Trial Guide

NetIQ® AppManager®

February 2012



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.

© 2012 NetIQ Corporation. All rights reserved.

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

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

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

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

This product claims FIPS compliance by use of one or more of the Microsoft cryptographic components listed below. These components were certified by Microsoft and obtained FIPS certificates via the CMVP.

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

This product may also claim FIPS compliance by use of one or more of the Open SSL cryptographic components listed below. These components were certified by the Open Source Software Institute and obtained the FIPS certificates as indicated.

918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1

1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1

1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

Note: Windows FIPS algorithms used in this product may have only been tested when the FIPS mode bit was set. While the modules have valid certificates at the time of this product release, it is the user's responsibility to validate the current module status.

EXCEPT AS MAY BE EXPLICITLY SET FORTH IN THE APPLICABLE END USER LICENSE AGREEMENT, NOTHING HEREIN SHALL CONSTITUTE A WARRANTY AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY NETIQ, ITS SUPPLIERS AND LICENSORS.

Contents

About this Book and the Library **7**
About NetIQ Corporation **9**

1 Introducing AppManager **11**

1.1 What is AppManager? . . . 12
1.2 What is Unique about AppManager? . . . 12
1.3 How Does AppManager Work? . . . 13
1.3.1 AppManager Architecture and Components . . . 13
1.3.2 Control Center Architecture and Components . . . 15
1.4 How Does Deployment Work? . . . 16
1.4.1 Rule-based Deployment . . . 16
1.4.2 Approval-based Deployment Tasks . . . 16
1.4.3 Agent Deployment Architecture and Components . . . 17
1.5 Does AppManager Provide Reporting Capabilities? . . . 17
1.5.1 Analysis Center . . . 18
1.6 Can AppManager Manage and Predict the Behavior of My IT Environment? . . . 19
1.7 Does AppManager Provide a VoIP Management Solution? . . . 20
1.8 How Do I Locate a Particular AppManager Module? . . . 21

2 Installing AppManager **23**

2.1 System Requirements for Evaluating AppManager . . . 23
2.2 Configuring Windows Application Services . . . 24
2.3 Starting the Installation . . . 25

3 Exploring AppManager **35**

3.1 Starting the Control Center Console . . . 35
3.2 Understanding Management Groups . . . 39
3.2.1 About Control Center Console Views . . . 39
3.2.2 Creating a Rule-based Management Group . . . 40
3.2.3 Creating a Server View . . . 46
3.3 Understanding Agent Deployment . . . 48
3.3.1 About the Deployment Pane . . . 49
3.3.2 Before You Begin . . . 49
3.3.3 Configuring a Rule to Deploy the Agent . . . 50
3.3.4 Enabling the Rule . . . 72
3.3.5 Approving Deployment Tasks . . . 73
3.4 Understanding Monitoring Policies . . . 74
3.4.1 Creating a Knowledge Script Group . . . 75
3.4.2 Enabling the Monitoring Policy . . . 91
3.5 Working with Server Views . . . 93
3.5.1 Looking at Jobs . . . 94
3.5.2 Viewing the Properties of a Job . . . 94
3.5.3 Looking at Events . . . 95
3.6 Working with Event Views . . . 96
3.6.1 Looking at Events . . . 96
3.6.2 About Filtering Events . . . 96
3.6.3 Filtering the Event View . . . 97

3.6.4 Acknowledging an Event . . . 102
3.6.5 Organizing and Managing Groups of Events . . . 104
3.7 Working with Job Views . . . 106
3.7.1 About Filtering Jobs . . . 107
3.7.2 Filtering the Job View . . . 107
3.8 Understanding Service Map Views . . . 110
3.9 Understanding Charts . . . 111
3.9.1 Viewing the Charts Tab . . . 112
3.9.2 Displaying the Chart . . . 113
3.9.3 Modifying the Chart Type . . . 114
3.9.4 Using the Chart Console . . . 115
3.10 What's Next? . . . 119

About this Book and the Library

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

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

Intended Audience

This guide provides step-by step instructions to help you evaluate and discover the main features of the AppManager Suite. Through this hands-on trial, you will be able to provide a centrally managed solution for performance, availability, and server health for a broad spectrum of operating environments, applications and server hardware.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

Upgrade and Migration Guide

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

Control Center User Guide

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

Administrator Guide

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

Management Guides

Provide information about installing and monitoring specific applications with AppManager.

Conventions

The library 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 CD-ROM titles ◆ Variable names and values ◆ Emphasized words
`Fixed Font`	◆ File and folder names ◆ Commands and code examples ◆ Text you must Specify ◆ Text (output) displayed in the command-line interface
Brackets, such as *[value*]	◆ Optional parameters of a command
Braces, such as {*value}*	◆ Required parameters of a command
Logical OR, such as *value1*|*value2*	◆ Exclusive parameters. Choose one parameter.

About NetIQ Corporation

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

Contacting Sales Support

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

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

Contacting Technical Support

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

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 Introducing AppManager

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 2007/2010
- BlackBerry Enterprise Server
- Oracle Grid Computing
- Cisco or Avaya/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.

1.1 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 provides 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.

1.2 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 are 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.

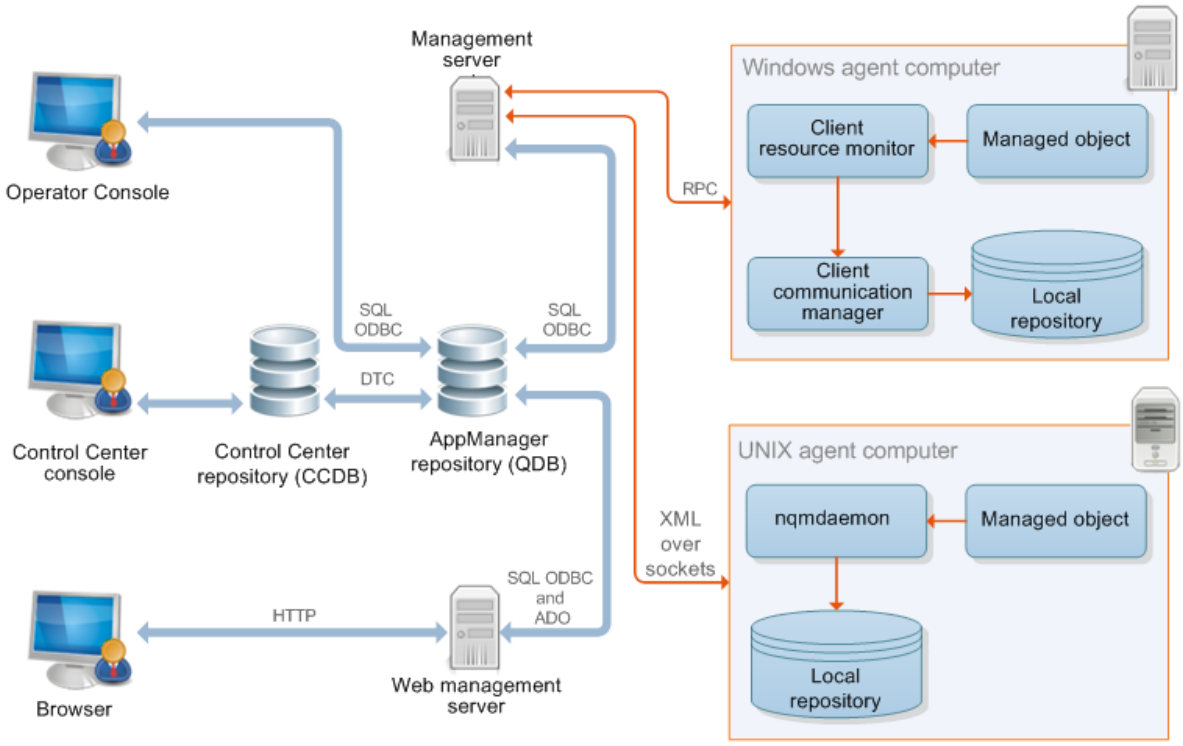
1.3 How Does AppManager Work?

AppManager uses a scalable, flexible, tiered architecture that allows components to communicate efficiently and allows you to distribute process load across multiple components. The advanced multi-tier architecture scales along with the growth of your organization's IT infrastructure.

1.3.1 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 following graphic illustrates the overall AppManager architecture and how components interact, including both the Operator Console and the Control Center Console.



The AppManager architecture consists of the following components:

- **AppManager Consoles:** A collection of programs for managing various aspects of your environment:
  - **Operator Console:** A Windows interface that allows you to view and control the jobs that monitor and manage your computers and server applications. It also allows you to make advanced configuration changes to the AppManager repository database.
  - **Control Center Console:** A Windows interface that connects to the Control Center repository and allows you to run jobs on the systems and applications you manage across multiple AppManager repositories.

The console provides a single user interface for managing most administrative functions and offers more powerful monitoring and deployment capabilities than the Operator Console. You can use the Control Center Console to deploy agents and modules to remote computers.

- **Operator Web Console:** A browser-based interface that 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.
- **Chart Console:** An interface that lets you generate and view charts of data streams generated by Knowledge Script jobs in a particular AppManager repository data. The Chart Console can run as a stand-alone application or inside the Operator Console, Control Center Console, and Operator Web Console.
- **Security Manager Console:** A Windows interface that allows AppManager administrators to control access to views and tasks in the Operator Console and manages application or computer-specific security information, such as SNMP community strings and passwords.
- **UNIX Agent Manager Console:** An interface that allows you to use the UNIX Agent Manager to deploy and manage UNIX agents.

- **AppManager Repository:** A SQL Server database that stores management information, such as jobs, events, data, and Knowledge Scripts. The Operator Console connects to the AppManager repository.
- **AppManager Management Server:** A Windows service, NetIQ AppManager Management Service (NetIQms), that manages event-driven communication between the AppManager repository and AppManager agents. It also handles the software inventory for AppManager agents.
- **AppManager Agent:** AppManager software you deploy in your environment that schedules and runs jobs to manage third-party products and enables communication between AppManager components. It receives requests from the management server to run, stop, or delete a Knowledge Script job. The agent communicates back to the management server, any relevant output from a Knowledge Script, at regular intervals.

  For Windows computers, the agent consists of the following components that reside locally on the agent computer:

  - NetIQ AppManager Client Resource Monitor (NetIQmc) Windows service
  - NetIQ AppManager Client Communication Manager (NetIQccm) Windows service
  - Local repository
  - AppManager for Microsoft Windows module

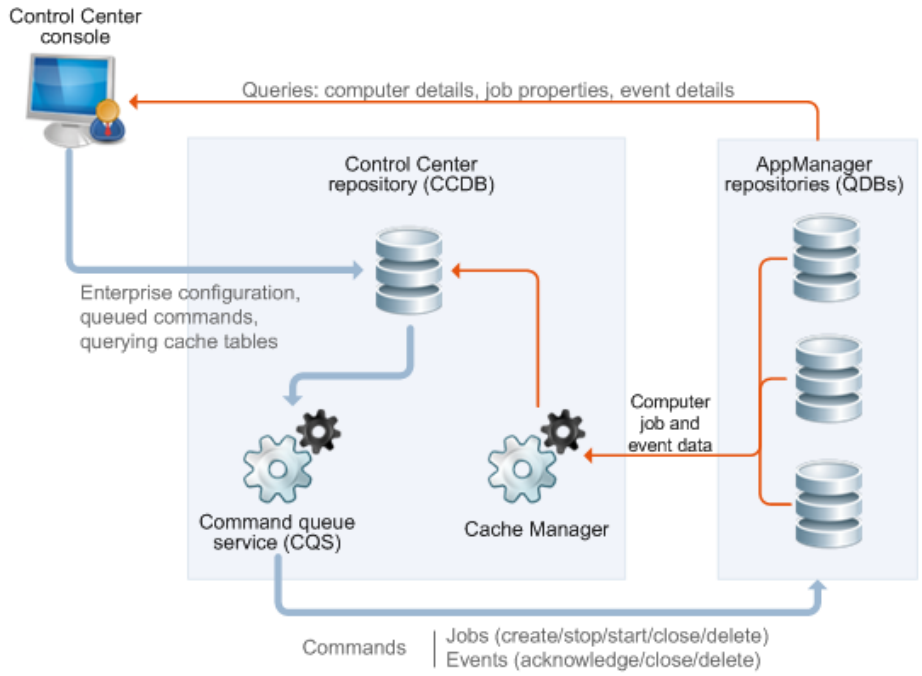
  For UNIX or Linux computers, the agent consists of a single daemon and the supporting files and directories that provide data persistence (equivalent to the local repository) and access to system statistics (equivalent to modules). AppManager uses the NetIQ UNIX agent, which can be used for other NetIQ products. For more information about how to install the UNIX agent, see the UNIX agent documentation, which is included in the AppManager UNIX download package.
- **Control Center Repository (CCDB):** A SQL Server database that stores information, such as user preferences, security settings, and management group definitions, which Control Center collects from the AppManager repository it manages.

- **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.

1.3.2 Control Center Architecture and Components

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



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:
- **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.
- **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.
- **Cache Manager:** 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.

- **Deployment Service:** Allows you to install agents and monitoring modules on remote computers across a firewall.
- **Deployment Web Service:** Distributes deployment packages to the Deployment Service and provides a communication proxy for Deployment Services that are across a firewall.

1.4 How Does Deployment Work?

The Control Center Console and UNIX Agent Manager allow you to quickly and easily deploy the AppManager agent and AppManager modules to the remote Windows computers in your environment. This section describes deploying Windows components. For more information about using UNIX Agent Manager, see the NetIQ UNIX Agent documentation, which is included with the AppManager UNIX agent installation kit.

TIP: An AppManager module is a downloadable package that provides an updated module for an application. A module includes a managed object, Knowledge Scripts, and Help. For the most current information about module updates, see Module updates.

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

1.4.1 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 identify computers where you want to install agents and appropriate modules based upon a variety of criteria, including:

- Agent
- Domain
- Specific computers
- Computer list file
- Management groups in the Control Center console

1.4.2 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.

1.4.3 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 agent computer using credentials provided in the deployment rule.

The computer where you install the Deployment Service is the **deployment server**. If you configure more than one Deployment Service to work with your Control Center repository, you can configure a deployment rule to deploy the agent or modules by using a certain deployment server.

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 sites that are installed on a Microsoft Internet Information Services (IIS) server. The computer where you install the Deployment Web Service and check in the installation packages is the **Web Depot**. The deployment web service performs the following actions:

- Checks in deployment packages to the Web Depot.
- Distributes installation packages to the Deployment Services. The Deployment Web Service uses Microsoft Background Intelligent Transfer Service (BITS) server extensions to distribute installation packages to the Deployment Service.
- Communicates with 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 using Control Center, but you can deploy using UNIX Agent Manager.

1.5 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:

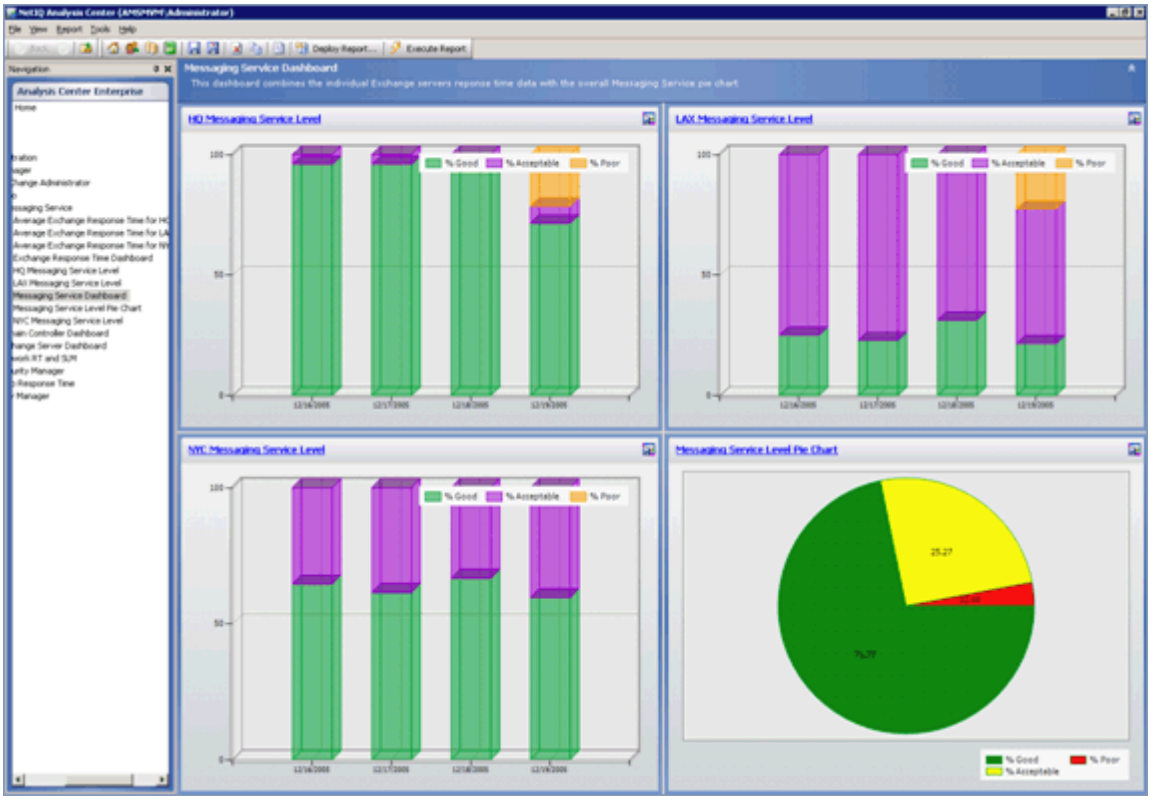
- **Performance-related reports** to help you understand the performance of your applications and systems.
- **Trend analysis reports** to help you plan for system or application upgrades.
- **Service level agreement reports** to quantify the availability of services and service response time.
- **Event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

1.5.1 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 exploring AppManager chapter. Please discuss your AppManager reporting needs with your NetIQ Sales Representative or NetIQ Partner.

1.6 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.

1.7 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.

1.8 How Do I Locate a Particular AppManager Module?

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\Module Guides
```

For the most current information about supported products, including version support, see AppManager Supported Products.

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.

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.

2.1 System Requirements for Evaluating AppManager

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

Requirement	Configuration for evaluation purposes
Processor	◆ Minimum: 2 GHz or higher ◆ Recommended: Dual-core, 2.4 GHz or higher
Memory	Minimum: 4 GB Recommended: 8 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

Operating System	Microsoft Windows Server 2008 or 2008 R2, Standard or Enterprise edition, with or without Service Pack 1, which includes the following required components: ◆ 128-bit encryption support ◆ 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) version 4.0

Requirement	Configuration for evaluation purposes
Database Server	Microsoft SQL Server 2008 or 2008 R2, Standard or Enterprise edition ◆ Microsoft .NET Framework 3.5 Service Pack 1 ◆ Microsoft XML Parser 6.0 (msxml6) Service Pack 1
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 2008. For trial purposes, you do not need to authenticate network DTC access. Configure the credentials for DTC service to use the NT AUTHORITY\NetworkService account. ◆ **ASP.NET** with v2.0.50727 Web Service Extension enabled ◆ **Internet Information Services (IIS) 6.0** Management Compatibility role service with the IIS 6 Metabase Compatibility component.
Web browser	◆ Minimum: Microsoft Internet Explorer 8.0.

2.2 Configuring Windows Application Services

If you did not install the Windows Application Services, including IIS and ASP.NET, when you installed Windows Server 2008, install and configure these services.

To configure Windows Application Services:

1. Select **Server Manager** from **Administrative Tools**.
2. In the **Server Manager**, select the **Features** in the left hand pane, and then click **Add Features** to start the Add Features Wizard.
3. On the **Select Features** page, select the **BITS Server Extensions** check box.

   BITS Server Extensions includes the BITS operating system feature and the BITS Server Extensions component of Microsoft IIS.

   When prompted, click **Add Required Role Services** to add the dependent components, including the Web Server (IIS) role.
4. Select the **Remote Differential Compression** check box, and click **Next**.
5. On the **Web Server (IIS)** page, click **Next**.
6. On the **Select Role Services** page, select the **ASP.NET** check box.

   When prompted, click **Add Required Role Services** to add the dependent components.
7. Select the **Windows Authentication** check box under Security. section
8. Under **Management Tools** section, ensure that both the **IIS 6 Metabase Compatibility** and **IIS 6 WMI Compatibility** check boxes are selected, and then click **Next**.
9. On the **Confirmation** page, click **Install**.
10. Click **Close** to exit the wizard, and then close Server Manager.

To install and configure Network DTC Access:

1. Select **Component Services** from **Administrative Tools**.
2. In the **Component Services** window, expand **Component Services** and then expand **Computers**.
3. Expand **My Computer** and then expand **Distributed Transaction Coordinator**.
4. Right-click **Local DTC** and select **Properties**.
5. On the **Security** tab, select the following items:
   - Network DTC Access check box
   - Allow Remote Clients check box
   - Allow Remote Administration check box
   - Allow Inbound check box
   - Allow Outbound check box
   - No Authentication Required radio button
   - Enable XA Transactions check box
6. Click **OK** to save the settings.

NOTE: Windows 2008 will automatically restart the DTC service once the settings are saved.

2.3 Starting the Installation

This guide provides information about installing and evaluating AppManager 8.0.1. You can download AppManager 8.0.1 from the AppManager Support Resources area of the NetIQ web site.

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 exploring the product, you can install the agent to monitor additional computers. For more information about installing the agent on remote computers, see Section 3.3, "Understanding Agent Deployment," on page 48.

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.

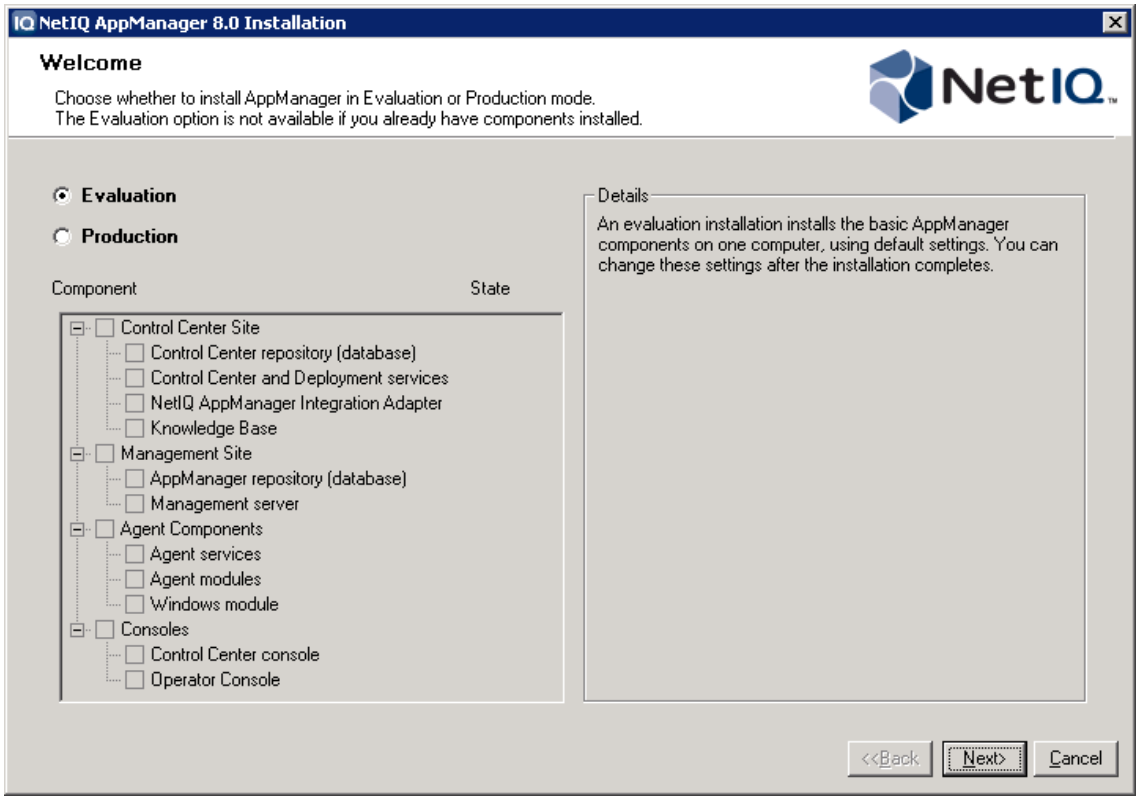
Before you install AppManager, log in using a Local or Domain Windows account with the following credentials:

- 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 `\Program Files\netiq\am8suite\Setup` folder, double-click `AMSetup.exe` to start the installation wizard and open the **Welcome** startup page.
3. At the **Welcome** dialog box, click the **Evaluation** option, and then click **Next**.

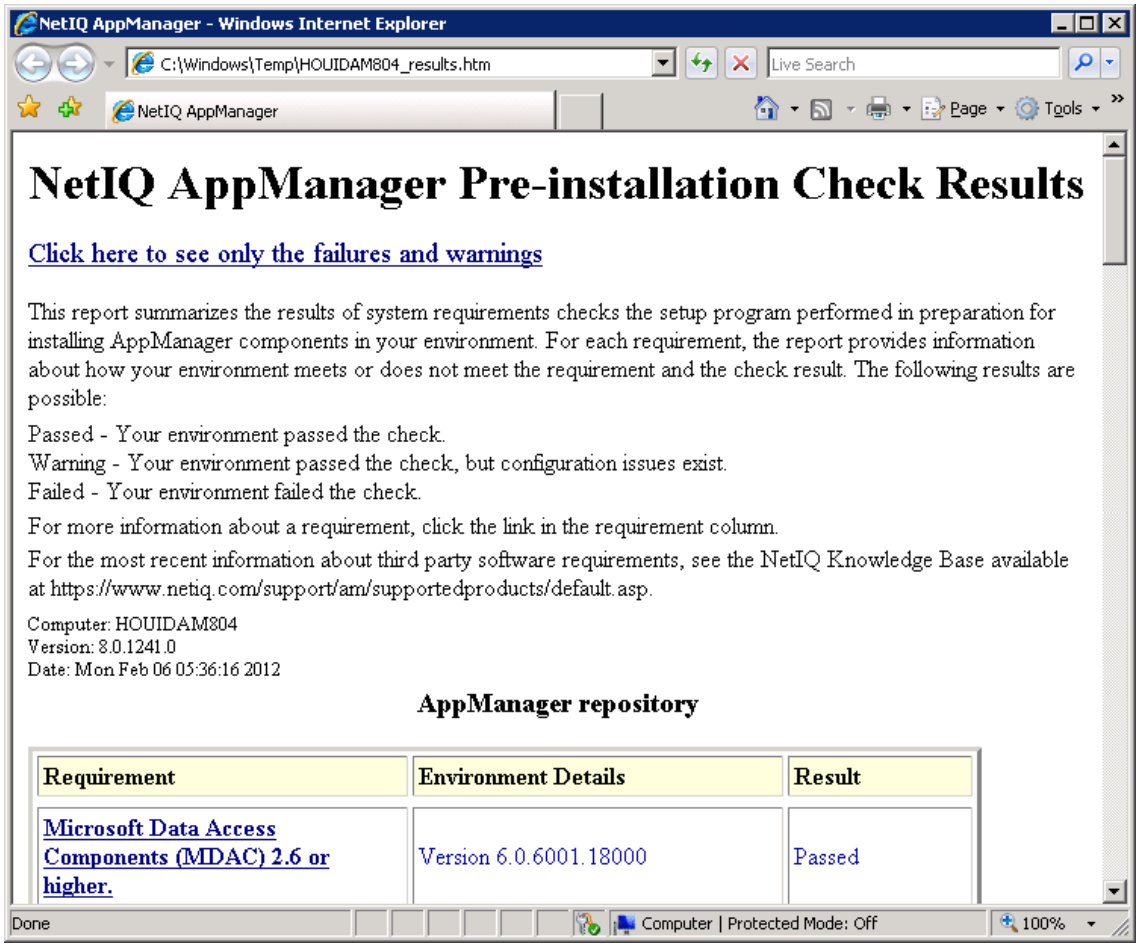
   The **Evaluation** installation includes full functionality and expires 30 days from the installation date.



4 At the **Confirmation** dialog box, use the **Click here to view the pre-installation check report** to run the pre-installation check. Clicking this link displays a browser page for the pre-installation check results.

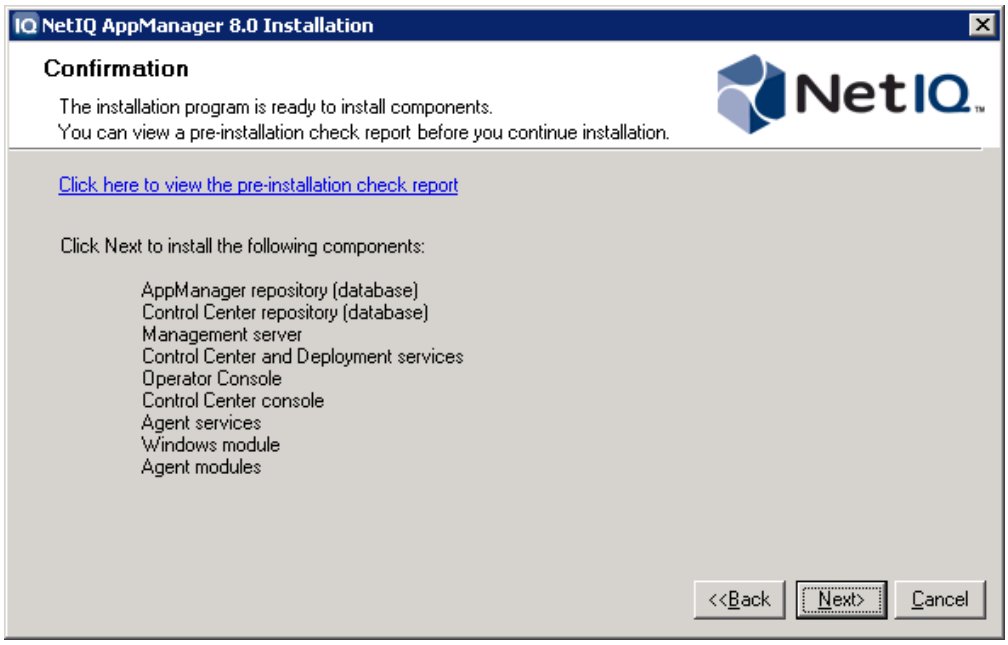
If the pre-installation check report indicates there are requirement failures for a particular component, resolve the failures for that component. Click the link to view the results and detailed information about how to resolve the problem.

If the pre-installation check is successful, close the browser page to display the **Confirmation** dialog box of the installation wizard. You are now ready to install AppManager.

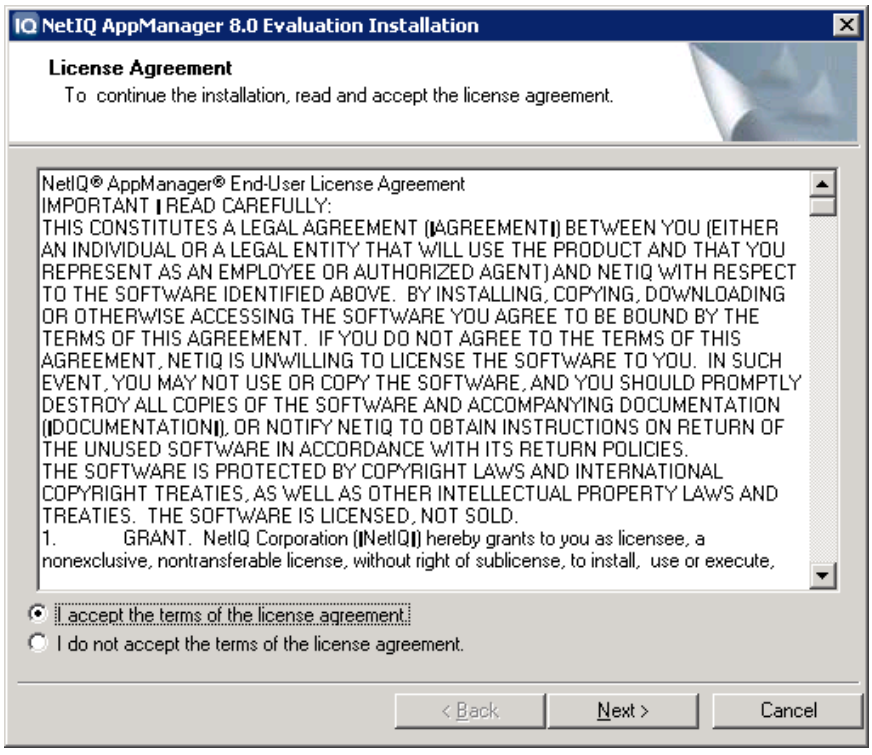


5 At the **Confirmation** dialog box, click **Next**.

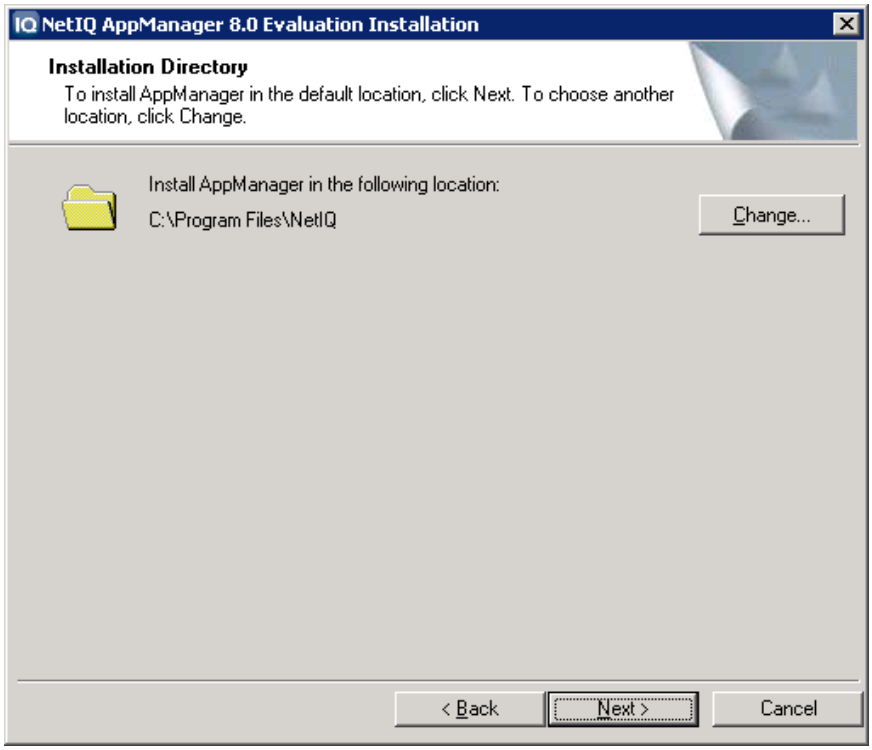
The installer will start installing the Runtime support installation packages and validate the prerequisites for Agent modules. Then it will display the license agreement.



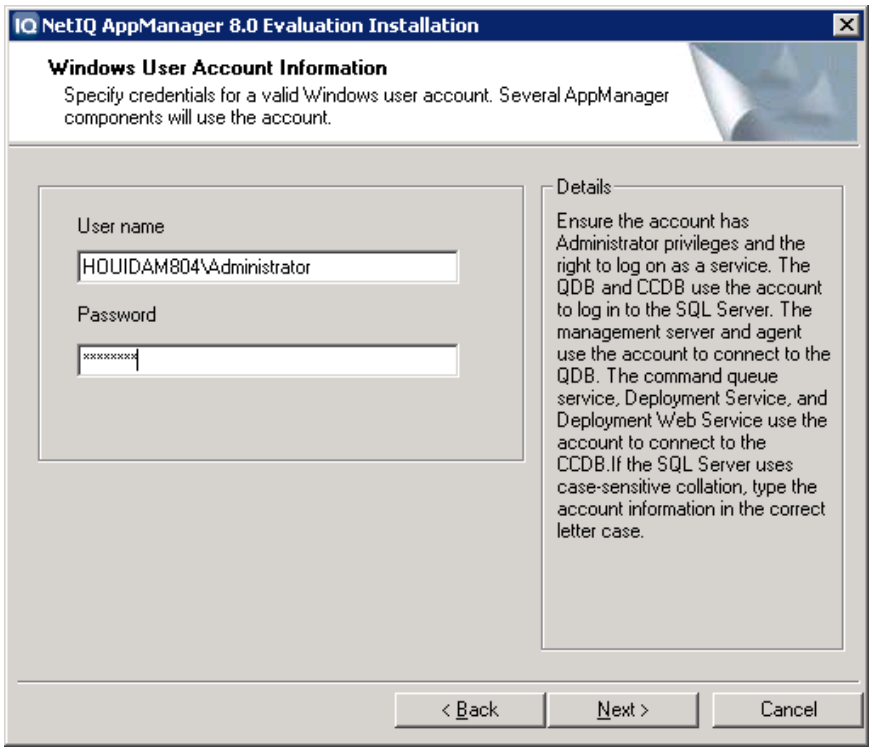
6 At the **License Agreement** dialog box, accept the license agreement, and then click **Next**.



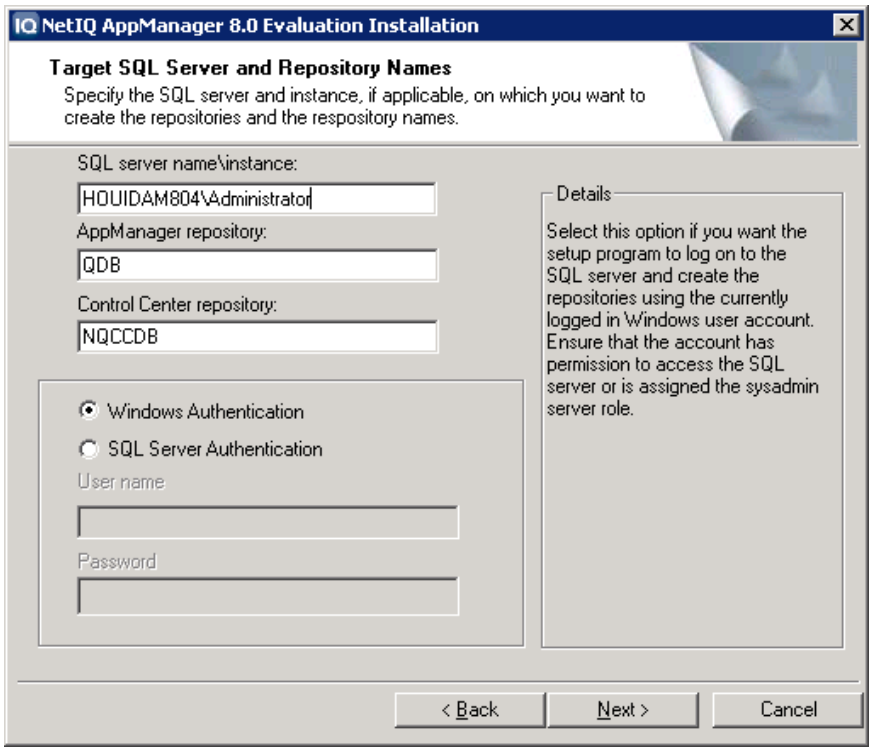
7 At the **Installation Directory** dialog box, to accept the default location, click **Next**.



8 At the **Windows Account Information** dialog box, specify the Windows credentials you are using to install AppManager, and then click **Next**.

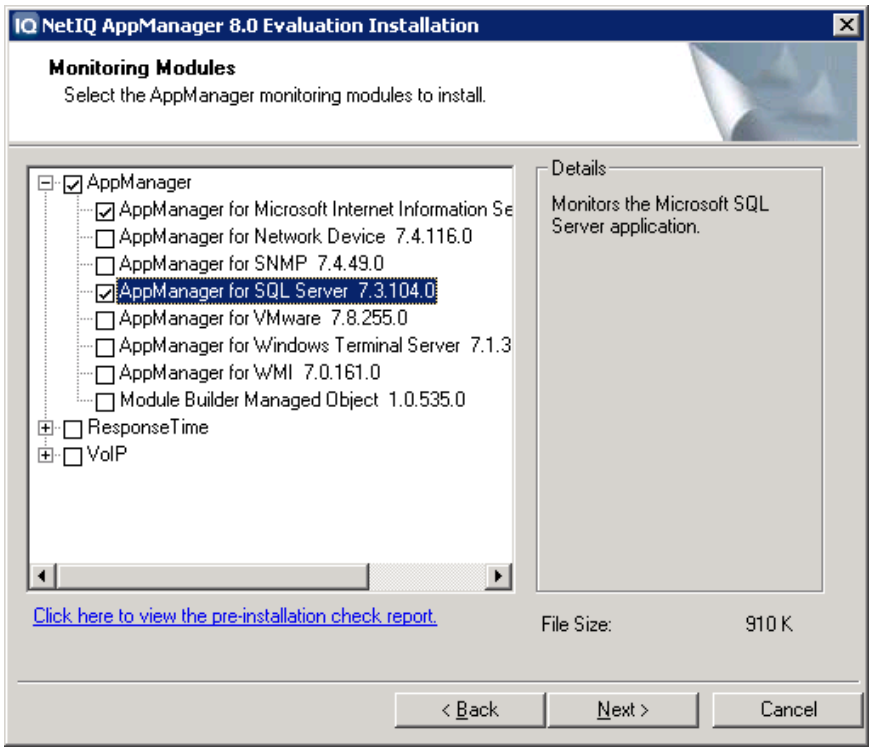


9 At the **Target SQL Server and Repository Name**s dialog box, specify the SQL Server instance where you want to install the AppManager repositories. Accept the default repositories name, `QDB` and `NQCCDB`, and then click **Next**.

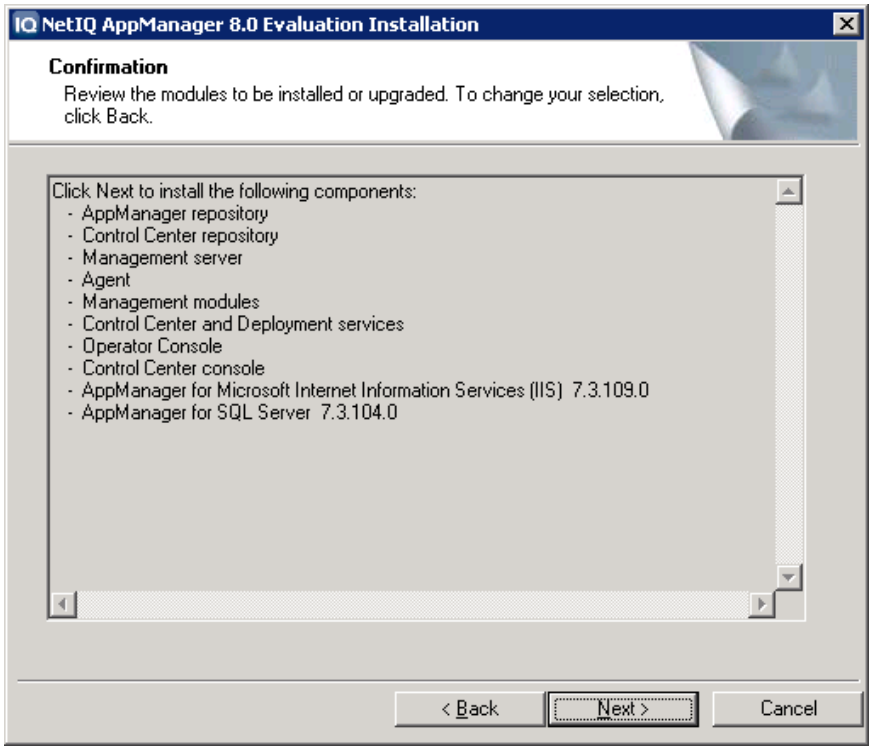


10 At the **Monitoring Modules** dialog box, select the check boxes for the following modules, and then click **Next**.

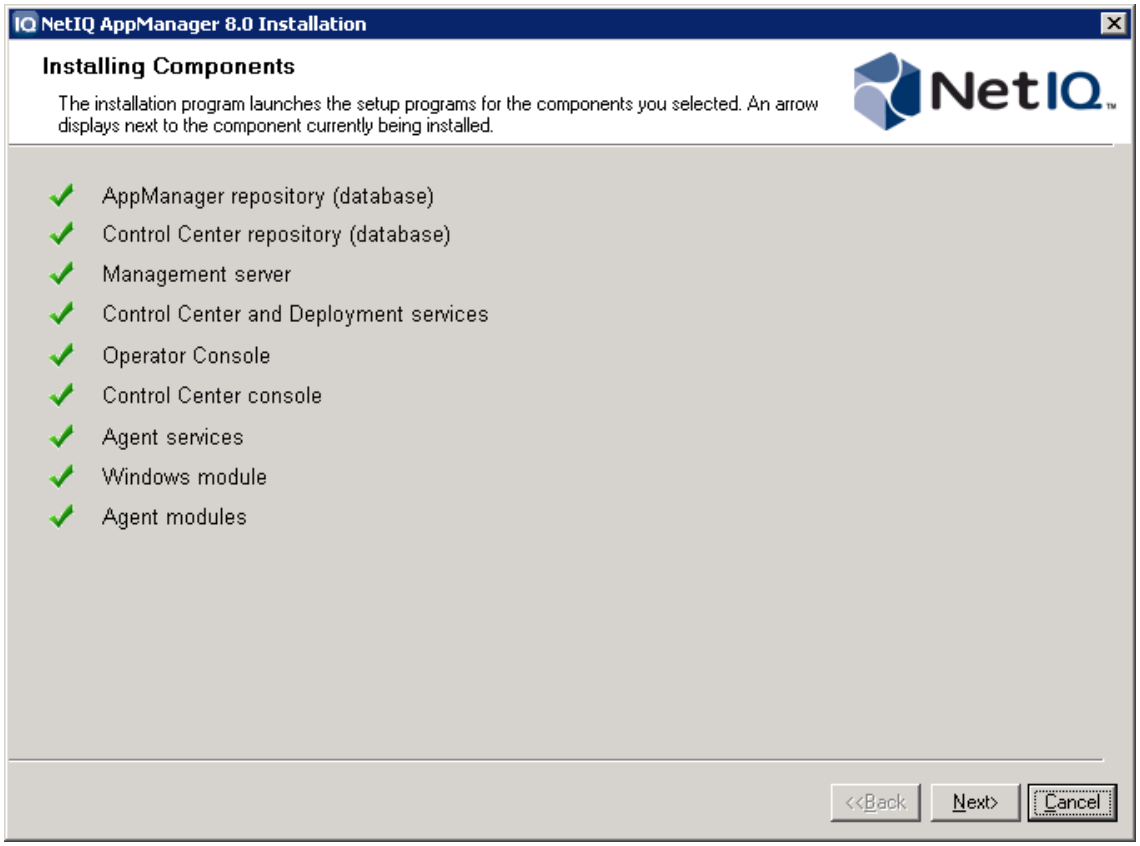
- AppManager for Microsoft Internet Information Service
- AppManager for SQL Server.



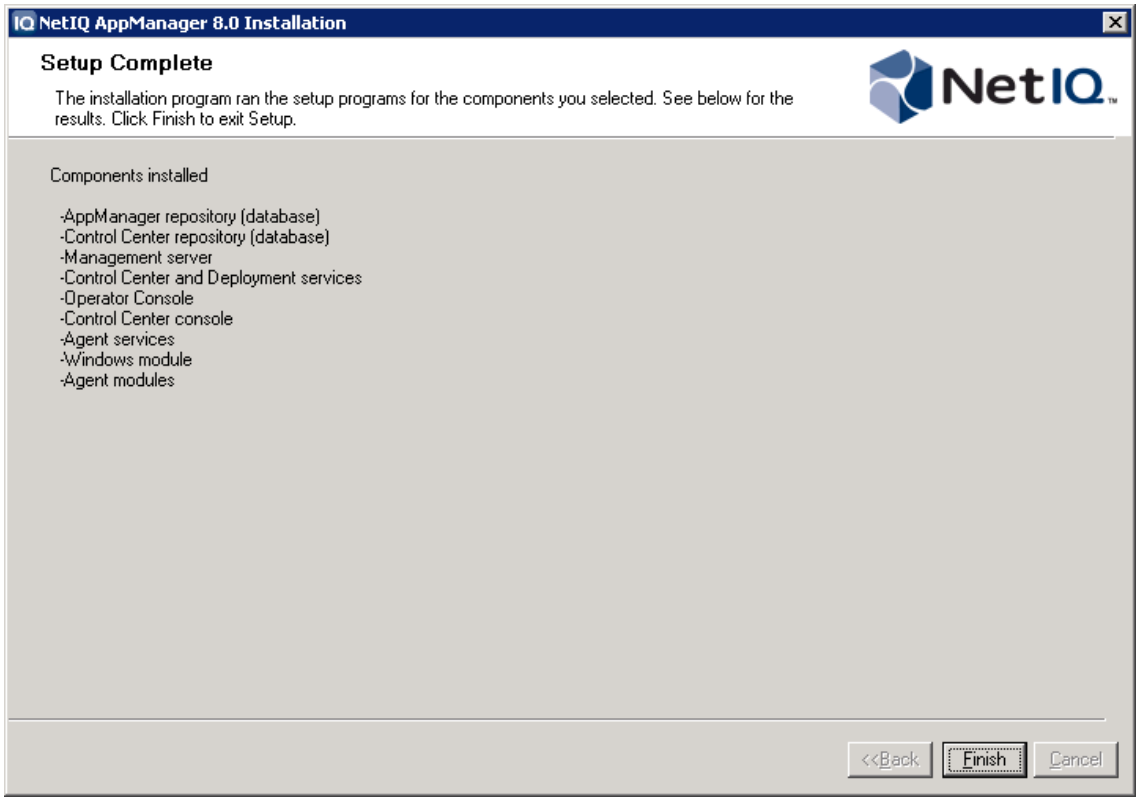
11 At the **Confirmation** dialog box, review the summary of the AppManager installation options, and then click **Next**.



After the components are installed, the **Installing Components** dialog box displays the list of components that are successfully installed with a green tick mark. Click **Next**.



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



You are now ready to explore AppManager. For more information, see Chapter 3, "Exploring AppManager," on page 35.

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.

Before you begin, make sure you have properly installed and configured AppManager. For more information, see Chapter 2, "Installing AppManager," on page 23.

- Section 3.1, "Starting the Control Center Console," on page 35
- Section 3.2, "Understanding Management Groups," on page 39
- Section 3.3, "Understanding Agent Deployment," on page 48
- Section 3.4, "Understanding Monitoring Policies," on page 74
- Section 3.5, "Working with Server Views," on page 93
- Section 3.6, "Working with Event Views," on page 96
- Section 3.7, "Working with Job Views," on page 106
- Section 3.8, "Understanding Service Map Views," on page 110
- Section 3.9, "Understanding Charts," on page 111
- Section 3.10, "What's Next?," on page 119

3.1 Starting the Control Center Console

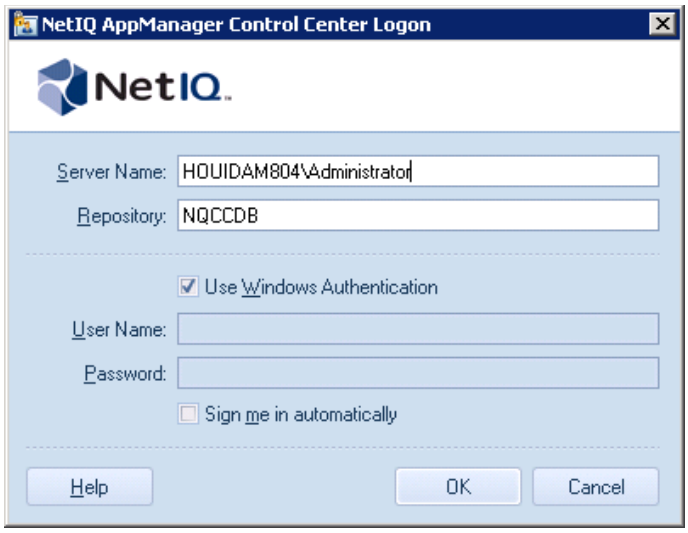
As a Control Center Console administrator, you have permission to start the Control Center Console and access all management groups.

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 **NetIQ AppManager Control Center Console Logon** dialog box, specify 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.

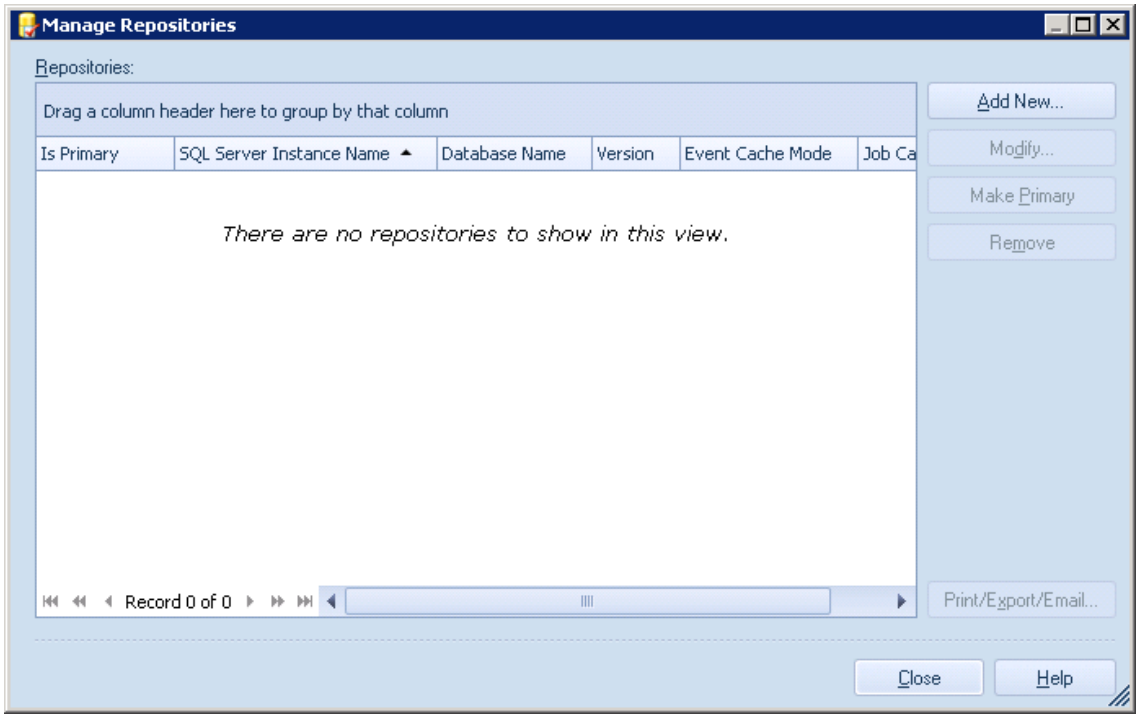


3. Click **OK**.

   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 **OK**.

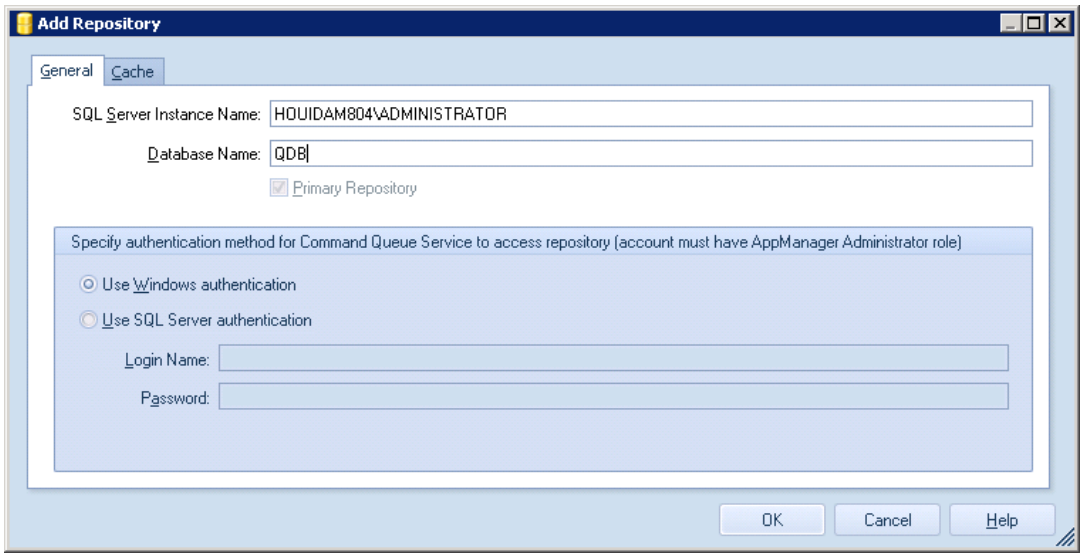
   The initialization will take few minutes, if you are starting the Control Center for the first time.

4 When you log in to the Control Center for the first time, the **Manage Repositories** dialog box displays that there are no repositories to show. As a one time procedure, designate the repository.



4a Click **Add New**.

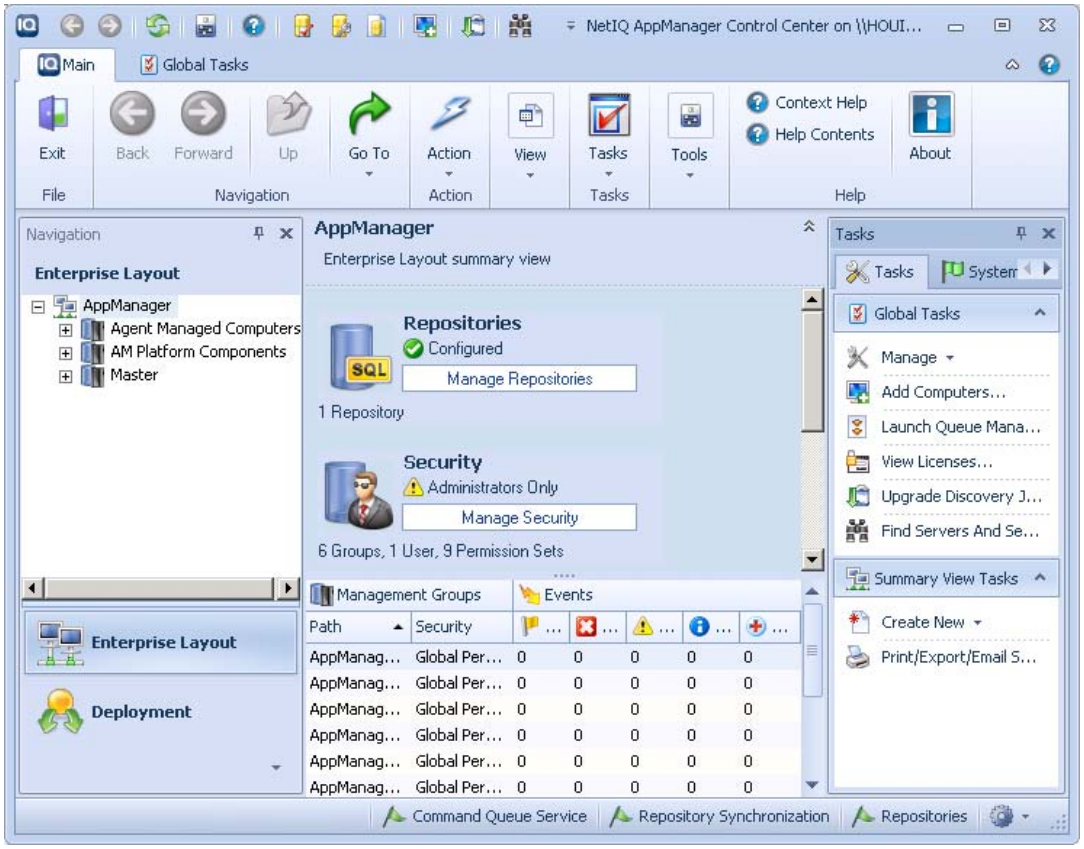
For	Do this
SQL Server Instance Name	Specify the name of the computer where you installed all of the AppManager components. If you installed the Control Center repository on a named instance of SQL Server, specify the server name using the *computer_name\instance_name* format. For example, `HOUIDAM804\Administrator`.
Database Name	Specify the name of the AppManager repository database. The default database name is `QDB`.
Primary Repository	This check box is selected by default, 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 Windows Authentication** if the repository is in the local computer. 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.



4b Click **OK**.

4c Click **Close**.

The **AppManager Control Center Console** is displayed.



3.2 Understanding Management Groups

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

- AppManager repository views such as NT or SQL.
- Rules that select servers based on their properties, such as the name of the computer or discovered resources.
- Groups of servers in an AppManager repository view.
- An ad hoc list of servers.

Rule-based management groups allow administrators to define criteria for grouping servers. Servers 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.

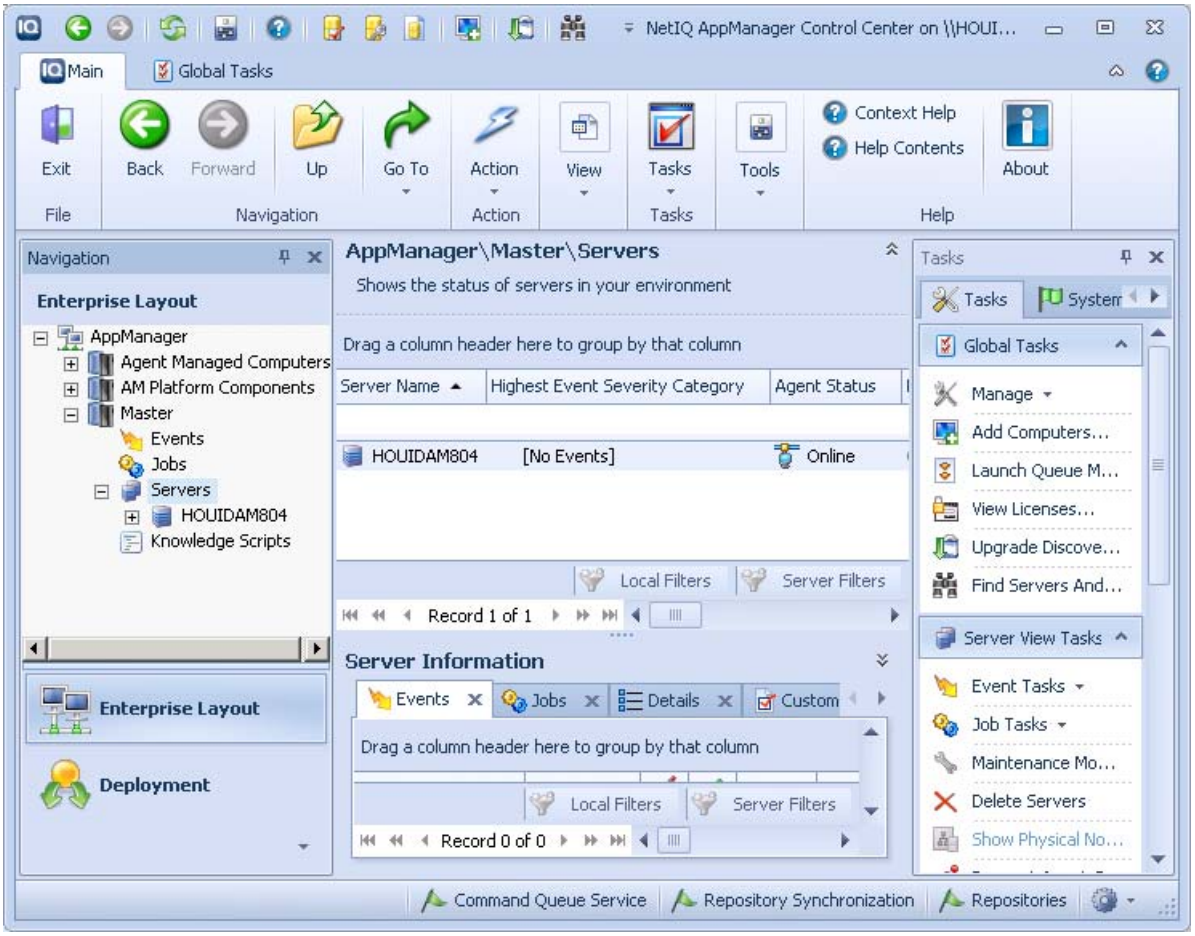
3.2.1 About Control Center Console Views

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

- **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 servers 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. A Knowledge Script view shows only those Knowledge Scripts pertaining to those objects discovered in your managed environment. This is different than the Knowledge Scripts pane, which shows all Knowledge Scripts checked into the primary QDB.
- **Summary view:** Displays a summary of the members of the management group, events, jobs, and servers information.

Service Map views manage events and display the overall health of a business process. For more information, see Section 3.8, “Understanding Service Map Views,” on page 110.

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



3.2.2 Creating a Rule-based Management Group

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

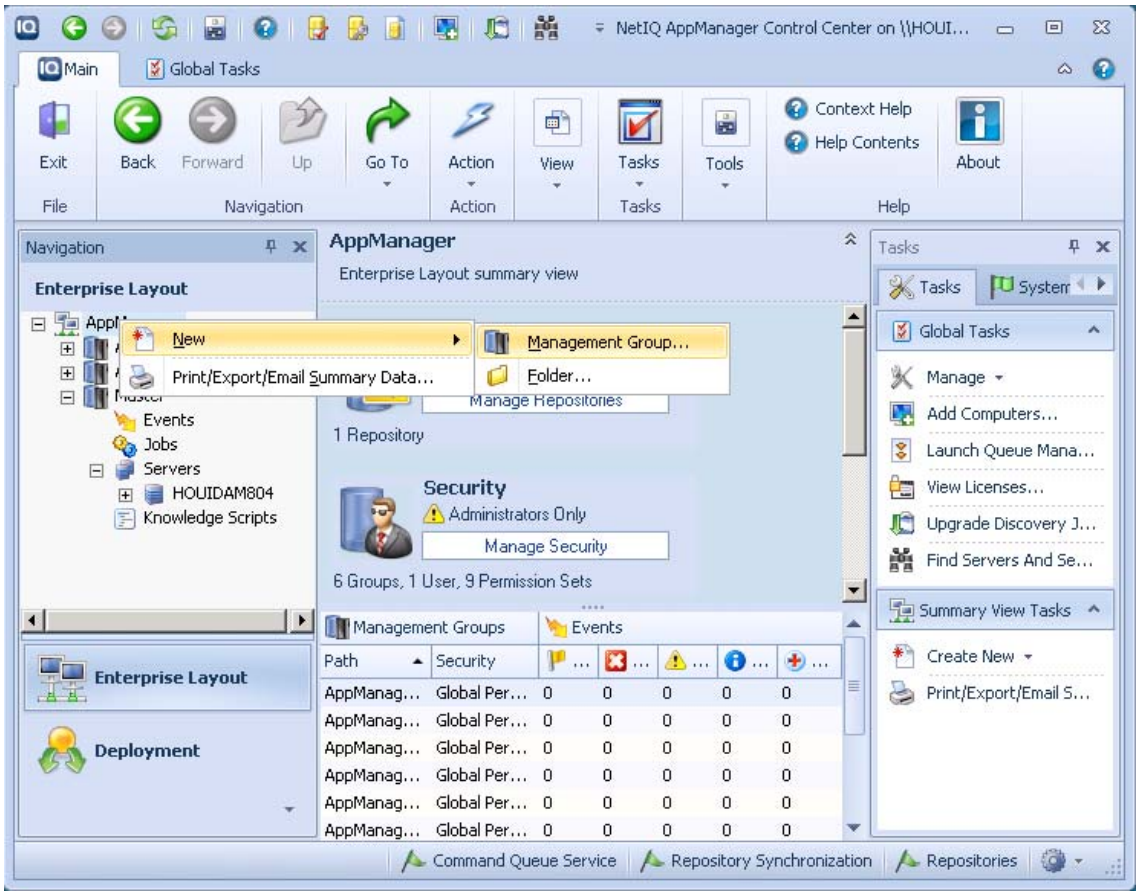
When you create a management group, you have the option to create the standard views which include Events, Jobs, Knowledge Scripts, and Servers. Do not create the standard views when you create the management group. You can create views later in this chapter.

In addition to creating standard views, this chapter covers creating Service Map views to illustrate and manage the business processes in your environment. For more information, see Section 3.8, “Understanding Service Map Views,” on page 110.

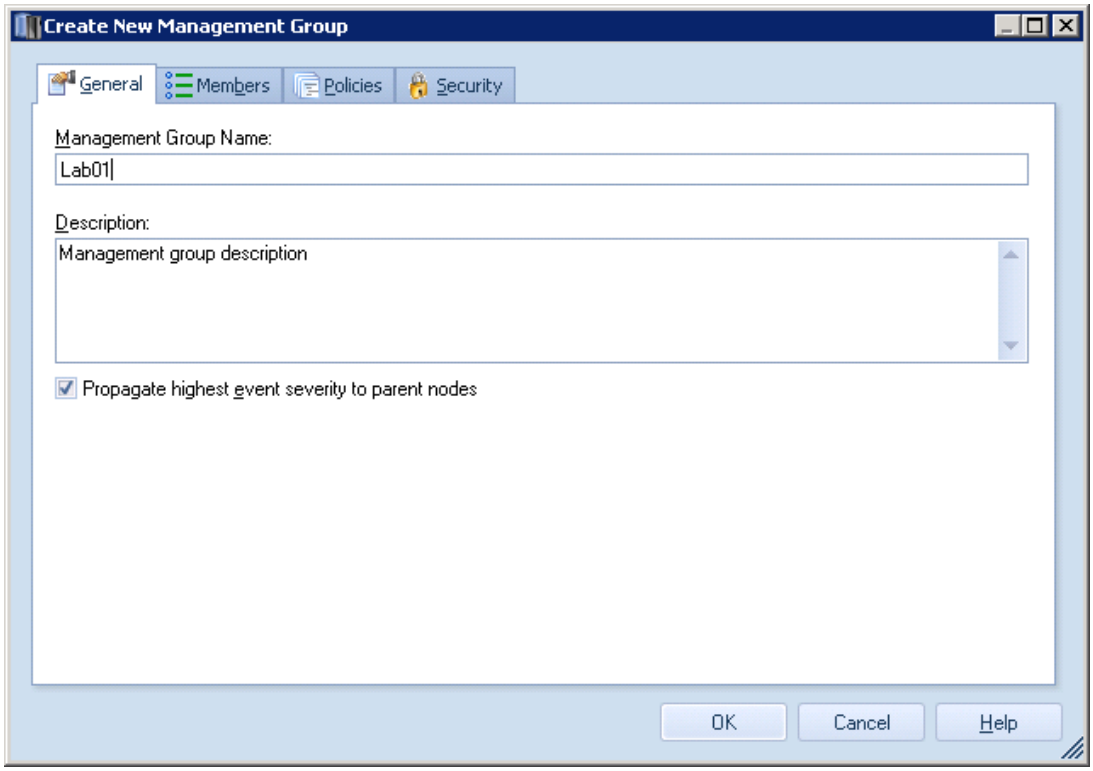
To create a rule-based management group:

1 Right-click the top-most **AppManager** icon in the **Enterprise Layout** pane, and then click **New > Management Group**.

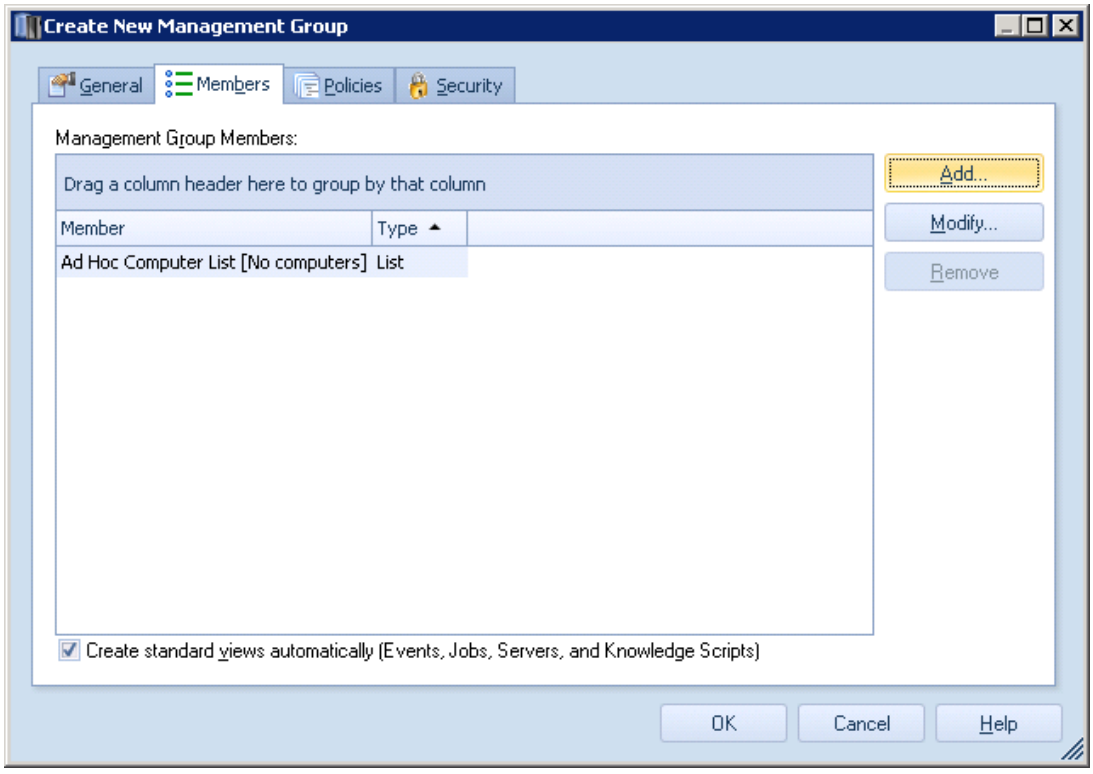
Alternatively, you can click the **Create Management Group** button in the **Enterprise Layout summary view** pane.



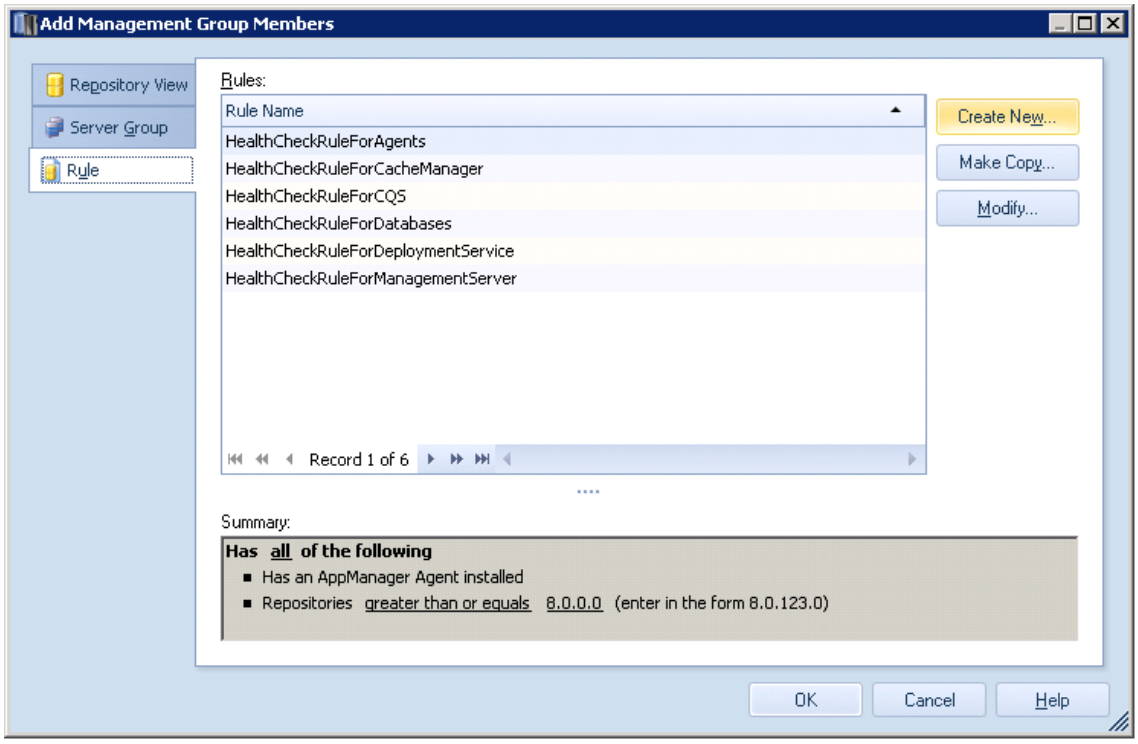
2 On the **General** tab of the **Create New Management Group** dialog box, specify a name for the management group. Name the management group `Lab01`.



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

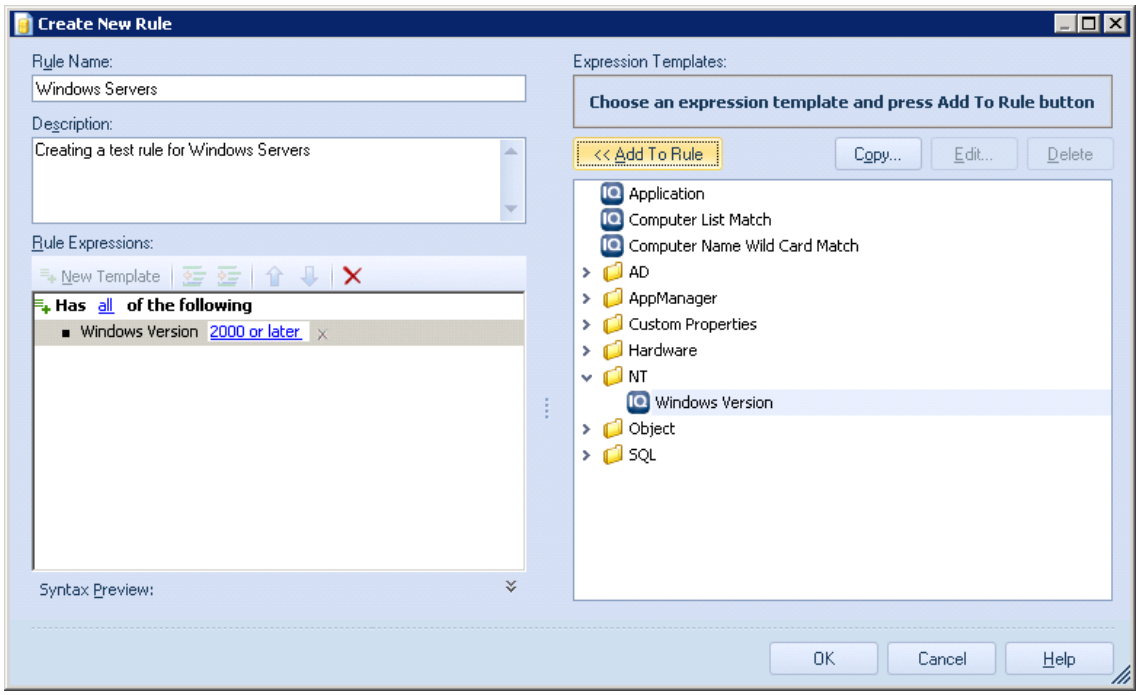


4 In the **Add Management Group Members** dialog box, click the **Rule** button to add a management group rule, and then click **Create New**.



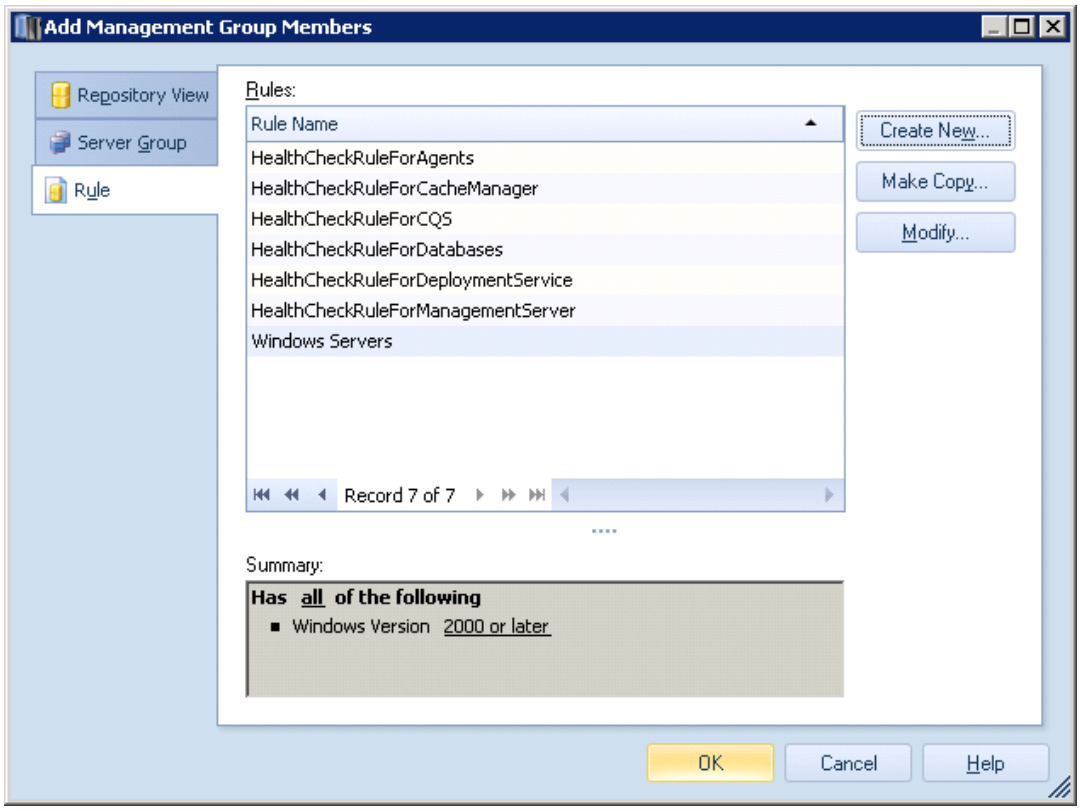
5 In the **Create New Rule** dialog box, configure an expression template to select the servers you want based on operating system version.

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

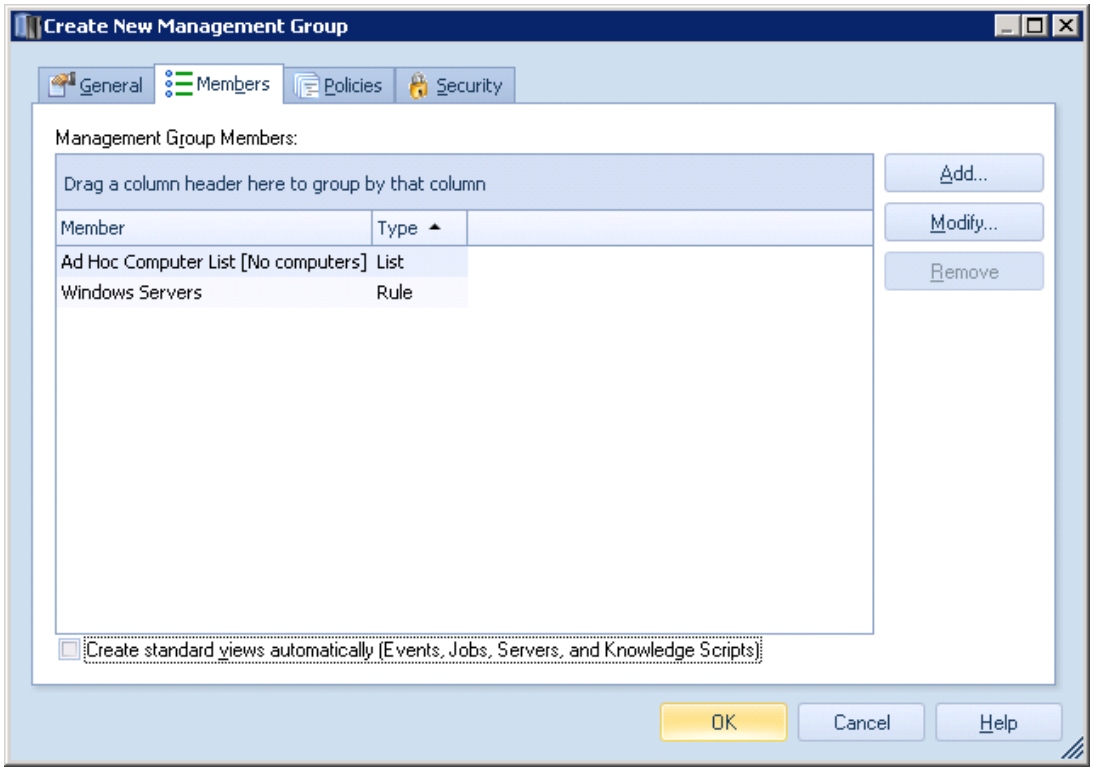


6 In the expression editor, accept the default, **2000 or later**, to enable the management group rule to select Windows computers with an operating system version of Windows 2000 or later, and then click **OK**.

7 In the **Add Management Group Members** dialog box, the `Windows Servers` management group rule is displayed. Click **OK**.



8 On the **Members** tab of the **Create New Management Group** dialog box, deselect the **Create standard views automatically** check box, and then click **OK**. You can create the views later.



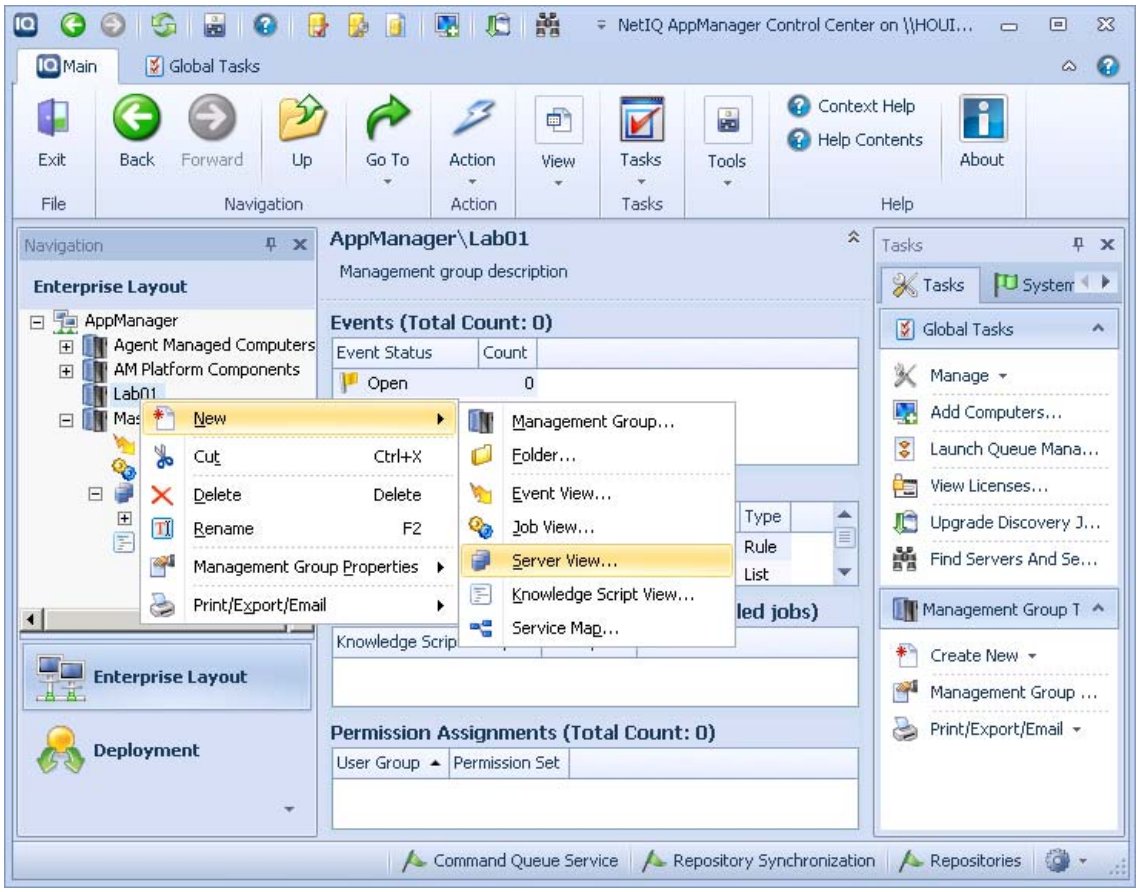
After you create the management group, in the Control Center Console, the newly added management group is displayed under the Management Groups.

3.2.3 Creating a Server View

Create a Server view to display the server information for the servers in the `Lab01` 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.

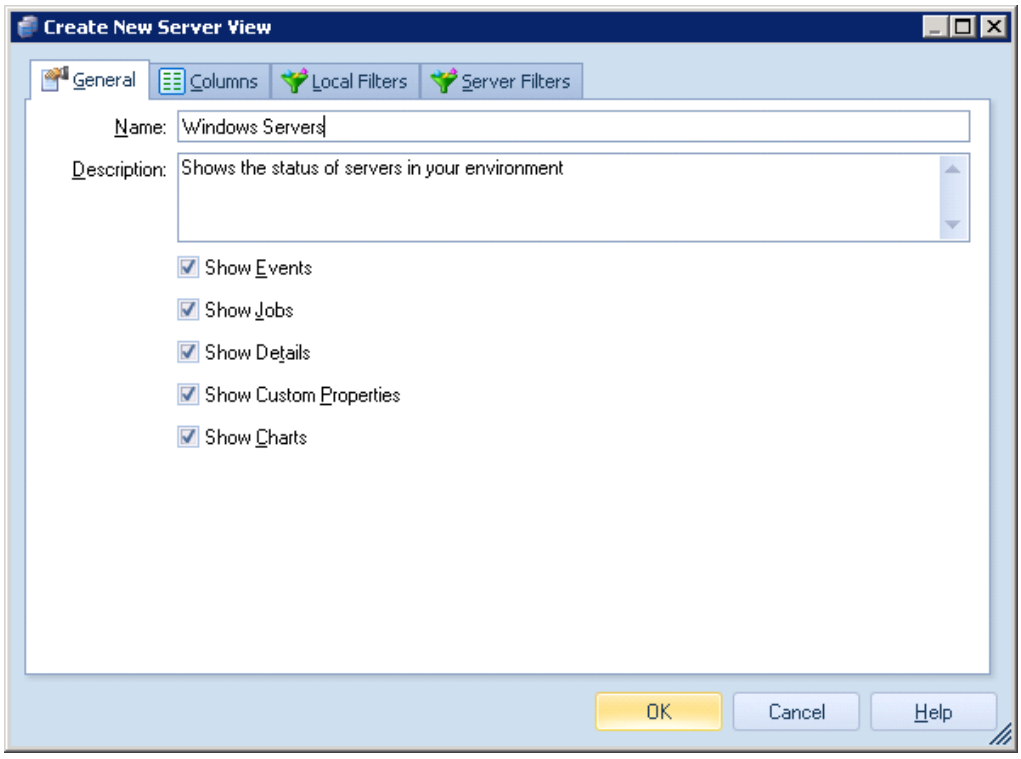
To create a Server view:

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

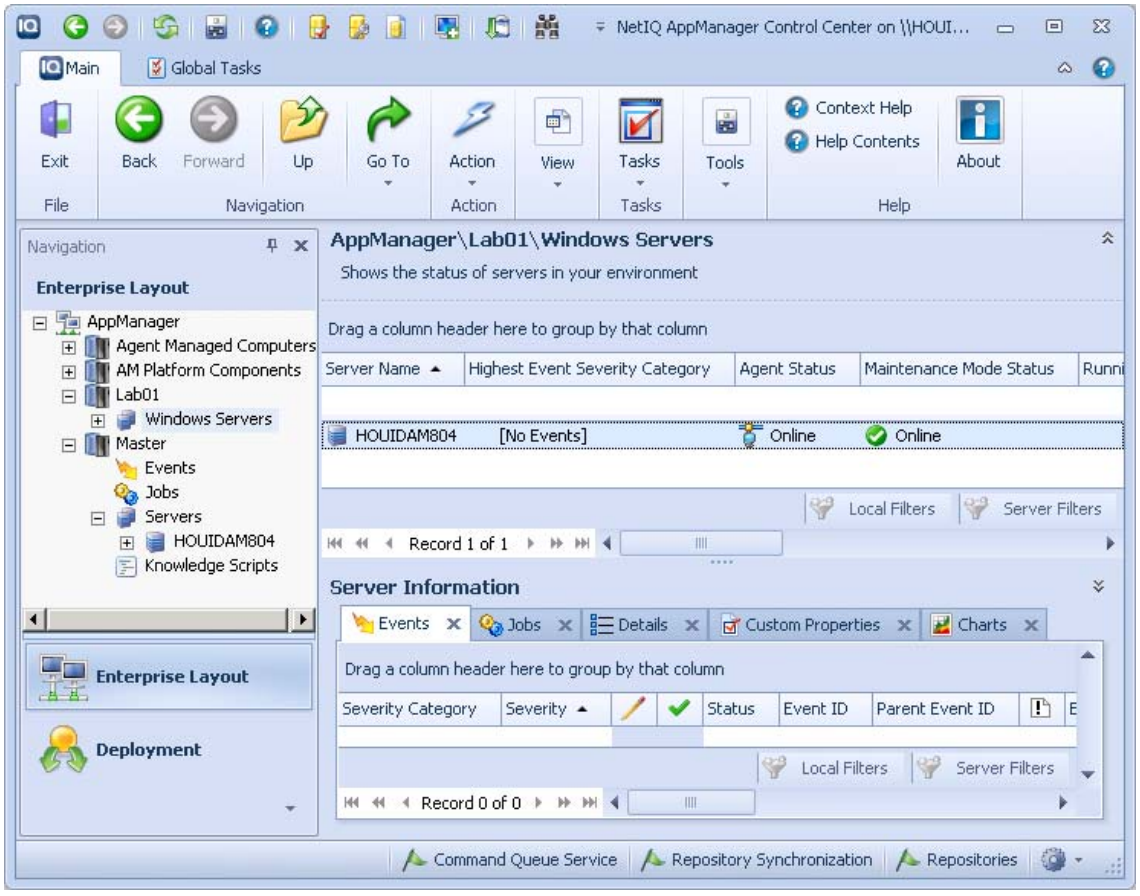


2 On the **General** tab of the **Create New Server View** dialog box, specify a name for the Server view, and then click **OK**.

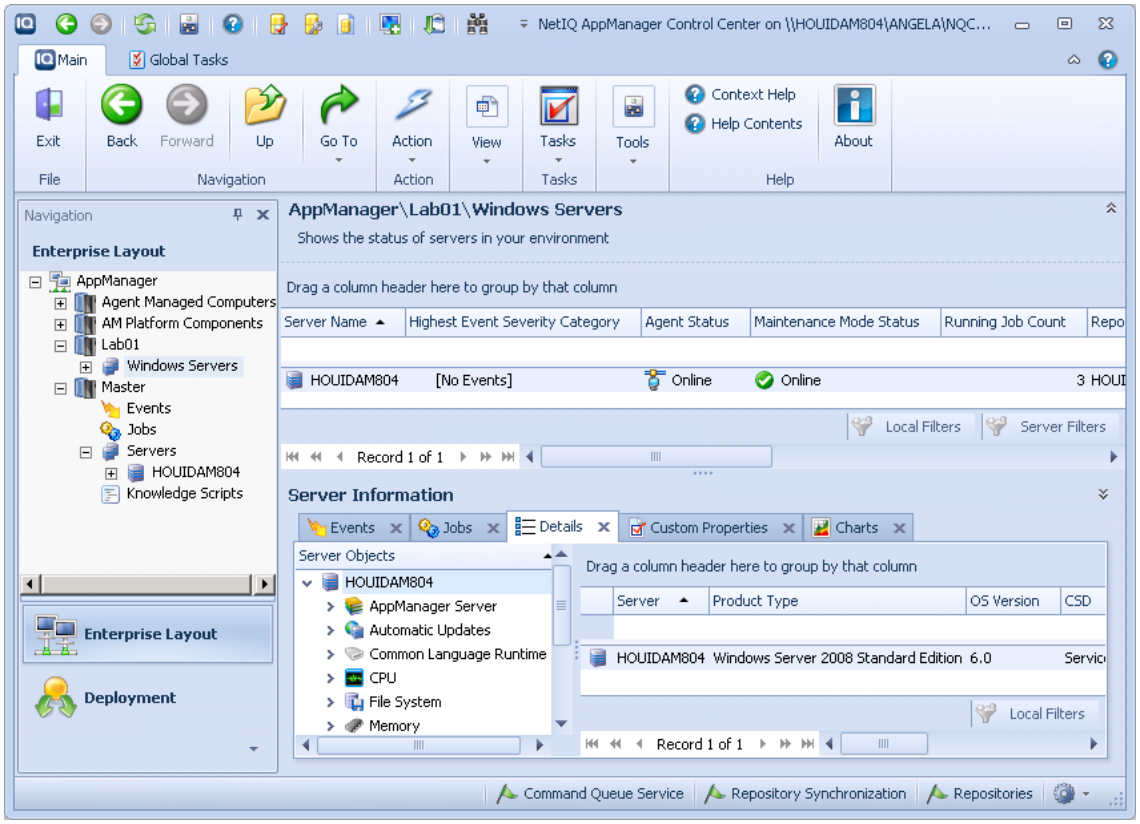
For	Do this
Name	Specify `Windows Servers`
Description	Provide a description or leave the default description. This parameter is optional.



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



4 Click the **Details** tab in the lower pane to view the AppManager discovery information for the selected server.



NOTE: The process by which AppManager is made aware of the servers 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.

3.3 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.

This section guides you through deploying agents to Windows computers. For more information about deploying agents to UNIX computers, see the AppManager UNIX documentation

3.3.1 About the Deployment Pane

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

You can use the **Rules** view in the **Deployment** 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 default deployment rules and packages 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.

3.3.2 Before You Begin

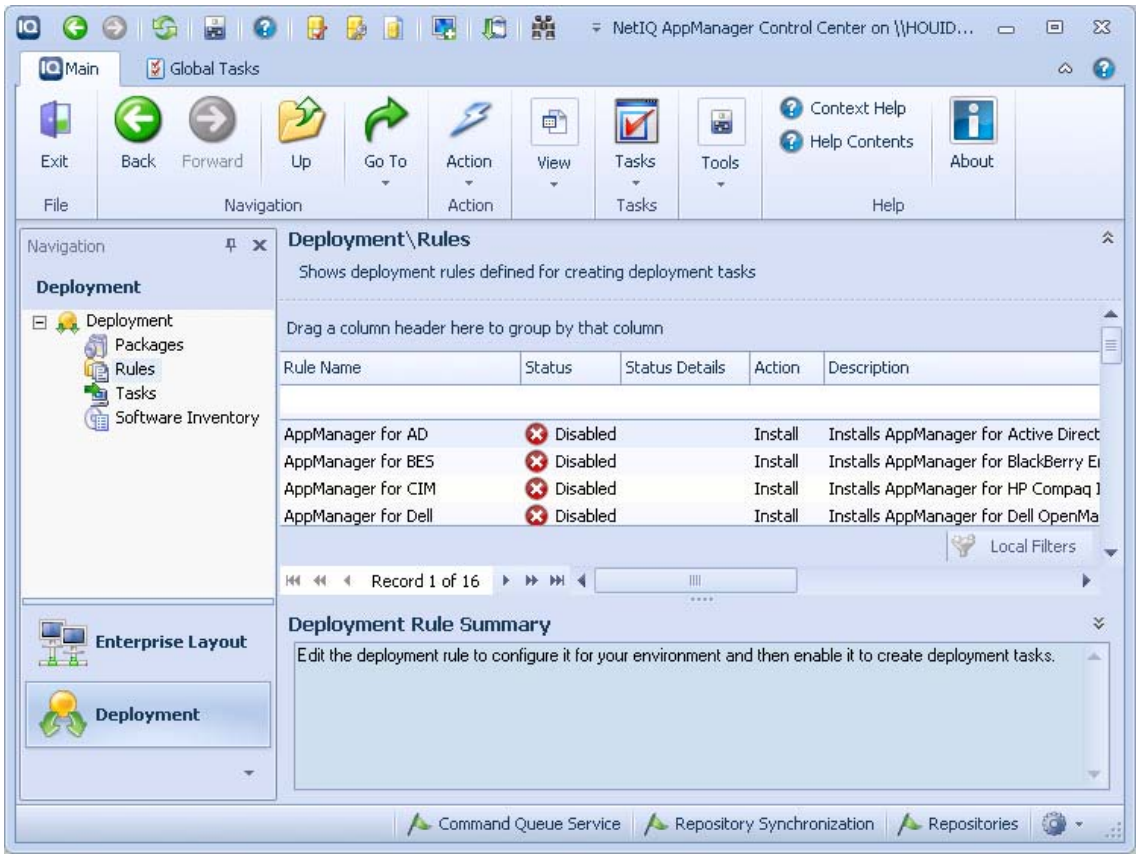
Before you configure a deployment rule to install the agent, make sure the domain user account you plan to use as the credentials for the deployment rule is also a member of the local Administrators group on the computers where you want to deploy the agent.

3.3.3 Configuring a Rule to Deploy the Agent

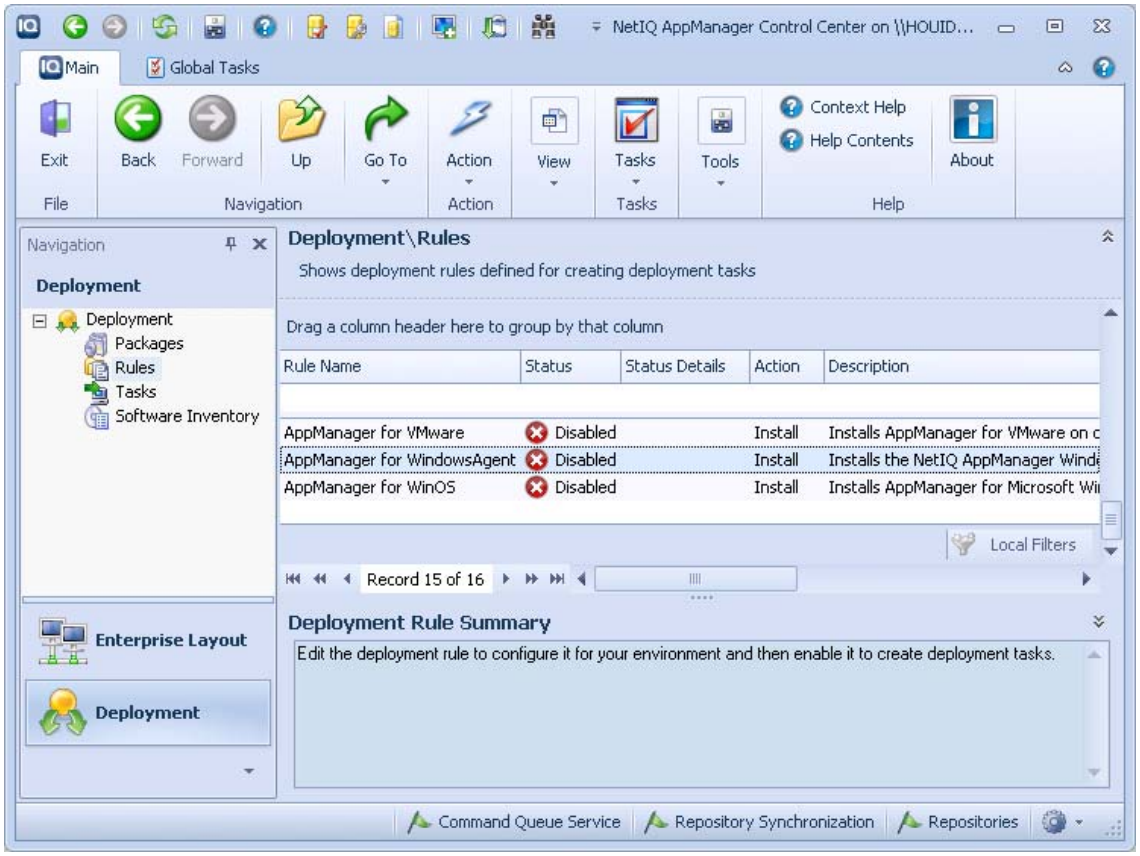
Configure a deployment rule to install the agent on one or more computers. For your convenience, the Control Center Console provides an out-of-the-box rule to install the agent.

To configure a deployment rule:

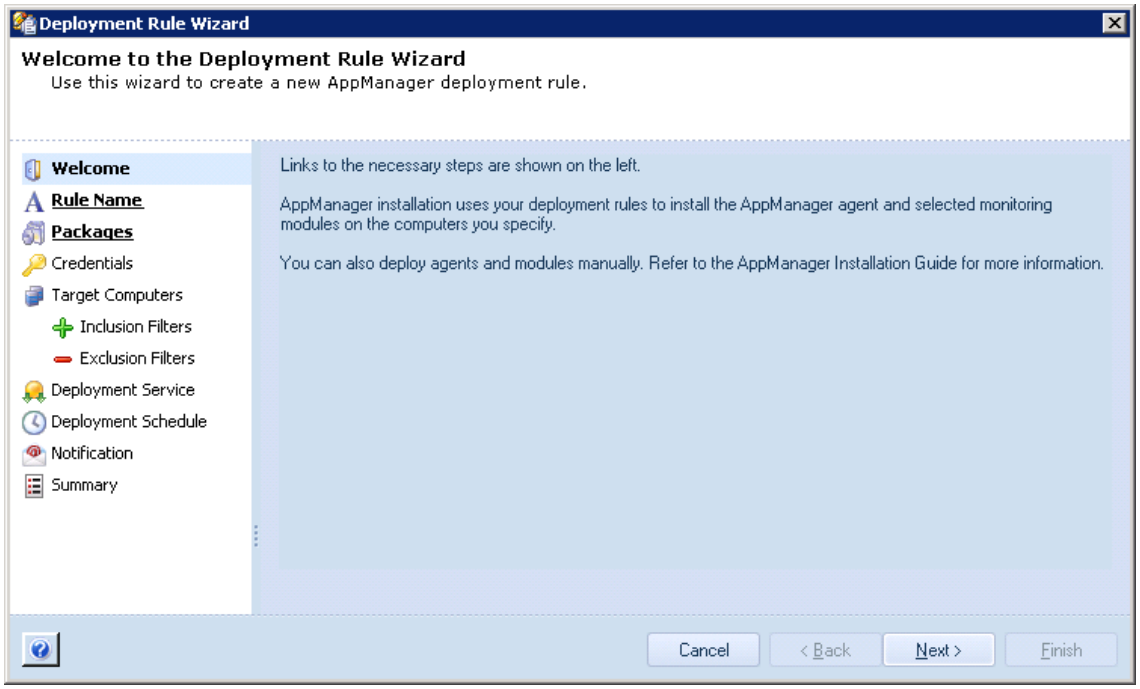
1 In the **Deployment** pane, click **Rules** to display the list of rules.



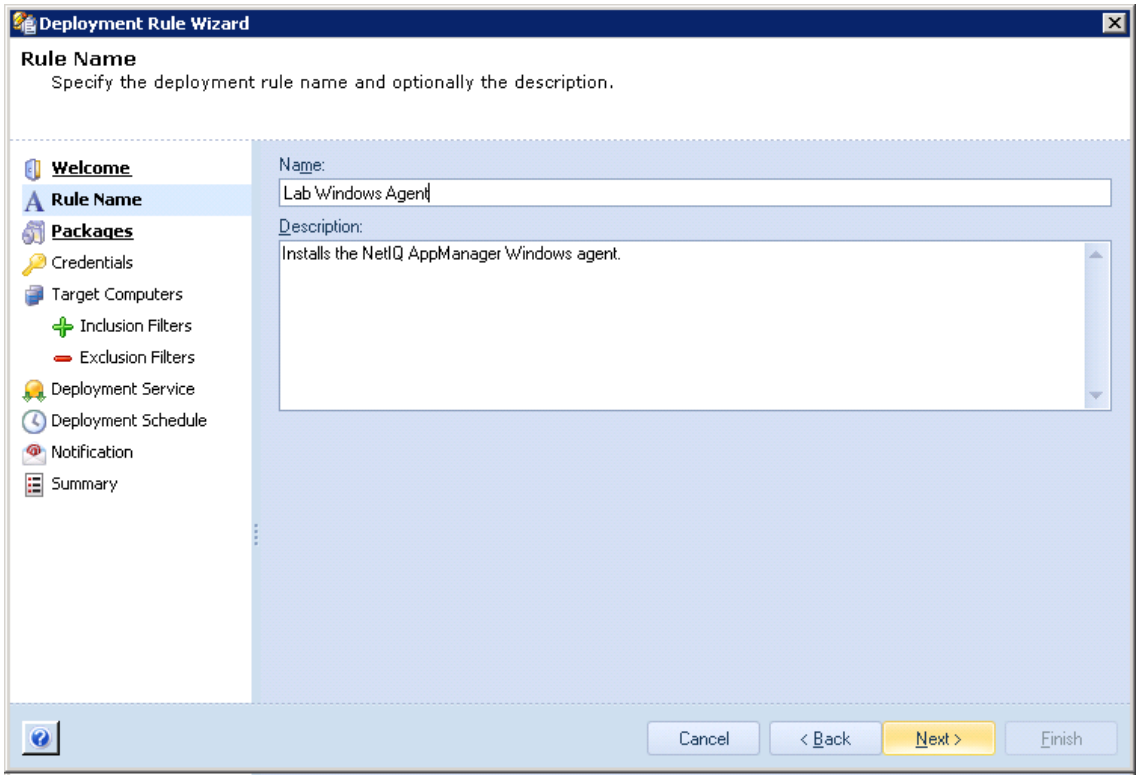
2 Scroll down and double-click the **AppManager for Windows Agent** rule to configure its properties in the Deployment Rule Wizard.



3 At the **Welcome** page, click **Next**.



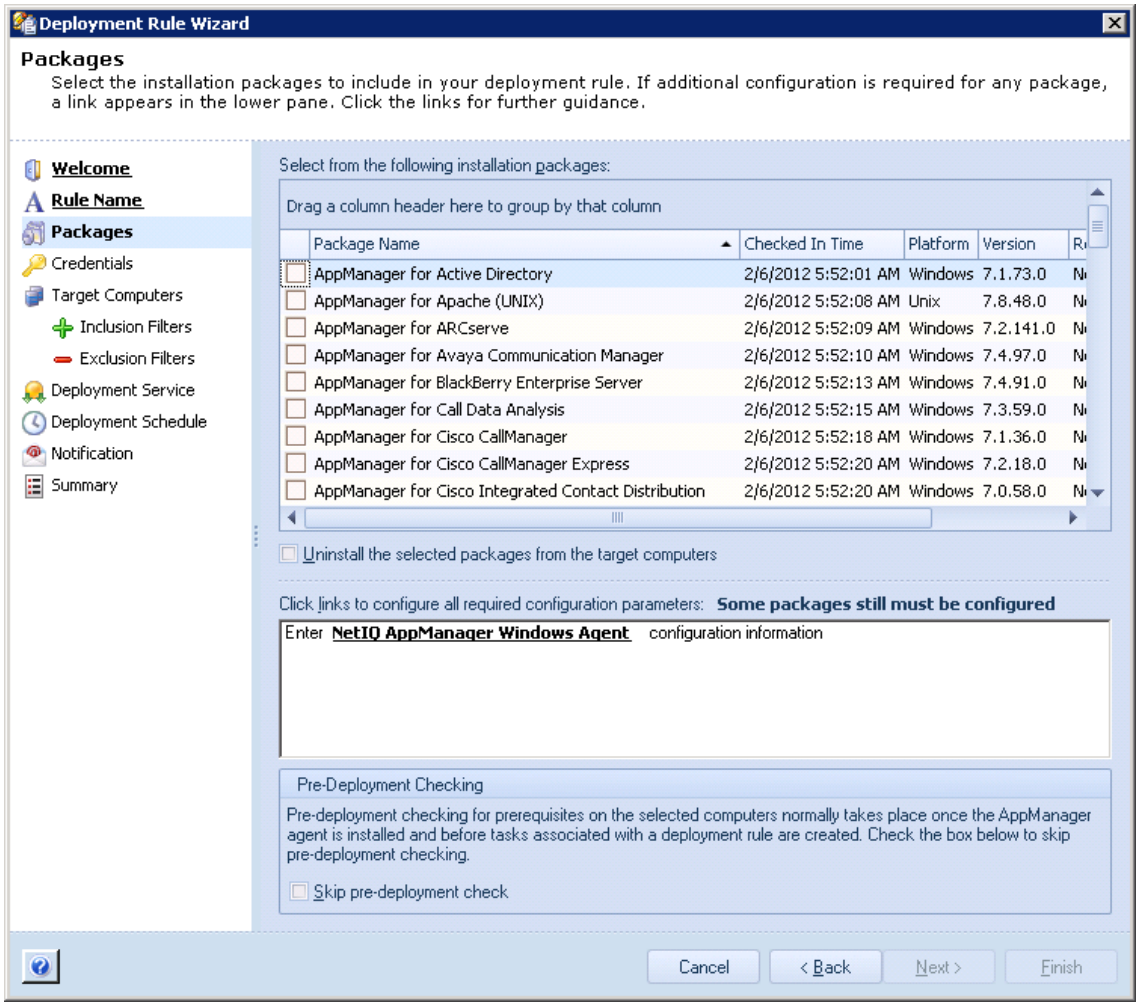
4 In the **Rule Name** page of the Deployment Rule Wizard, change the rule name. Specify `Lab Windows Agent` in the **Name** field, and then click **Next**.



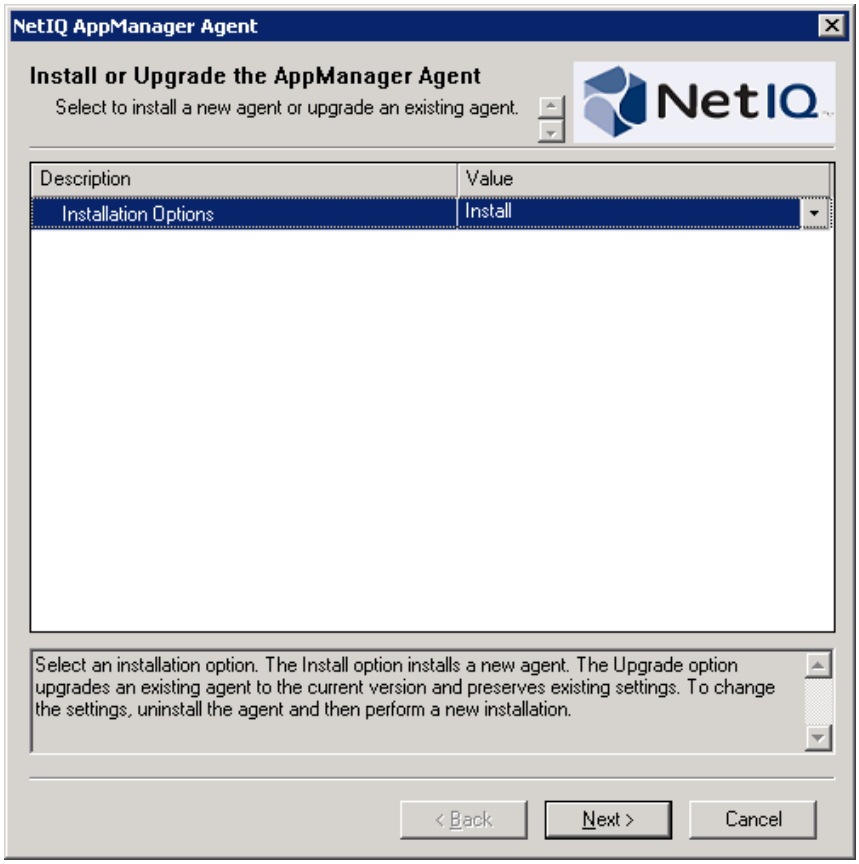
5 In the **Packages** page of the Deployment Rule Wizard, the default installation package for the selected deployment rule (**AppManager for Windows Agent**) is selected by default. The additional configuration required for the selected package is displayed as link in the lower pane.

The installation packages are displayed in the alphabetical order and you can scroll up or down to see the selected packages.

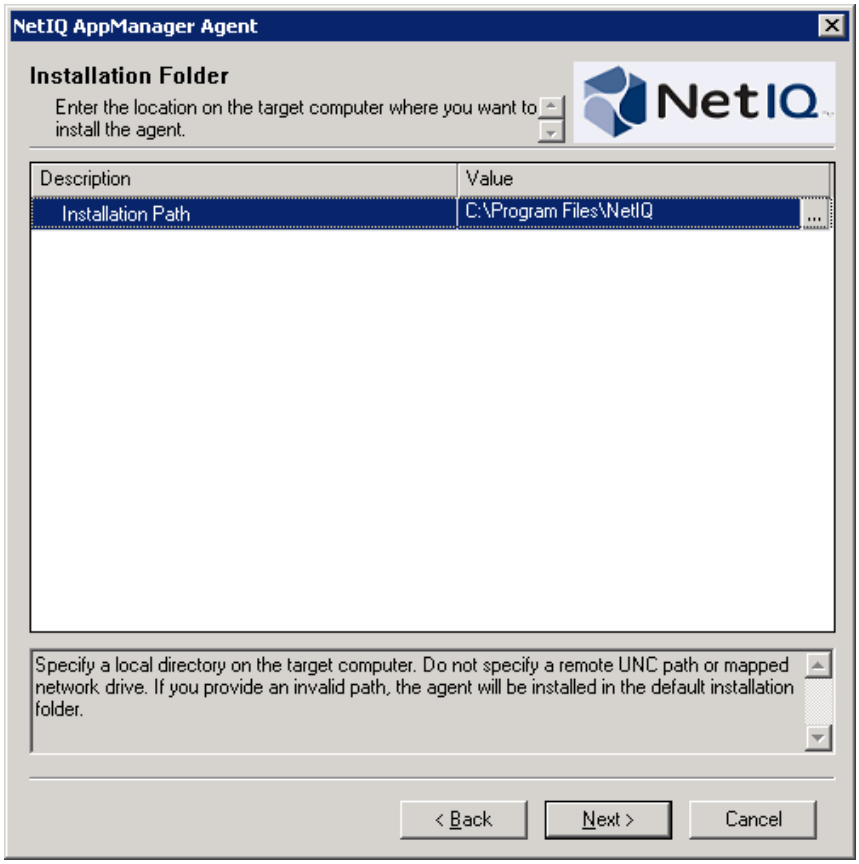
Click the **NetIQ AppManager Windows Agent** link in the lower pane to configure the default installation package.



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



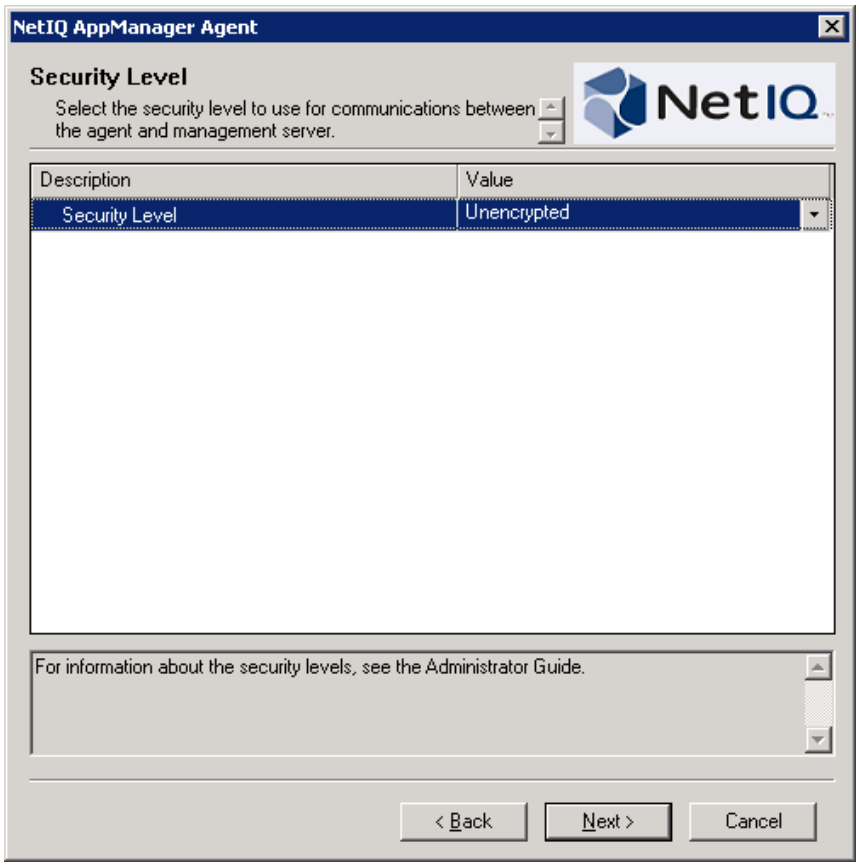
7 At the **Installation Folder** dialog box, click **Next** to accept the default location to install the agent on the target computer.



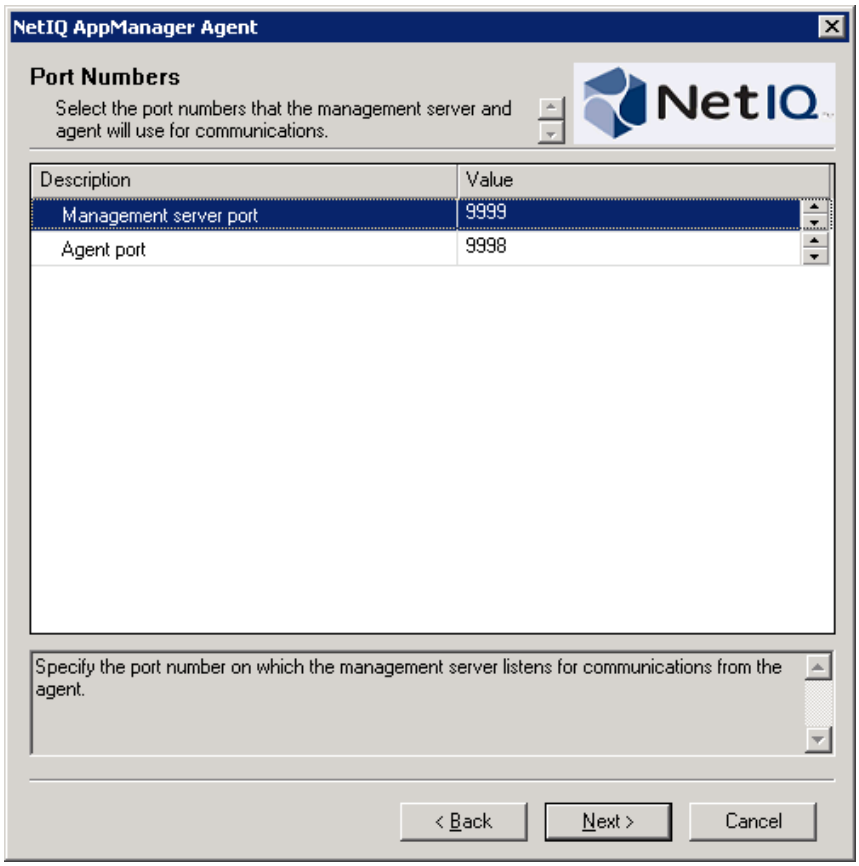
8 At the **Reporting Capability and Service Account** dialog box, click **Next** to accept the default values.



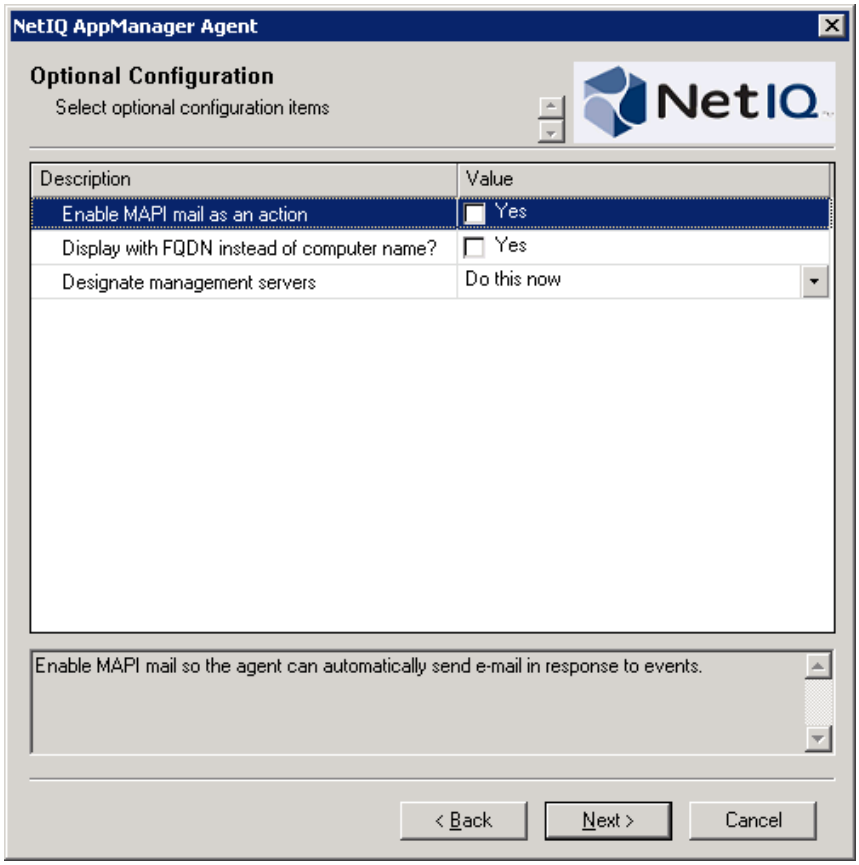
9 At the **Security Level** dialog box, click **Next** to accept the default value to configure the agent to communicate with the management server using unencrypted text. Because the management server uses unencrypted text, the agent must also use unencrypted text.



10 At the **Port Numbers** dialog box, click **Next** to 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.

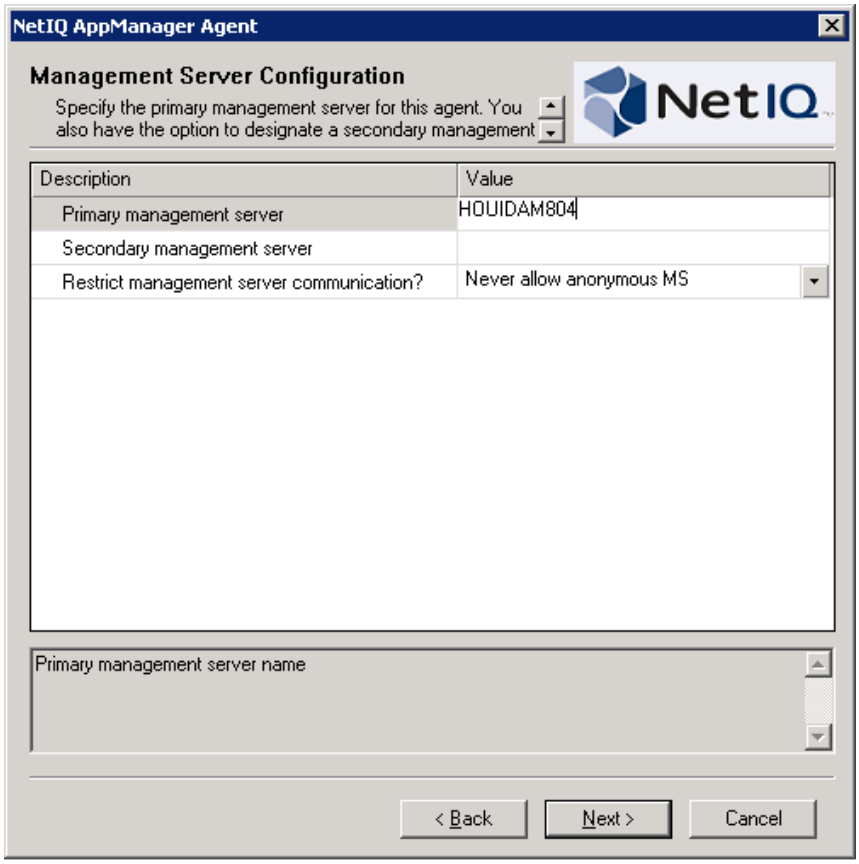


11 At the **Optional Configuration** dialog box, click **Next** to accept the default values.

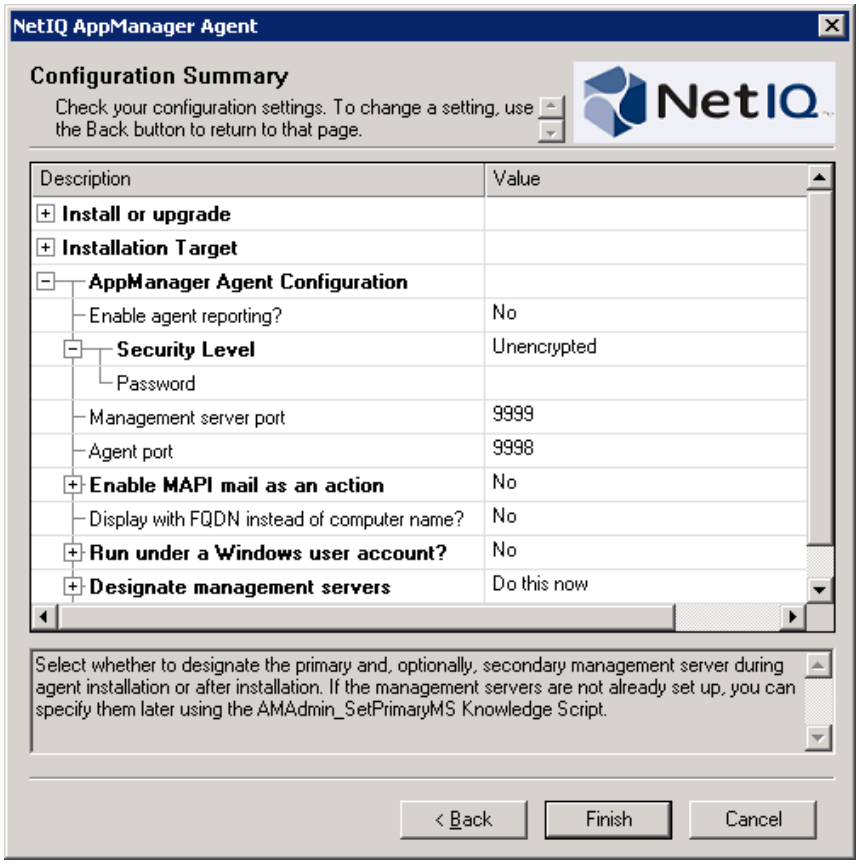


12 At the **Management Server Configuration** dialog box, specify the name of the local computer for the **Primary management server**. For example, `HOUIDAM804`, where you installed all of the AppManager components, including the management server, and then click **Next**.

The agent will only communicate with its primary management server.



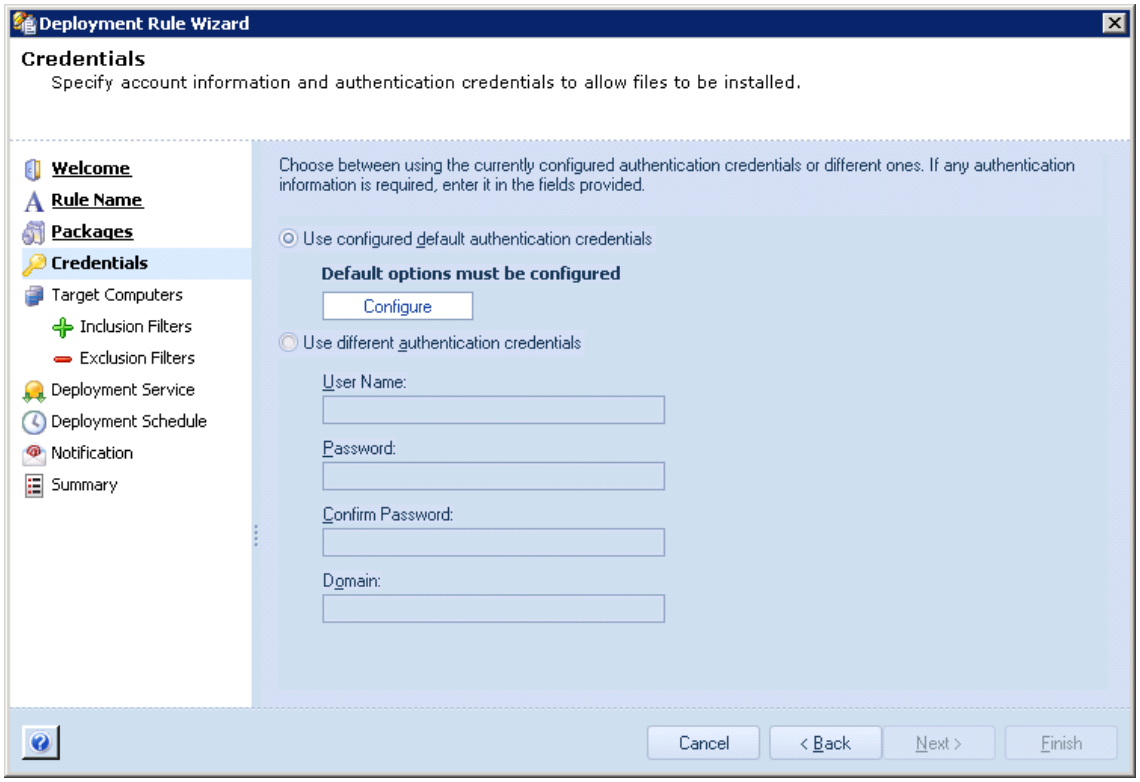
13 At the **Configuration Summary** dialog box, review the summary of the agent installation options, and then click **Finish**.



14 At the **Packages** page of Deployment Rule Wizard, click **Next**.

15 At the **Credentials** page of the Deployment Rule Wizard, if you have configured the default credentials, click **Next**.

(Optional) You can also specify different authentication credentials, by using this **Credentials** page. Ensure that the credentials that you enter for the user is a member of the local **Administrators** group on the target computer. The credentials that you specify here are used to run the deployment package on the target computer.

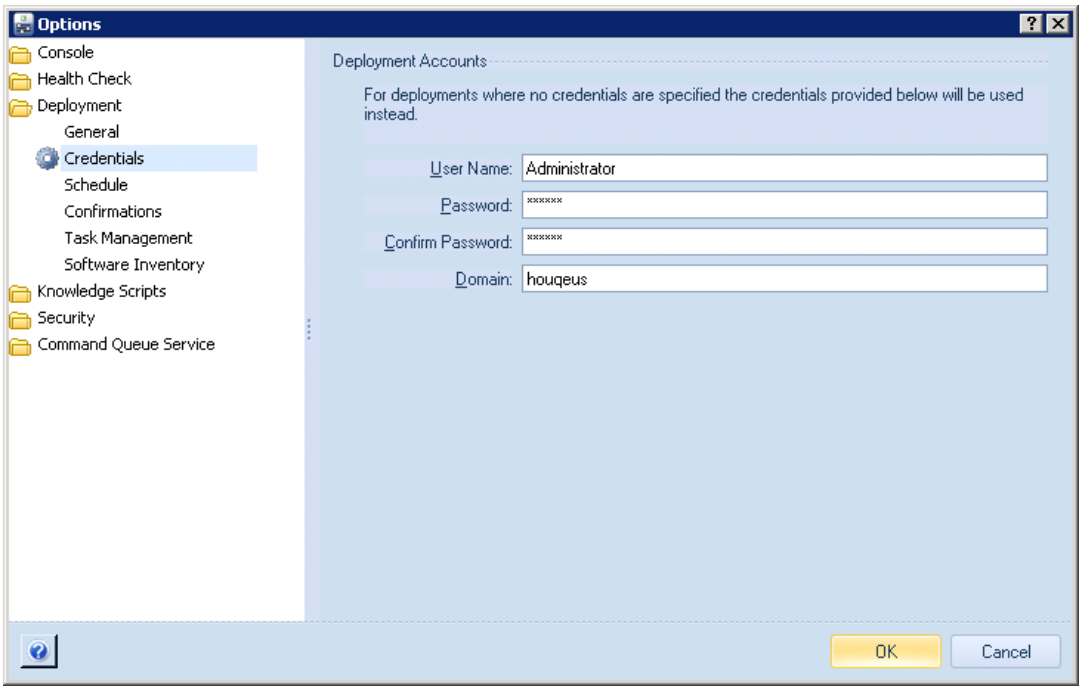


If you have not yet configured the default credentials, you must configure them now.

To configure the default credentials:

15a Click **Configure**.

15b In the **Deployment Accounts** dialog box, specify the credentials of a domain user account that is member of the **Administrators** group on the target computer, and then click **OK**.



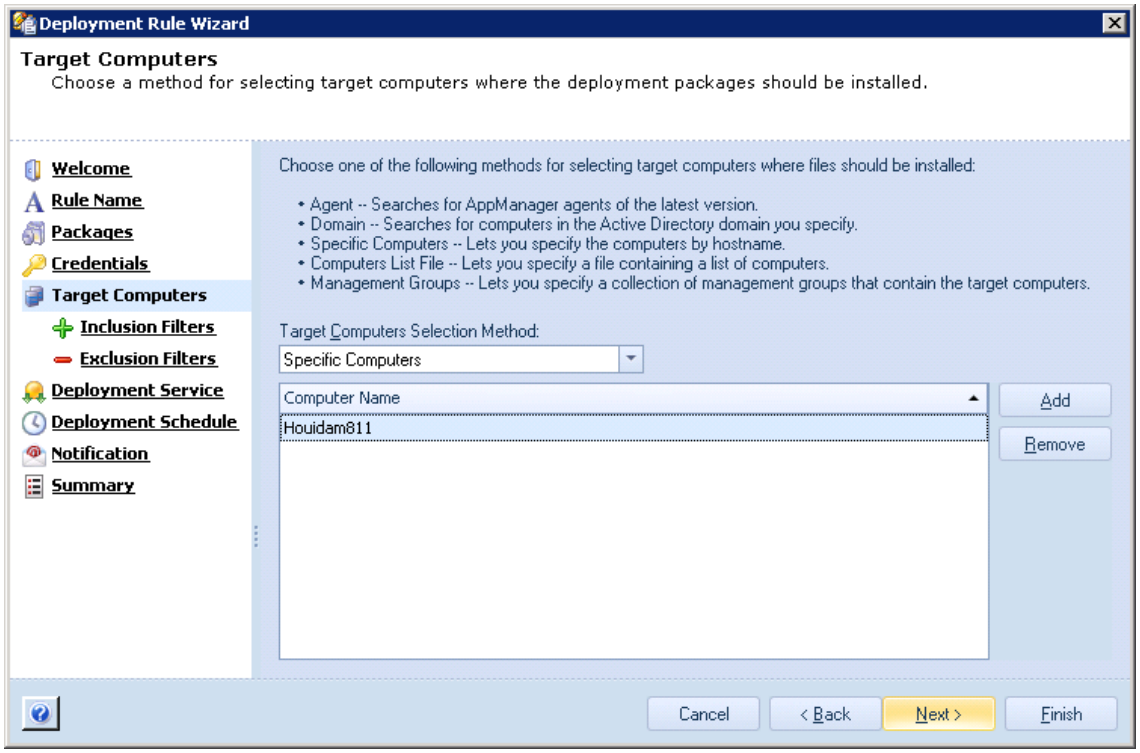
TIP: If you specify invalid credentials, the Control Center Console does not raise a warning until after you enable the deployment rule. In the **Rules** view of the Administration pane, the Status Details column displays information about any problems with the configuration of the rule.

---

16 Click **Next**.

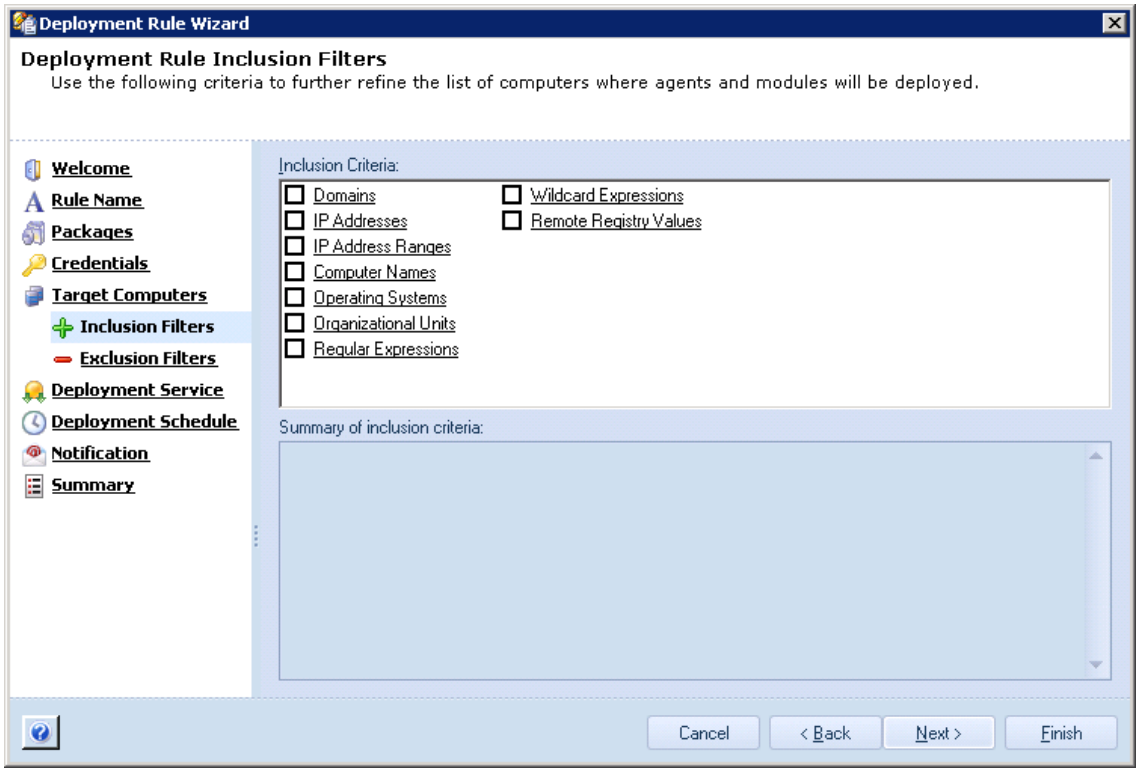
17 In the **Target Computers** page of the Deployment Rule Wizard, select **Specific Computers** from the **Target Computers Selection Method** list.

18 Click **Add**, enter the target computer name where you want to install the deployment package, press **Enter**, and then click **Next**.



19 In the **Deployment Rule Inclusion Filter** page, select the **Wildcard Expression** check box.

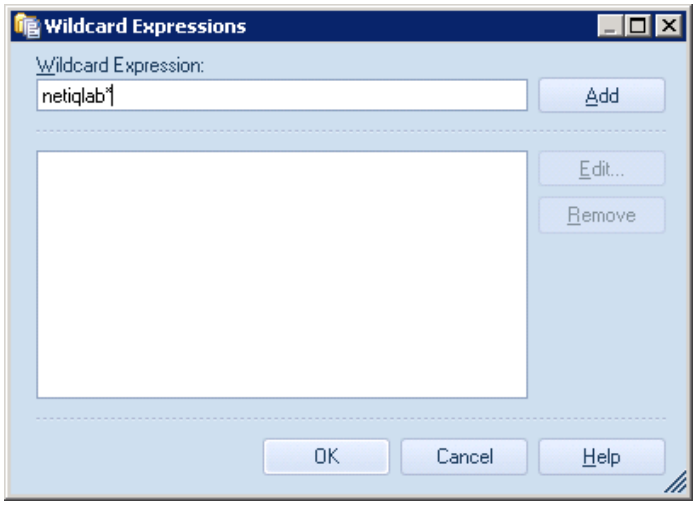
An **inclusion filter** refines the list of computers that match the target computer selection method. Only computers that match the target computer selection method and the inclusion filter are included.



20 Selecting the check box displays the **Wildcard Expression** dialog box to specify a wildcard expression.

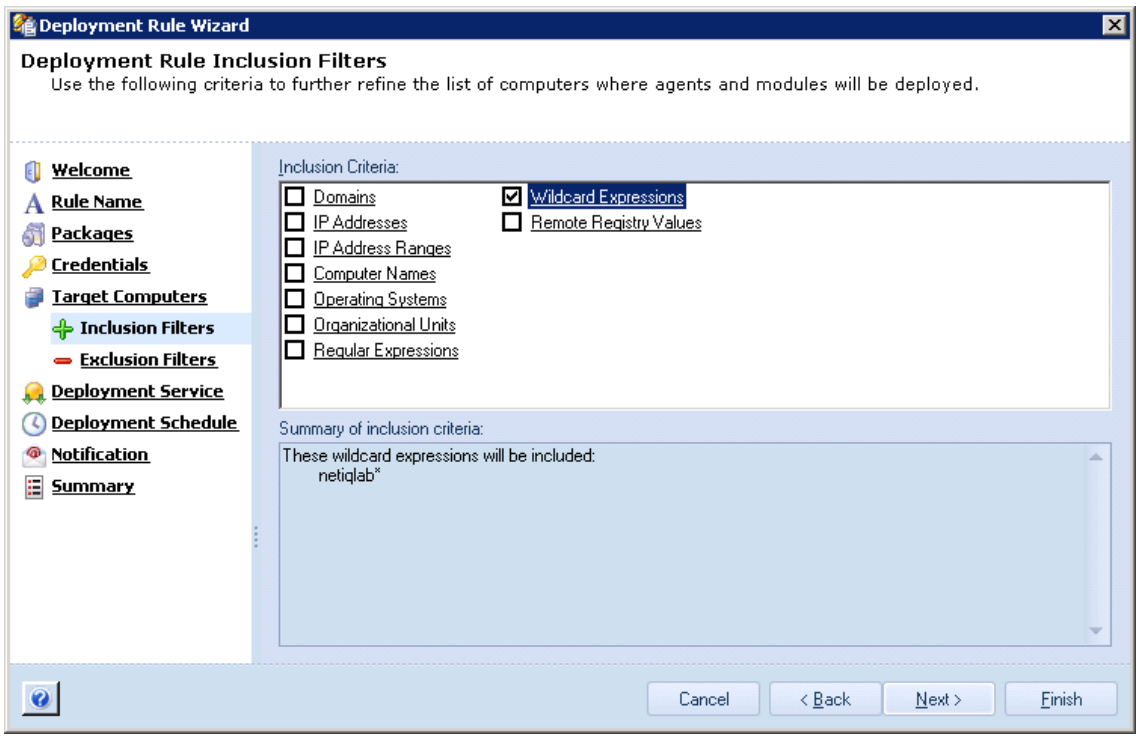
Specify a pattern-matching expression that selects the computers you want. Use the following pattern-matching characters:

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



21 Click **Add**, and then click **OK**.

The wildcard expression is displayed in the summary field.

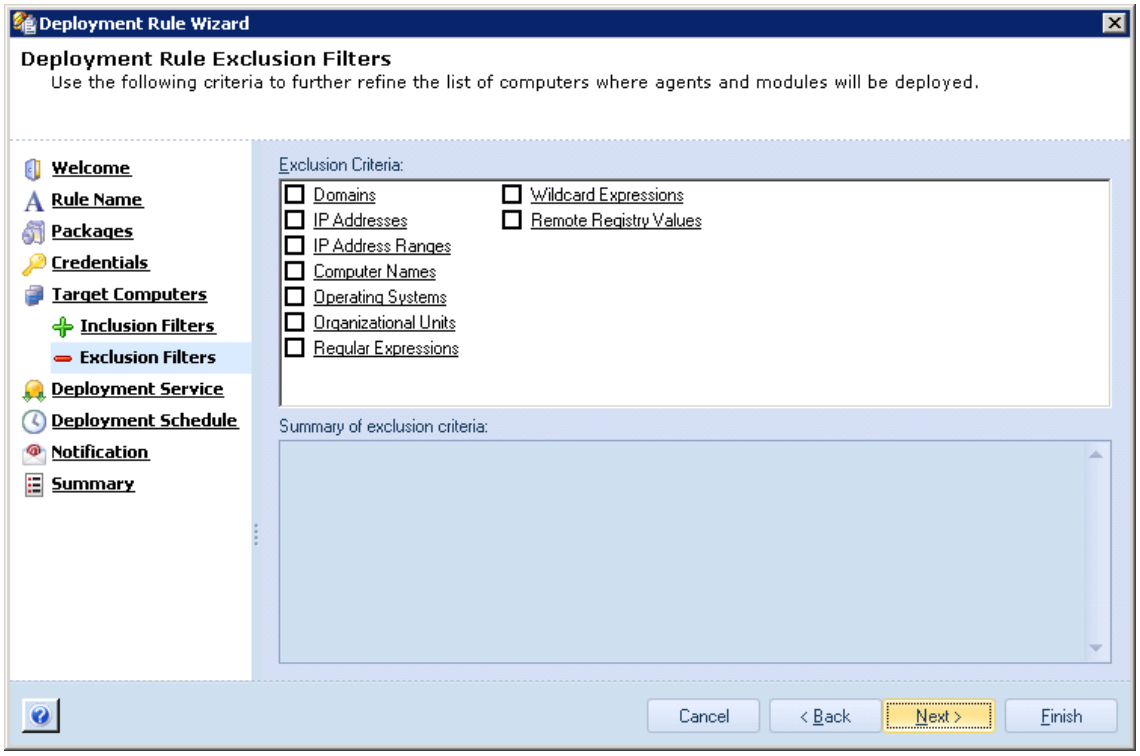


22 Click **Next**.

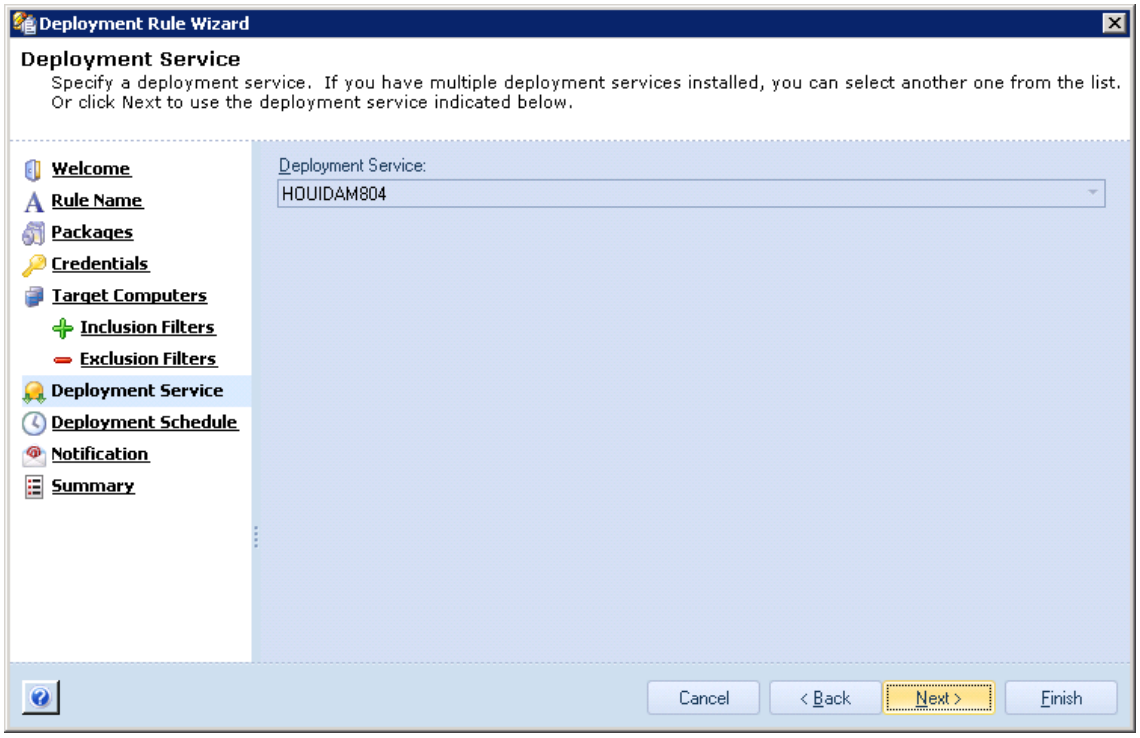
23 At the **Deployment Rule Exclusion Filters** page, click **Next** to accept the default value.

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.

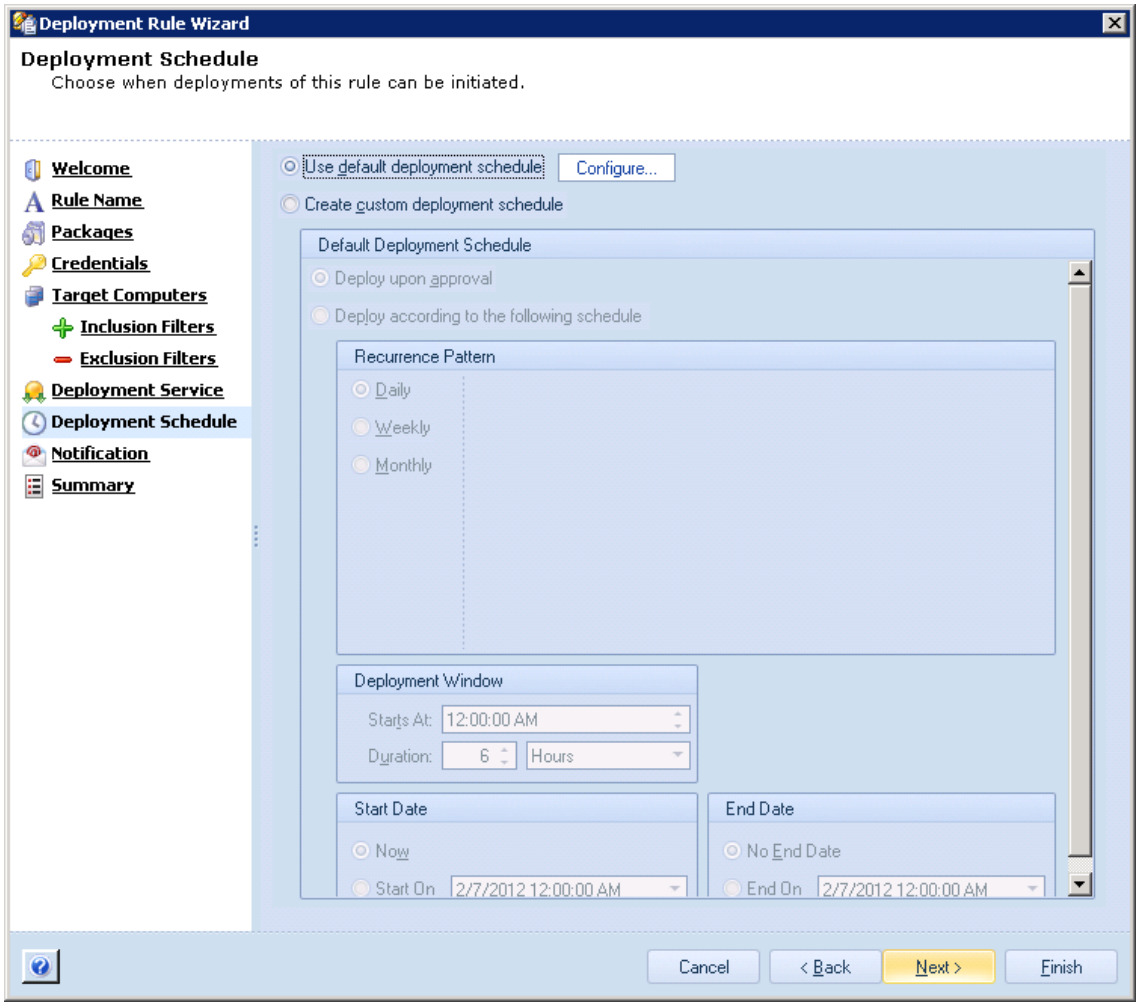
The deployment service processes all computers that match the target computer selection method before applying the inclusion and exclusion filters. For example, after you enable a deployment rule that is configured to select target computers from an Active Directory domain, the deployment service queries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



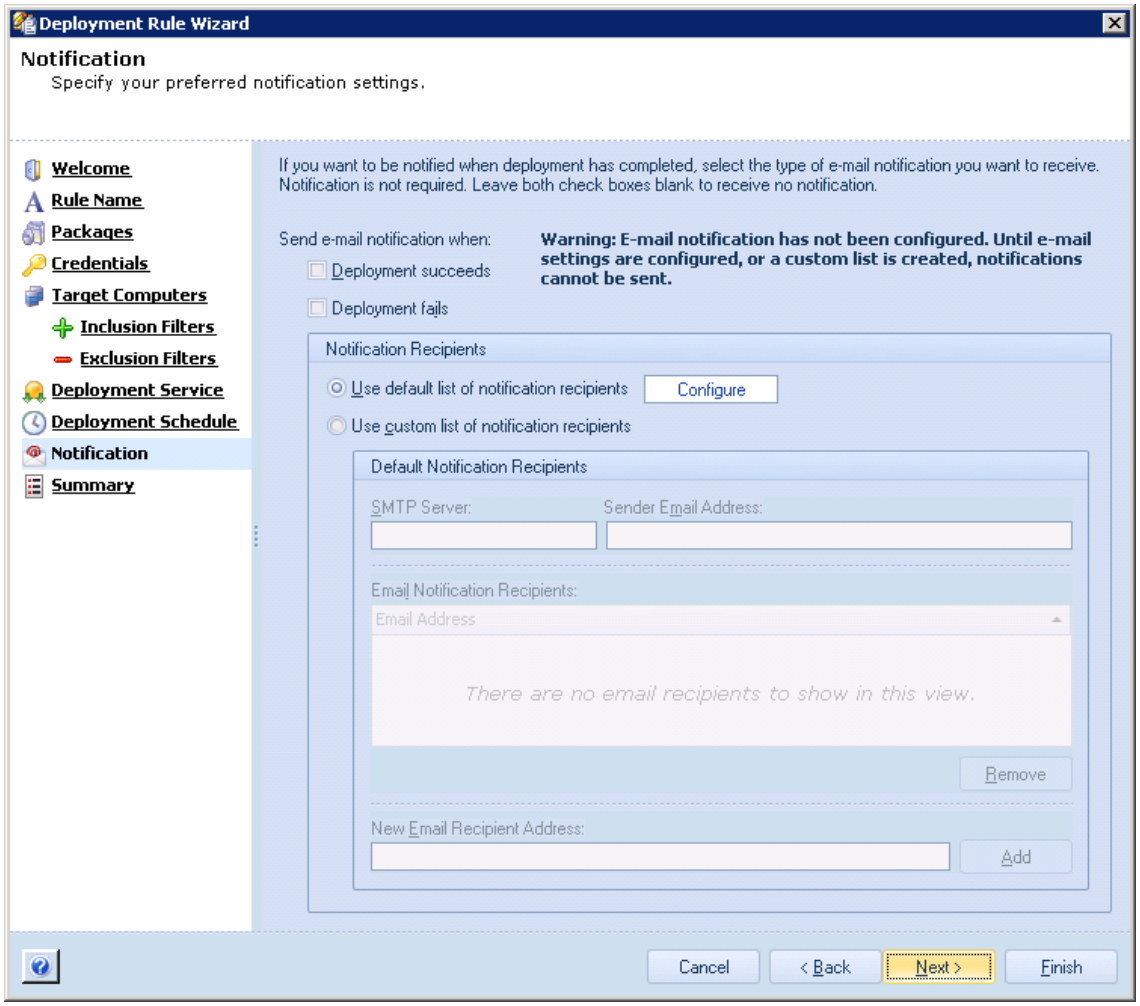
24 At the **Deployment Service** page, click **Next** to accept the default deployment service.



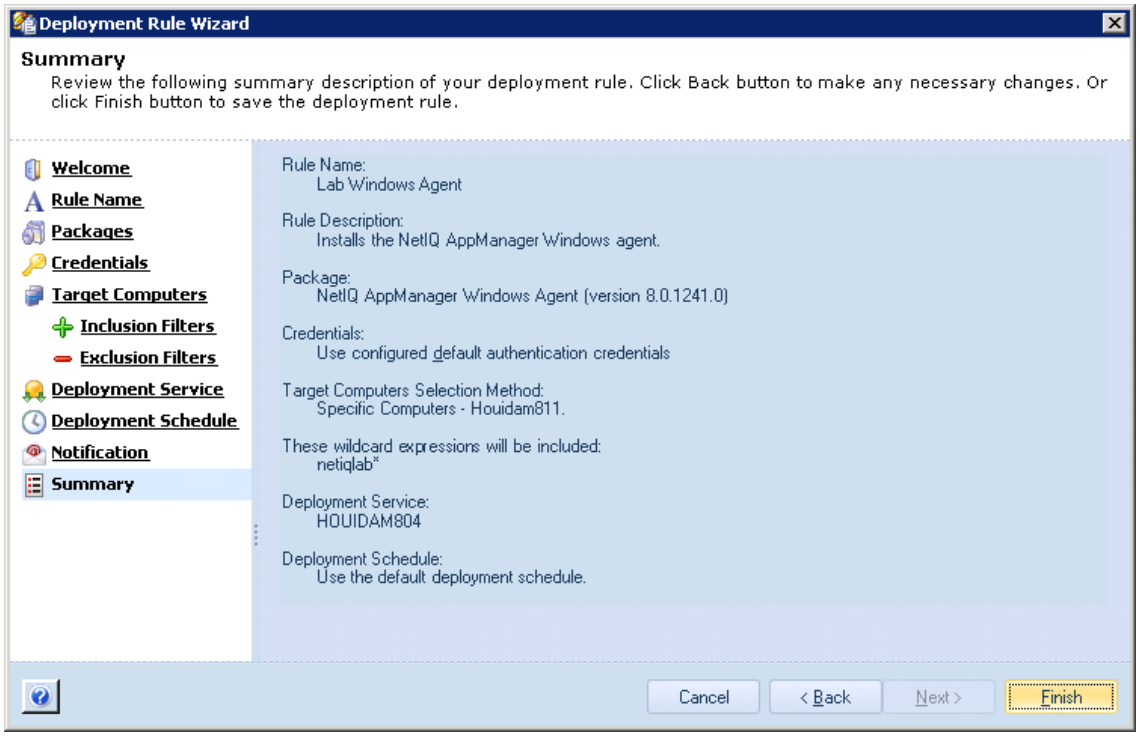
25 At the **Deployment Schedule** page, click **Next** to accept the default deployment schedule.



26 At the **Notification** page, click **Next** to accept the default values.



27 In the **Summary** section of the Deployment Rule Wizard, view a summary of how the rule is configured, and then click **Finish**.



28 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 Section 3.3.4, "Enabling the Rule," on page 72.

29 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 Section 3.3.5, "Approving Deployment Tasks," on page 73.

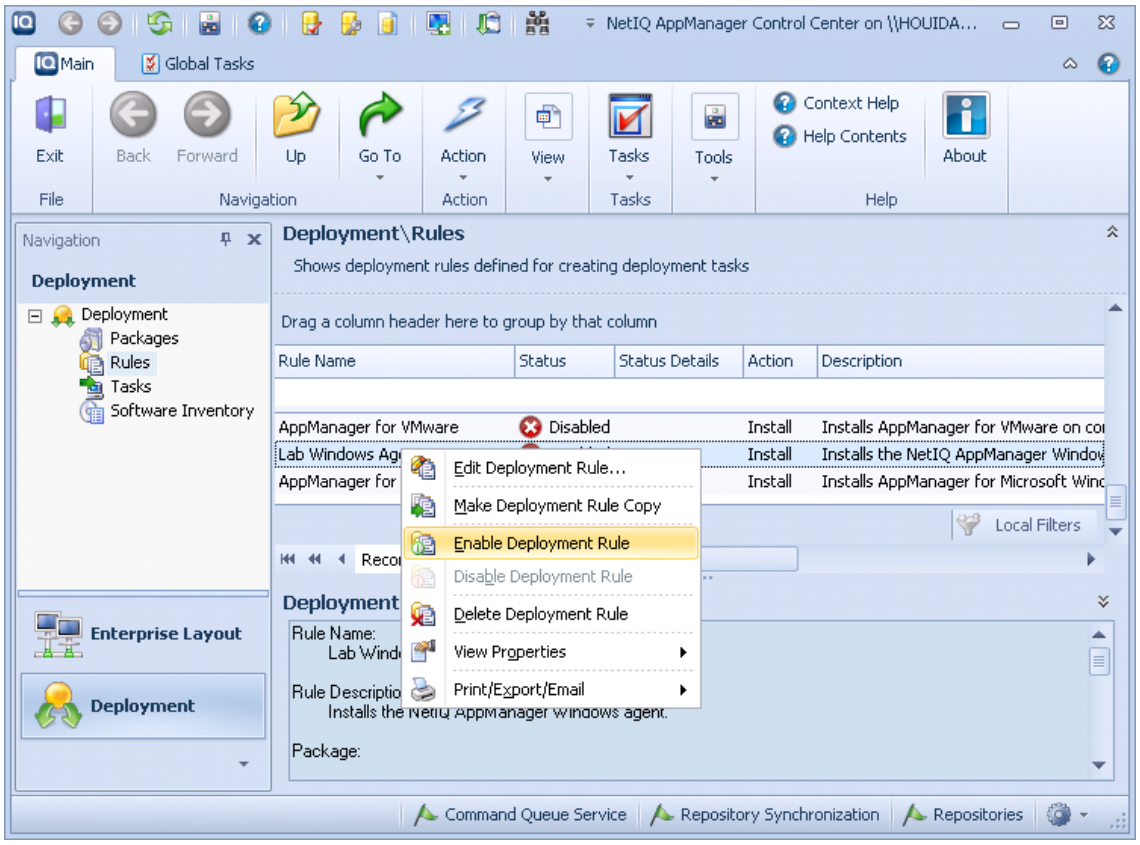
3.3.4 Enabling the Rule

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.

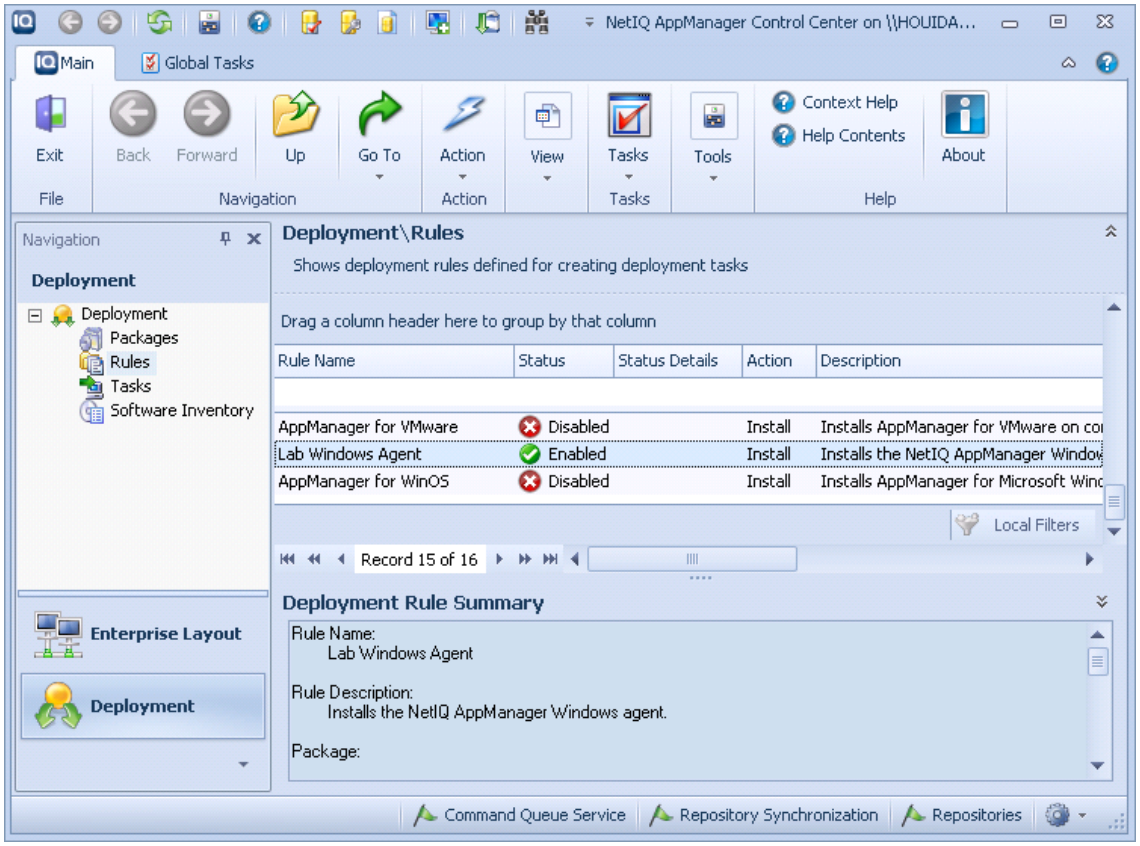
To enable the rule:

1 In the **Rules** view, right-click the **Lab Windows Agent** rule, and then click **Enable Deployment 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 is change to `Enabled`.



3 If the rule status does not change to `Enabled`, manually refresh the list of rules by pressing F5 to refresh the current view or by pressing F6 to refresh all data.

Alternatively, you can click the **Refresh current View** icon in the **Quick Access** Toolbar.

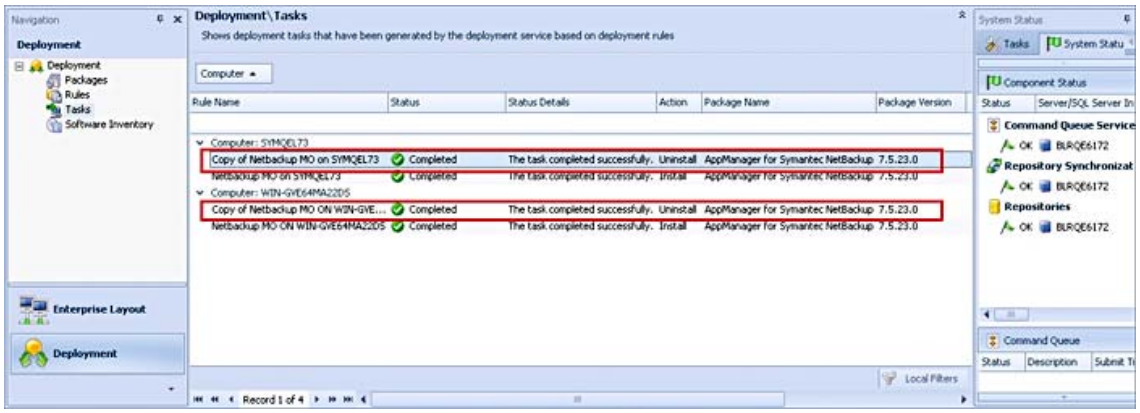
3.3.5 Approving Deployment Tasks

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 Section 3.4, “Understanding Monitoring Policies,” on page 74.

To approve a deployment task:

1 In the **Deployment Tasks** 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 "Section 3.4, "Understanding Monitoring Policies," on page 74," to configure the `Lab01` management group to automatically monitor servers that match its target selection criteria.

3.4 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 chapter 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.

3.4.1 Creating a Knowledge Script Group

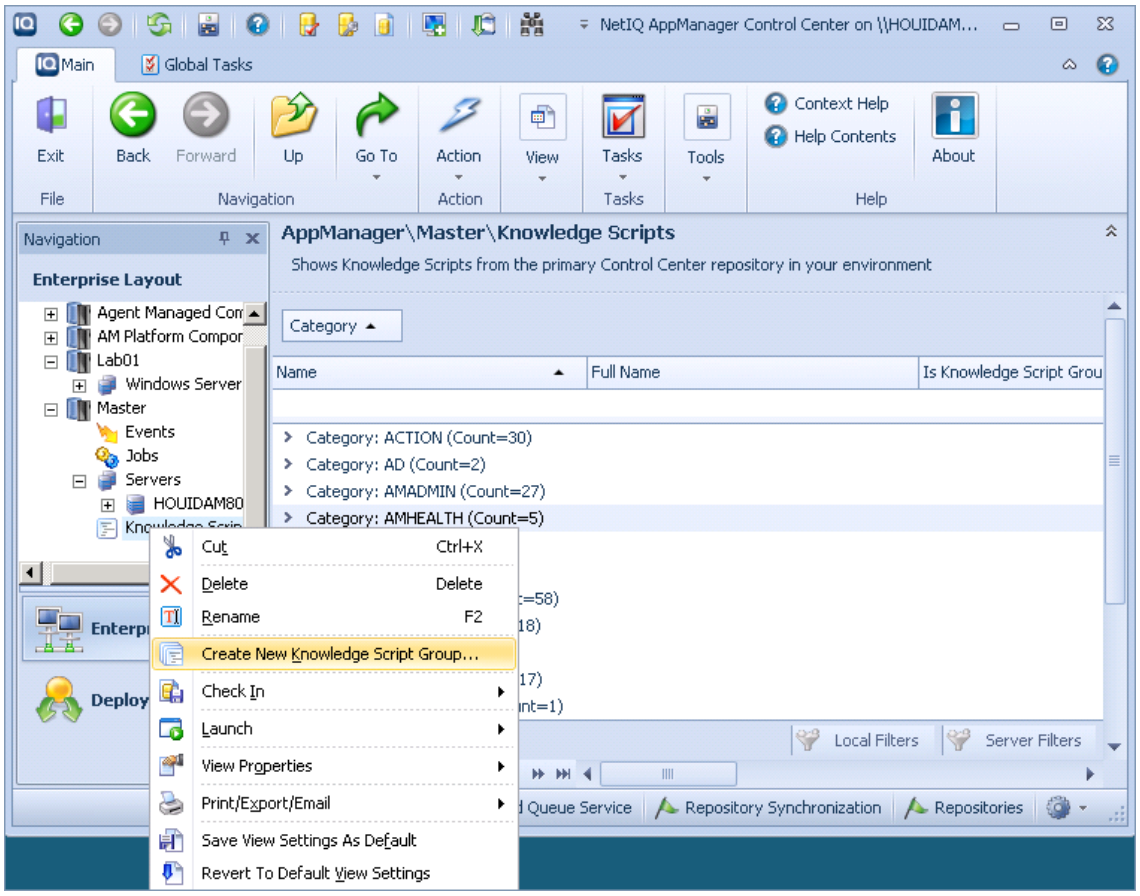
Create a Knowledge Script Group that includes the following **NT** Knowledge Scripts:

- **CpuLoaded** monitors total CPU usage and queue length to determine whether the CPU is overloaded.
- **DiskSpace** 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.

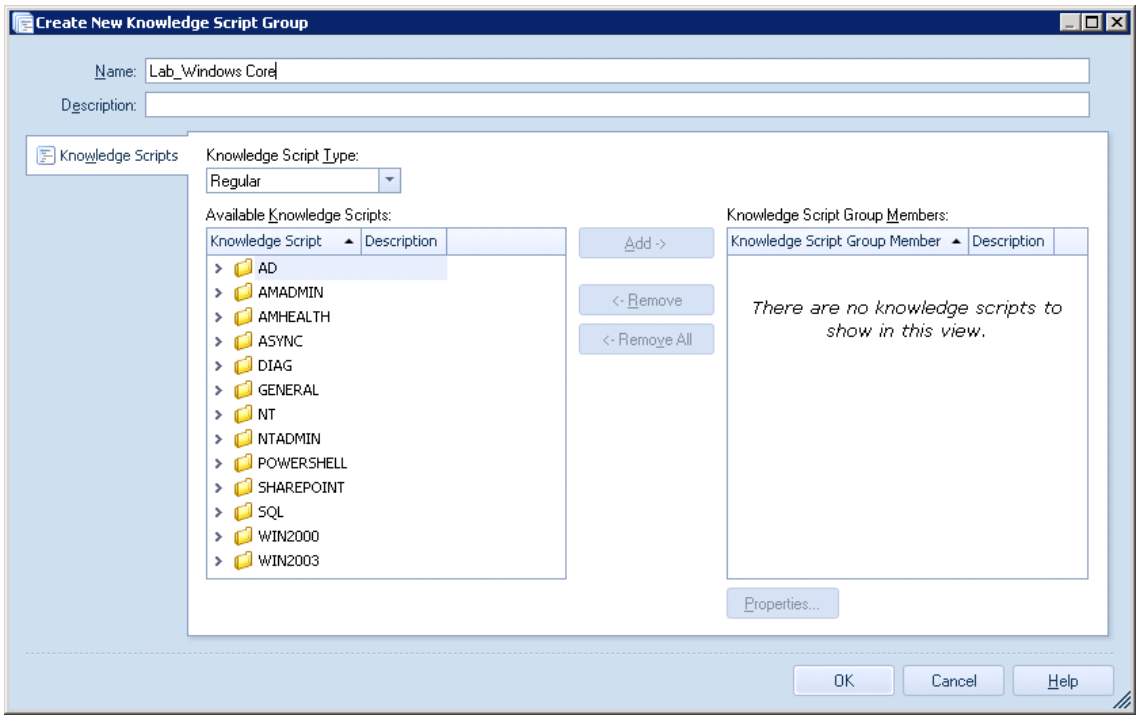
Configure these Knowledge Scripts to run on a particular schedule, collect data, and raise events.

To create a Knowledge Script Group:

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



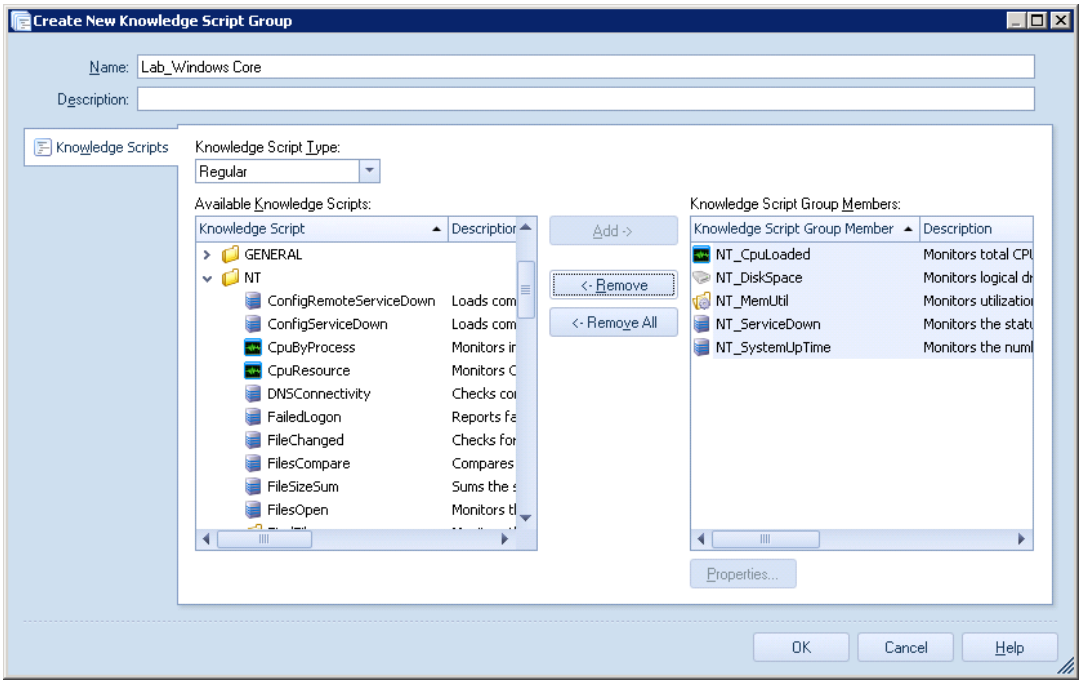
2 In the **Name** field of the Knowledge Script Group dialog box, specify `Lab_Windows Core` to create a new Knowledge Script category called **Lab**, and to create a new Knowledge Script Group called **Windows Core** under the **Lab** category.



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 following Knowledge Scripts by pressing the `Ctrl` key, and then click **Add**:

- CpuLoaded
- DiskSpace
- MemUtil
- ServiceDown
- SystemUpTime

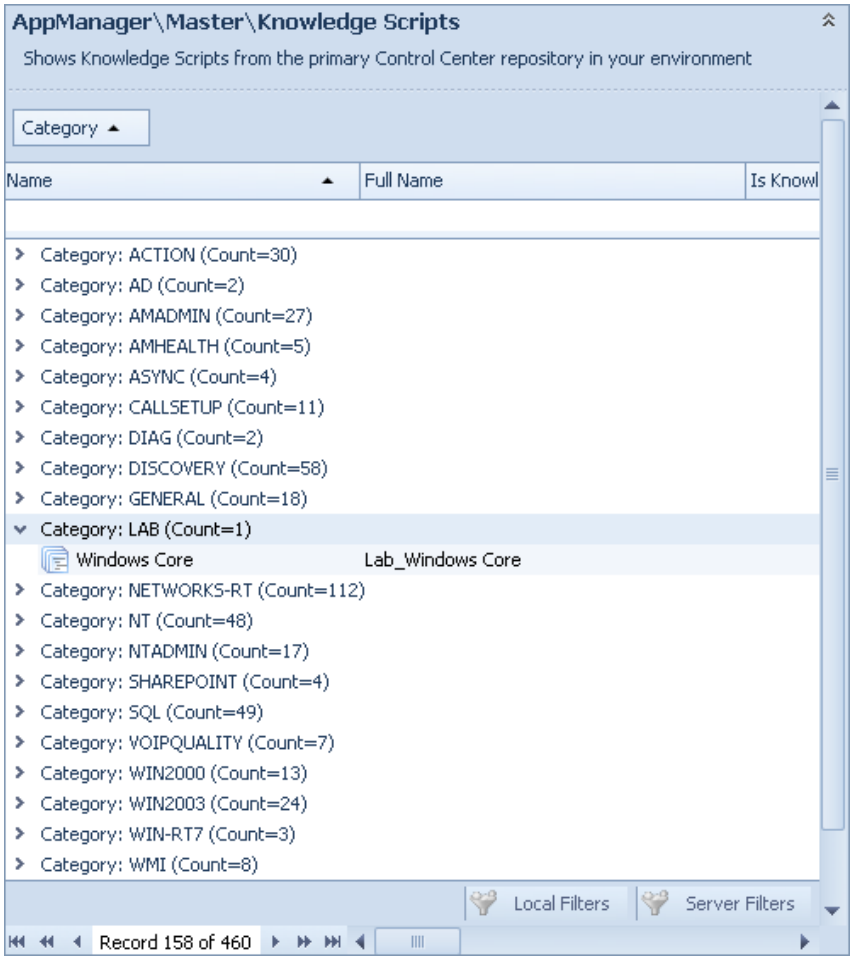


4 Configure the properties of each Knowledge Script Group member.

For information about	See
NT_CpuLoaded	“Configuring NT_CpuLoaded” on page 79
NT_DiskSpace	“Configuring NT_DiskSpace” on page 82
NT_MemUtil	“Configuring NT_MemUtil” on page 84
NT_ServiceDown	“Configuring NT_ServiceDown” on page 86
NT_SystemUpTime	“Configuring NT_SystemUpTime” on page 88

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 Section 3.4.2, "Enabling the Monitoring Policy," on page 91.

Configuring NT_CpuLoaded

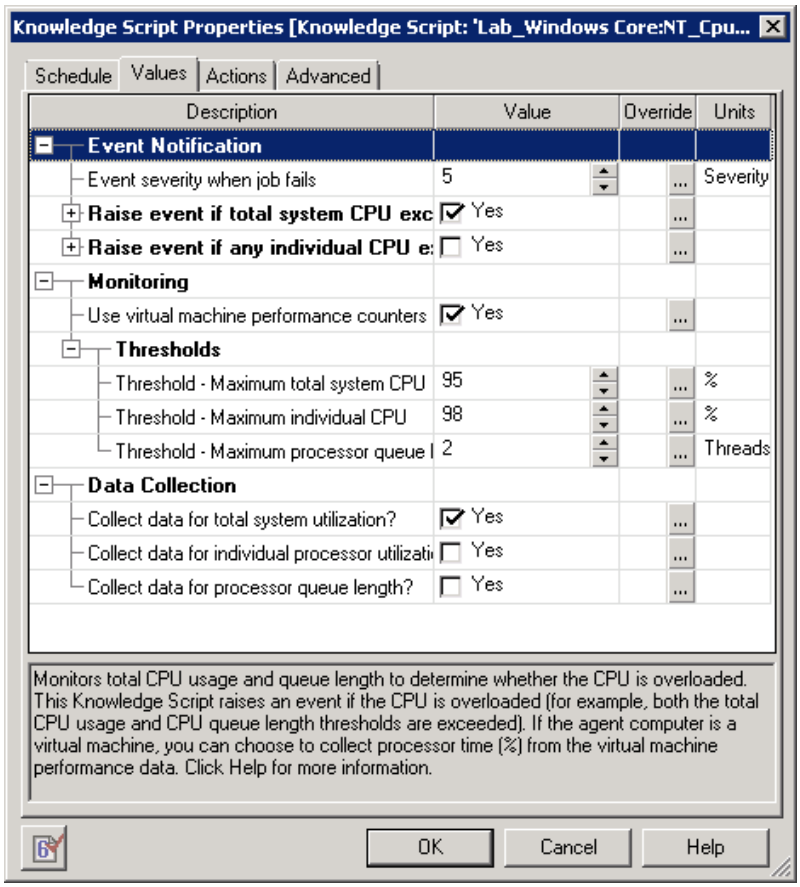
Configure NT_CpuLoaded to collect data on the overall percentage of CPU time used. The detail data contains information about:

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

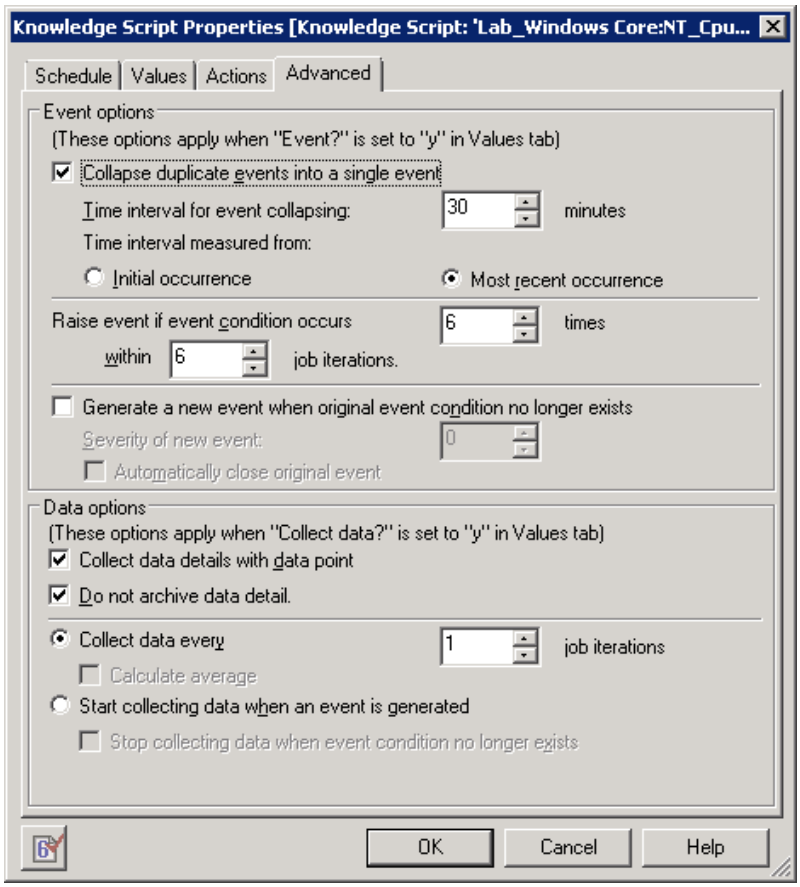
To ensure that temporary spikes in CPU utilization do not raise a false-positive event, configure the event options to raise an event if the threshold is exceeded every time the job runs during any 30-minute interval.

To configure NT_CpuLoaded:

1. In the **Knowledge Script Group** dialog box, click **NT_CpuLoaded** in the Member column and click **Properties**.
2. On the **Values** tab of the **Properties** dialog box, select the **Collect data for total system utilization?** 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.

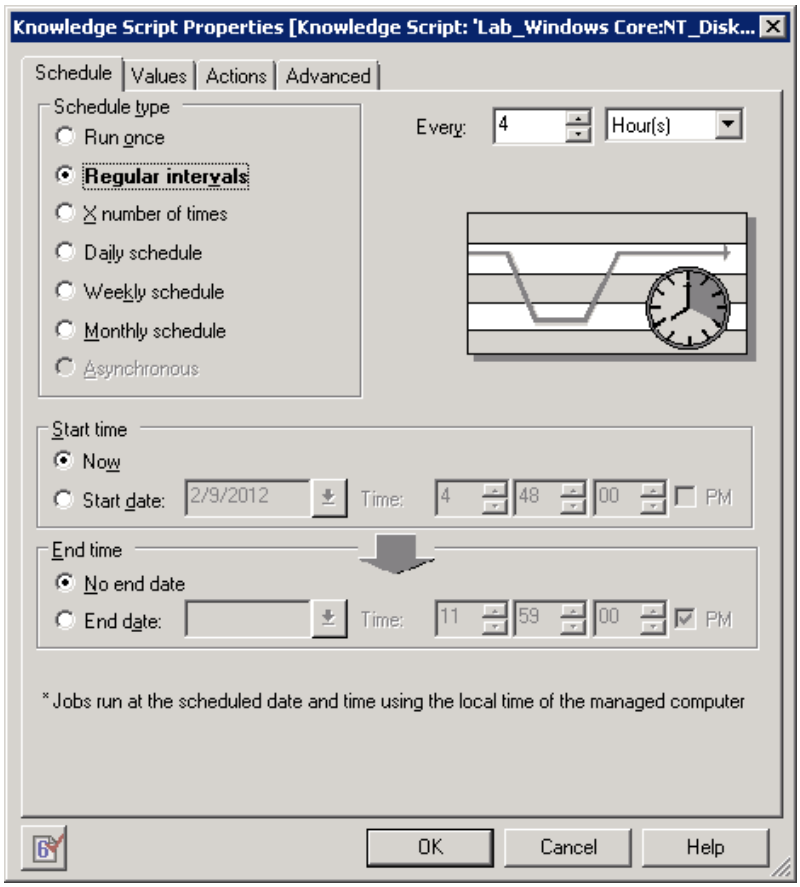
4 Click **OK**.

Configuring NT_DiskSpace

Configure the schedule for NT_DiskSpace 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.

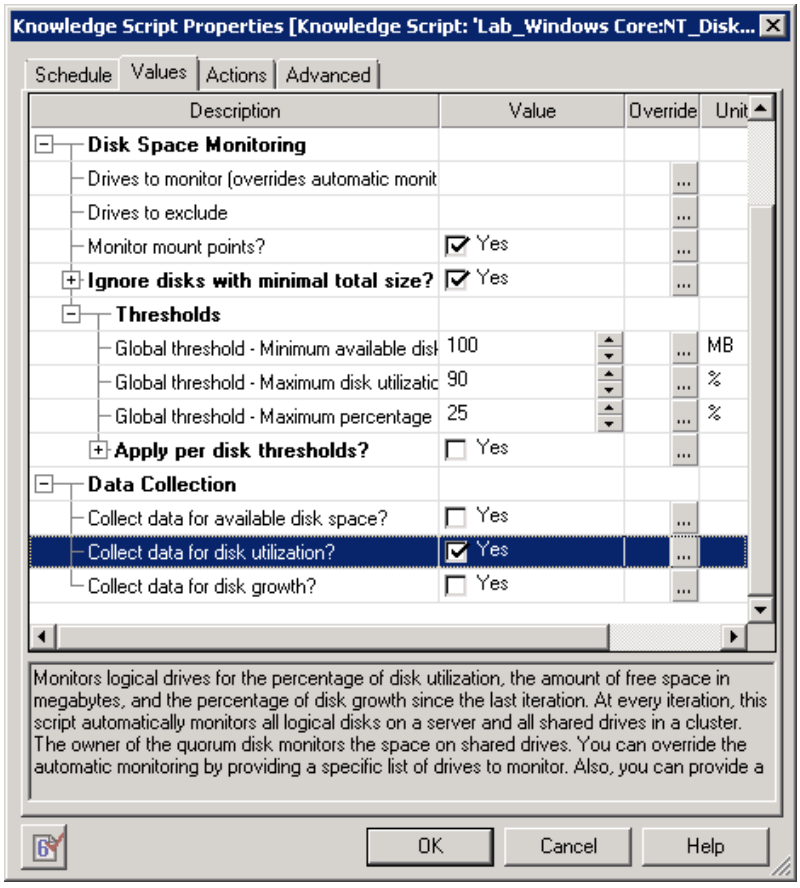
To configure NT_DiskSpace:

1. In the **Knowledge Script Group** dialog box, click **NT_DiskSpace** in the **Member** column and click **Properties**.
2. On the **Schedule** tab of the **Properties** dialog box, specify **Regular intervals** to every **4 hours**.

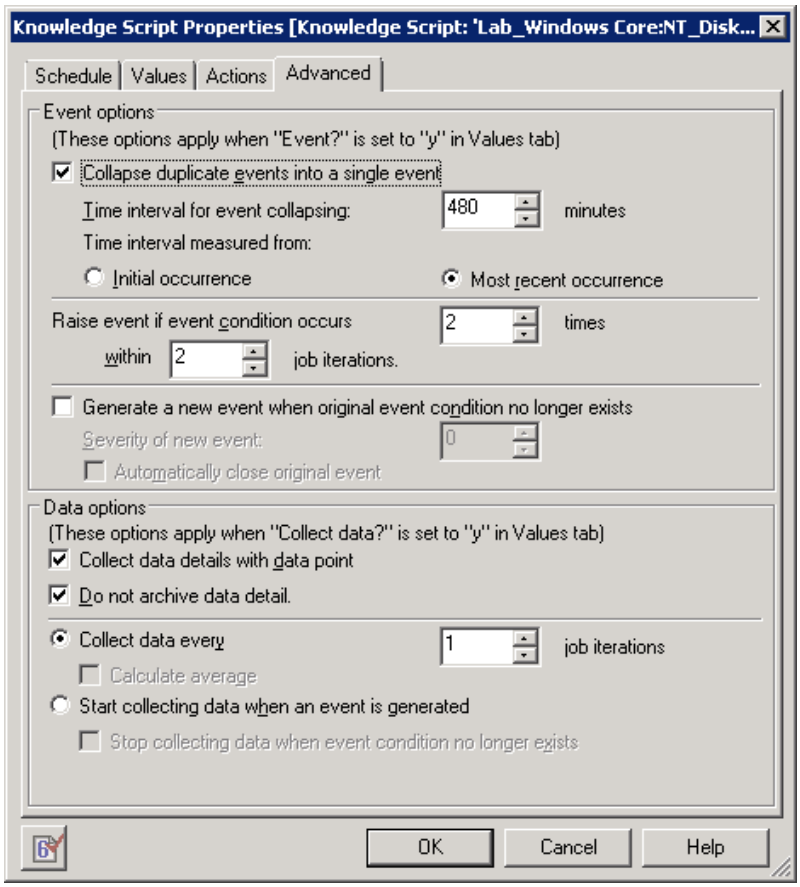


3 On the **Values** tab of the **Properties** dialog box, select the **Collect data for disk utilization?** check box to collect data for charts and reports.

If selected, it 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_MemUtil

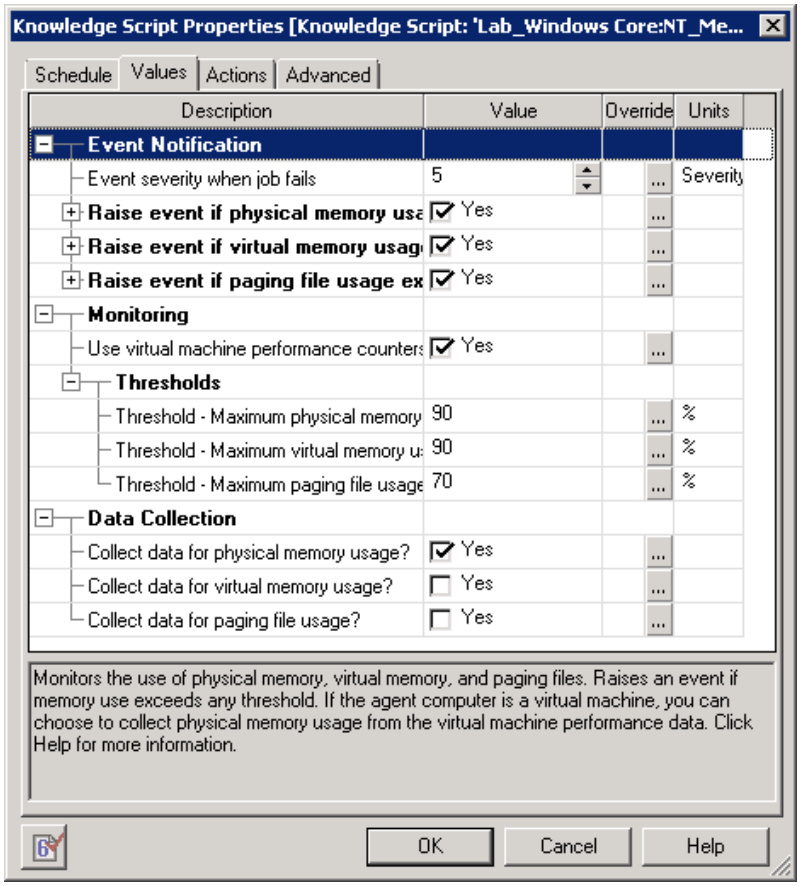
Configure NT_MemUtil to collect data for physical memory usage. To ensure that temporary spikes in memory utilization do not raise a false-positive event, configure the event options to only raise an event if the threshold is exceeded every time the job runs during any 30-minute interval.

To configure NT_MemUtil:

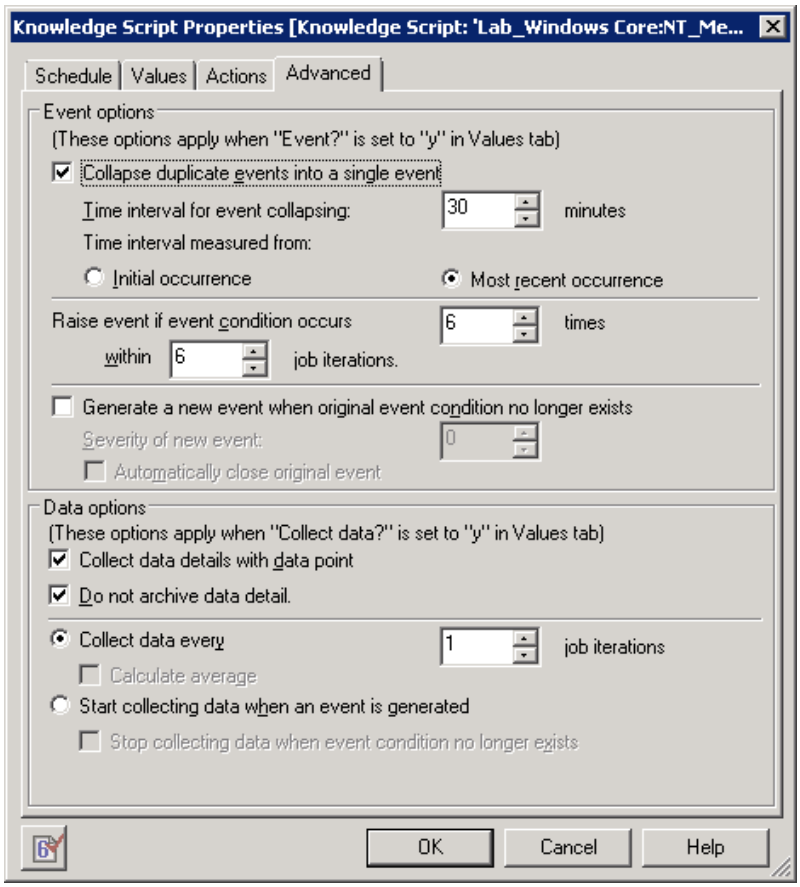
1 In the **Knowledge Script Group** dialog box, click **NT_MemUtil** in the **Member** column and click **Properties**.

2 On the **Values** tab of the **Properties** dialog box, select the **Collect data for physical memory?** check box 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_ServiceDown

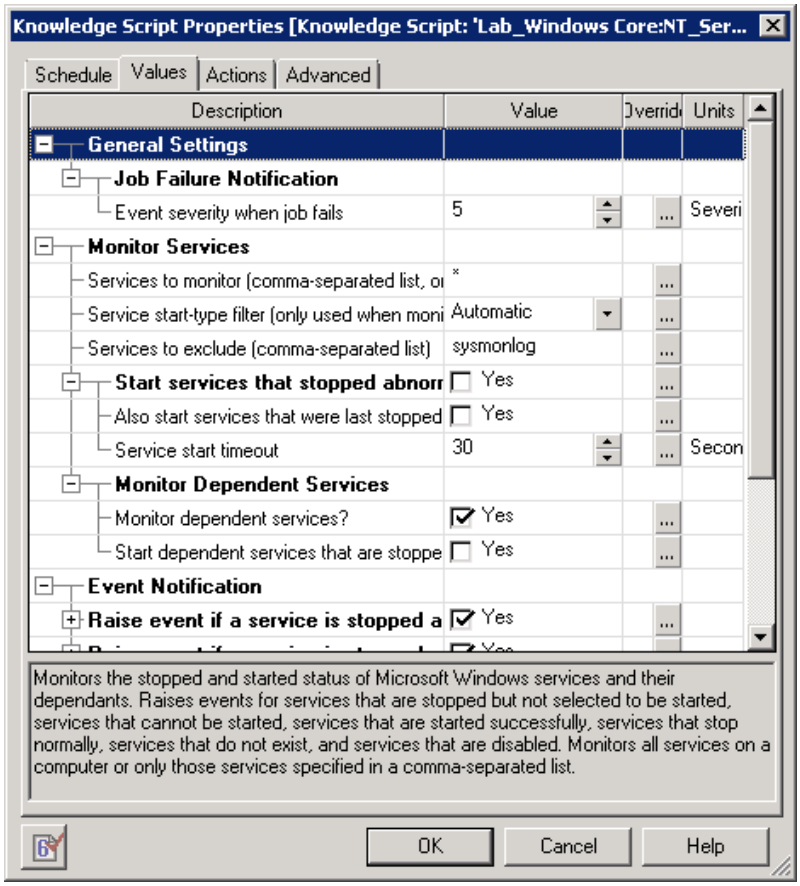
Configure NT_ServiceDown to monitor Windows services and raise an event if they stop. This Knowledge Script optionally restarts a service that is down.

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

To configure NT_ServiceDown:

1. In the **Knowledge Script Group** 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
Services to monitor	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 services that stopped abnormally?	Deselect this check box.

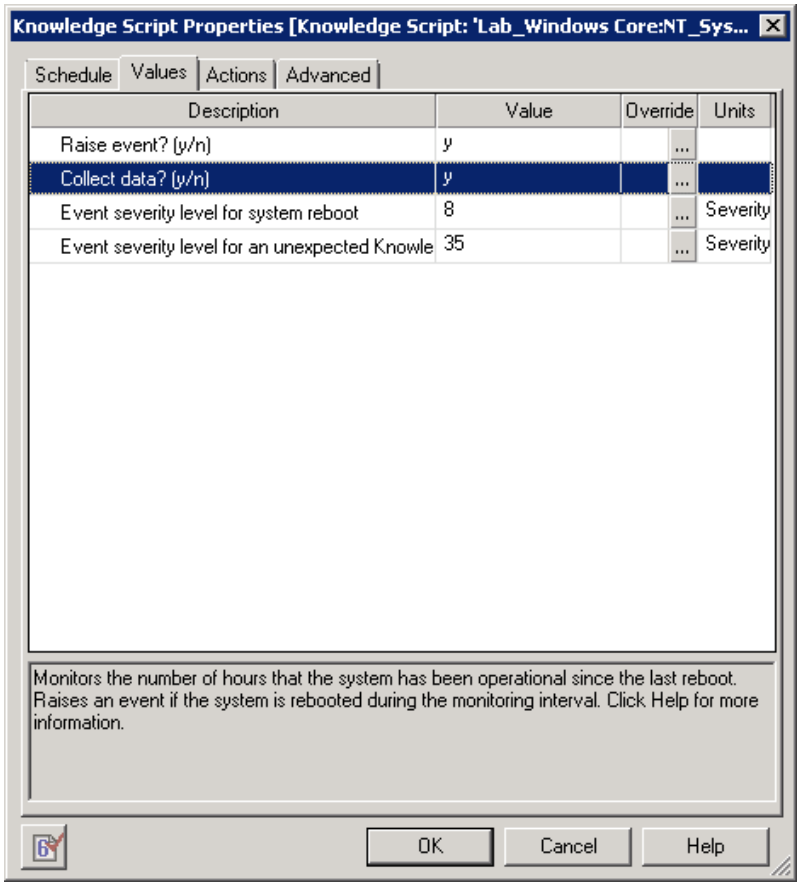


3. Click **OK**.

Configuring NT_SystemUpTime

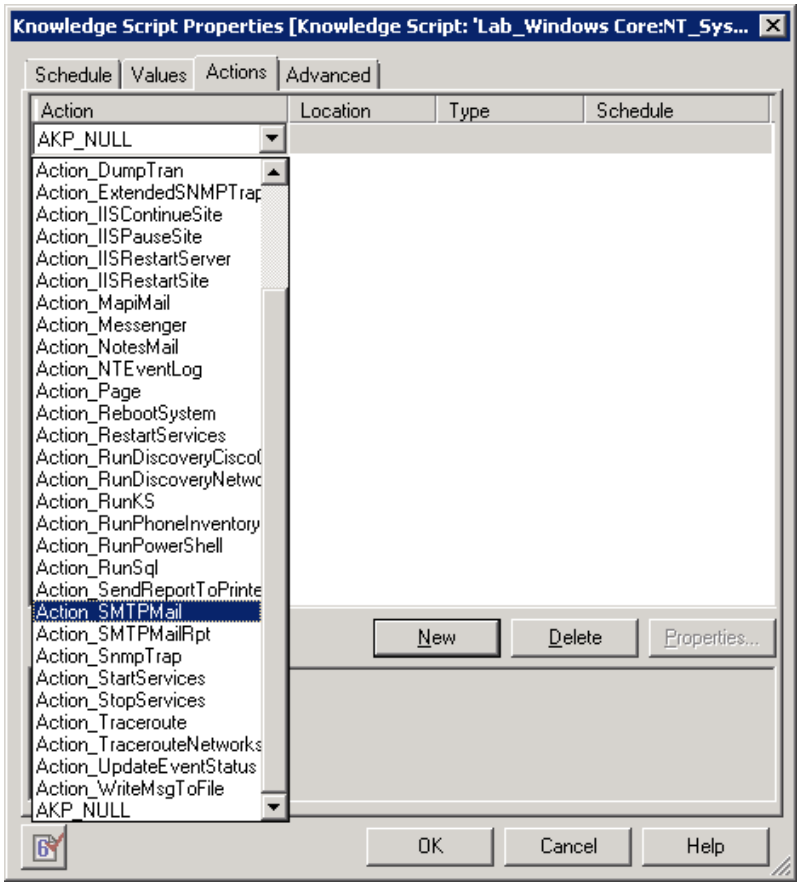
Configure NT_SystemUpTime to collect data and raise events, and send an e-mail message as a responsive action if an event is raised.

1. In the **Knowledge Script Group** dialog box, click **NT_SystemUpTime** in the **Member** column and click the **Properties** button.
2. On the **Values** tab of the **Properties** dialog box, for **Collect data?** property, specify Y to collect data for charts and reports. When set to y, it returns the number of hours the operating system has been up since the computer was last rebooted.

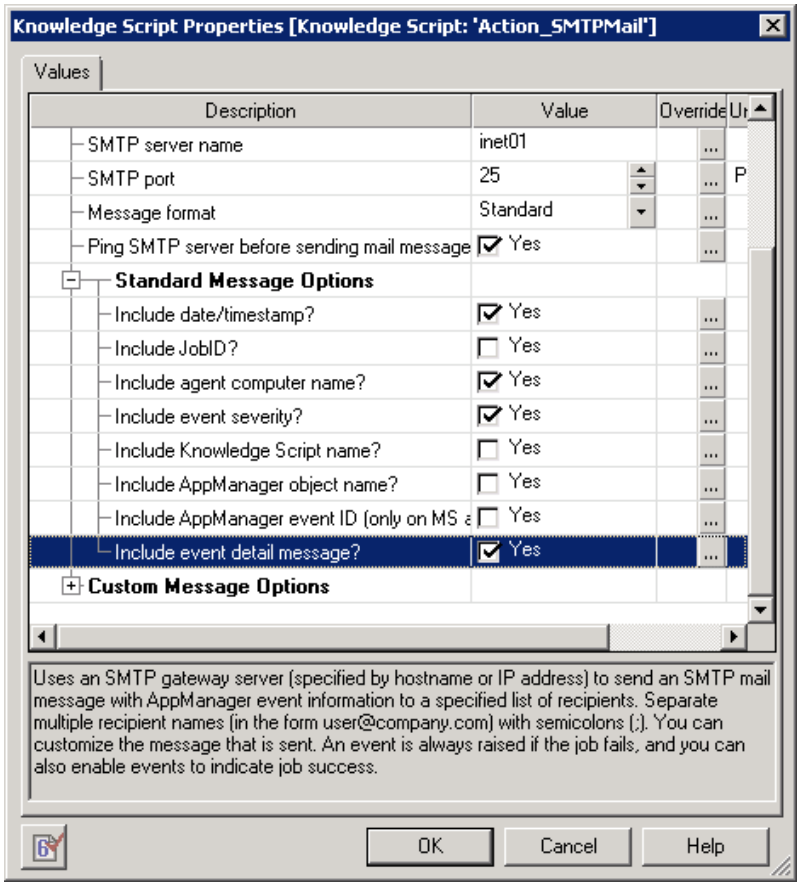


3 On the **Actions** tab of the Properties dialog box, click **New** and select the **SMTPMail** Action Knowledge Script from the **Action** drop-down list.

This Action Knowledge Script sends an e-mail message as a responsive action when an event is raised.



4 Click **Properties** and specify your SMTP mail server properties.



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. **NOTE**: Some Exchange configurations might require additional settings or values. For security restrictions and other information, check with the Exchange/SMTP administrator.
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?`

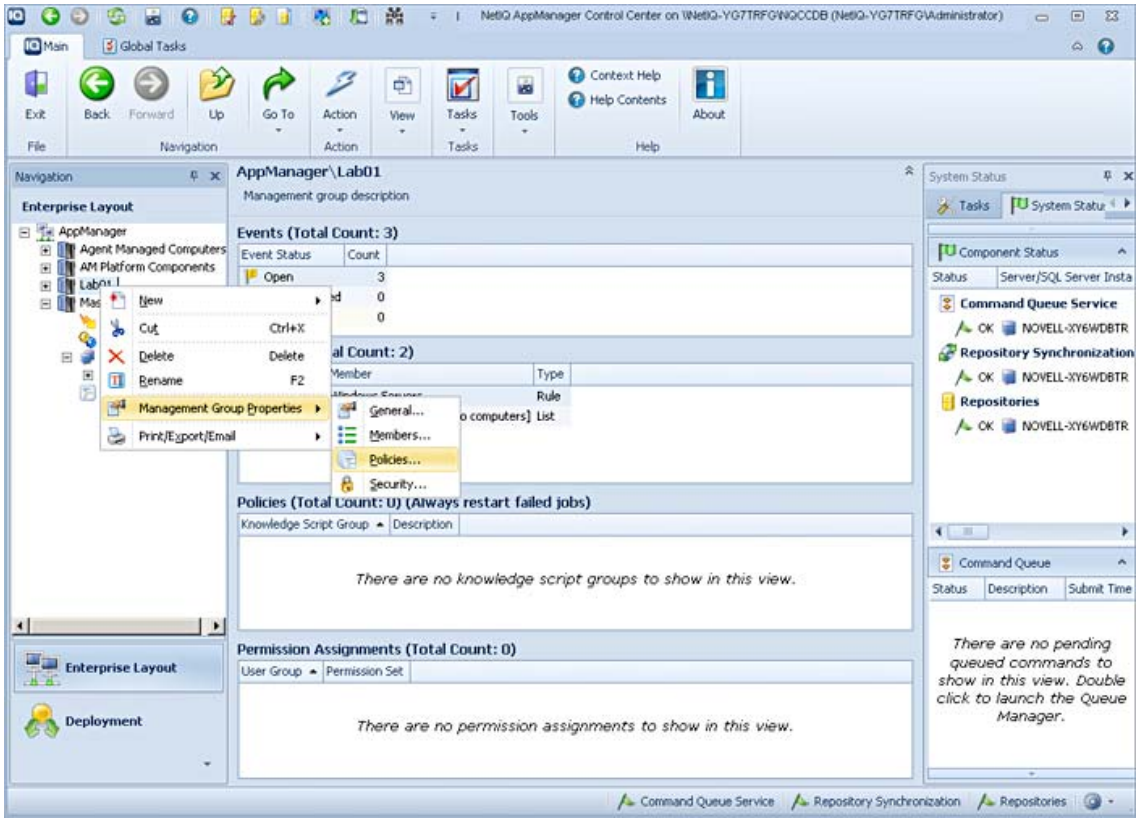
5 Click **OK** thrice.

3.4.2 Enabling the Monitoring Policy

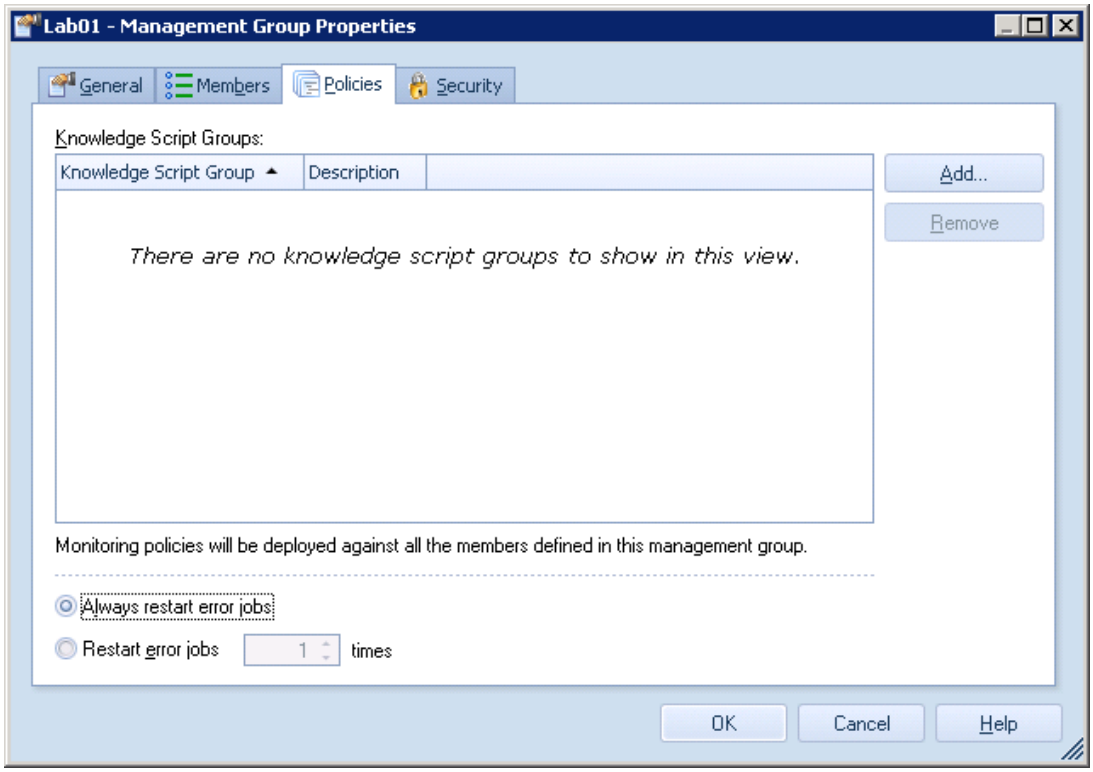
Configure the monitoring policy for the `Lab01` management group to use the `Windows Core` Knowledge Script Group. Any computers in the `Lab01` management group are automatically monitored by the members of the `Windows Core` Knowledge Script Group.

To enable a monitoring policy for the Lab01 management group:

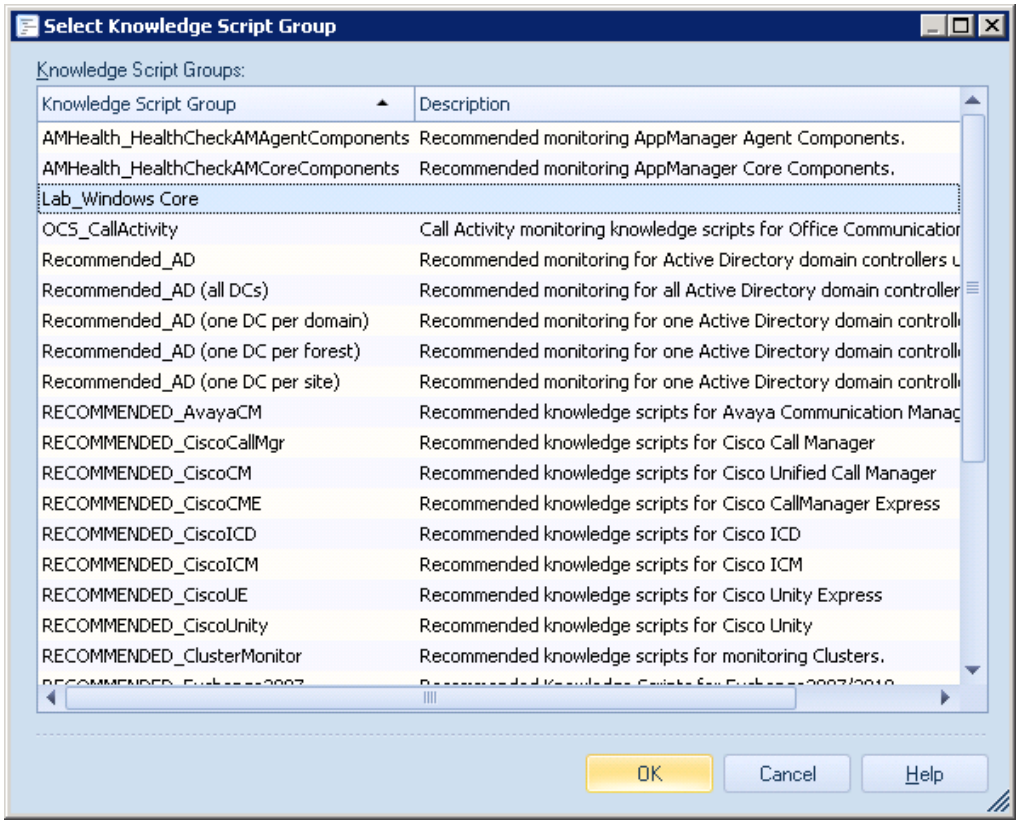
1 In the Enterprise Layout pane, right-click the `Lab01` management group, click **Management Group Properties**, and then click **Policies**.



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



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



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

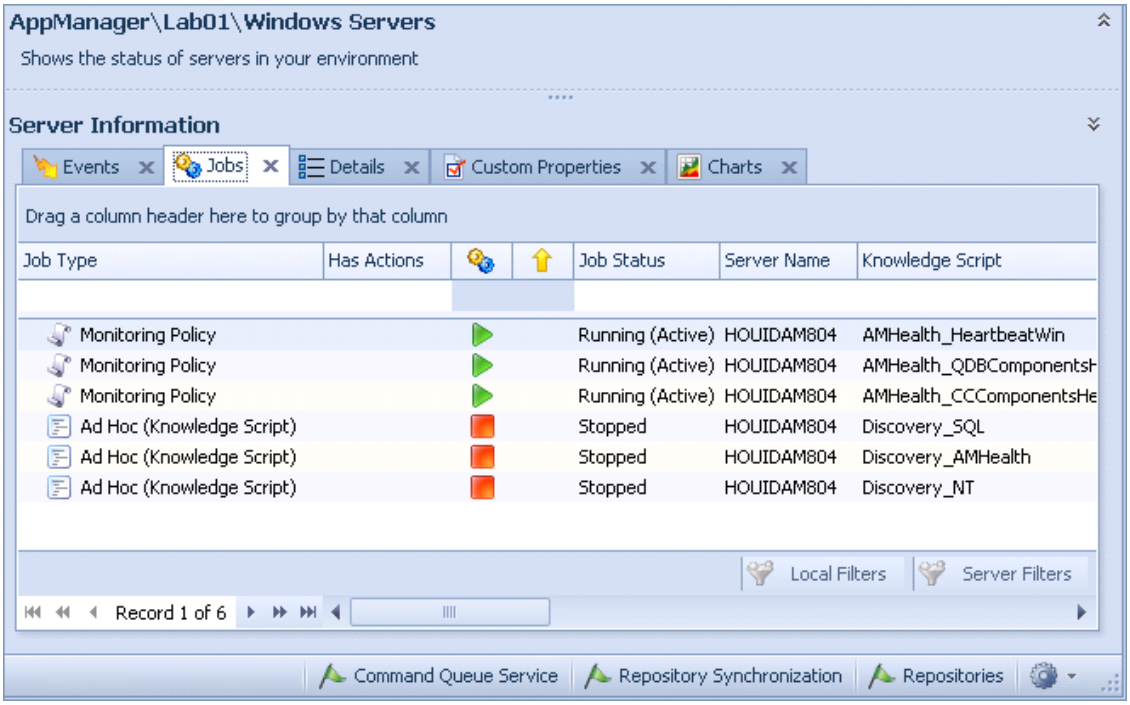
3.5 Working with Server Views

Use a Server view to 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.

3.5.1 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`.

3.5.2 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**.

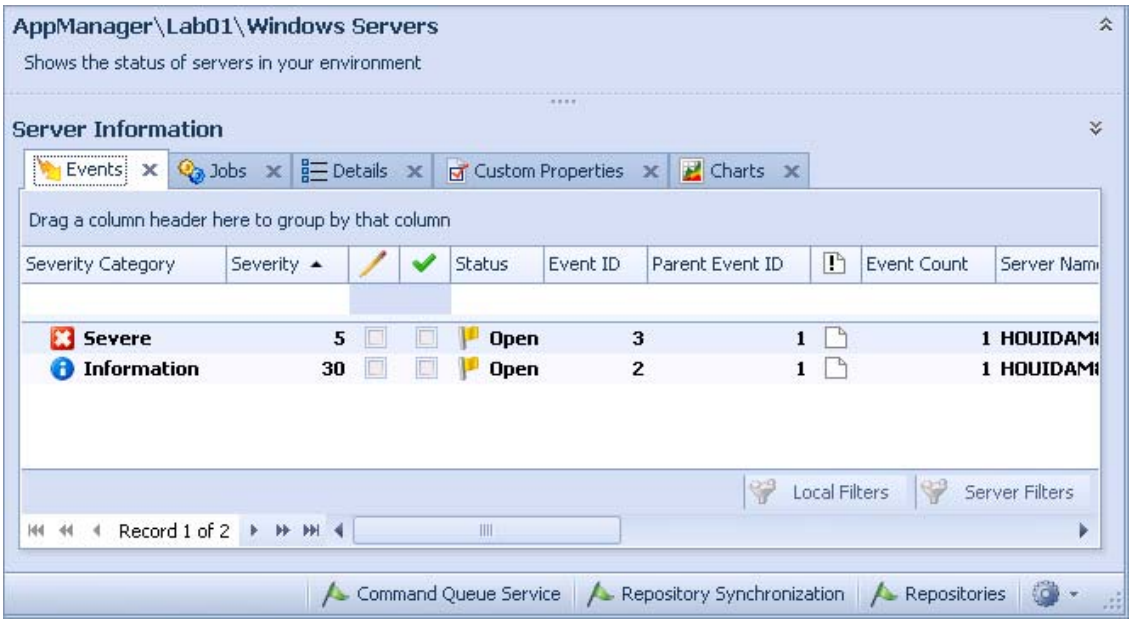
3.5.3 Looking at Events

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** tab 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		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		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		A task was successfully completed, for example, a service is successfully started or a discovery is completed.
Diagnostic Levels 31 to 40		Diagnostic information is returned, for example, when debugging problems.

3.6 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 Section 3.5.3, "Looking at Events," on page 95.

3.6.1 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.

3.6.2 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:

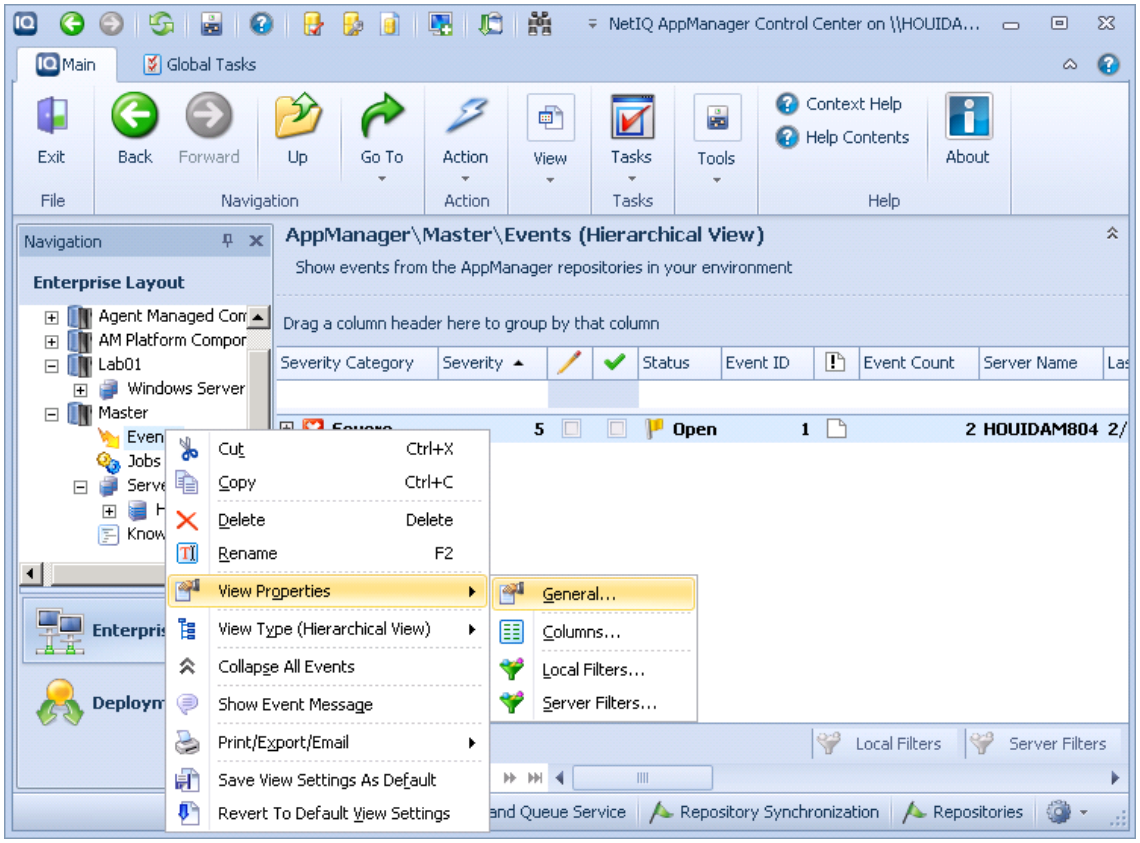
- Filter the Event view to improve the overall performance of the Control Center Console. View filters allow you to reduce the amount of information that is available for display in the Control Center Console.
- Filter the list of events in the Event view to only display the events you want. The event 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.

3.6.3 Filtering the Event View

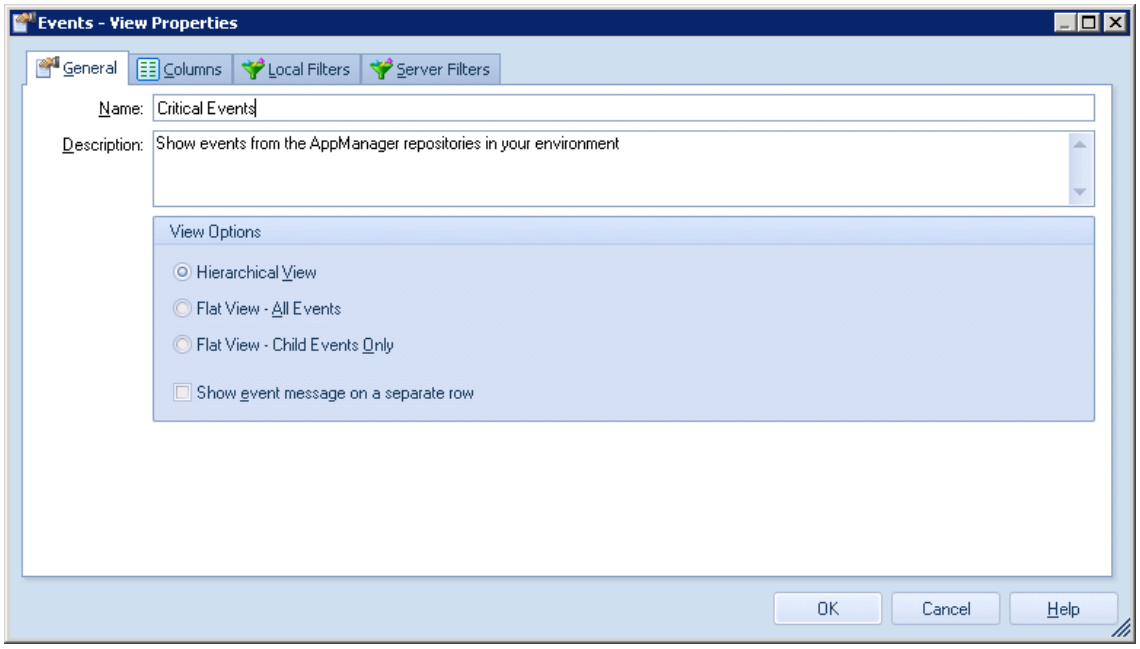
The monitoring policy you configured for the management group raises events with different event severity levels. Filter the standard, out-of-the-box Events view provided with the Master management group to only display events with a `Severe` or `Warning` status.

To filter the default Events view:

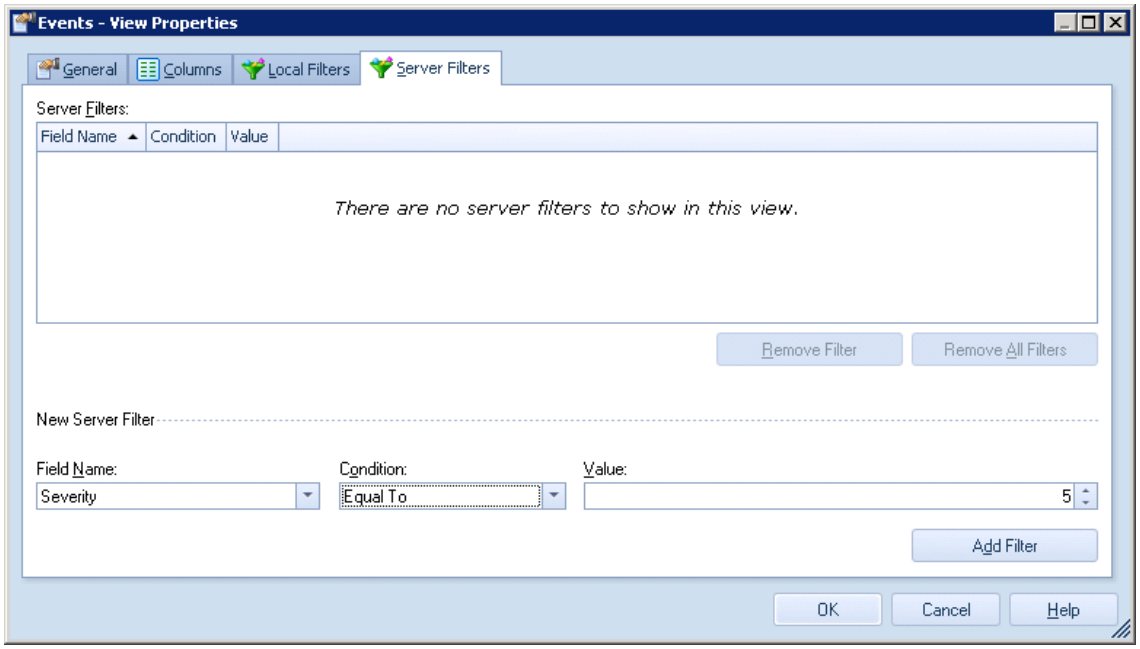
1 In the **Master** management group, right-click the **Events** view, then click **View Properties**, and then click **General**.



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

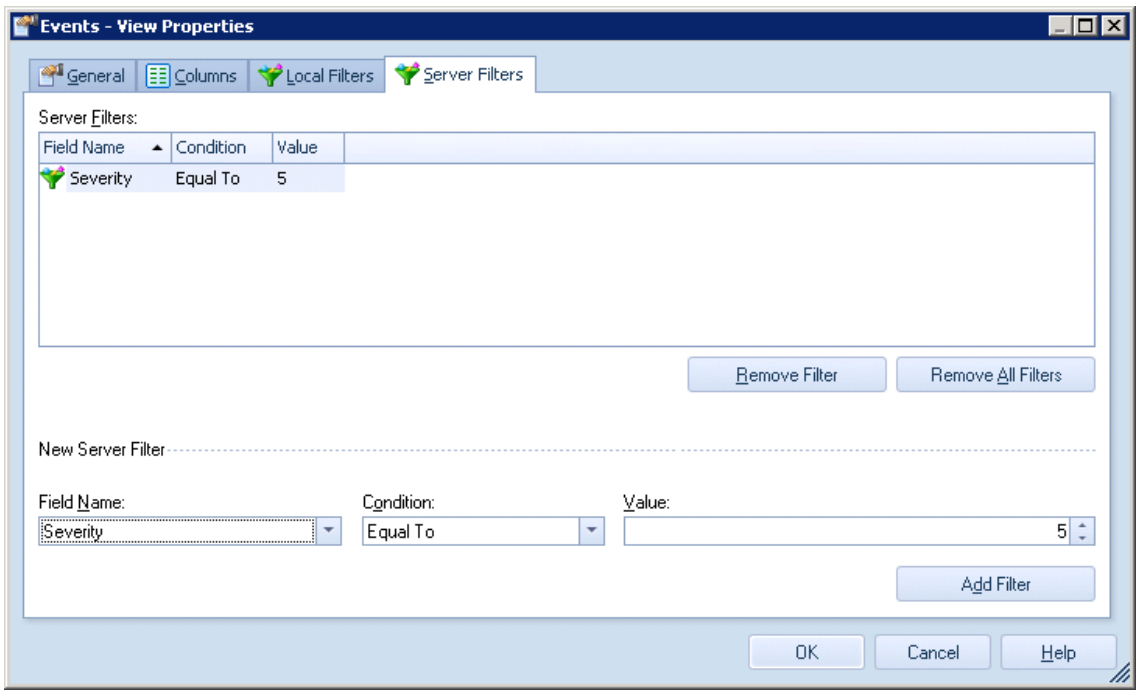


3 On the **Server Filters** tab, create filter criteria to select events with a `Severe` status.

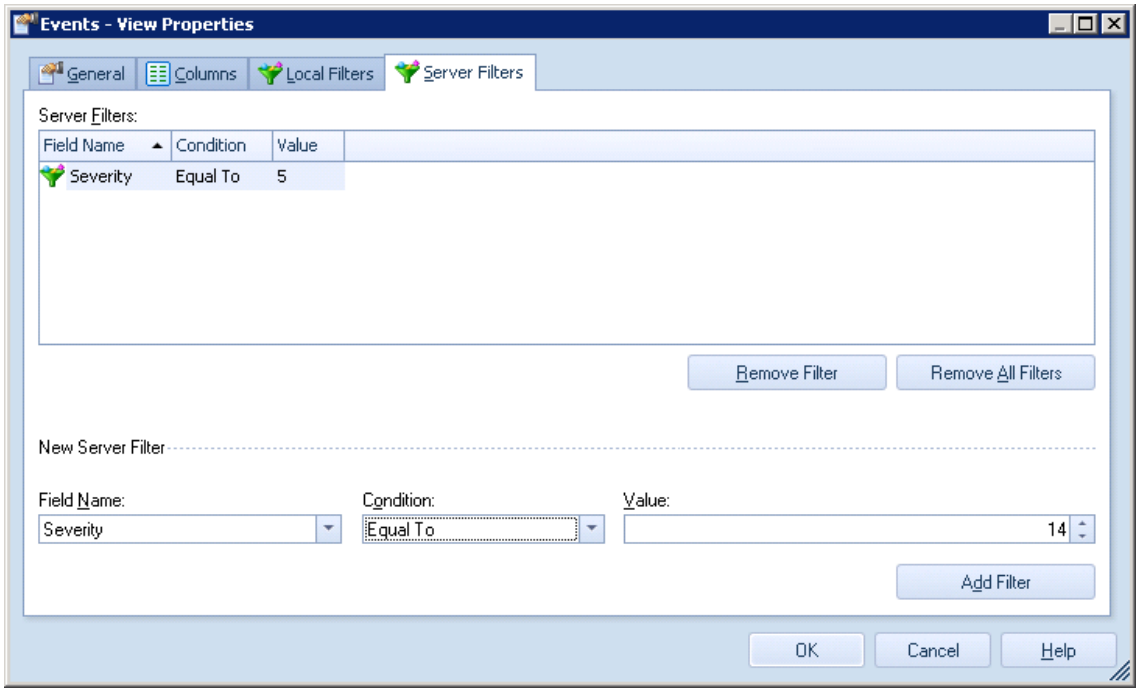


For	Do this
Field Name	Select `Severity`
Condition	Select `Equal To`
Value	Select any number between 1-10. In this example we have selected 5

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

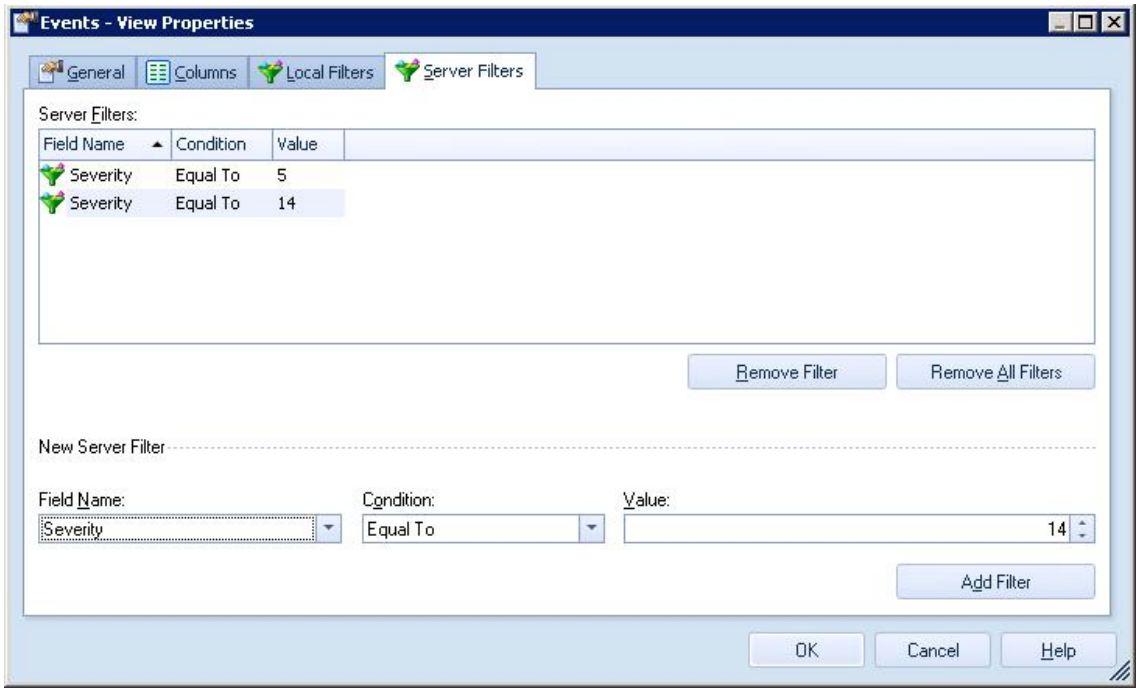


5 On the **Filters** tab, create filter criteria to select events with a `Warning` status.



For	Do this
Field	Select `Severity`
Condition	Select `Equal To`
Value	Select any number between 11-20. In this example we have selected 14

6 Click **Add Filter** to add the filter to the list, and then click OK to save your settings.

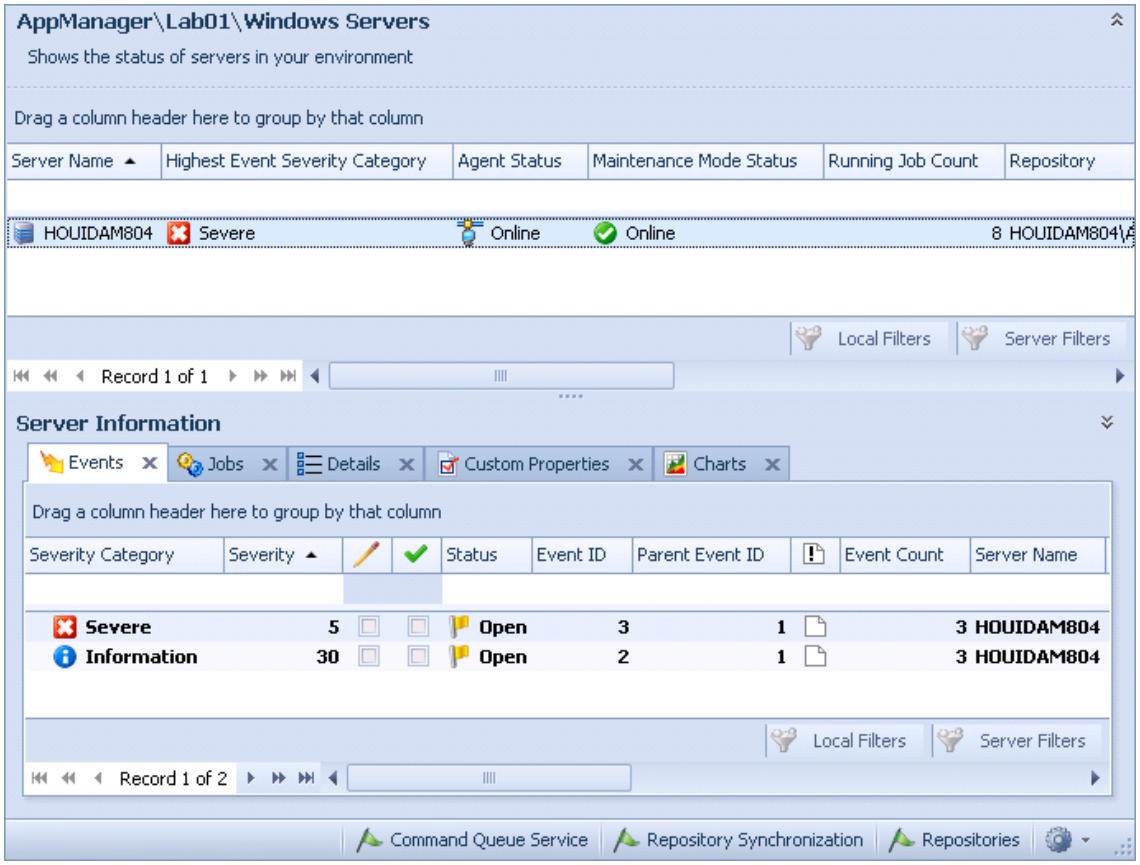


3.6.4 Acknowledging an Event

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

To acknowledge an event:

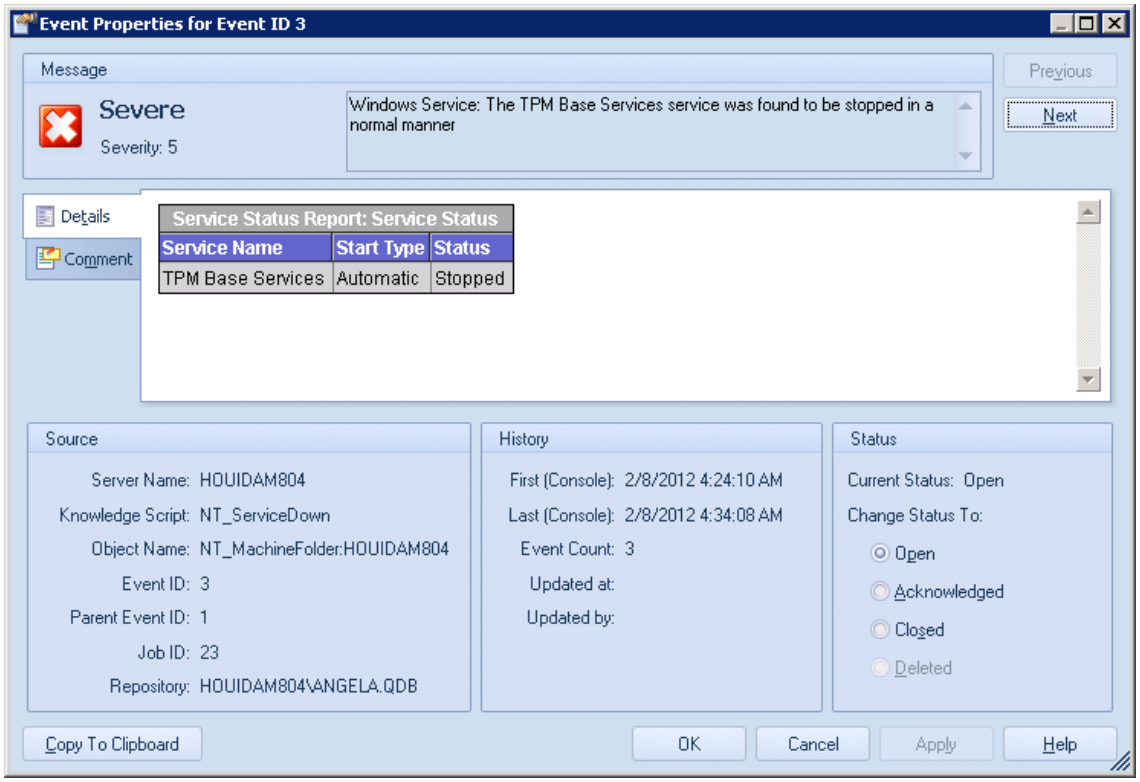
1 In the **Windows Servers** view, browse the list of computers and in the **Highest Event Severity Category** column, look for an event with a Severe status. In the example below, there is an event with a `Severe` status on `HOUIDAM804`.



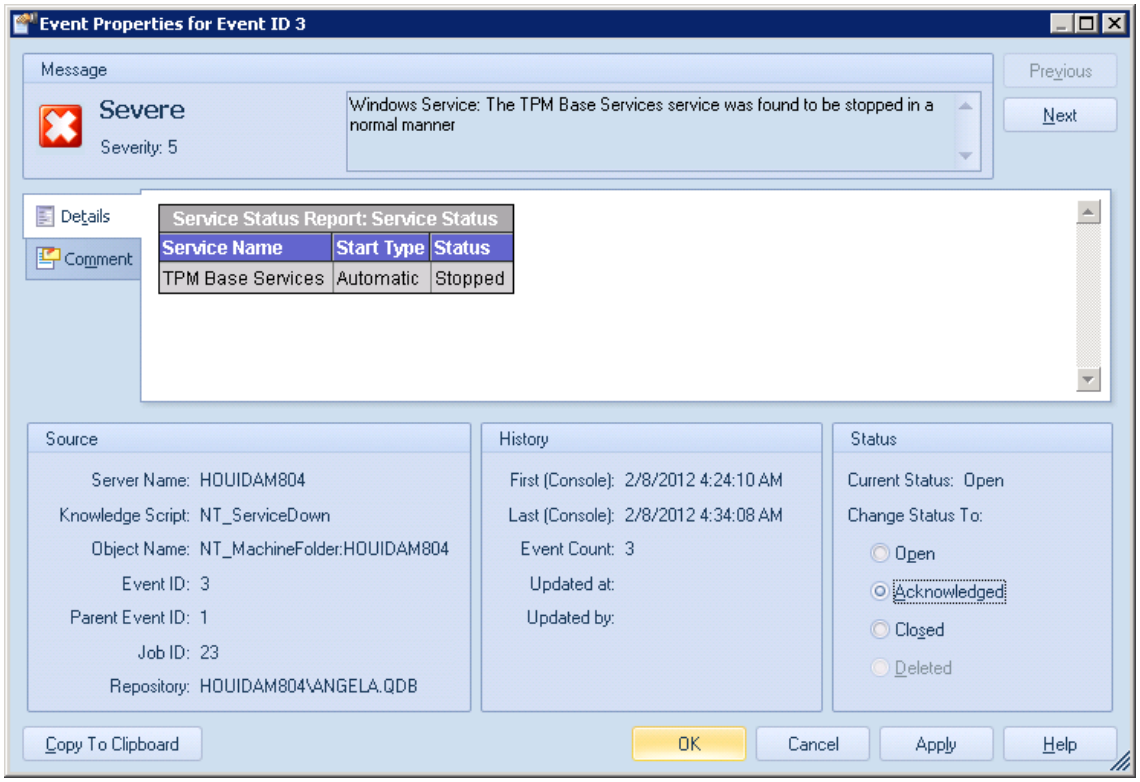
2 Select the computer with the `Severe` event status and click the **Events** tab.

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 properties dialog box, acknowledge the event by clicking **Acknowledged**, and then clicking **OK**.



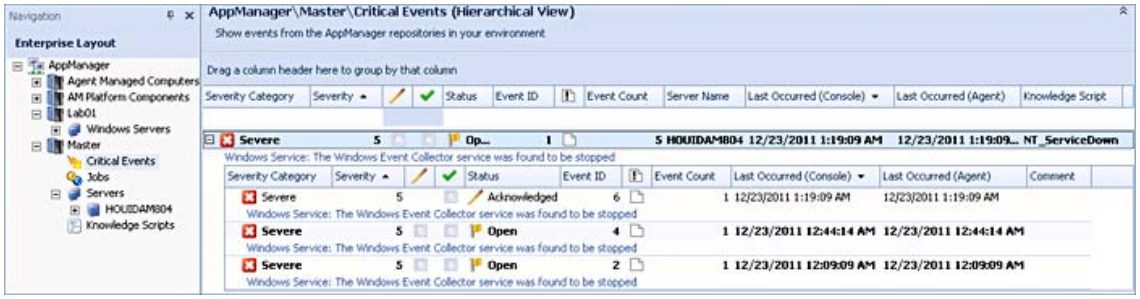
6 In the **Events** tab, the status of the event changes to **Acknowledged**.

3.6.5 Organizing and Managing Groups of Events

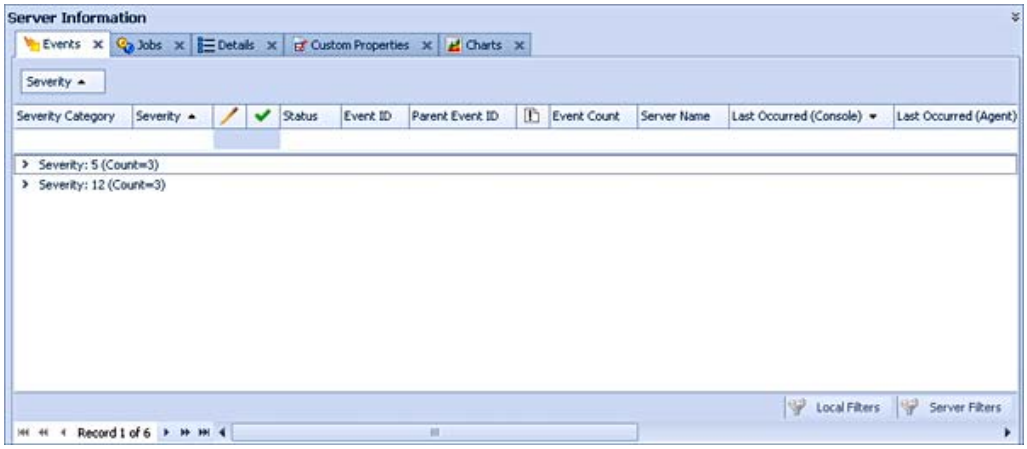
To help you quickly and easily manage a large number of events, you can organize events into groups. Group events by Severity and Computer. You can also respond to the events that belong to a group, for example, by acknowledging all of the events on a computer.

To group events by Severity and Computer:

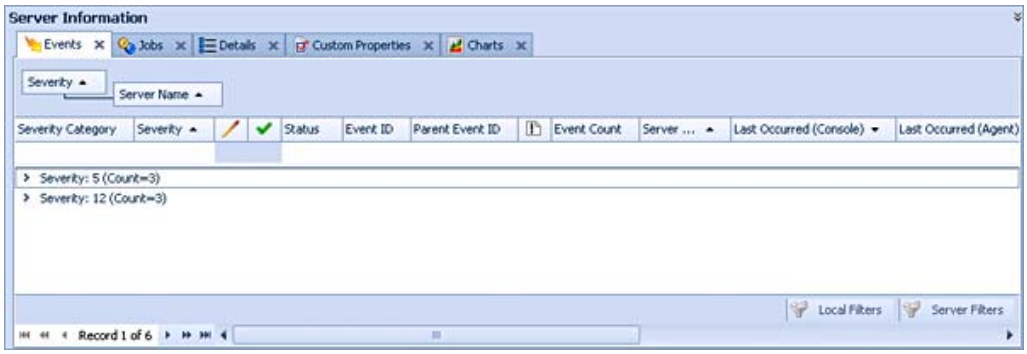
1 In the **Critical Events** view, find the **Severity** column.



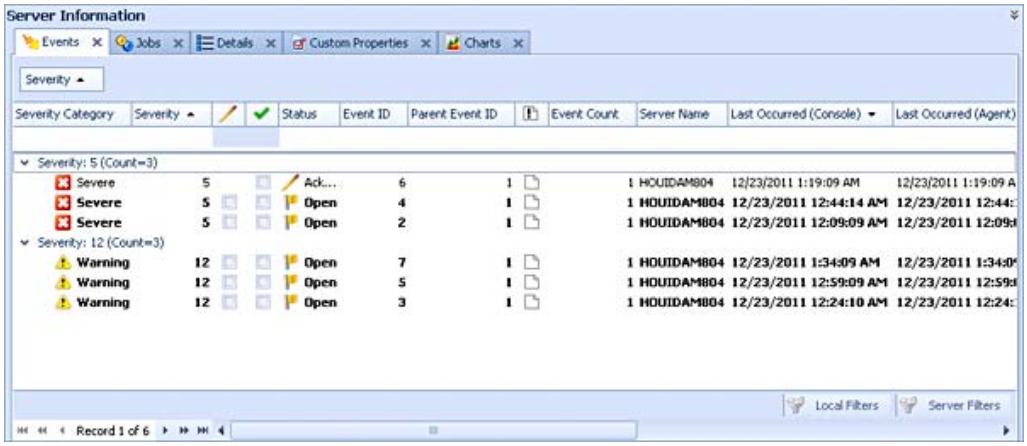
2 Drag the **Severity** column into the Group By field to group events by Severity.



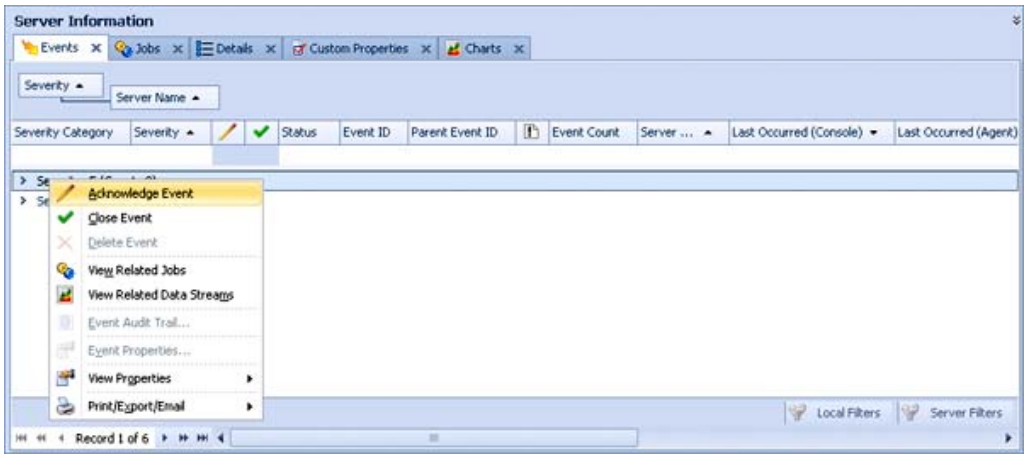
3 You can drag the **Server Name** column under `Severity` in the Group By field to group the servers by Severity and then by Server Name.



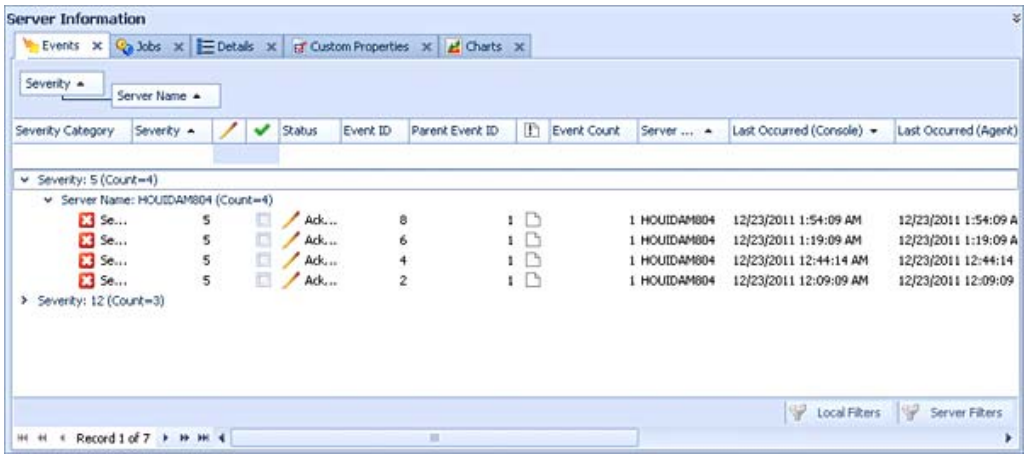
4 To expand the detailed event information for any group, click the > (arrow sign) to the left of the group.



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 Event**.



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.

3.7 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 Section 3.5.1, “Looking at Jobs,” on page 94. However, unlike a Server view, you cannot create jobs from a Job view.

3.7.1 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.

3.7.2 Filtering the Job View

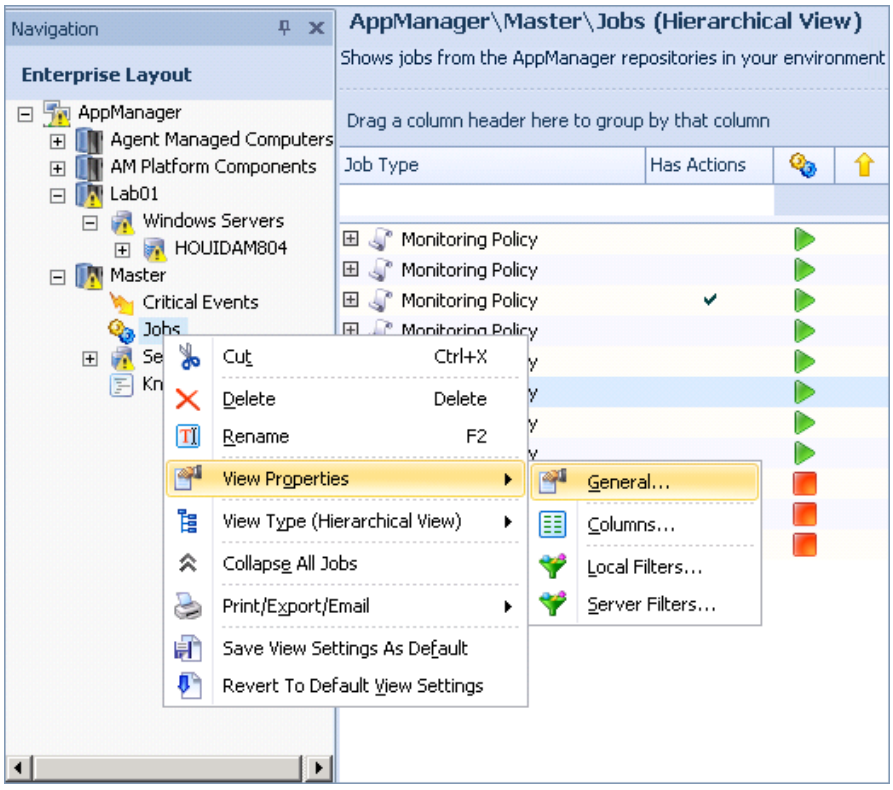
Filter the standard, out-of-the-box Jobs view to only display jobs with a status of `Running`. The policy-based jobs that are created by the monitoring policy on the management group have a status of `Running`.

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.

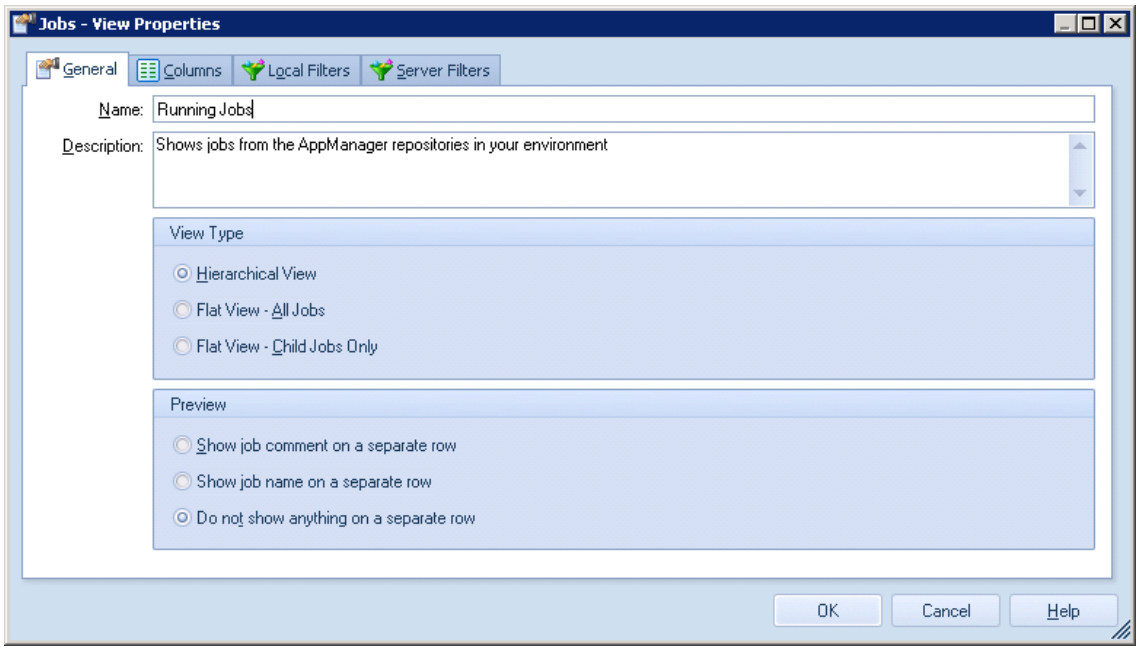
TIP: Not all Discovery jobs run once. Some run on a weekly schedule in order to detect new devices.

To filter the default Jobs view:

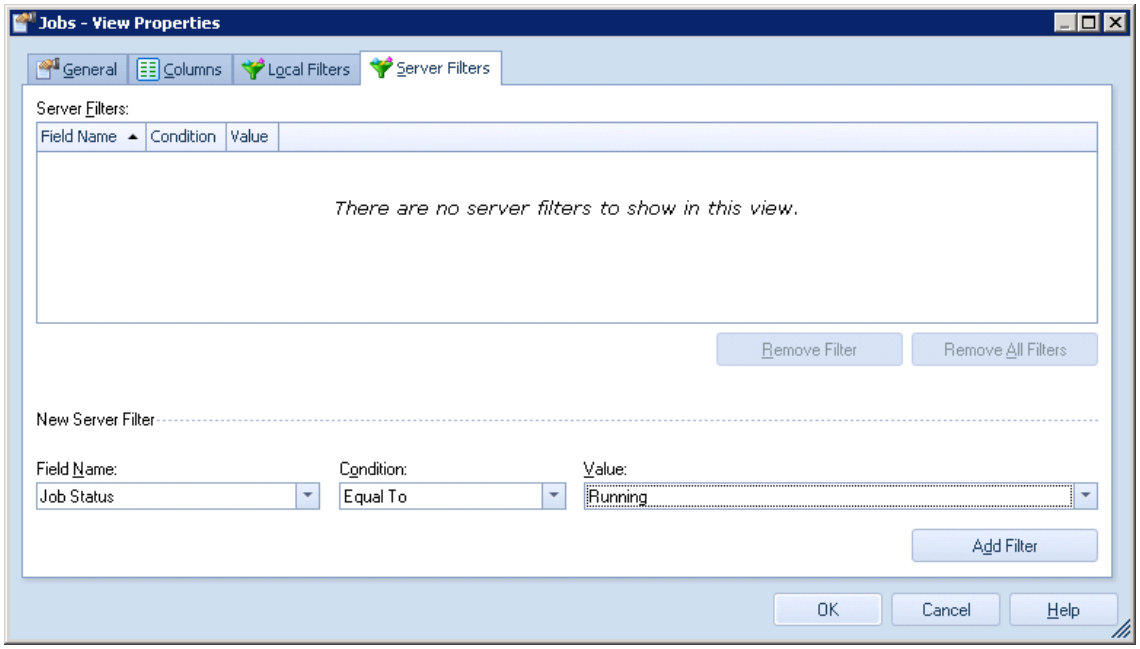
1 In the Master management group, right-click the **Jobs** view, then click **View Properties**, and then click **General**.



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

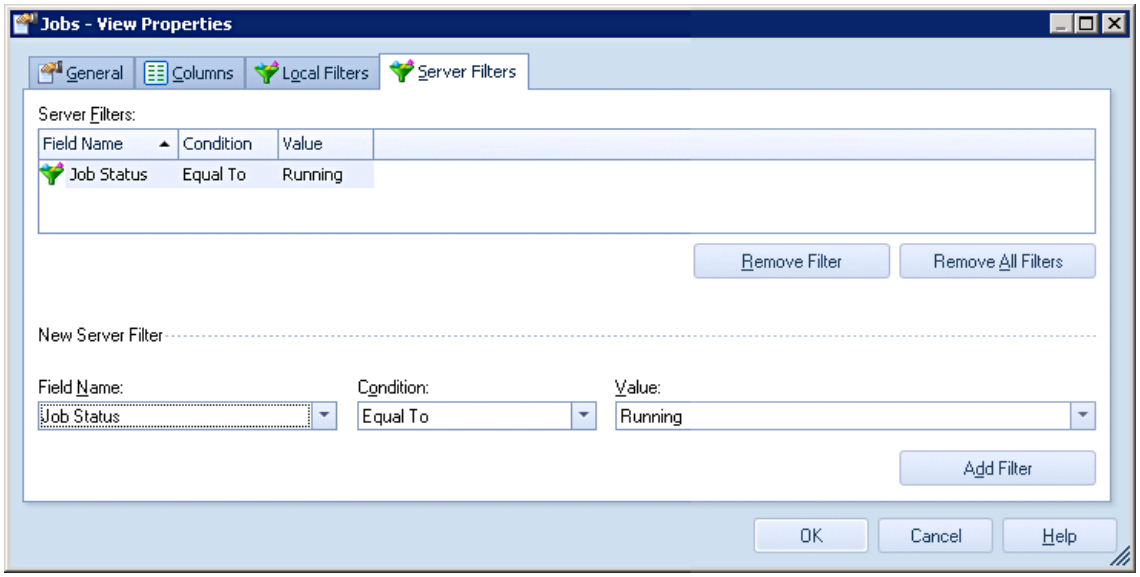


3 On the **Server Filters** tab, create filter criteria to select jobs with a `Running` status.

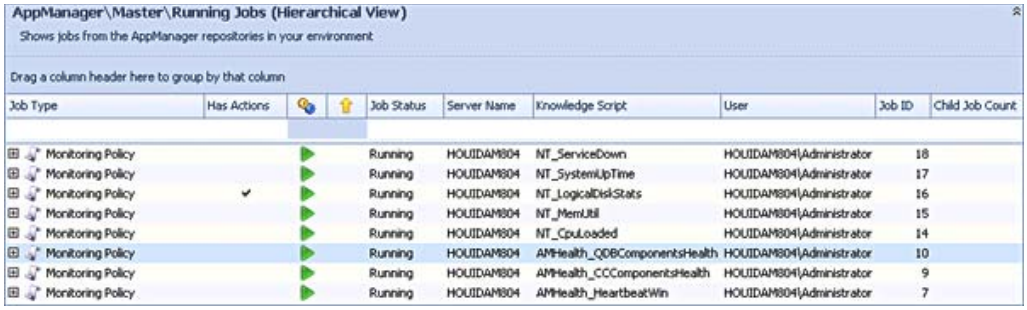


For	Do this
Field	Select `Job Status`
Condition	Select `Equal To`
Value	Select `Running`

4 Click **Add Filter**, and then click **OK**.

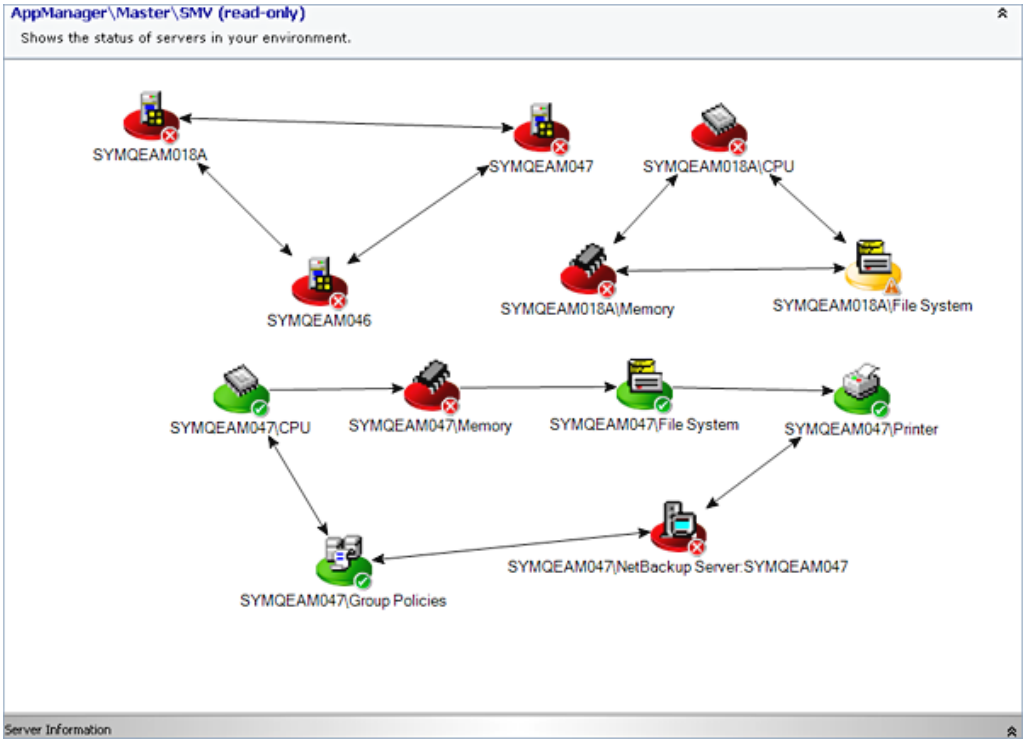


The **Jobs** view of the Control Center Console displays jobs with a status of `Running`. The Jobs view does not display Discovery jobs with a `Stopped` status.



3.8 Understanding Service Map Views

A **Service Map view** provides a visual representation of the relationships between objects you monitor with AppManager and displays event conditions on these objects that might disrupt any interactions between objects. Service Map views also allow you to respond to those events. You can use a single Service Map view to visually represent and monitor all of the computing and network infrastructure that underlies a particular business process.



A Service Map view allows you to:

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

- Manage custom properties
- Manage data streams

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

- The computers, servers, and databases that make up your customer relationship management system
- The computers, servers, and mail stores that support corporate e-mail
- The domain controllers, sites, and domains of your Active Directory

The discovered AppManager objects in a Service Map view indicate the most severe Open event condition associated with that object or one of its child objects. When 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.

You can use the Control Center console to create and edit Service Map views. From the Enterprise Layout pane, you can create a new Service Map view or check out an existing Service Map view from the Control Center repository. You can continue to use other Control Center views while a Service Map view is checked out.

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.

3.9 Understanding Charts

The **Charts** tab in the Control Center 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.

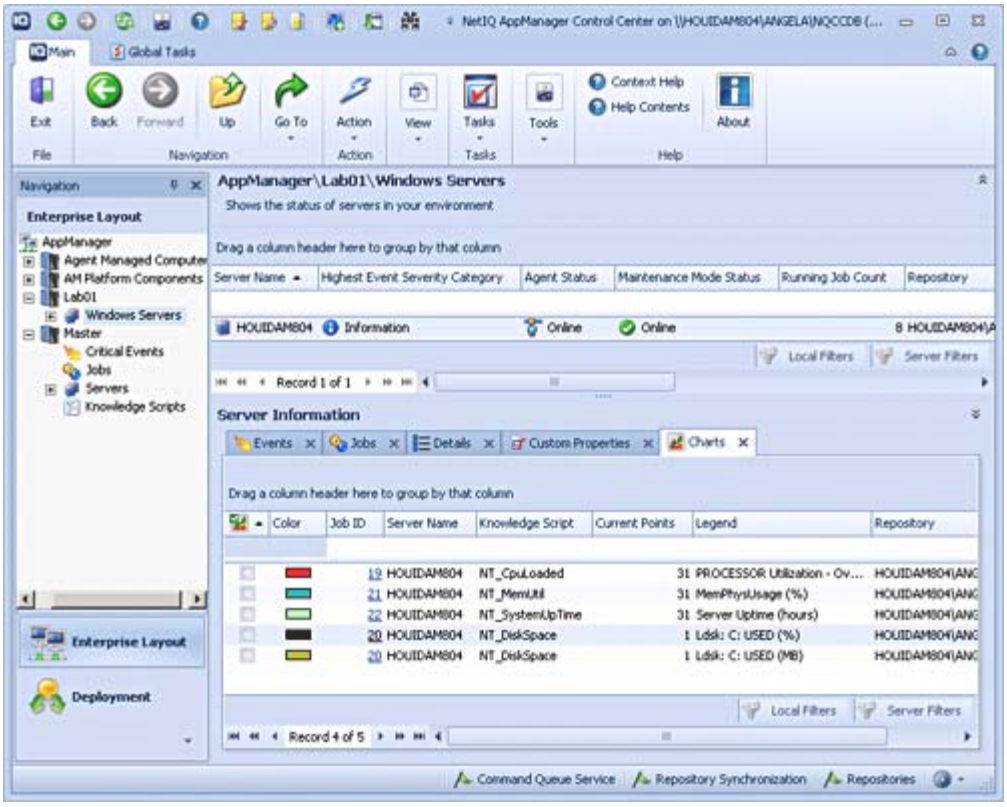
To understand possible causes, use AppManager reports to analyze the data over periods longer than 8 days. AppManager reporting is not featured in this chapter of exploring the AppManager. Please discuss your AppManager reporting needs with your NetIQ Sales Representative or NetIQ Partner.

To view data in a 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_CpuLoaded, NT_DiskSpace, NT_SystemUpTime, and NT_MemUtil monitoring policy jobs to collect data. You can view this data by using the **Charts** tab.

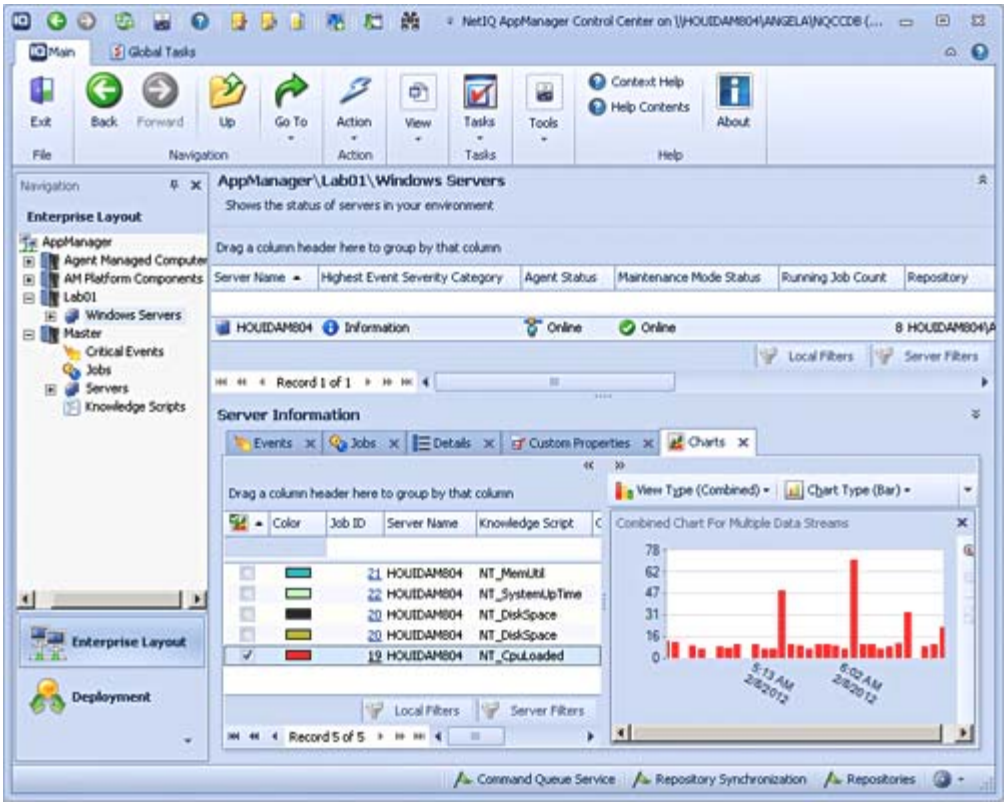
3.9.1 Viewing the Charts Tab

Select a server in the Management group for which you want to view the chart, and then select the **Charts** tab. The Jobs running on that server are displayed. Each Job is color coded.

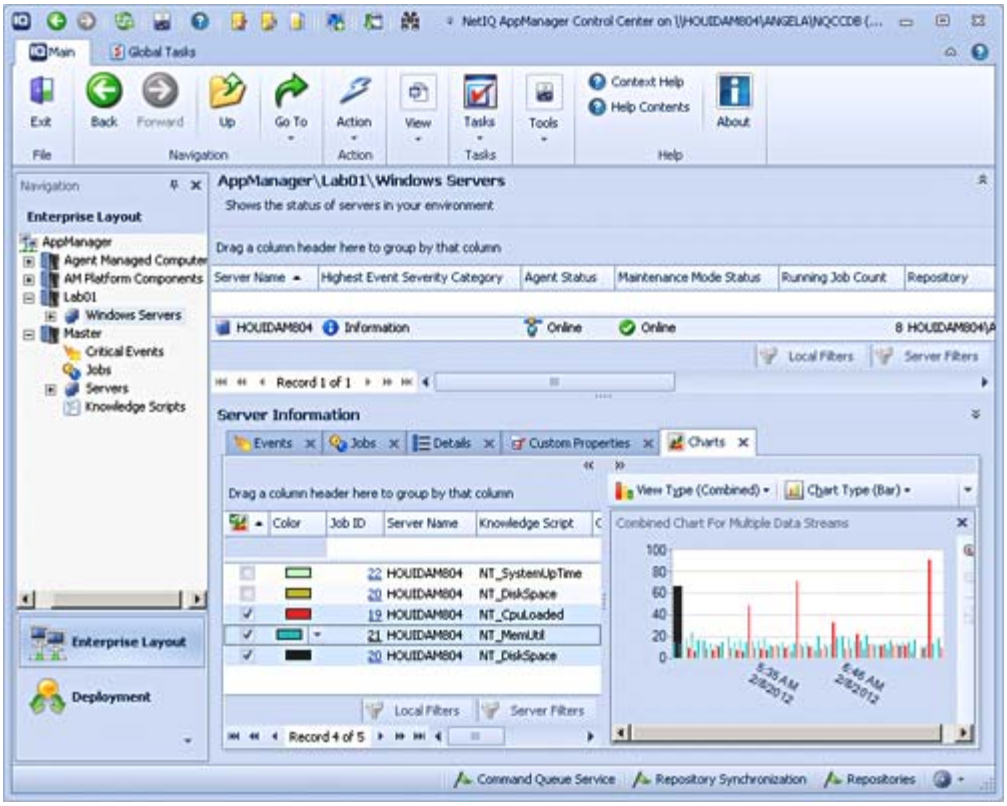


3.9.2 Displaying the Chart

To view a data in chart format, right-click a Job, and then select **Chart Data Stream**.This displays the chart for the selected job on the right side of the **Server Information** pane.

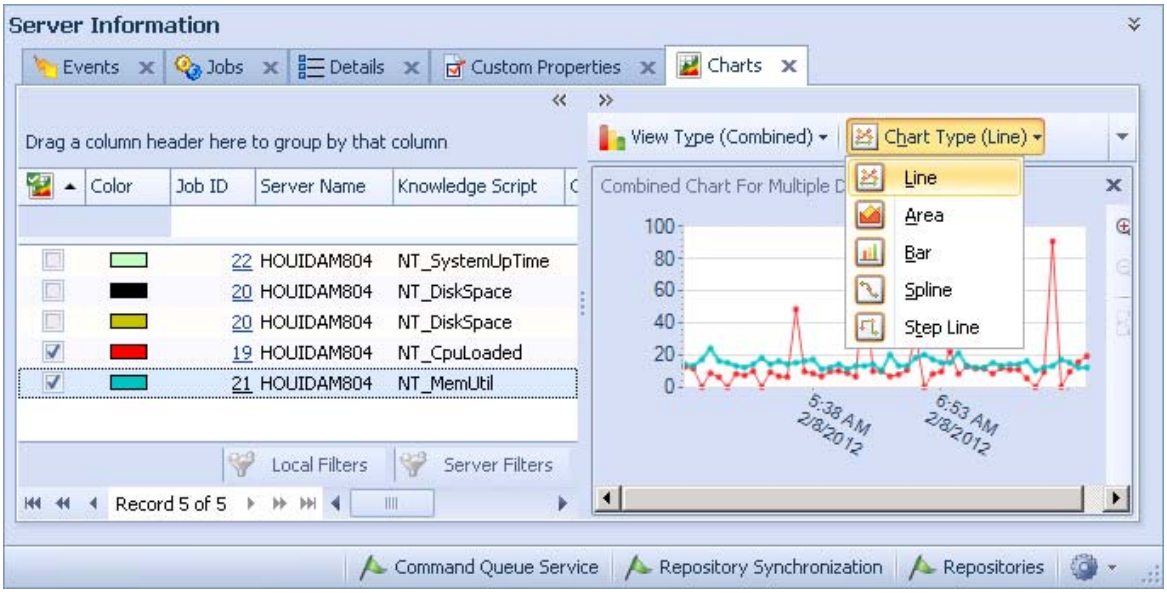


You can select multiple jobs either by pressing `Shift` or `Ctrl` key. Alternatively, you can select the box in the Chart Data Stream column to include that job in the chart display.



3.9.3 Modifying the Chart Type

To modify the chart type, select the type from the Chart Type list.



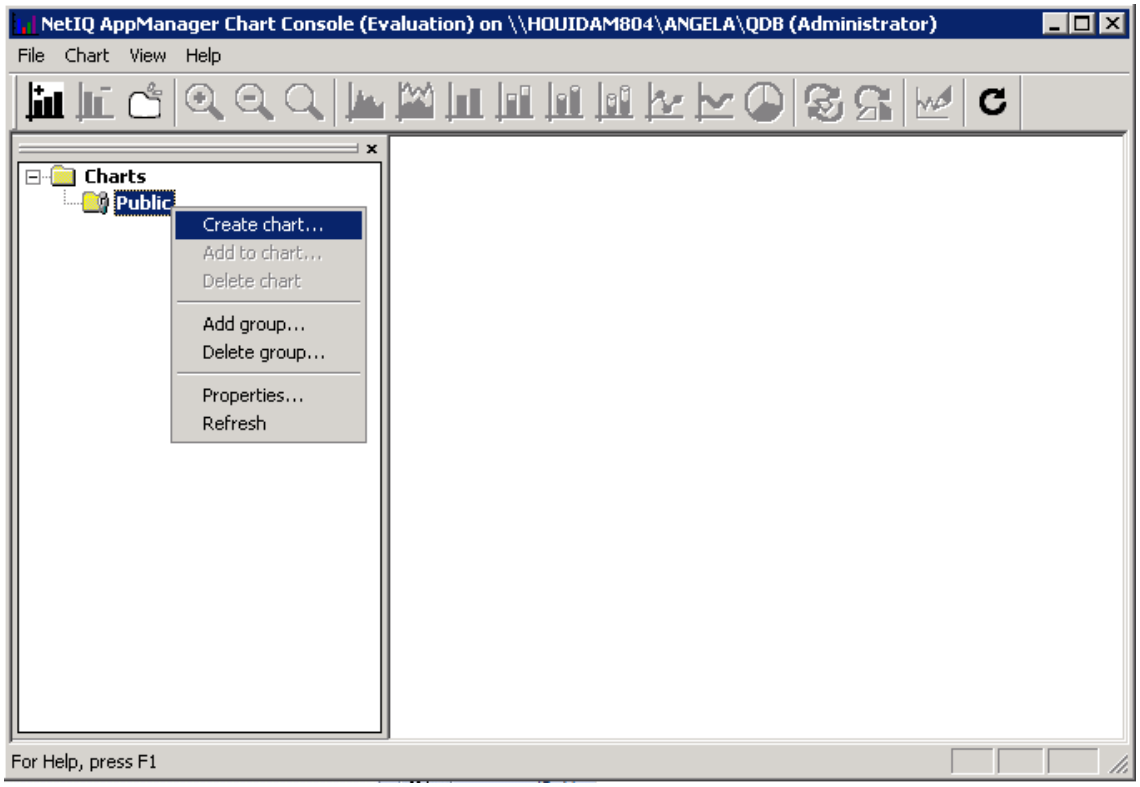
3.9.4 Using the Chart Console

You can create charts by using the stand-alone Chart Console. By using this console, you can create 3-D charts.

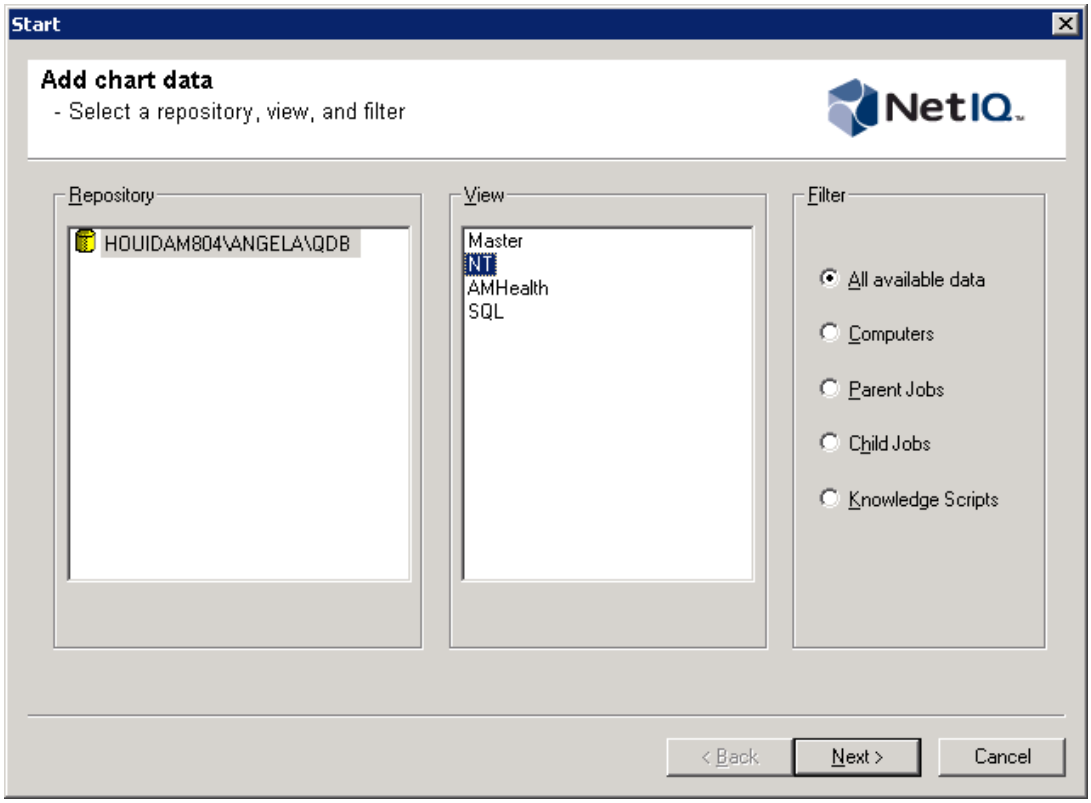
To create a 3-D chart:

1. Start the **Chart Console** in the **NetIQ > AppManager** program group.
2. In the Chart Console, click the **Public** folder and click **Chart > Create Chart**.

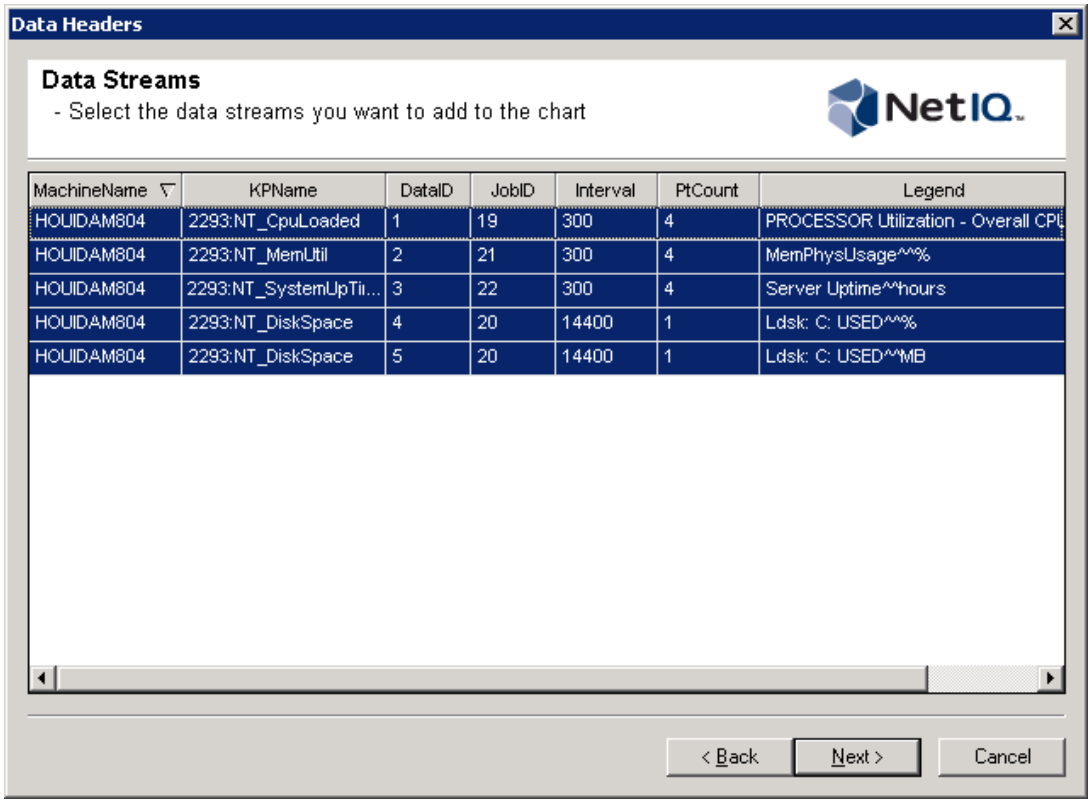
TIP: AppManager console users must have permission to view charts in the Public folder.



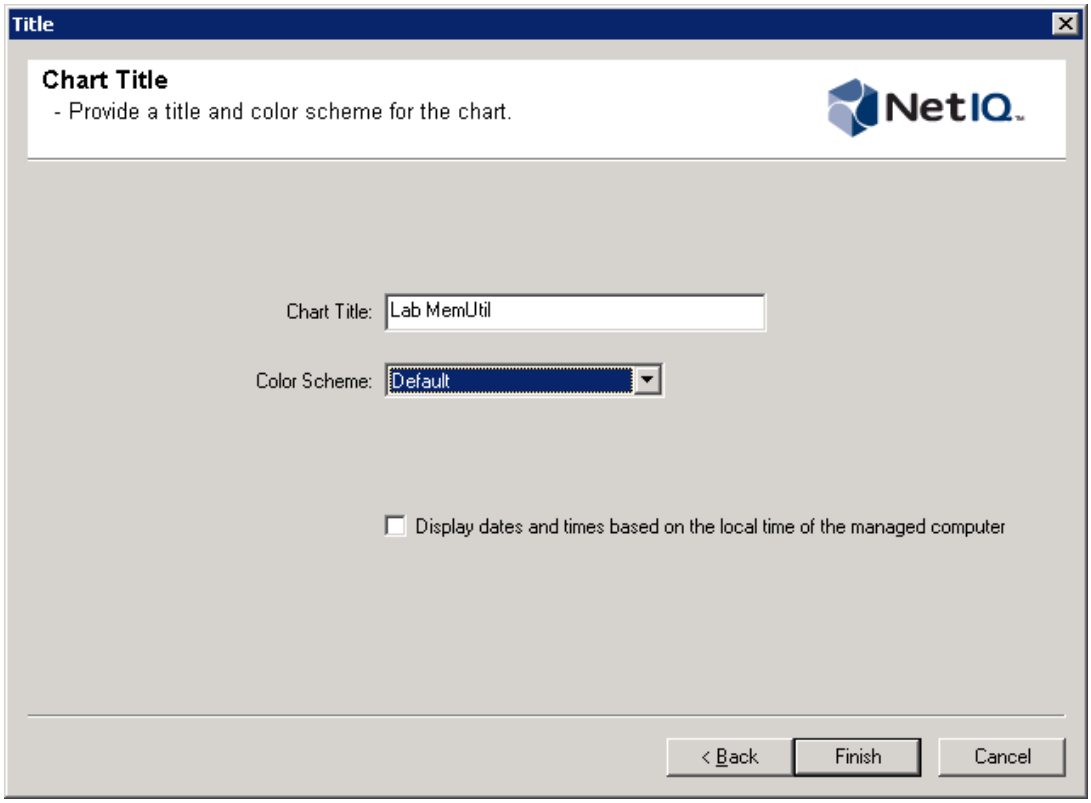
3 At the **Add chart data** dialog box, select the **NT** view to select from data collected by NT Knowledge Scripts, and then click **Next**.



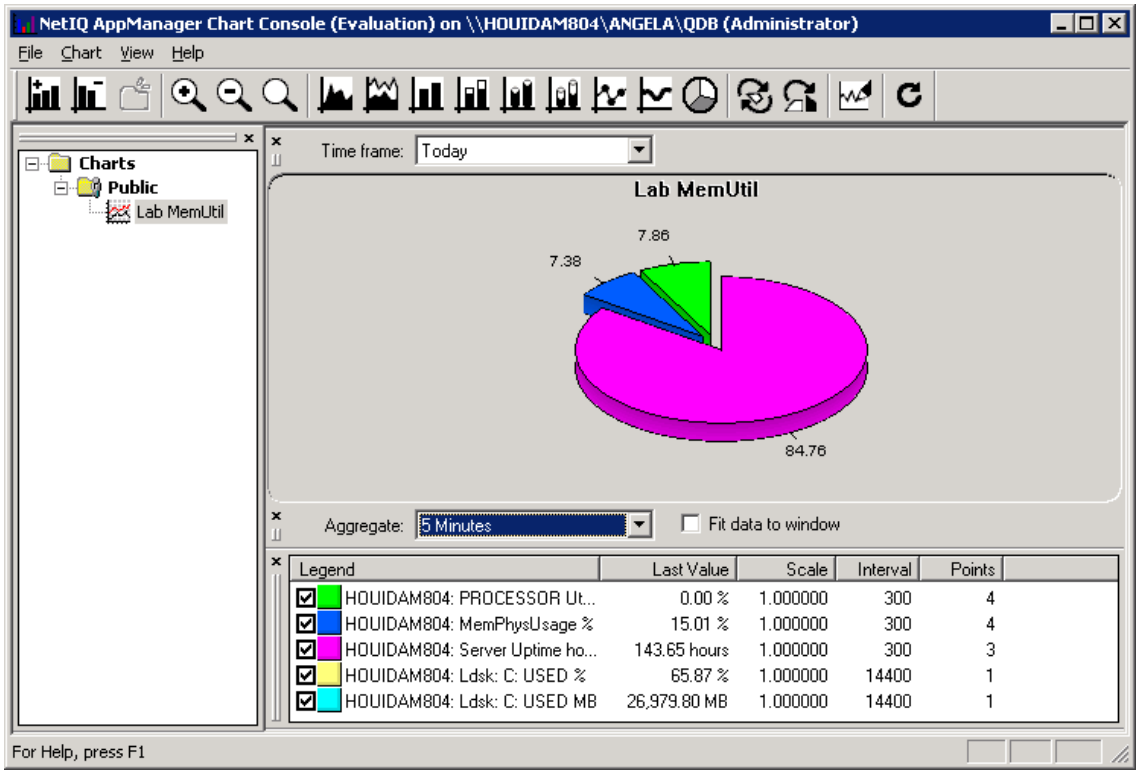
4 In the Chart wizard, select the data streams you want to add to the chart. Press `Shift+Click` or `Ctlr+Click` to select multiple data streams, and then click **Next**.



5 In the Chart wizard, specify a chart title, for example, `Lab MemUtil`. Optionally, choose a color scheme for the chart, and then click **Finish**.



6 In the left pane of the Chart Console, click **Lab MemUtil** to display the chart.



3.10 What's Next?

After you complete exploring AppManager 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.