

Quest[®] Reporter

Quick Start Guide

Version 5.5



© 2006 Quest Software, Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

If you have any questions regarding your potential use of this material, please contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

TRADEMARKS

Quest® Reporter is a trademark of Quest Software, Inc.

Adobe® Reader® is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Quest Reporter Quick Start Guide
Updated - September 2006
Software Version - 5.5

Contents

About This Guide	5
Conventions	5
About Quest Windows Management	6
Contacting Quest Software	6
Contacting Quest Support	6
Product Overview	7
Introducing Quest Reporter	7
Managing a Network with Quest Reporter	7
Business Problem Statement	8
Business Rationale for Quest Reporter	9
System Requirements	11
Hardware Requirements	11
Software Requirements	11
Downloading Quest Reporter	12
Installing Quest Reporter for the First Time	12
Best Practices - New Installations	12
Choosing a Data Transport Mode	13
Installing the Direct Data Transport Mode Only	13
Installing the Compressed Data Transport Mode	15
Upgrading Quest Reporter from an Earlier Version	17
Best Practices	17

Removing Quest Reporter	18
Upgrading from Version 5.3 or 5.4 to Version 5.5	18
Upgrading Remote RDCs	20
Running Quest Reporter	20
Step-By-Step Walkthrough	21
Example Scenario for Ad Hoc Reporting	21
Example Scenario for Scheduled Reporting	23
Example Scenario for Action-Enabled Reporting	27
Example Scenario for Change History Reporting	31
Quest Reporter Terminology	34

About This Guide

This document has been prepared to assist you in becoming familiar with Quest® Reporter, an integral component of Quest Windows Management Suite. The Quick Start Guide contains the information required to install and use Quest Reporter. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

ELEMENT	CONVENTION
Select	This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons.
Bolded text	Interface elements that appear in Quest Software products, such as menus and commands.
<i>Italic text</i>	Used for comments.
<i>Bold Italic text</i>	Used for emphasis.
Blue text	Indicates a cross-reference. When viewed in Adobe® Reader®, this format can be used as a hyperlink.
	Used to highlight additional information pertinent to the process being described.
	Used to provide Best Practice information. A best practice details the recommended course of action for the best result.
	Used to highlight processes that should be performed with care.
+	A plus sign between two keystrokes means that you must press them at the same time.
	A pipe sign between elements means that you must select the elements in that particular sequence.

About Quest Windows Management

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases, and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest's Windows Management solutions simplify, automate and secure Active Directory, Exchange and Windows, as well as integrate Unix and Linux into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone	949.754.8000 (United States and Canada)
Email	info@quest.com
Mail	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at <http://support.quest.com>.

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update you case, and check its status.

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The Guide is available at [http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf).

Product Overview

Introducing Quest Reporter

Quest Reporter enables administrators, security officers, and helpdesk staff to collect the data they need for configuration change auditing, security assessment of their Windows infrastructure or Active Directory pre- and post-migration analysis. Quest Reporter ensures adherence to sound network management practices by auditing compliance with corporate standards for user, group, and share permissions management.

Quest Reporter helps you administer the network by generating comprehensive enterprise-wide reports, on both real-time and stored data. It is distinguished by its ability to report on network objects across multiple domains, as well as by its information-rich interface. The interface conveys the scope of the report, the available directories on which you can report, all available reports, and reports that you have previously scheduled.

Managing a Network with Quest Reporter

Network administration involves creating, maintaining, and modifying network objects. To administer dynamic enterprise networks, you must be able to assemble pertinent information quickly and easily.

Quest Reporter helps you maintain and manage enterprise directories through security, standards conformance, and general administration reports. With its streamlined approach to report generation, many operations that have traditionally required personal visits to individual computers can now be accomplished locally from your computer.

You can use Quest Reporter to accomplish the following:

- Create reports by selecting objects and containers visually from Active Directory, Windows NT, the Windows NT File System (NTFS), and Novell
- Access reports grouped to match directory object classes such as users, groups, domains, computers, and Access Control Lists (ACLs)
- Modify predefined reports to suit your requirements
- Schedule reports to run automatically and store the results to a location of your choice
- Gather information remotely by installing Report Data Collectors (RDCs) in remote offices
- Schedule data collections for later use by a stored data report
- Access NTFS reports to audit users and groups contained in ACLs, ensuring compliance with your company's standards for protecting sensitive data
- Create reports faster with reusable, user-defined selections of network objects (object sets) from one or more domains
- Create a category of favorite reports to access on a regular basis and share your list of favorites with other users
- Automate changes to objects in reports based on report results through the use of action enabled reporting

Business Problem Statement

On a daily basis, IT organizations require accurate, timely information to make both strategic and tactical decisions involving their Windows infrastructures. Individual departments within IT organizations are independent data consumers of this critical data. These data consumers have different requirements to support their specific areas of responsibility. The following illustrates the questions that these departments must answer.

Compliance/Auditing

- Who has access to what?
- What level of access has been granted?
- How is that access granted?

Operations

DEPARTMENT/GROUP	CONCERN
Active Directory Administrators	Who is a member of tightly controlled groups such as domain admins or enterprise admins? What servers are holding FSMO roles? What is the size of my Active Directory database?
Server Administrators	Who has logged on to this server? What are the user rights for this server? What are the different types of operating systems deployed? What service packs are installed? What programs have been installed? What services are running and by whom? What are the network settings? Are standard settings configured before I deploy the server to production? What shares are being hosted and how are the permissions configured?
Desktop Administrators	What local accounts exist on the workstation? Who has administrative access? Are standard settings configured such as network settings, computer name fits the standard, appropriate hardware and software, and so forth?
Helpdesk	When was this individual's last password changed? Is their account disabled or locked out? What groups were they a member of? What logon script are they running?

Security

- Are there any users who are logging in with blank passwords?
- Are there any user accounts that are inactive?
- What security hotfixes have been applied throughout the environment?
- Who is a member of a highly sensitive group?

- Are the event log settings configured appropriately?
- Are there any computers configured for "autologon"?

Engineering

- What is the current hardware configuration?
- How much disk space is being consumed?
- What other applications are being leveraged on that same system?

Technology Adoption Projects

- What operating systems are deployed?
- What is the hardware/software configuration?
- What user accounts do not have to be migrated as they are inactive?
- Do I have any migration specific concerns like duplicate names?
- What servers and computers must be refreshed because they do not meet minimum hardware requirements?

To answer these questions, IT organizations are forced to rely on in-house developed scripts that are very costly to maintain and modify for the numerous data consumers mentioned above. Furthermore, third-party vendors offer very narrowly-focused solutions that cannot be leveraged throughout the entire organization.

In the end, IT organizations are left with departmentalized, cumbersome, and resource-intensive processes with which to make strategic and tactical IT decisions involving their Windows infrastructures. This leads to a lack of data integrity and the inability to have this information readily available, not to mention the increased costs of maintaining the numerous different methods. To make matters worse, in some instances IT organizations must respond immediately to address either a security breach or adherence to adopted internal policies that ensure tight security and maintenance of the highest service levels.

Business Rationale for Quest Reporter

Quest Reporter provides your entire organization with a flexible, powerful and cost-effective solution to collect, store, and report on critical Active Directory, NT, Novell NDS/eDirectory and Windows-based configuration items. Also, Quest Reporter provides an extra benefit by allowing bulk changes to occur in order to address a security breach or change settings to conform to standards. This innovative solution provides clear-cut advantages and benefits:

- Day-to-Day Security and Standards Enforcement

Many organizations have policies and standards prescribing how their IT environments are managed. These policies cover such areas as user creation and deletion, and group population. Network and security administrators need to know that policies are being followed and standards are being applied correctly on a daily basis. In large environments, this can be time-consuming as there may be thousands of users, groups, and computers to track. To prevent security breaches, Quest Reporter allows you to frequently audit your environment.

- Audit Preparation

Preparing for comprehensive IT security audits can be tedious and frustrating. You need tools to demonstrate that the environment is secure and being managed according to the organizational policies. Quest Reporter provides the information needed to prepare for a security audit.

- Downtime Reduction and Performance Optimization

Quest Reporter's network configuration reports result in faster resolution for configuration-related problems and performance setbacks. Quest Reporter provides the information you need to standardize configuration, thereby reducing the cost of administration and facilitating the use of best practices for network performance.

- Cost Reduction and Reduced Administrative Workload

Quest Reporter decreases your workload by automating data collection and report generation. Minimizing network impact, it allows data collection to occur as close as possible to the data source and enables off-hour scheduling of data collections. As a result, less time and money are required to manage the network and you can dedicate more time to network improvements.

- Environment Change Preparation

Any change in large IT environments must be accomplished quickly and securely, using minimal resources and without any loss of productivity. Quest Reporter provides the information needed to plan smooth transitions, ensuring that nothing is overlooked.

- Migration Preparation

Before attempting a migration from Windows NT to Active Directory (AD), AD to AD, or Novell to AD, you need to plan out how the migration will be staged. Quest Reporter provides detailed information about permissions, user accounts, disabled or expired accounts, and group membership from NT, AD, and Novell based networks. By identifying all groups, domains, computers, and users, and defining their relationships, Quest Reporter allows you to design Active Directory in a way that meets the specific needs of your organization. This produces a more relevant environment and simplifies the migration project.

System Requirements

Before installing Quest Reporter, ensure that your system meets the following minimum hardware and software requirements.

Hardware Requirements

- 1 GHz Pentium
- 512 MB RAM (Any requirements required by a particular operating system supersede product requirements.)
- 25 MB of disk space for the application
- 500 MB of disk space for processing
- 10 MB of disk space for RDC deployment
- Database size is dependent on the amount of information collected
- Color depth—16 bit (for example, 65 536 colors)
- Screen resolution—minimum 800 x 600 (1024 x 768 strongly recommended)
- Network Interface Card
- Pointing device

File System Requirements

- NTFS

Software Requirements

Installation computers

The following requirements apply to computers where you are installing the Quest Reporter console or RDCs:

- Microsoft Windows 2000 Professional, Server or Advanced Server (Service Pack 4), Windows XP (Service Pack 2), or Windows 2003 Server (Service Pack 1), or Windows 2003 R2 Server—computers must be members in a domain
- Supported database servers include MSDE 2000 (recommended for evaluation purposes), SQL Server 2000 (Service Pack 3 or later), or SQL Server 2005 (Service Pack 1)
- For compressed data transport mode on Windows 2000 computers: Microsoft Message Queuing (MSMQ) 2.0 or later in workgroup mode, Independent client setup
- Microsoft Data Access Control (MDAC) 2.7 or later
- .NET framework 1.1 or later
- Microsoft Excel 2000 or later (if you are saving the report output in an Excel spreadsheet)



Some customers may want to run the Quest Reporter console in a Terminal Services or Remote Desktop window.

Quest Reporter has been tested to run on Microsoft Windows Terminal Services in Application Mode. For more information about deploying applications under Terminal Services, see the relevant Microsoft documentation.

Collection computers

The following requirements apply to only those computers where you are collecting data:

- Microsoft Windows NT 4.0 (Service Pack 6)
- Microsoft Windows XP (Service Pack 2)
- Microsoft Windows Server 2003 Server (Service Pack 1)
- Microsoft Windows 2000 Professional, Server or Advanced Server (Service Pack 4)
- Microsoft Windows 2003 R2 Server

Downloading Quest Reporter

If you do not already have Quest Reporter, you can download it from the Quest Software web site.

To download Quest Reporter

1. Go to the Quest web site at <http://www.quest.com/reporter>.
2. Follow the instructions provided for product downloads.

Installing Quest Reporter for the First Time

Best Practices - New Installations

Use the following best practice information to achieve optimum performance with Quest Reporter:

- **New database**

Create a new database for Quest Reporter to use. You will have an opportunity to do this at the end of the installation process. You should set up your central SQL Server database on a member server. This central database will be the primary data source.

Ensure that you are following Microsoft's best practices for deploying a SQL Server database.
- **Report field customization**

If you customize the fields in the report you are generating, save the report as a favorite on the print preview screen so you do not have to repeat the process.
- **Database configuration**

Configure the database to allow for growth in size, as collections can increase the size of the database continuously.
- **Performance**
 - Be selective when choosing event types to log, as this affects the size of the log file.
 - Increase the thread count to improve performance. For more information, see appendix A, "Configuration Settings" of your Reporter User Guide.
- **Scheduled collection guidelines**
 - Determine whether the scheduled collection is the appropriate method to obtain your data. If you only need to generate the report at a particular time once each day, a scheduled favorite report might be more appropriate.
 - Avoid collecting redundant data. For example, a local user on a DC is identical to a domain user.
 - Plan your data collection carefully and deploy data collectors based on the data collection requirements. You can often significantly reduce the number of required collectors. For more information, see chapter 2, "Deploying Quest Reporter" of your Reporter User Guide.

Choosing a Data Transport Mode

Quest Reporter provides you with two different types of data transport modes. The collection modes are configured per Reporter Data Collector (RDC). During installation, you can specify installation of one or both. The following describes the two modes in detail:

- Direct

Installed automatically, this mode is used in earlier versions of Quest Reporter. Direct data transport mode collects the data and stores it directly to the database. Direct data transport mode is available with live reports and scheduled collections.

- Compressed

This mode collects and compresses the data on the RDC host. The compressed data pack is then streamed to the Console host, decompressed and uploaded to the database. This mode minimizes bandwidth consumption as the data being transferred back to the main console is compressed and thus improves the delivery speed over WANs.

With the exception of remote permission-based scheduled collections, Compressed data transport mode is available for all remote scheduled collections. Permissions-based collections such as Active Directory and NTFS currently leverage direct mode only.

If you use the compressed data transport mode, then Microsoft Message Queuing (MSMQ) must be installed on the Console host and RDC host. If MSMQ is not detected, Quest Reporter installs MSMQ 2.0 or later automatically in workgroup mode (using independent client setup).

If you want to use the compressed data transport mode, see [“To install Quest Reporter with the compressed data transport mode” on page 15](#).



If you choose not to install the compressed data transport now, you can always change the transport mode later using the Quest Reporter Configuration utility. For more information, refer to the Quest Reporter User Guide or Help.

Installing the Direct Data Transport Mode Only

To install Quest Reporter with the direct data transport mode

1. When you have finished downloading Quest Reporter, unzip the files to an appropriate directory (for example, c:\temp).
2. Double-click **autorun.exe**, click **Setup**, and then click the **Quest Reporter** link.
3. Read the Welcome screen and click **Next**.
4. Read and accept the licensing information and click **Next**.
5. Enter your name and company name and click **Next**.

You can choose to install the application settings for the current user or for all users that share the computer.

6. Accept the default program folder name.

– OR –

Select **Browse** to change the drive or location.

7. Click **Next**.
8. Click to clear the Compressed Data Transport Mode check box and click **Next**.
9. Click **Next** to start the installation.

10. Enter your company name and activation key, click **Register** and click **Exit**.

If Quest Reporter was shipped to you, your activation key is on the enclosed license agreement.

If you did not purchase Quest Reporter or did not receive an activation key, contact your Sales Representative or email sales@quest.com. If you have a licensed version of Quest Reporter, contact license@quest.com to obtain an activation key.

11. Click **Finish**.

At this point, it is recommended that you set up the Quest Reporter database.



You can use the Quest Reporter Database Setup wizard to select or set up a different database after you install Quest Reporter. You can run this wizard by selecting **Start | All Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter Database Setup**.

12. Click **Next** on the welcome page of the Database Setup Wizard.

Quest Reporter uses one database for both real-time (live) data and stored data. The Database Setup Wizard guides you through the process of creating and selecting the database used by Quest Reporter. You can use the following three user security scenarios to create the databases:

The user is in the Administrators group of the workstation, and is added to SQL Server with permissions to create a database.

The user is in any group of the workstation and is added to SQL Server with permissions to create a database.

The user connects to the database using SQL Server authentication with an account that has permissions to create a database.

13. Select the domain and computer where you want to create the database.
14. Select the authentication method for database access.

NT authentication requires a valid Windows NT user name and password.

SQL Server authentication requires a valid SQL Server user name and password.

15. Click **Next**.
16. Enter a name for the new database or select an existing database and click **Next**.
17. Click **Next**.
18. Review the summary information, then click **Finish**.

Installing the Compressed Data Transport Mode

The compressed data transport mode of Quest Reporter requires services running on the Quest Reporter Console host and on the RDC host. To run these services You must provide a user account with which to run these services.

Service Accounts

To use the compressed data transport mode, services are installed on the Quest Reporter Console host and all deployed RDCs. Keep the following in mind when setting up services accounts:

- The Console host requires a domain account. The account must have local administrative rights on the server and must follow the format: domain\user name.
- The RDC host requires either a local system account or a domain account with administrative rights.



If you are scheduling collections later, you need to provide an account for the RDC and an account for the compressed data transport mode. You can use the same account if you want. However, the account that you use for the RDC must be a domain account with administrative rights.

- In the case of Windows NT and Active Directory where there is a one-way trust, you must manually set the credentials on the RDC host.

Deploying MSMQ

Quest Reporter uses MSMQ technology. By default, MSMQ files are installed with Windows XP and Windows 2003. If you are installing Quest Reporter on a Windows 2000 computer, you need to provide the location of the Windows 2000 CD and related Service Pack files during the installation.

MSMQ 2.0 in workgroup mode (independent clients) is deployed to RDC (Report Data Collector) hosts during the installation.



IF YOU ARE INSTALLING QUEST REPORTER ON A WINDOWS 2000 COMPUTER

Before you start the installation, ensure that the Windows 2000 CD and related Service Pack versions are accessible from a computer—either on CD or through a network path. You need to provide the location of these files during the installation.

To install Quest Reporter with the compressed data transport mode

1. When you have finished downloading Quest Reporter, unzip the files to an appropriate directory (for example, c:\temp).
2. Double-click **autorun.exe**, click **Setup**, and then click the **Quest Reporter** link.
3. Read the Welcome screen and click **Next**.
4. Read and accept the licensing information and click **Next**.
5. Enter your name and company name and click **Next**.

You can choose to install the application settings for the current user or for all users that share the computer.

6. Accept the default program folder name.

– OR –

Select **Browse** to change the drive or location.
7. Click **Next**.
By default, the compressed data transport mode is selected.
8. Click **Next**.
9. Enter the user name and password that will run the services and click **Next**.
This account requires the right Log on as a service. This right is assigned automatically to the account if it is not already assigned.
10. Click **Next** to start the installation.
*If you are installing on Windows 2000 and MSMQ is not detected then a dialog box opens that allows you to install it. To install MSMQ, enter a valid path for the Windows 2000 installation files and a valid path for the Service Pack files, click **Next**, and click **Finish**.*
11. Click **Finish**.
12. Enter your company name and activation key, click **Register**, and click **Exit**.
If Quest Reporter was shipped to you, your activation key is on the enclosed license agreement. If you did not purchase Quest Reporter or did not receive an activation key, contact your Sales Representative or email sales@quest.com. If you have a licensed version of Quest Reporter, contact license@quest.com to obtain an activation key.
13. Click **Next** on the welcome page of the Database Setup Wizard.
Quest Reporter uses one database for both real-time (live) data and stored data. The Database Setup Wizard guides you through the process of creating and selecting the database used by Quest Reporter.

You can use the following three user security scenarios to create the databases:

The user is in the Administrators group of the workstation, and is added to SQL Server with permissions to create a database.

The user is in any group of the workstation and is added to SQL Server with permissions to create a database.

The user connects to the database using SQL Server authentication with an account that has permissions to create a database.
14. Select the domain and computer where you want to create the database.
15. Select the authentication method for database access.
NT authentication requires a valid Windows NT user name and password.
SQL Server authentication requires a valid SQL Server user name and password.
16. Click **Next**.
17. Enter a name for the new database or select an existing database and click **Next**.
18. Click **Next**.

19. Review the summary information, then click **Finish**.



You can use the Quest Reporter Database Setup wizard to select or set up the database after you install Quest Reporter. You can run this wizard by selecting **Start | All Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter Database Setup**.

You have to start the Compressed Data Transport Services after you install Quest Reporter. These services transfer the compressed data from the Report Data Collector to the computer where you installed Quest Reporter, decompress the data, and store it in the Quest Reporter database.

To start the services

1. select **Start | All Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Compressed Data Mode** tab.
3. Click **Start**.

Upgrading Quest Reporter from an Earlier Version

The following upgrade paths are supported:

- Version 5.4 to 5.5
- Version 5.3 to 5.5

Best Practices

Before installing Quest Reporter 5.5, remove all components of Quest Reporter.

- Ensure any remote or local RDC executables are stopped.
Ensure there are no collections running. On any computer where an RDC exists, ensure the RDC process is not running. If you want to upgrade right now and an RDC is running then terminate the process.
- Remove Quest Reporter.
Open Add or Remove Programs, select **Quest Reporter**, and click **Remove**.
- For safety reasons, the program will not remove files that it did not explicitly place on the computer. Because of this, there may be several files remaining.
To preserve your Favorite reports, ensure that the contents of the folder below are not disturbed (the uninstall process will not remove files from this folder):
 - C:\Program Files\Common Files\Quest Shared\Quest Management Suite\Favorites
- Clean your database before you upgrade.

Some upgrades of Quest Reporter may require an upgrade of the database. Any unused data can be cleaned using the Database Cleanup utility provided with Quest Reporter. Less data in the database may increase the speed of the upgrade.

Removing Quest Reporter

You must remove earlier versions of Quest Reporter before you upgrade to Quest Reporter version 5.5. If you used compressed data transport mode, you must use native Microsoft tools to delete the MSMQ queues.

To remove Quest Reporter

1. Select **Start | Control Panel | Add/Remove Programs**.
2. Select **Quest Reporter**.
3. Click **Remove**.
4. Click **Yes**.
5. Click **Close**.



Only the files that were installed with Quest Reporter will be removed. Any files that were created after the installation, such as license registration and help files, will remain in the installation folder after the product has been removed.

Upgrading from Version 5.3 or 5.4 to Version 5.5

To upgrade from version 5.3 or 5.4 to version 5.5

1. Uninstall Quest Reporter.



If you have installed the 5.4.0.660 patch for Reporter 5.4, you must uninstall it prior to uninstalling Quest Reporter 5.4. To remove this patch, use Add or Remove Programs in the Microsoft Windows Control Panel.

2. Double-click **autorun.exe**, click **Setup**, and then click the **Quest Reporter** link.
3. Read the Welcome screen and click **Next**.
4. Read and accept the licensing information and click **Next**.
5. Enter your name and company name and click **Next**.
You can choose to install the application settings for the current user or for all users that share the computer.
6. Accept the default program folder name.

– OR –

Select **Browse** to change the drive or location.
7. Click **Next**.
By default, both modes are selected.
8. Click **Next**.
9. Enter the user name and password that will run the services and click **Next**.
This account requires the right Log on as a service. This right is assigned automatically to the account if it is not already assigned.
10. Click **Next** to start the installation.
11. Click **Finish**.

12. If necessary, enter your company name and activation key, click **Register**, and click **Exit**.
If Quest Reporter was shipped to you, your activation key is on the enclosed license agreement. If you did not purchase Quest Reporter or did not receive an activation key, contact your Sales Representative or email sales@quest.com. If you have a licensed version of Quest Reporter, contact license@quest.com to obtain an activation key.

13. Click **Yes** to upgrade the existing database and go to step 15.

– OR –

Click **No** if you want to upgrade the database later and go to step 14.

If you want to upgrade your database later, you can use the Quest Reporter Database Setup utility that is included with Quest Reporter. For more information, see the section called "Setting Up a Database" in your Quest Reporter User Guide.

14. Click **Yes**.
15. Click **OK**.

You have to start the Compressed Data Transport Services after you install Quest Reporter. These services transfer the compressed data from the Report Data Collector to the computer where you installed Quest Reporter, decompress the data, and store it in the Quest Reporter database.

To start the services

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Compressed Data Mode** tab.
3. Click **Start**.

Upgrading Remote RDCs

Local RDCs are upgraded automatically when you install a new version of Quest Reporter. Remote RDCs are not upgraded automatically. Instead, you must upgrade each one before you use it with the new version of Quest Reporter.

To upgrade a remote RDC

1. Click a remote RDC under the Scheduled Collections node.
2. Click **Yes** on the Upgrade RDC message.
3. Click **Next** on the RDC Upgrade welcome page.
4. Click **Direct to Database Mode** and click **Next**.

– OR –

Click **Compressed Data Transport Mode** and click **Next**.

*If the computer where the RDC is installed is a Windows 2000 computer, Quest Reporter will check to see if Microsoft Message Queuing (MSMQ) version 2.0 or later is installed on it. If it is not, you have to enter the location of the Windows 2000 CD and the location of the appropriate service pack. Once you have done that, click **Next**.*

5. Click **Finish**.

Running Quest Reporter

To run Quest Reporter

- Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter**.

You are now ready to use Quest Reporter.

Step-By-Step Walkthrough

There are four different approaches that can be leveraged by Quest Reporter.

- Ad hoc reporting — Requires immediate results for subset of your environment with minimal impact to the network and is highly efficient.
- Scheduled reporting — Supports information gathering and report generation on a regular basis such as daily, weekly or monthly reports.
- Action enabled reporting — Supports addressing operational changes in bulk such as changing the administrator password on all computers or disabling accounts that have not logged on in over 30 days.
- Change history reporting — Supports quickly identifying changes to objects to resolve configuration related concerns such as changes to software and hardware, group membership changes, and so forth.

This walkthrough will guide you through each of these use cases for Quest Reporter. Each scenario involves selecting different object categories to support each of the different approaches.

Example Scenario for Ad Hoc Reporting

Ad hoc reporting is generally required to fulfill a specific need or address an immediate issue. Organizations must be able to collect, store and report on their environment at that moment in time and provide results immediately. With a focus on flexibility and performance, Quest Reporter ad hoc reporting capabilities meet this need.

In the following example, you will go through the four main steps required for ad hoc reporting:

- Select a report template and initiate a report instance.
- Define the objects you want to report on.
- Define a collection mechanism (live or stored).
- Select the output format.

The scenario used here to demonstrate ad hoc reporting is a typical one. As network administrator, you have received an urgent request from the company auditor. He needs to identify all computer accounts that are inactive, and he needs this information as soon as possible.

To perform ad hoc reporting

1. If you do not already have Quest Reporter running, select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter**.
2. Expand **Reporting | Reports** and select the **Domains** folder.
3. Select the **Computer Account Status** report template.
Details on this report template, such as Notes and the attributes and groupings that are included, appear in the lower right pane.
4. Double-click the **Computer Account Status** report template.
This initiates a report instance for this report. The Run Report dialog box is displayed.
5. Click the **Objects** tab and click **Add**.
The Object Picker dialog box is displayed. Here you can select individual objects, Active Directory based containers such as domains or Organizational Units (OUs), and object sets you have created.

6. Select a domain from the upper-right pane, click **Add**, then click **OK**.
This defines the objects you want to report on.
7. Click the **Collections** tab and verify that Live collection is selected as the content source for the report.
This defines the collection mechanism you want to use. The other collection option is Stored data, where the report content would be generated from data previously collected and stored in the Reporter database.
8. Click the **Output** tab and verify that Screen is selected.
This defines the output format. You can also choose any of the following file types as the output format: .html, .rtf, .txt, .xls, and .pdf.
9. Click **OK** to generate the report.
Once generated, the report is displayed. The first page always shows information such as the report name, collection source, filters and the number of objects returned. Subsequent pages show the report findings, organized using the attributes and groupings for this report template.

Quest Reporter is a very flexible tool. For example, suppose the company auditor only wants information showing inactive computer accounts for the last two weeks. You can save the report instance you have just generated as a favorite and then modify it.

To save a report as a favorite

1. In the print preview pane, click **Save**.
2. Select **Favorite** and click **OK**.
*As you are now done with the generated report, click **Close** to return to the Reporter console.*

To modify a favorite report

1. In the treeview of the Reporter console, select **Reports | Favorites**.
The report you have saved as a favorite should appear in the upper-right pane. If necessary, press F5 to refresh the view.
2. Right-click the report and select **Properties**.
The Properties dialog box is displayed. The Attribute and Filter tabs allow you to modify Favorites by adding or removing attributes, and by filtering data to meet specific criteria.
3. Select the **Attribute** tab.
4. Select the **Operating System Build Number** and **Operating System Caption (WMI)** check boxes.
This will add the operating system build number and caption attributes to the report results.
5. Select the **Filters** tab and click **Add**.
6. Double-click **<Attribute>** and select **Last Logon**.
7. Double-click **<Condition>** and select **is less than**.
8. Double-click **<Value>** and select **Or**.
9. Enter 2 for the value, select **weeks**, and then select **ago**.
10. Click **OK**.
This sets the filtering criteria needed to find computer accounts that have been inactive for the last two weeks.
11. Click **OK** to save your modifications and return to the Reporter console.
The report you have created is displayed in the upper-right pane of the Reporter console.

To run your favorite report

- Right-click the favorite report and select **Run**.

Example Scenario for Scheduled Reporting

Scheduled reporting is suited to situations where you know what information you want to collect and how often you want to collect it. Collection occurs on a regular basis, for example, daily, weekly or monthly. You would normally use scheduled reporting when your entire environment is of interest but data collection cannot be run during normal business hours as it will significantly impact your end users.

With scheduled reporting, you have the flexibility to collect what you want, when you want it, and generate report output without adversely impacting the network. Collect all the data at once, and then run reports against the stored data versus querying your live network again and again. This can significantly improve performance. Another performance benefit is in the data collection process itself. Reporter data collectors (RDCs) can be deployed in close proximity to the targeted system, typically on the same LAN segment. The data can then be compressed before it is transported over the WAN, minimizing the load on the network.

The following example demonstrates the two main phases of scheduled reporting:

- Data collection
- Report generation

These two phases take place independently of one another. Data collection is handled by the scheduled collections task, while report generation is done through the use of favorites. A favorite is a user-defined and saved configuration for a data collection and report generation instance. Favorites contain user-defined configurations such as object scope, collection mechanisms, filters, report output, and so forth.

The scenario used here to demonstrate scheduled reporting is one you may be acquainted with. As network administrator, you need to baseline share and folder permissions for your file servers. To support auditing and security requirements, your organization deems that this type of report should be performed on a monthly basis.

Data Collection

In this first part of the scenario, you need to schedule the collection and storage of the share/folder permissions data for the servers of interest. To do this, you must:

- Create an appropriate report template to use for the data collection
- Create an object set to be used for scheduled reporting purposes
- Create a scheduled collection to accumulate data in the database

To create the report needed for data collection

1. If you do not already have Quest Reporter running, select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter**.
2. Expand **Reporting | Reports** and select the **Permissions** folder.
3. Select the **NTFS** subfolder.
4. Select the **Share and Folder Permissions** report template in the upper-right pane.
5. Right-click the **Share and Folder Permissions** report and select **Duplicate**.

A copy of the Share and Folder Permissions report, called the Duplicate of Share and Folder Permissions report, is added to the list of report templates.

6. Right-click the **Duplicate of Share and Folder Permissions** report and select **Properties**.
The Properties dialog box is displayed, with the name of the report highlighted.
7. Enter **Shared Directories Monthly Report** as the name of the report template.
8. Click the **Attributes** tab and select **Size** from the list of attributes.
The Size attribute was not one of the attributes that the Shares and Folder Permissions report collects data for. By selecting it in this manner, you have added it to the attributes list.
9. Select the **Only show selected attributes** check box.
The list of attributes will be refreshed to show only the selected attributes, including Size.
10. Right-click the **Account** attribute and select **Link in**.
The "Linked In" Attributes Selection dialog box is displayed, listing additional attributes that can be collected. These attributes are linked from the "Accounts" attribute.
11. Select **Members** and click **OK**.
12. Click **OK** again to exit the report template dialog box and return to the Reporter console.



When creating a report template for scheduled data collections, it is recommended that you test the report template by running it against a small subset of objects. This will allow you to verify that the appropriate data is being collected and displayed properly.

Now that you have completed your customized report template, you need to create the object sets you will use for scheduled reporting. An object set is a collection of objects that are of interest to you as Administrator. The benefit of creating an object set is that it can be reused as part of the scheduled collection process and report generation.

Object sets should contain objects of the same category, and can be dynamic, where a query is used to select objects, or static, where the objects to be included are selected or imported from a list. Further, you can also specify that an object set is to be used for offline purposes.

In this scenario you will create an object set that is dynamic and also searches for particular shares on the objects selected.

To create an object set that will be used for scheduled reporting purposes

1. In the left pane of the Reporter console under Reporting, right-click the **Object Sets** node and select **New | Object Set**.
This opens the Object Set Wizard.
2. Click **Next**.
3. Enter **Share Directories - Dynamic** as the name of the object set.
4. Click **Next**.
5. Click **Add**.
The Object Picker dialog box is displayed.
6. Click **Query**.
The Find Computer dialog box that displays allows you to define the parameters for your query.
7. Click **Find** and select **Computers**.
8. Click the **Advanced** tab.

9. Click **Field** and select **Name**.
10. Click **Condition** and select **ends with**.
11. Enter a parameter value in the Value box.
This value will be used to define the query. For example, if you were to enter DC1, the query would select all computers with a name that ended in DC1.
12. Click **Add** and then click **Find Now** to show the query results.
13. Click **OK**.
This returns you to the Object Picker dialog box.
14. Click **Shares**.
15. Click the **Search** option and enter ^ followed by the text you want to search on.
The carrot symbol (^) is a regular expression that is interpreted as "Only look for shares that have names that begin with" followed by the text to search for. For example, if you entered ^sales, the search would return all shares whose name ends with "sales".
16. Select **Retrieve Folder ACL** and then select **All levels**.
The Retrieve Share ACL option is selected by default. By also selecting the Retrieve Folder ACL and All levels options, you are ensuring that folder permissions are collected and that recursion includes all folders in the tree.
17. Click **OK** and click **OK** again to return to the Object Set Wizard.
18. Click **Next**.
19. Click **Next**.
20. Click **Finish**.
The advantage to creating an object set this way is that anytime any new server comes on line that ends with the values you have specified, then it will be included in the data collection.

Finally, you need to schedule the collection and storage of the share/folder permissions data for the servers of interest.

To create the scheduled collection

1. In the left pane of the Reporter console under Reporting, right-click the **Scheduled Collections** node and select **New | Scheduled Collection**.
This opens the Scheduled Collection Wizard.
2. Click **Next**.
The Computer Selection page is displayed, where you select the computer you want to run the collection on. Remote computers must have report data collectors (RDCs) installed before you can select them. For more information on RDCs, refer to your Quest Reporter User Guide. In this scenario you will use the local computer, which is selected by default.
3. Click **Next**.
The Data Transport Mode page is displayed. Quest Reporter provides you with two different data transport modes. However, as you selected the local computer, only the option for direct data transport mode is available. For more information on these modes, see ["Choosing a Data Transport Mode" on page 13](#).
4. Click **Next**.
5. Enter a name and description for the scheduled collection.
6. Click **Next** to select the report template you want to use.
7. Select **Shared Directories Monthly Report**.

8. Click **Next** to select the object set you want to use.
9. Click **Add**.
The Object Picker is displayed.
10. Click **Object Sets** in the upper-left pane.
11. Click **Share Directories - Dynamic** in the upper-right pane, drag it down to the lower pane, and click **OK**.
12. Click **Next**.
13. If you are prompted to continue without adding any offline object sets, click **Yes**.
14. Enter the credentials that this scheduled collection will run under.
15. Click **Next**.
16. Click **Schedule Task** and select **Monthly**.
17. Enter the time, day of the month, and the months when you want the collection to run.
18. Click **Next**, then click **Next** again.
19. Click **Finish**.
The scheduled collection is now ready to run.

Report Generation

In the second part of this scenario, you need to schedule the collection and storage of the share/folder permissions data for the servers of interest. To do this, you need to:

- Create a favorite report template to use for the scheduled reporting
- Schedule the favorite report to run

To create a favorite report template for the scheduled reporting

1. In the treeview of the Reporter console, expand **Reporting | Reports**.
2. Right-click **Favorites** and select **New | Favorite**.
3. Select the **Shared Directories Monthly Report** template and click **Add**.
4. Click **OK**.
A Properties dialog box opens for the report template you selected.
5. Click the **Objects** tab.
6. Click **Add**.
7. Select the **Share Directories - Dynamic** object set.
This is the same object set you created to collect the data you will now be reporting on.
8. Click **Add** and then click **OK**.
9. Click the **Collection** tab.
10. Select **Stored Data** as the source content for the report.
11. Select the **Output** tab.
12. Select **File** and then select the file type you want to use.
13. Browse to the folder where you want to save the report and enter a file name for the report.
The Screen option is checked by default. When you also select the File option, the report content is also written to a file in addition to the results being displayed on screen.
14. Click **OK**.

To schedule running the favorite report

1. In the treeview of the Reporter console, expand **Reporting | Reports**.
2. Select **Favorites**.
3. Right-click the **Shared Directories Monthly Report** template and select **Schedule**.
The Favorite Report Schedule wizard is displayed.
4. Click **Next**.
5. Enter the credentials that this scheduled collection will run under.
6. Click **Next**.
7. Click **Schedule Task** and select **Monthly**.
8. Enter the time, day of the month, and the months when you want the collection to run.



Keep in mind the schedule settings you set when creating the scheduled collection. The report should be run after the collection has taken place.

9. Click **Next**.
10. Click **Next**.
11. Click **Finish**.

The favorite report is now scheduled to run on a regular basis.

Example Scenario for Action-Enabled Reporting

Action-enabled reporting takes ad-hoc reporting one step further. While ad-hoc reporting provides you with results, with action-enabled reporting you can perform actions based on those results. This allows you the flexibility to respond immediately to address security and operational concerns conveniently through the Reporter console. These types of concerns may be resolving a security breach or making changes to adhere to standards.

Action-enabled reporting should occur regularly, as dictated by your own internal policies. This approach is needed in order to maintain tight security controls and minimize operational impact. With it, organizations not only collect, store and report on their environment but can also perform actions based on the results in a timely manner and on a regular basis.

Here are some examples where action-enabled reporting would be beneficial:

- Changing administrator password on all local computers every 30 days
- Disabling any account that has not logged on in 60 days
- Changing startup options for a particular service on local computers

Quest Reporter's action enabled capabilities are quite extensible. You can launch the existing predefined actions, associate the predefined actions to other objects and attributes or create your own actions.

With action-enabled reporting, you can

- Create and modify action scripts
- Run an action-enabled report against objects and/or attributes

In this action-enabled reporting scenario, you, as network administrator, must modify the administrator password on all the local computers in your domain.



Instructions in the following walkthrough will result in changes to administrator passwords. Keep this in mind to avoid affecting a live network environment. It is recommended that you create a test environment in which to walk through this scenario.

Creating and Modifying Action Scripts

Quest Reporter includes a number of predefined action scripts. These scripts are already associated with the four different categories of object types: users, groups, computers, and domains. Using the Configure utility provided, you can add scripts to objects and attributes, or copy the predefined scripts and use them as a basis to create your own action scripts.

When using action enabled scripts, you must consider whether you want to perform the action against the object itself or against an attribute of that object. An action enabled script associated to an object performs an action against the object itself like move, delete, reset password, and so forth. An action enabled script associated to an attribute is specifically targeted against an object's attribute such as modifying the home directory or enabling/disabling the user account.

To demonstrate the adaptability of action scripts, you will create an action script for the Groups object type and use that script to modify selected objects. To do this, you need to

- Create a custom action script
There are a couple of ways to do this. You could add a new script and use the supplied script template as a starting point, but in this scenario you will copy and modify an existing script.
- Run the action-enabled report to generate report results
- Select objects from the report results and perform the selected action against them

To create a custom action script by copying and modifying an existing action script

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Select the **Action Enabled** tab.
3. Click **Category** and select **Groups**.
The predefined scripts associated with groups are displayed in the right pane. These are the actions you can apply against the results of an action-enabled report.
4. Right-click in the Scripts window and select **Add | Pre-existing Script | Move User**.
The Move User script is added to the list. This script is actually a move object script and not specific to only users.
5. Right-click the **Move User** script and select **Modify**.
The script is displayed in an editing window.
6. Select all of the script and press **CTRL+C** to copy.
7. Click **Cancel** to close the editing window.
8. Right-click in the Scripts window and select **Add | New Script**.
A script template is displayed in an editing window.
9. Select all of the script and press **CTRL+V** to replace it with the Move User script you copied.
10. Locate the line that starts with "displayname" and change the value to Move Groups.

11. Click **OK**.
12. Click **OK** to exit the Configure utility.

Now you need to run the action-enabled report "All Global Groups" on global groups. From the report results, you will select objects and move them to another container using the Move Groups action script.

To generate report results

1. If you do not already have Quest Reporter running, select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter**.
2. Expand **Reporting | Reports** and select the **Groups** folder.
3. Right-click the **All Global Groups** report template and select **Run Action Enabled Report**.
The Run Report dialog box is displayed.
4. Click the **Objects** tab and click **Add**.
5. Select a domain from the upper-right pane, click **Add**, then click **OK**.
6. Click **OK** to generate the report.

Once generated, the report results are displayed in a separate dialog box. Here, you can highlight the groups of interest by single selection or multi-selecting and choose the appropriate action which, in this case, is to move groups.

To select objects from the report results and perform the selected action against them

1. Select the groups you want to move in the report results dialog box and right-click.
2. Select **Object Script | Move Group**.
The Choose New Container dialog box is displayed.
3. Expand the treeview and select the container that you want to move the groups to.
4. Click **OK**.
The lower pane displays a log of the script execution results.
5. Click **Close** to exit the report results dialog box.

To confirm that the groups have been moved, in the Reporter console expand the Active Directory node in the treeview and select the container you specified. The groups should be listed in the upper-right pane of the Reporter console.

Running an Action-enabled Report Against Objects and Attributes

In this part of the scenario, you need to use an action-enabled report to generate report results that you can modify. To do this, you need to

- Create a custom report template
- Run the custom report and modify the results

To begin, create the custom report template and add a filter to only display user names that equal administrator.

To create a custom report template

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter**.

2. Expand **Reporting | Reports** and select the **Users** folder.
3. Right-click the **General User Information** report template and select **Duplicate**.
A copy of the General User Information report, called the Duplicate of General User Information report, is added to the list of report templates.
4. Right-click the **Duplicate of General User Information** report and select **Properties**.
The Properties dialog box is displayed, with the name of the report highlighted.
5. Enter **Local Administrator Account - Action Enabled** as the name of the report template.
6. Click the **Filter** tab and then click **Add**.
7. Double-click **<Attribute>**, select **User Name**, and click **OK**.
8. Double-click **<Condition>**, select **equals**, and click **OK**.
9. Double-click **<Value>** and click **Values**.
10. Select **Administrator** and click **OK**.



The list is populated with existing values from previously collected data. If you have not yet run any data collections, the list will be empty. If this occurs type in the value, for example, Guest or Administrator.

11. Click **OK**.
This sets the filtering criteria needed to find all user names that equal "administrator".
12. Click **OK** to save your modifications and return to the Reporter console.

You are now ready to run the report and modify the report results.

To run the custom report and modify the administrator password

1. Right-click the **Local Administrator Account - Action Enabled** report template in the upper-right pane.
2. Select **Run Action Enabled Report**.
The Run Report dialog box is displayed.
3. Click the **Objects** tab and click **Add**.
The Object Picker dialog box is displayed.
4. Expand the domain node in the upper-left pane and select **Computers**.
A list of computers appears in the upper-right pane.
5. Select the computers you want to include, click **Add**, then click **OK**.
6. Click **OK** to run the report.
The report findings are displayed.
7. Right-click the accounts whose password you want to change.
8. Click **Object Script** and select **Reset Password**.
The Password dialog box is displayed.
9. Enter the new password, and re-enter to confirm.
10. Click **OK** to return to the report findings.
11. Click **Close** to apply the password change.

To verify the password change, log on to one of the computers you included in the selection. Use an Administrator's account on that computer and log on using the new password.

Example Scenario for Change History Reporting

Reporter was designed for history reporting; its data collection and storage was built with this feature in mind. When data is collected, the data is compared to what is currently stored in the Reporter database. If the data is different, then this information is updated; the update change and the initial information are also saved in the database. As with all database entries, this information can be easily and quickly retrieved.

The best way to use change history reporting is with scheduled collections. Once the appropriate information has been stored in the database, you can report against it using a favorite created for just that purpose. This favorite has one important difference; the collection tab option to include change history is selected.

With change history reporting, you can quickly identify changes that have occurred in your environment, such as

- Group membership changes
- Service and network setting changes
- Installed software changes
- NTFS Permission ACL changes

Change history reporting is quite flexible. You can schedule it to occur automatically or run it interactively against stored or live data. With live data, the reporting is done using current information collected from the network and stored data from the database.

In the following scenario, you will use change history reporting to focus on changes to group memberships. This involves the following two main tasks you may recall from scheduled reporting:

- Data collection
- Report generation

Data Collection

As the tasks involved in setting up and scheduling data collections have been covered in the example scenario for scheduling reporting, those details will not be repeated here. The main tasks are

- Create an appropriate report template to use for the data collection
Use the Group Membership report template as the basis for your duplicate. For more information on this procedure, see ["To create the report needed for data collection"](#) on [page 23](#).
- Create an object set to be used for scheduled reporting purposes
The object set should target local and global groups. For more information on this procedure, see ["To create an object set that will be used for scheduled reporting purposes"](#) on [page 24](#).
- Create a scheduled collection to accumulate data in the database
For more information on this procedure, see ["To create the scheduled collection"](#) on [page 25](#).

Report Generation

Once you have set up your data collection and populated the Reporter database with a few collections, you are ready to run a report template against the stored data. To automate the process, you can save the report template as a favorite and schedule it to run on a regular basis. That way, you can stay current regarding changes to your local and global groups.

In this part of the history reporting scenario, you need to

- Create a favorite report template to use for the scheduled reporting
- Schedule the favorite report to run

To create a favorite for the scheduled reporting

1. In the treeview of the Reporter console, expand **Reporting | Reports**.
2. Right-click **Favorites** and select **New | Favorite**.
3. Select the **Groups** subfolder.
4. Select the **Group Membership** report template, click **Add**, and click **OK**.
A Properties dialog box opens for the report template you selected.
5. Enter **Group Membership - 5 Day History Report** as the name of the report template.
6. Click the **Objects** tab.
7. Click **Add**.
8. Select the same object set you leveraged for the scheduled collection.
9. Click **Add** and then click **OK**.
10. Click the **Collection** tab.
11. Select **Stored Data** as the source content for the report.



If you want an up-to-the-minute status at the time of running the report, select **Live collection** as the source content. However, be aware that this will take some time as the data must be collected from the live environment. Since the data was collected previously you may not need to collect it again right now for accurate results.

12. Select **Change History**.
13. Select **Or** and specify a number of days, weeks or months against which to report.
When you specify a number of days, weeks, or months, this value is applied based on the current date and time when the report template is run. For example, if you specify five days and run the report template today at 18:00 hours, the report content is based on data from the last five days counting back from today at 18:00 hours until five days ago at 18:00 hours.
If you use this option in combination with scheduled reporting, you are in effect defining a moving timeframe against which to report. The value you specify is applied against the schedule you set up to run the favorite report template. Continuing with the above example, if you schedule the favorite to run daily, the timeframe of five days will shift forward by one day each time the favorite runs.
14. Select the **Output** tab.
15. Select **File** and then select the file type you want to use.
16. Browse to the folder where you want to save the report and enter a file name for the report.
The Screen option is checked by default. When you also select the File option, the report content is also written to a file in addition to the results being displayed on screen.
17. Click **OK**.

To schedule running the favorite report

1. In the treeview of the Reporter console, expand **Reporting | Reports**.
2. Select **Favorites**.
3. Right-click the **Group Membership - 5 Day History Report** template and select **Schedule**.
The Favorite Report Schedule wizard is displayed.
4. Click **Next**.
5. Enter the credentials that this scheduled favorite will run under.
6. Click **Next**.
7. Select **Daily** from the Schedule Task list.
8. Enter the start time at which the favorite will run.



Keep in mind the schedule settings you have set for your scheduled collections. The report should run after the collection has taken place.

9. Click **Next**.
10. Click **Next**.
11. Click **Finish**.

The favorite report is now scheduled to run on a daily basis, providing you with an ongoing status of changes to the group memberships in your environment.

Quest Reporter Terminology

Quest Reporter uses the following terms:

Access Control Entry (ACE)

An object such as a user or group that is present on an Access Control List.

Access Control List (ACL)

A table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file.

Active Directory

The Windows 2000/2003 directory service.

Administrative rights

The rights granted to a member of the Administrators local group. This member can perform such actions as creating user accounts, creating groups, and adding group members.

Authentication

The process required to log on locally to a computer. Authentication requires a valid user name and password that exists in the local accounts database. An access token is created if the information provided matches the account in the database.

Compressed data transport mode

One of two types of data transport modes used by Quest Reporter. This mode collects and compresses the data on the Reporter Data Collector (RDC) host. The compressed data pack is then streamed to the Console host, decompressed and uploaded to the database. Compressed data transport is available only with remote scheduled collections and is only leveraged during computer based collections. See also Direct data transport mode.

Connected domains

Domains managed by Reporter and instantiated within the Reporter user interface.

Container object

An object that can logically contain other objects. For example, a folder is a container object.

Data collection

The phase of the reporting process where data is gathered from the network.

Direct data transport mode

One of two types of data transport modes used by Quest Reporter. In this mode, collected data is stored directly to the database. See also Compressed data transport mode.

Distinguished name (DN)

The fully qualified name of an object in a hierarchical system. Distinguished names are used for all Active Directory objects and in the Domain Name System (DNS). No two objects in these systems should have the same distinguished name.

Domain

In relation to a Microsoft network, a domain is a logical collection of resources consisting of computers, printers, computer accounts, user accounts, and other related objects. The domain also has a system of logon authentication of user accounts and computer accounts.

Domain controller (DC)

A server that authenticates domain logon passwords and maintains security policy and the security accounts master database for a domain.

Favorite

A user-configured, ready-to-run version of a report template which already includes scope (selected objects) and output options for the report. Because they already contain the scope and output options, favorites require no user input and can be executed by the task scheduler as well as interactively.

File system

The File system data source is used to extract configuration information from remote server file systems. When defining data items, the Quest Reporter administrator must identify the file, and the polling characteristic. These characteristics include the following: size, version, presence, access date, create date, or modify date.

Forest

One or more domain trees that do not form a contiguous namespace, but share a common schema, configuration, and global catalog.

Group

In relation to a Microsoft network, a group is a logical collection of user accounts and/or other groups. Groups of the local or global type are security principals often used for assigning access to resources. Windows 2000 also supports non-security principal groups known as distribution groups.

Local Area Network (LAN)

A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area.

Lightweight Directory Access Protocol (LDAP)

A protocol used for querying and modifying information stored within directory services. The Active Directory can be queried and modified through the use of LDAP-compatible tools.

Live report

A reporting process during which content for the desired report is collected from the original source (for example, Active Directory or NTFS permissions) when the report is launched. The user running the report must have appropriate rights on the original source to run a report in this fashion. By contrast, see Stored data report.

Load balancing

The fine tuning of a computer system, network or disk subsystem in order to more evenly distribute the data or processing across available resources.

Network Interface Card (NIC)

A network adapter that plugs into both the client and server and controls the exchange of data between them. The NIC object represents a grouping of information related to network interface cards. This grouping allows one server to have one or more network interface cards.

NT file system (NTFS)

The system that the Windows NT operating system uses for storing and retrieving files on a hard disk.

Notification

Email notification can be enabled or disabled for data collection activities. When notification is enabled, an email is sent once the data collection is complete.

Object

A Windows NT entity. Examples include users, groups, and computers. Access rights to objects include create, read, edit, and delete.

Object class

Within Reporter, object classes represent the different object types for which Reporter collects data, such as users, groups, computers, NTFS, domains, and so on. Each report template defined in Reporter is associated with one and only one object class.

Object set

A collection of objects that can be reused for purposes of data collection and report generation.

Offline object set

An object set that has been configured for offline purposes. The objects are enumerated and the necessary information required by Reporter for retrieving stored report data is stored in the database. Report generation against stored data is much faster as the database is referenced instead of querying the live network in order to enumerate the appropriate objects. As well, this allows the generation of stored reports when disconnected from the network.

Organizational Unit (OU)

A container object used to organize the Active Directory objects logically within a domain.

Permission

A rule associated with an object to regulate access to a particular object on the network. For example, a user may have read and write access to a file on the network.

Primary Domain Controller (PDC)

The first controller created in a Windows NT 4.0 domain. It contains the primary read-writable database instance for domain security data, such as user, group, and computer accounts.

Property

An attribute of a Windows NT network object. Examples include a user's password, groups to which a user belongs, and a group's description.

Registry

A hierarchical database in Windows NT and Windows 2000/2003 that contains configuration information about applications, users, and devices.

Report template

A predefined template containing an object category and corresponding attributes that is presented in a meaningful fashion. A report template requires a scope in order to be executed. Quest Reporter ships with over 180 unique report templates.

Reporter console

The main installation of Quest Reporter, including the MMC console and all the components necessary for the collecting, storing and scheduling mechanisms. This is the interface where you browse your network, manage object properties, schedule data collections and launch reports.

Reporter Data Collector (RDC)

A group of deployable components that allow execution of scheduled collections on a local or remote computer.

Root directory

The top-level directory on a computer, a partition, or volume.

Scheduled collection

A scheduled process that performs the data collection process by leveraging report templates against the appropriate object scope. This process places the data in the Reporter database for later use, and no report output is generated. See also Stored data report.

Schema

In Windows 2000, this describes the definition of the Active Directory database, including all classes of objects, their mandatory and optional attributes, and the data types used for storing.

Server

A computer in a network shared by multiple users.

Shares

Folders that can be accessed through the network from a computer.

Security Identifier (SID)

In Windows NT and Windows 2000 operating systems, the SID is a unique alphanumeric character string that identifies each security principal (domain, user, group, computer). SIDs are used by the Windows operating system to represent these objects in resource permissions and other applications requiring reliable security authentication.

SLA

Software License Agreement.

Simple Mail Transfer Protocol (SMTP)

The standard email protocol on the Internet for sending email messages between servers.

Stored data report

A reporting process during which only the scope of the report is effectively enumerated from the network. The content itself is extracted from previously collected information existing in the Reporter database. By contrast, see Live report.

Thread

A unit of execution that shares its memory space with other threads. Threads can be implemented within processes on some systems or may be used in place of processes in others (for instance, in Windows NT).

Wide Area Network (WAN)

A communications network connecting geographically separated computers, printers, and other devices.