a `Severe` or `Warning` status.

To filter the default Events view:

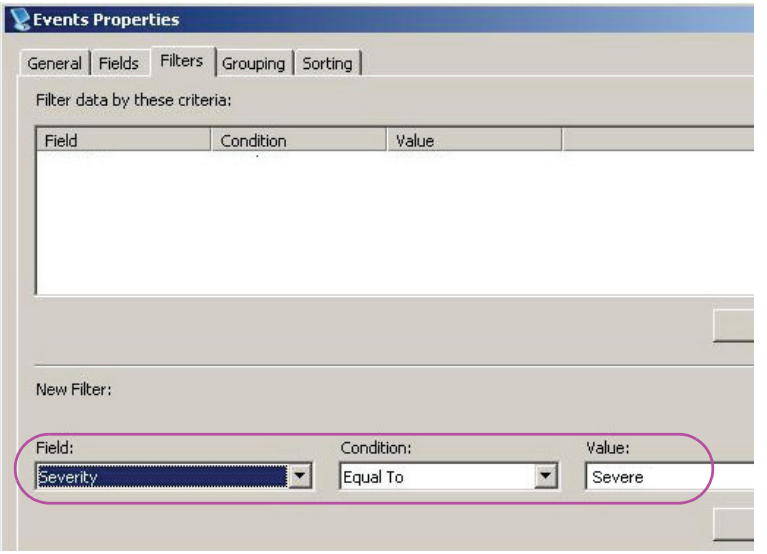
1 In the Master management group, right-click the **Events** view, then click **Properties**.



2 On the General tab of the Events Properties dialog box, change name of the view. In the Name field, type `Critical Events`.

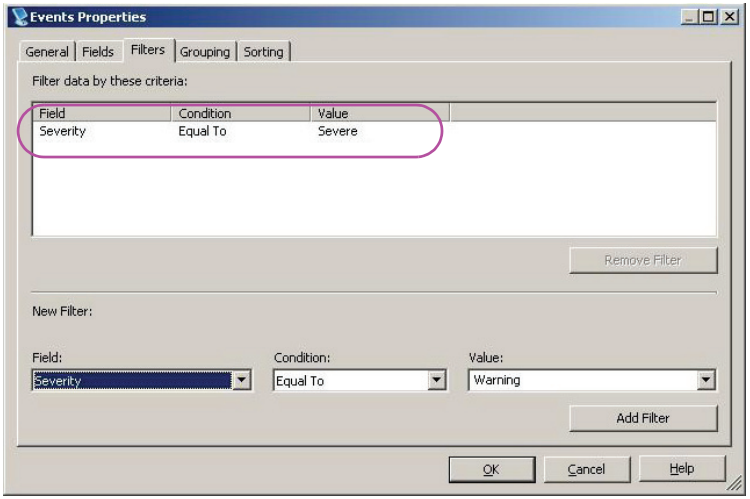


3 On the Filters tab, create filter criteria to select events with a `Severe` status.

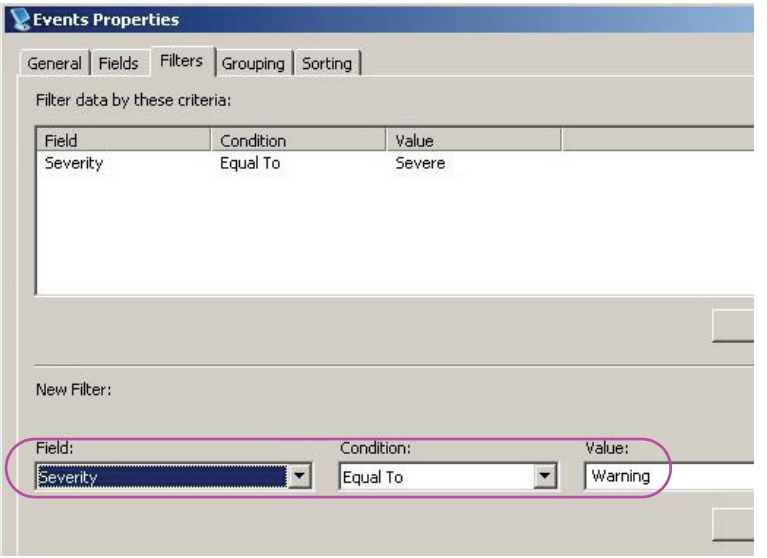


For	Do this
Field	Select `Severity`
Condition	Select `Equal To`
Value	Select `Severe`

4 Click **Add Filter** to add the filter to the list.

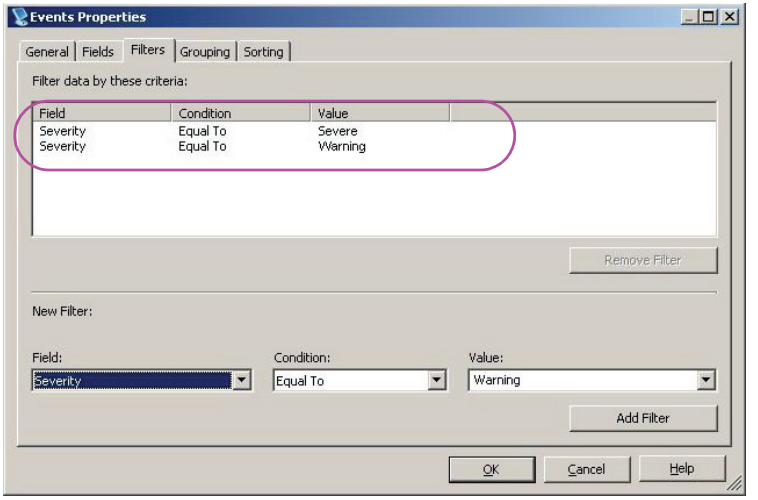


5 On the Filters tab, create filter criteria to select events with a `Warning` status.



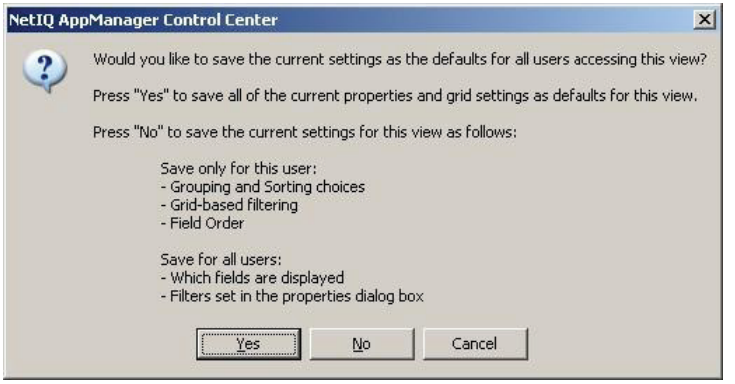
For	Do this
Field	Select `Severity`
Condition	Select `Equal To`
Value	Select `Warning`

6 Click **Add Filter** to add the filter to the list.



7 Click **OK**.

8 Click **Yes** to save your filter settings for all Control Center Console users.



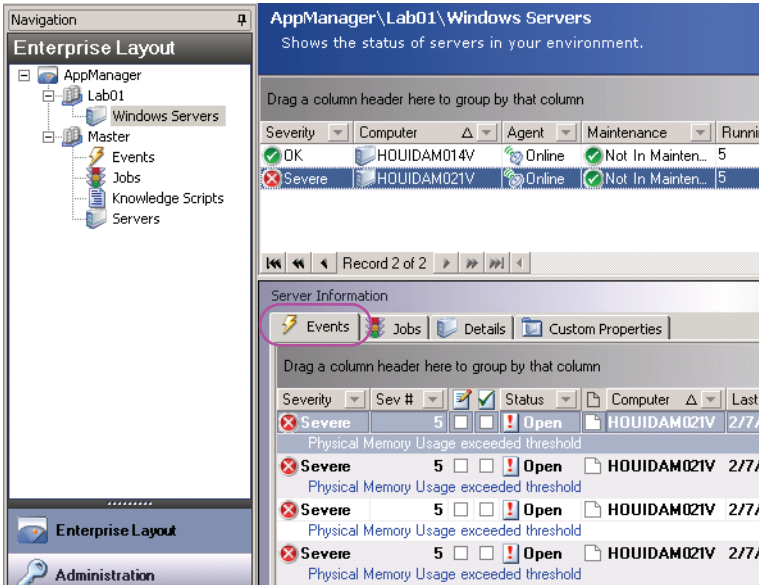
The Events view of the Control Center Console displays events with a severity of `Critical` and `Warning`.

Acknowledging an Event

The monitoring policy you configured for the management group raises events with different event severity levels. For trial purposes, acknowledge an event to indicate that you are aware of the event condition.

To acknowledge an event:

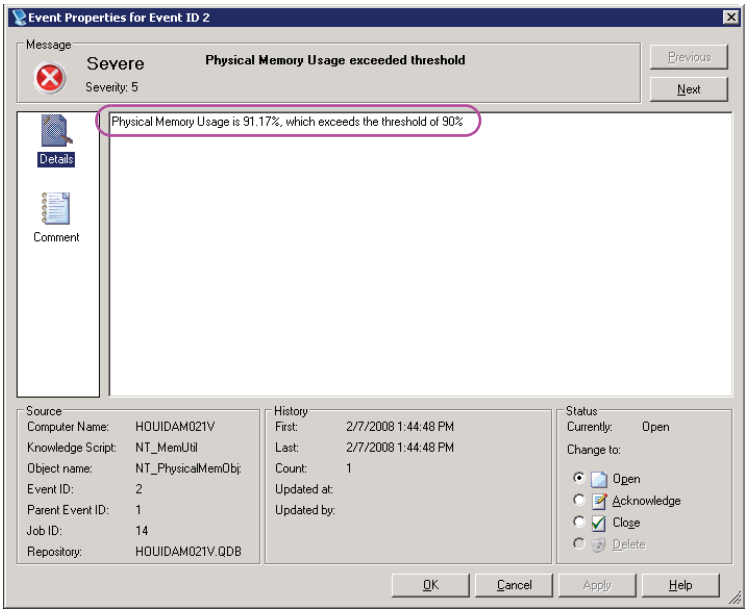
1 In the Windows Servers view, browse the list of computers and in the Severity column, look for an event with a Severe status. In the example below, there is an event with a `Severe` status on `HOUIDAM021V`.



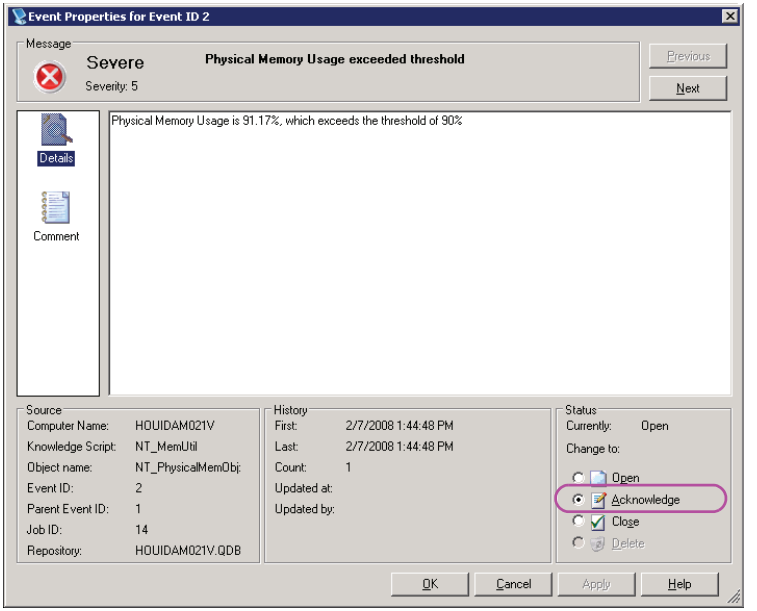
2 Select the computer with the `Severe` event status and click the **Events** tab.

3 On the Events tab, you see a list of events on the computer. Double-click an event to display more information about the event.

4 In the Event Properties dialog box, view the event details message.



5 From this dialog box, acknowledge the event by clicking **Acknowledge** and then clicking **OK**.



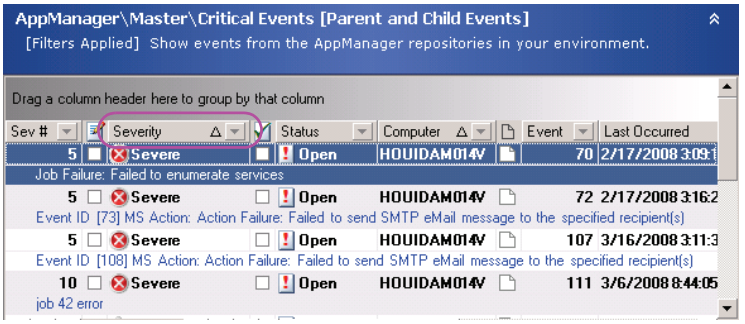
6 In the Events tab, the status of the event changes to Acknowledged.

Organizing and Managing Groups of Events

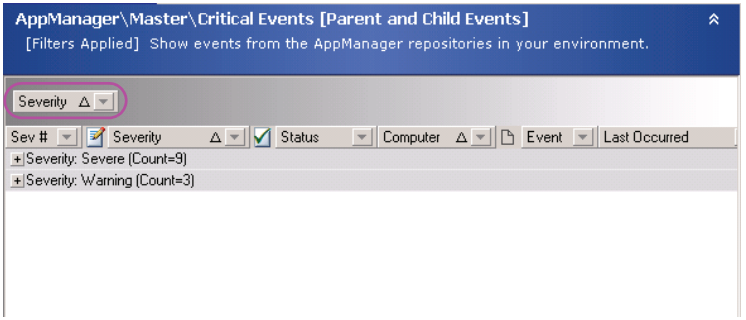
To help you quickly and easily manage a large number of events, you can organize events into groups. For trial purposes, group events by Severity and Computer. You can also respond to the events that belong to a group, for example, by acknowledging all of the events on a computer.

To group events by Severity and Computer:

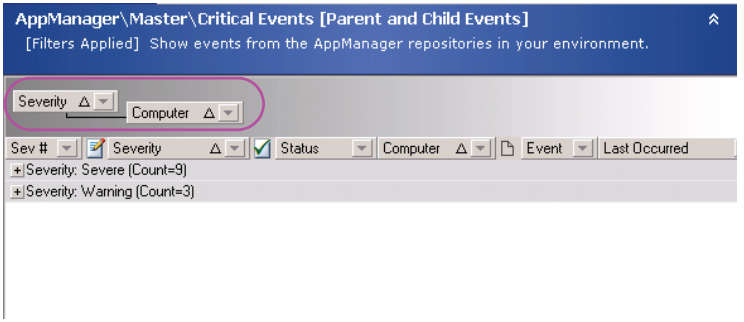
1 In the Critical Events view, find the Severity column.



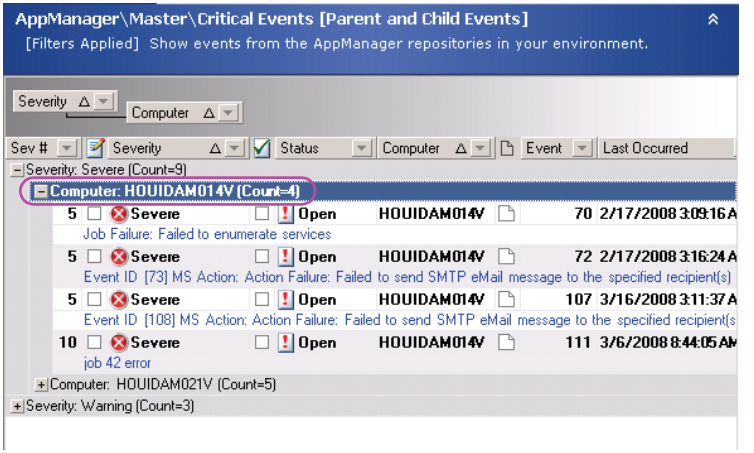
2 Drag the **Severity** column into the Group By field to group events by Severity.



3 Drag the **Computer** column under Severity in the Group By field to group Computers by Severity.

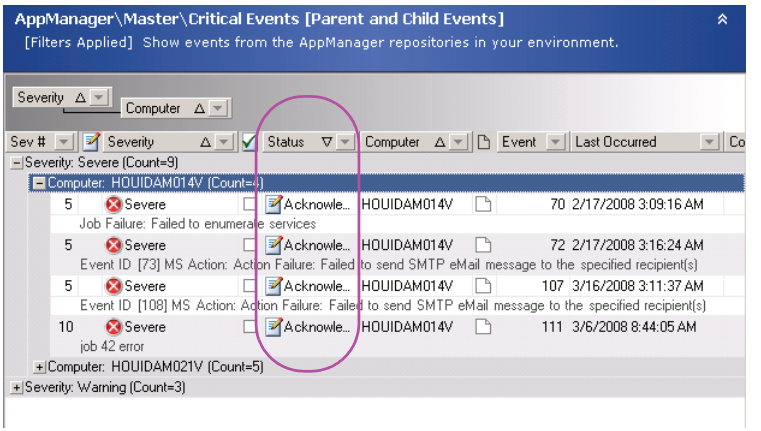


4 To expand the detailed event information for any group, click the + (plus sign) to the left of the group.



5 To respond to a group of events, right-click a group and click a command. For example, to indicate that you are aware of all events on a computer, right-click the group and click **Acknowledge Events**.

6 In the Status column, the status of the event changes to Acknowledged.



7 To remove a group, right-click a group in the Group By field and click **Ungroup**. For example, if you initially group computers by event severity, and you notice several events, you can investigate whether a particular computer is experiencing problems by removing the Severity grouping to see events by Computer.

Working with Job Views

A Job view provides an easy way to view and manage a subset of the jobs in a management group. For example, if you have created jobs to monitor a particular resource, you can update the job properties to change the job schedule or event thresholds. To modify policy-based jobs, you must do so from the properties of the management group.

A Job view works like the Jobs tab in the Server view discussed in "Looking at Jobs" on page 125. However, unlike a Server view, you cannot create jobs from a Job view.

About Filtering Jobs

By default, the Control Center Console displays all of the jobs in your management group in list form, with each job as a separate entry. As you add more jobs across all of the computers in your enterprise, you may want to filter the information displayed to make jobs easier to manage.

For example, you may want to organize jobs by Status or Computer. Creating a Job view for Stopped, Errored, and Pending jobs provides a great quick check for IT administrators to make sure their system is healthy.

There are two ways to filter jobs:

- Filter the Job view to improve the overall performance of the Control Center Console. View filters allow you to reduce the amount of information that is available for display in the Control Center Console.
- Filter the list of jobs in the Job view to only display the jobs you want. The job information is still available from the Control Center Console and there is no reduction in the amount of information managed by the Control Center Console.

Filtering the Job View

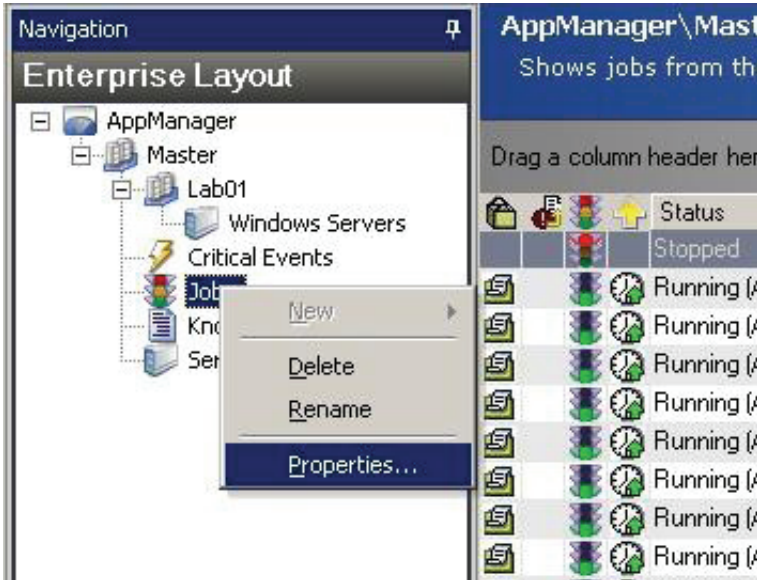
For trial purposes, filter the standard, out-of-the-box Jobs view to only display jobs with a status of `Running`. The policy-based jobs that are created by the monitoring policy on the management group have a status of `Running`.

The Discovery jobs that were created as part of the agent installation process, such as Discovery_NT, have a status of `Stopped` because they are scheduled to `Run Once`. After you filter the Job view, the Control Center Console hides the Discovery jobs from the Job view.

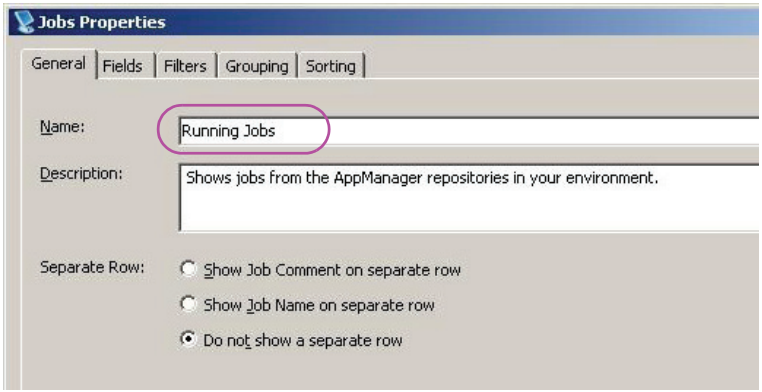
Tip Not all Discovery jobs run once. Some run on a weekly schedule in order to detect new devices.

To filter the default Jobs view:

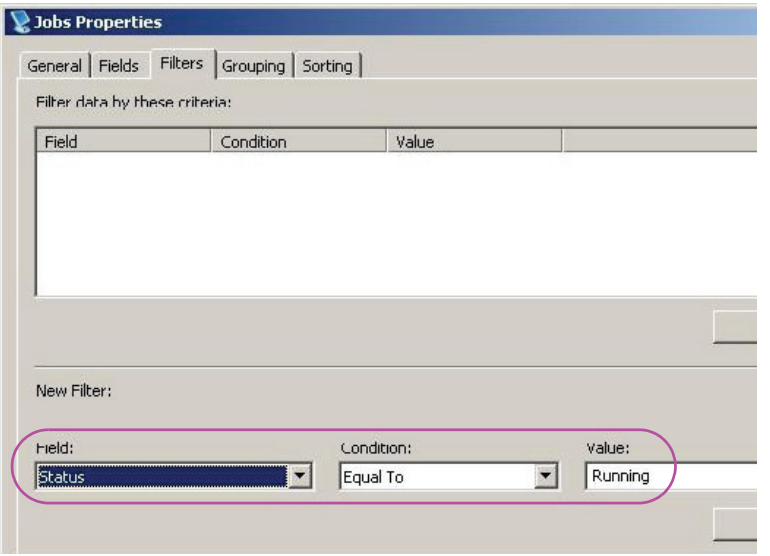
1 In the Master management group, right-click the **Jobs** view, then click **Properties**.



2 On the General tab of the Jobs Properties dialog box, change name of the view. In the Name field, type `Running Jobs`.

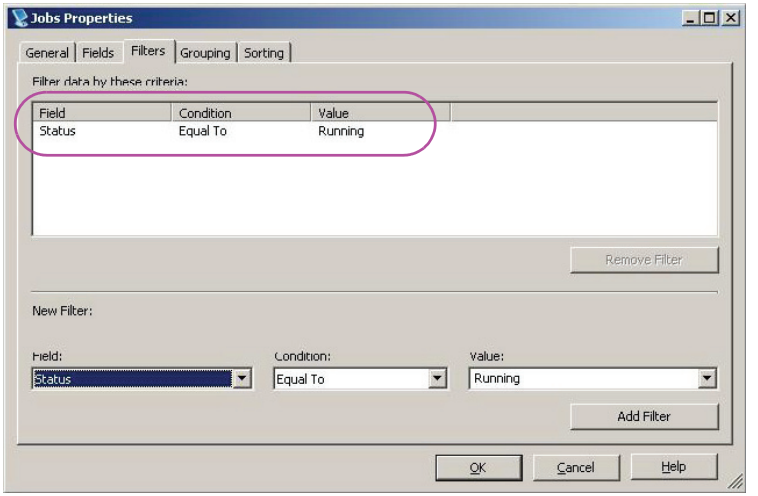


3 On the Filters tab, create filter criteria to select jobs with a `Running` status.



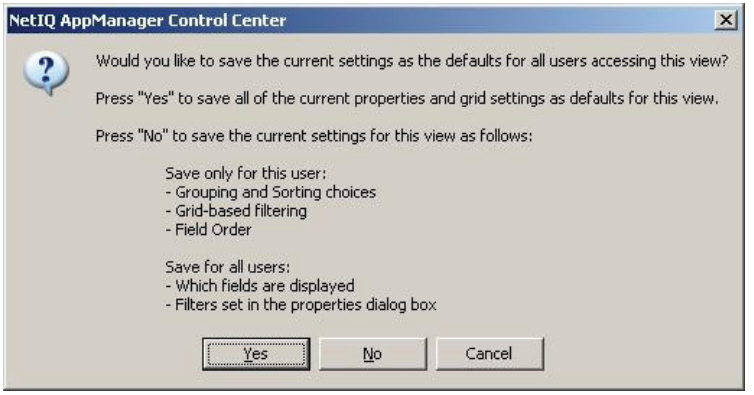
For	Do this
Field	Select `Status`
Condition	Select `Equal To`
Value	Select `Running`

4 Click **Add Filter**.



5 Click **OK**.

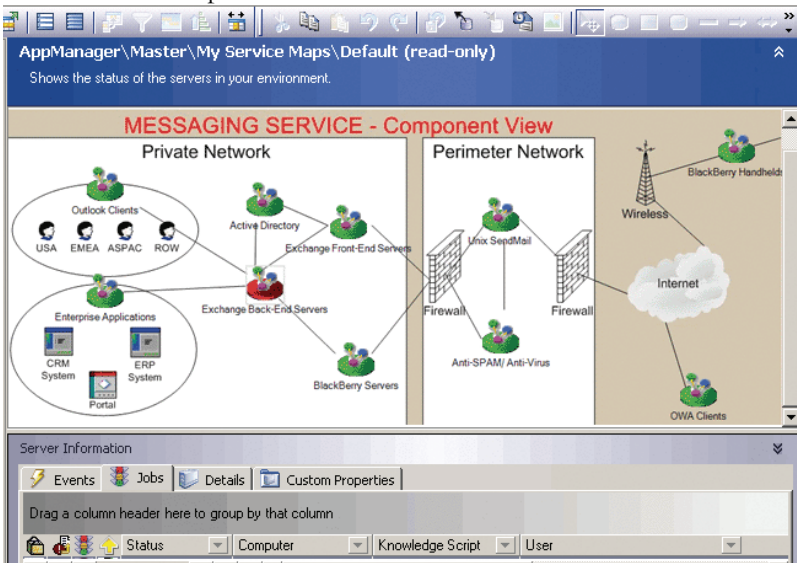
6 Click **Yes** save your filter settings for all Control Center Console users.



The Jobs view of the Control Center Console displays jobs with a status of `Running`. The Jobs view does not display Discovery jobs with a `Stopped` status.

Understanding Service Map Views

A **Service Map view** provides a visual representation of IT resources mapped to business applications or services, enabling you to prioritize problem response. By mapping services to elements, you can visually recognize all elements the service depends upon and understand how element failure impacts the service.



A Service Map view allows you to:

- Manage events
- Manage jobs
- View details about discovered resources
- Manage custom properties

A Service Map view visually represents the computing infrastructure that underlies a business process, such as:

- The computers, servers, databases, and network devices that allow customers to make purchases from a Web site
- The computers, servers, and mail stores that support e-mail
- The domain controllers, sites, and domains of your Active Directory

The discovered AppManager objects in a Service Map view change color to indicate the most severe Open event condition associated with that object or one of its child objects. If you see an indication of a problem, respond to the problem, for example, by acknowledging the event or changing the corresponding job properties.

To simplify the management of the resources in a Service Map view, create filtered views that select the resources represented in the Service Map view, and embed the views into the Service Map view.

The Control Center Console allows you to embed a Service Map view, Event view, or Server view into a Service Map view. A Service Map view uses an icon to represent an embedded view. The embedded view icon changes color to indicate the most severe Open event conditions associated with that view.

When you see an indication of a problem, open the embedded view or perform additional tasks on that view from the Service Map view, such as acknowledge the event or change the corresponding job properties.

For assistance with evaluating service maps, contact your NetIQ Sales Representative or NetIQ Partner.

Understanding Charts

The Chart Console allows you to investigate problems on a computer by analyzing recent data collected by AppManager. By default, you can chart data collected by AppManager from the past 8 days to identify when and where a problem started. Charts show raw data only, and unlike reports, do not calculate averages, maximums, minimums, and comparisons.

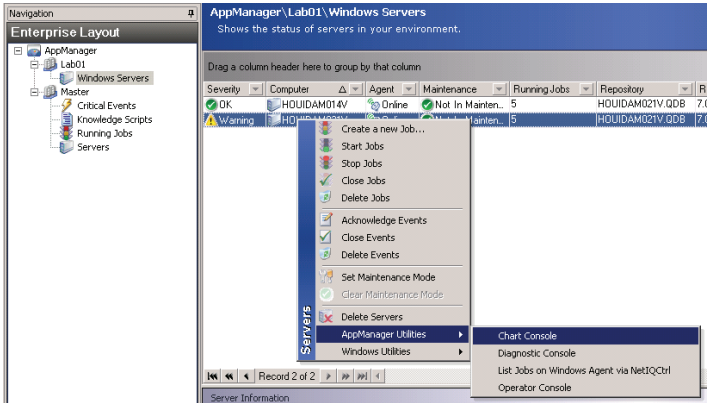
To understand possible causes, use AppManager reports to analyze the data over periods longer than 8 days. AppManager reporting is not featured in the product tour. Please discuss your AppManager reporting needs with your NetIQ Sales Representative or NetIQ Partner.

To view data in a 3-D chart, you first need to create a Knowledge Script job that collects data. When the Knowledge Script job runs at its scheduled interval, the job collects data points and stores them in the AppManager repository. The data collected in a single iteration of a Knowledge Script job is considered a **data point**. A series of these data points, collected as a Knowledge Script job runs on its scheduled interval, is called a **data stream**.

You configured the NT_SystemPolicy, NT_SystemUptime, and NT_MemUtil monitoring policy jobs to collect data. Use the Chart Console to view this data in a chart.

To create a 3-D chart:

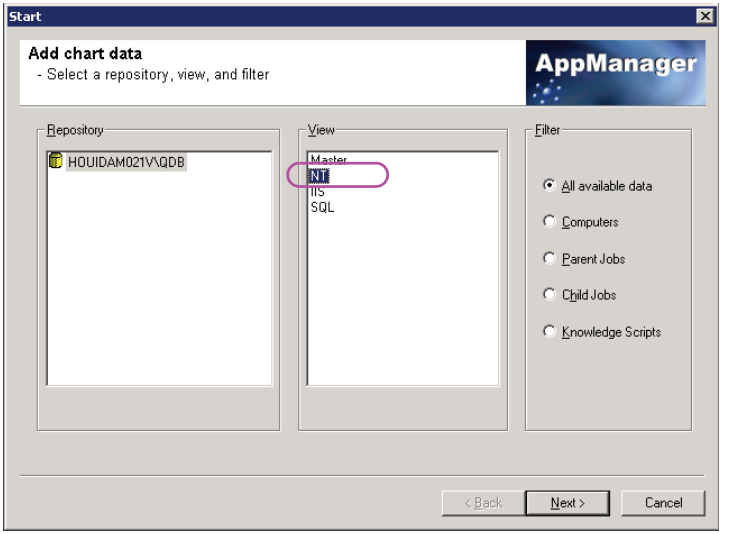
1 In the Windows Server view, right-click a server and click **AppManager Utilities > Chart Console**.



2 In the Chart Console, click the **Public** folder and click **Chart > Create Chart**.

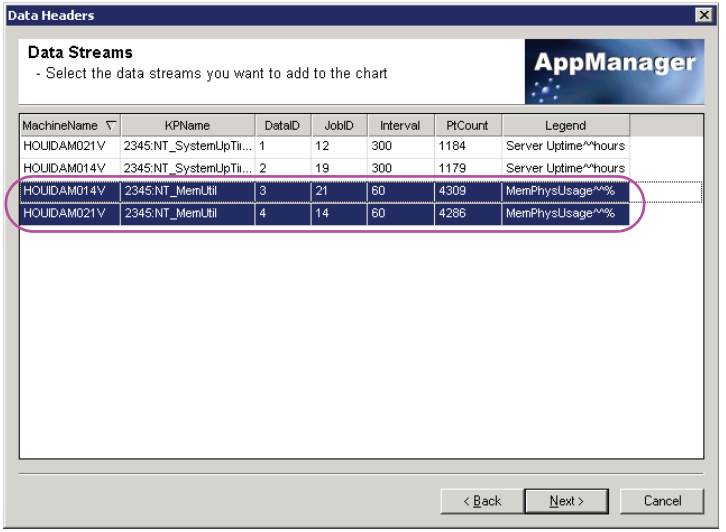
Tip AppManager console users must have permission to view charts in the Public folder.

3 In the Chart wizard, select the **NT** view to select from data collected by NT Knowledge Scripts.



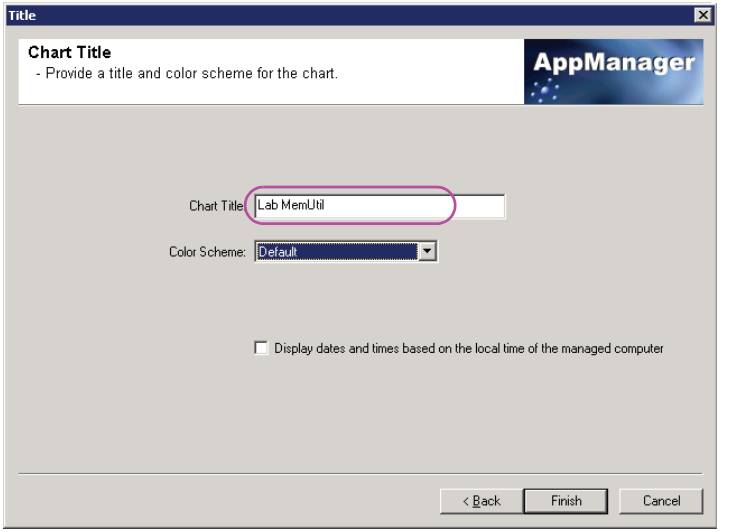
4 Click **Next**.

5 In the Chart wizard, select the data streams you want to add to the chart. Press Shift+Click or Ctlr+Click to select multiple data streams.



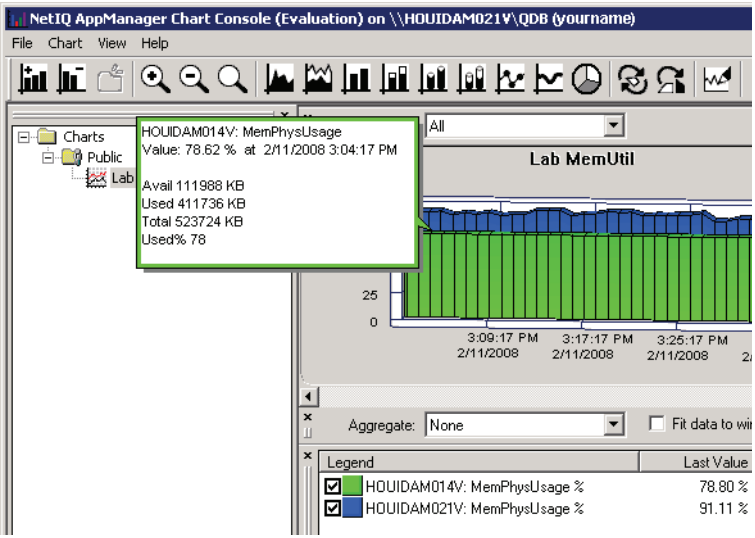
6 Click **Next**.

7 In the Chart wizard, type a chart title, for example, `Lab MemUtil`. Optionally, choose a color scheme for the chart.



8 Click **Finish**.

9 In the left pane of the Chart Console, click **Lab SystemUptime** to display the chart.



Place your cursor over a data point to display its details.

You have completed the product tour. For more information and assistance with evaluating AppManager, contact your NetIQ Sales Representative or NetIQ Partner.

Index

A

acknowledging events 128
Administration pane 86
agent
  deployment 10
  role in architecture 6
Analysis Center, introduction 14
applications, monitoring 18
AppManager
  Chart Console 5
  extended support x
  features and benefits 3, 4
  installing 19
  management server 6
  Operator Console 5
  Operator Web Console 5
  product tour 73
  repository 6
  Security Manager 5
  Web management server 6
automation, AppManager 3

C

Chart Console
  role in AppManager architecture 5
  viewing 3-D charts 148
charts, viewing data 148
child events 129
closing events 128
configuration, for evaluating AppManager 19
Control Center
  Cache Manager 8
  Command Queue Service 8
  console security 74
  Control Center Console 8
  deployment
    package 87
    rule 87
    service 11
    tasks 87
    web service 12
  repositories 8
customization, AppManager 3

D

data
  data point 148
  data stream 148
database
  AppManager repository 6
  Control Center repository 8
  primary AppManager repository 8
discovery, introduction 85
dynamic thresholding, Performance Profiler 14

E

end-user perspective, monitoring 1
evaluation period, AppManager 28

events
acknowledging 127, 136
checking status 127
closing 127
filtering 130, 142
grouping 138
parent-child relationship 129
severity levels 128
viewing details 137

F

features and benefits, AppManager 3
filtering
events 130, 142
jobs 141

I

installing AppManager
AppManager
agent 42
consoles 67
database 27
management server 37
Web management server 52
Control Center components 57
license keys 28
permissions 24
pre-installation check 25

J

jobs
changing properties 110
filtering 141
icon for policy-based jobs 125
introduction 106
starting automatically 122
status 125
viewing properties 125

K

Knowledge Scripts
Discovery 85
introduction 1
Knowledge Script Groups 107
Report 13
viewing categories 111

L

Linux
agent architecture 6
monitoring 18

M

managed object, role in architecture 6
management groups
introduction 77
policy-based monitoring 107
using rules to select computers 78
management server 6
module, introduction 10

N

netiq account
- AppManager repository installation 32
- Control Center installation 60
- management server installation 40

NetIQ technical support 18
`No Repositories` message 75

O

Operator Console 5
Operator Web Console 5

P

parent events 129
Performance Profiler, introduction 14
permissions
- database owner
  - AppManager 32
  - Control Center 60
- management groups 77
- running the setup program 24
- starting the Control Center Console 74

policy-based monitoring 107
predicting behavior, Performance Profiler 14
pre-installation check
- introduction 24
- viewing results 26

primary AppManager repository 76

R

remote agent installation, see *agent deployment*
reporting
- Analysis Center 14
- capabilities 12
- report agent installation 43
- Report Knowledge Scripts 13

requirements, for evaluating AppManager 19
responsetime 1
rules
- for a management group 77
- for deploying AppManager 86

S

Server view, creating 84
Service Map views
- embedding views 147
- introduction 146

severity, for events 128
SMTP mail, responsive action 113
supported applications 18
system requirements, for evaluating AppManager 19

T

technical support 18
time to value 3
troubleshooting, `No Repositories` message 75

U

UNIX
- agent architecture 6
- monitoring support 18

V
views
embedding in a service map 147
Event view 128
introduction 77
Job view 141
Knowledge Script view 111
Server view 84, 124
Service Map view 146
VoIP, monitoring with AppManager 17

W
Web Management Server 6
Windows
agent architecture 6
monitoring support 18