NETWRIX GROUP POLICY CHANGE REPORTER

QUICK-START GUIDE

Product Version: 7.2

November 2012

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from NetWrix Corporation of any features or functions discussed. NetWrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

NetWrix is a registered trademark of NetWrix Corporation. The NetWrix logo and all other NetWrix product or service names and slogans are registered trademarks or trademarks of NetWrix Corporation. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-NetWrix products. Please note that this information is provided as a courtesy to assist you. While NetWrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-NetWrix product and contact the supplier for confirmation. NetWrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-NetWrix products.

Table of Contents

Suggestions or comments about this document? www.netwrix.com/feedback

1. INTRODUCTION

1.1. Overview

This guide is intended for the product evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided.

With this guide you can:

- Install and configure NetWrix Group Policy Change Reporter

- Create a Managed Object to monitor Group Policy objects changes in your domain

- Run data collection for your Managed Object and see how Group Policy objects changes can be reported

This guide only covers simple installation and configuration options. For advanced installation scenarios and configuration options, as well as for information on various reporting possibilities and advanced product features, refer to NetWrix Group Policy Change Reporter Administrator's Guide.

1.2. How This Guide is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter 1 Introduction is the current chapter. It explains the purpose of this document, defines its audience and outlines its structure.

- Chapter 2 Product Overview provides an overview of the NetWrix Group Policy Change Reporter functionality, lists its main features and benefits, and explains the product workflow. It also contains the information on the product editions and a side-by-side comparison of their features.

- Chapter 3 Installing NetWrix Exchange Change Reporter lists hardware and software requirements, and instructions on the installation of NetWrix Group Policy Change Reporter.

- Chapter 4 Configuring Target AD Domain explains how to adjust audit settings in your target AD domain and prepare it for monitoring.

- Chapter 5 Configuring Managed Object explains how to configure a Managed Object, which is an AD domain with Group Policy configuration that you monitor for changes.

- Chapter 6 Collecting the Initial Snapshot explains how to run data collection to perform the initial analysis of your domain current state.

- Chapter 7 Monitoring Your Target Domain for Changes provides instructions on how to make test changes to the monitored domain and see how they are reported by the product.

- Appendix: Related Documentation contains a list of all documents published to support NetWrix Group Policy Change Reporter.

1.3. Free Pre-Sales Support

You are eligible for free technical support during the evaluation period of all NetWrix products. If you encounter any problems, or would like assistance with the installation, configuration or implementation of NetWrix Group Policy Change Reporter, contact NetWrix support specialists.

2. PRODUCT OVERVIEW

Group Policy auditing is a must-have procedure for all organizations relying on Group Policy infrastructure. Relatively small changes to security policies, desktop configurations, software deployment and other settings can severely impact enterprise security, compliance, and performance. An uncontrolled and unaudited change process imposes major security and compliance risks for an IT infrastructure run by multiple IT professionals.

Built-in Group Policy management tools do not provide any auditing and change reporting capabilities, and it is just impossible to track the WHO, WHAT, WHERE and WHEN data for critical modifications by using these tools. For example, auditing with the native Windows tools can only indicate that a Group Policy changed, but it does not say WHAT setting has been changed; you can get only cryptic GUIDs for cross-referencing as a source of information.

Windows 2003 and earlier versions do not provide the before and after values for the Group Policy Object (GPO) link. Windows 2008 provides this data but it is difficult to use it efficiently. For detailed comparison of the native auditing tools and NetWrix products refer to Summary: Limitations of Native Active Directory Auditing Tools.

Powered by the NetWrix AuditAssurance™ technology, NetWrix Group Policy Change Reporter makes the Group Policy change auditing an easy and straightforward process, resulting in a complete and concise picture of all changes taking place in your monitored environment. AuditAssurance™ is a patent-pending technology that consolidates audit data from multiple independent sources such as event logs, configuration snapshots, change history records, and others. This allows detecting WHO changed WHAT, WHERE and WHEN, even if one or several sources of information do not contain all of the required data, for example because it was deleted, overwritten, and so on.

NetWrix Group Policy Change Reporter provides data on every single change made to the Group Policy configuration, including newly created and deleted GPOs, GPO link changes, changes made to audit policy, password policy, software deployment, user desktops, and other settings. The data includes detailed information for all changes with the previous and current values for all modified settings.

The product records all Group Policy modifications and archives them to enable historical reporting. You can build a summary of changes made to Group Policy during any period. For example, you can analyze any policy violations that took place in the past, see who turned off invalid logon auditing in your domain security policy, who added new software to deploy on client computers, who changed desktop firewall and lockdown settings, and so on.

NetWrix offers long-term data archiving that uses a two-tiered system:

- Audit Archive, a local file-based storage
- SQL Server database

NetWrix offers both agent-based and agentless data collection methods. The use of agents is recommended for distributed deployments or multi-site networks due to their ability to compress network traffic.

NetWrix Group Policy Change Reporter is a module included into a larger NetWrix Active Directory Change Reporter pack that automates auditing of the entire Active Directory infrastructure. The NetWrix Active Directory Change Reporter pack consists of the following modules:

- NetWrix Active Directory Change Reporter
- NetWrix Group Policy Change Reporter
- NetWrix Exchange Change Reporter

2.1. Key Features and Benefits

NetWrix Group Policy Change Reporter is a tool for automated auditing and reporting on changes to Group Policy objects configuration in the monitored domain. It allows you to do the following:

- **Monitor day-to-day administrative activities**: the product captures detailed information on all changes made to Group Policy objects and their settings in the monitored Active Directory environment, including the information on WHO changed WHAT, WHEN and WHERE.

- **Sustain compliance** by using in-depth change information. Audit data can be archived and stored for more than 7 years to be used for reports generation.

- **Streamline change control**: paint the most complete picture of Group Policy security settings throughout Active Directory by monitoring all settings and permission changes.

The main NetWrix Group Policy Change Reporter features are:

- **Reports** with the previous and current values for every object- and setting-level change. Reports are based on SQL Server Reporting Services (SSRS) with over 40 predefined report templates and support for custom reports.

- **Report subscriptions** allow for scheduled report generation and delivery to the specified recipients. You can apply different report filters and select report output format.

- **Automatic Backup and Recovery of Group Policy Objects**: the product supports recovery of unwanted Group Policy objects changes.

- **Long-term data storage**: allows for recreating the full audit trail of changes made to the monitored Active Directory environment and provides historical reporting for any specified period of time. Organizations can analyze any policy violations which occurred in the past, and maintain ongoing compliance with internal and external regulations.

- **Integration with SIEM systems**: the product can be integrated with multiple SIEM systems, including RSA enVision®, ArcSight® Logger™, Novell® Sentinel™, NetIQ® Security Manager™, IBM Tivoli® Security Information and Event Manager™ and more. The product can also be configured to feed data to Microsoft System Center Operations Manager, thus providing organizations that use SCOM with fully automated Active Directory auditing and helping protect these investments.

2.2. Product Workflow

A typical NetWrix Group Policy Change Reporter data collection and reporting workflow is as follows:

1. An administrator configures a Managed Object and sets the parameters for automated data collection and reporting.

2. NetWrix Group Policy Change Reporter monitors AD domain and collects audit data on changes and AD configuration snapshots. Audit data is written to a local file-based storage, referred to as the Audit Archive.

3. The product emails Change Summaries to the specified recipients daily at 3:00 AM by default.

4. If the integration with SCOM is enabled, the product will record all changes to the event log.

5. If the Reports functionality is enabled and configured, data is imported from the Audit Archive to a dedicated SQL database. Reports based on audit data can be viewed via NetWrix Enterprise Management Console or in a web browser.

2.3. Product Editions

NetWrix Group Policy Change Reporter is available in two editions: Freeware and Enterprise. The Freeware Edition can be used by companies or individuals for an unlimited period of time. The Enterprise Edition can be evaluated free of charge for 20 days.

Note: Licenses for different modules of the NetWrix Active Directory Change Reporter pack (consisting of NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter) have to be purchased separately.

Table 1: below outlines the difference between the NetWrix Group Policy Change Reporter editions:

Table 1: NetWrix Group Policy Change Reporter Editions

Feature	Freeware Edition	Enterprise Edition
WHO, WHEN and WHERE fields for every change	No	Yes
The before and after values for every change	No	Yes
SSRS-based Reports, with filtering, grouping and sorting, and dozens of predefined report templates	No	Yes
Custom reports	No	Yes Create manually, or order from NetWrix
Predefined reports for SOX, HIPAA, GLBA, and FISMA compliance	No	Yes
Report Subscriptions	No	Yes
Integration with Microsoft System Center Operations Manager Pack (SCOM) (via NetWrix SCOM Management Pack for Group Policy Change Reporter)	No	Yes
Long-term archiving of audit data	No Data is only stored for 4 days	Yes Any period of time
Daily Change Summary email reflecting the changes made during the last day	Yes	Yes
A single installation handles multiple Managed Objects, each with its own individual settings	No	Yes
Integrated interface for all NetWrix products, which provides centralized configuration and settings management	No	Yes
Reports can be viewed directly from NetWrix Enterprise Management Console	No	Yes

Technical Support	Support Forum Knowledge Base	Full range of options: Phone, email, submission of support tickets, Support Forum, Knowledge Base
Licensing	Free of charge	Per server Request a quote

3. INSTALLING NETWRIX EXCHANGE CHANGE REPORTER

3.1 Installation Prerequisites

NetWrix Group Policy Change Reporter can be installed on any computer in the monitored domain, or in a trusted domain.

3.1.1. Hardware Requirements

Before installing NetWrix Group Policy Change Reporter, make sure that your hardware meets the following requirements:

Table 2: NetWrix Group Policy Change Reporter Hardware Requirements

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2GHz	Intel Core 2 Duo 2x 64 bit, 2GHz
Memory	512MB RAM	4GB RAM
Disk space	• 50MB physical disk space for product installation. • Additional space is required for the Audit Archive and depends on the number of AD objects and changes per day.	Two physical drives with a total of 50GB free space

3.1.2. Software Requirements

Before installing NetWrix Group Policy Change Reporter, make sure that your software meets the following requirements:

Table 3: NetWrix Group Policy Change Reporter Software Requirements

Component	Requirement
Operating System	• Windows XP SP2 (both 32-bit and 64-bit systems) and above
Additional software	• .NET Framework 2.0, 3.0 or 3.5 • Windows Installer 3.1 or later • Microsoft Management Console 3.0 or later • Group Policy Management Console • IIS 5.1 or later (IIS 7.0 or later requires IIS 6 Management Compatibility – all components)*

* **Only required if you are going to use SQL Server 2005 to store audit data.**

3.1.3. Supported Environments

This section lists the requirements to the monitored domain:

• Active Directory (domain and forest functional levels)

• Domain controller OS versions:

o   Windows Server 2000 SP4

o   Windows Server 2003 SP2

o   Windows Server 2003 R2 SP2

o   Windows Server 2008 SP2

o   Windows Server 2008 R2 SP1

o   Windows Server 2012

3.2. Installing NetWrix Group Policy Change Reporter

Procedure 1.   To install NetWrix Group Policy Change Reporter

1.   [Download](#) the NetWrix Active Directory Change Reporter pack.

2.   Run the setup package called adcrfree_setup.msi.

3.   Follow the instructions of the installation wizard. When prompted, accept the license agreement and specify the installation folder.

4.   On the last step, click **Finish** to complete the installation.

Shortcuts of all products forming the NetWrix Active Directory Change Reporter pack will be added to your **Start** menu.

> **Note:**   NetWrix Exchange Change Reporter runs as a scheduled task, therefore it is not necessary to keep the program open once it has been configured.

4. CONFIGURING TARGET AD DOMAIN

Successful change monitoring requires a certain configuration of the audit settings in the monitored Active Directory domain. If audit is not configured properly, your change reports may contain errors and incomplete audit data. For example, you can receive a report containing the "System" value instead of an account name in the "Who changed" column.

Therefore, you need to verify and, if necessary, adjust your audit settings prior to using NetWrix Group Policy Change Reporter. You can configure audit automatically through the Active Directory Audit Configuration Wizard. If you wish to configure audit manually, refer to NetWrix Active Directory Change Reporter Installation and Configuration Guide for the detailed step-by-step instructions.

Procedure 2.   To configure target AD domain automatically

1. Launch the Active Directory Audit Configuration wizard: navigate to **Start → All Programs → NetWrix → Group Policy Change Reporter → Active Directory Audit Configuration**.

   Note: For the wizard to work properly, you must run it under a Domain admin or an Enterprise admin account.

2. On the first step of the wizard, specify a name of the domain where you want to configure audit settings:

   *Figure 1:   Audit Configuration Wizard: Select the Domain*

3. Click **Next**. In the dialog that appears, select the effective policy that is currently applied to the domain controllers and that is subject to change, and click **OK**:

   Figure 2:   Audit Configuration Wizard: Select the Effective Policy
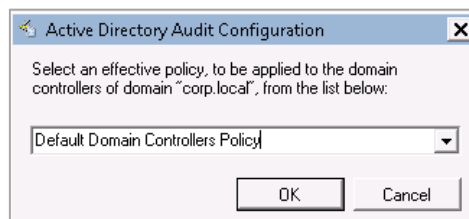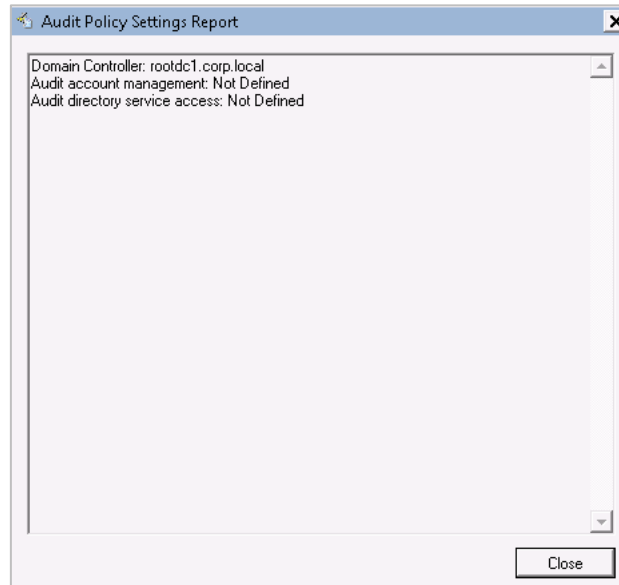

4. On the next step, specify the account that will be used by the product to collect data from the monitored domain.

Figure 3:   Audit Configuration Wizard: Specify the Data Processing Account
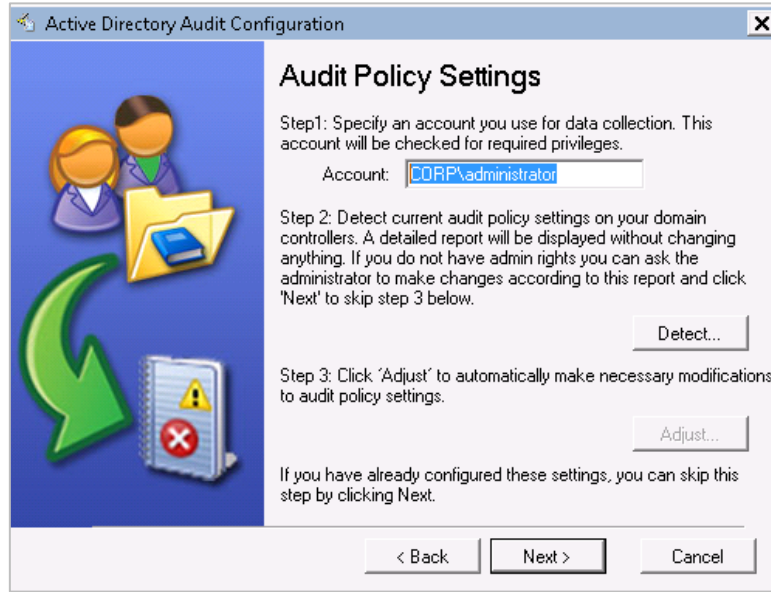
5.   Click the **Detect** button. A report will be displayed showing your current audit policy settings in the monitored domain:

Figure 4:   Audit Policy Settings Report

6.   Close the report and click the **Adjust** button. Your audit policy settings and the Data Processing Account permissions will be adjusted automatically.

7.   On the next step, repeat these operations for the object-level audit settings. Object-level auditing must be configured so that the "Who" and "When" information appears in audit reports:

Figure 5:   Audit Configuration Wizard: Adjust the Object-Level Audit Settings

8.   On the next step, repeat these operations for your Security event log retention settings. On clicking the **Adjust** button, the size of your Security event log will be set to 300 MB, and the event log auto backup will be enabled if needed:

Figure 6:   Audit Configuration Wizard: Adjust the Event Log Retention Settings

9.   Skip the Exchange Server Administrator Audit Logging Settings step of the wizard (it is only required to adjust this settings for the NetWrix Exchange Change Reporter Module if the monitored AD domain has an Exchange organization running Microsoft Exchange Server 2010).

10. On the last step, review your settings and exit the wizard.

5. CONFIGURING MANAGED OBJECT

In NetWrix Group Policy Change Reporter, a Managed Object is an Active Directory domain that is monitored for changes.

Procedure 3. To create and configure a Managed Object

1. In NetWrix Enterprise Management Console click the **Managed Objects** node in the left pane. The Managed Objects page will be displayed:

Figure 7:   The Managed Objects Page
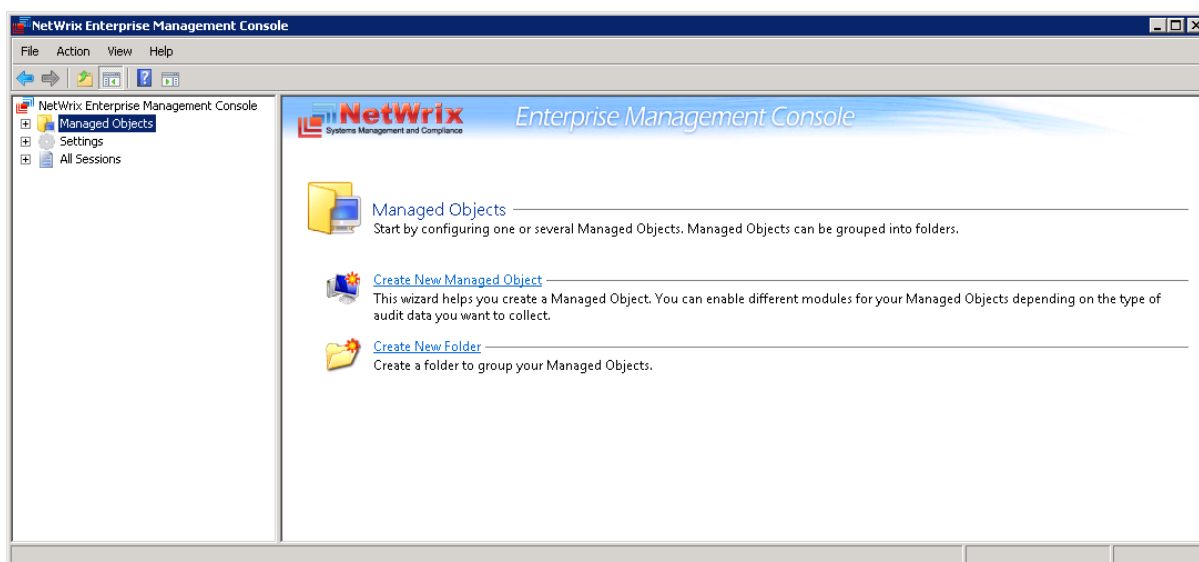
2. In the right pane, click **Create New Managed Object**. Alternatively, right-click the **Managed Objects** node and select **New Managed Object** from the pop-up menu to start the **New Managed Object** wizard.

3. On the **Select Managed Object Type** step, select **Domain** as the Managed Object type and click **Next**.

   Note: If you have installed other NetWrix products before, the list of Managed Object types may contain several options.

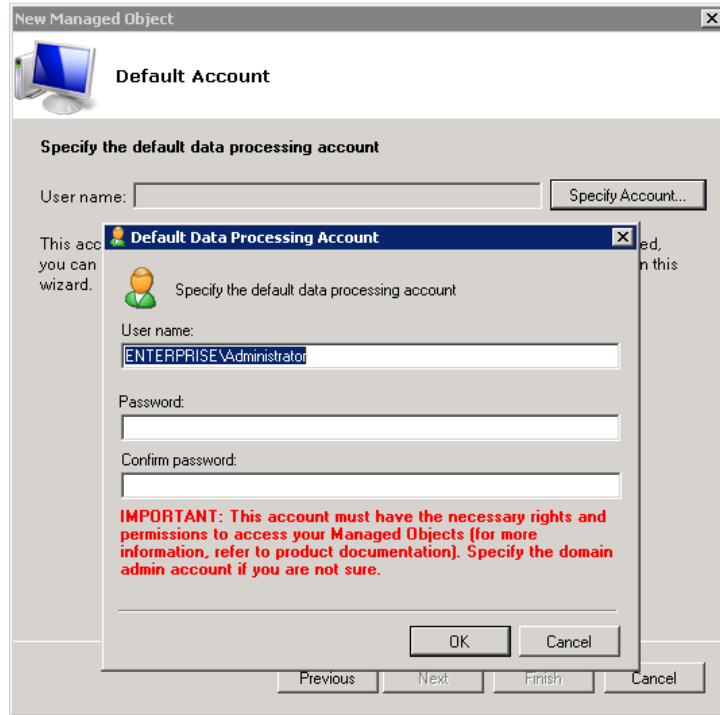*Figure 8:   New Managed Object: Select Managed Object Type*
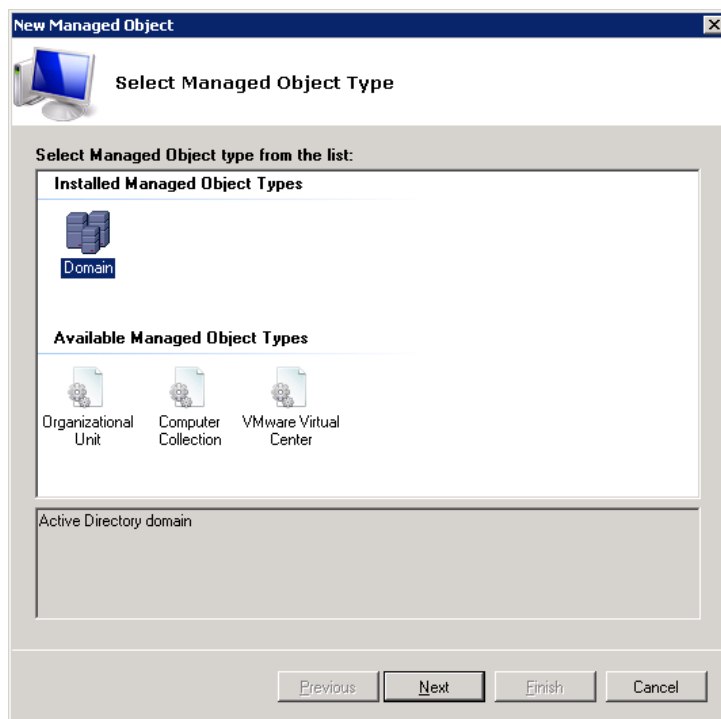
4. On the **Default Account** step, click the **Specify Account** button.

    Note: If you have installed other NetWrix change reporting products before and specified the default Data Processing Account and the email settings on their configuration, the **Default Account** and **Configure Email Settings** steps of the wizard will be omitted.

5. In the dialog that opens, specify the default Data Processing Account (in the domain_name\account_name format) that will be used by NetWrix Exchange Change Reporter for data collection. This account must have the following rights:

    • Local administrator on the computer where NetWrix Exchange Change Reporter is installed.

    • Domain administrator in the monitored domain. Alternatively, it must have the "Manage auditing and security log" right enabled.

    • If this account will be used to access the SQL database with audit data, it must also belong to the target database owner (dbo) role.

    • If your monitored servers run Exchange 2010, the Data Processing Account must also belong to the Organization Management or the Records Management group. Alternatively, the account must be assigned the Audit Logs role.

    Note: This must be the same account you have specified when configuring audit as described in Procedure 2 To configure target AD domain automatically.
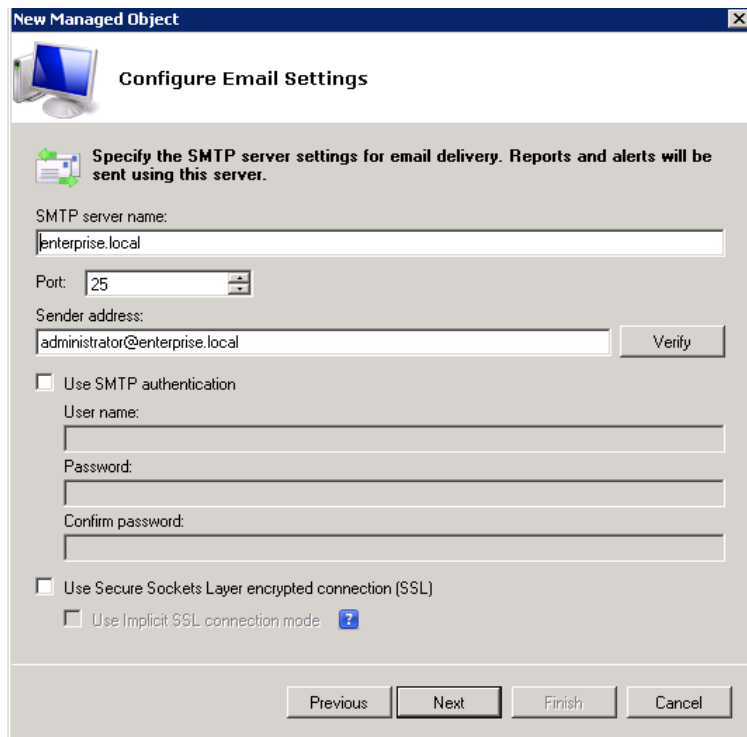
Figure 9:   New Managed Object: Default Account

Click **OK** to continue and then **Next**.

6. On the **Configure Email Settings** step, specify the email settings that will be used for the Change Summary delivery:

*Figure 10:   New Managed Object: Configure Email Settings*

The following parameters must be specified:

Table 4:   Email Settings Parameters

Parameter	Description
SMTP server name	Enter your SMTP server name.
Port	Enter your SMTP server port number.
Sender address	Enter the address that will appear in the "From" field in reports and Change Summaries. To check the email address, click **Verify**. The system will send a test message to the specified address and will inform you if any problems are detected.
Use SMTP authentication	Select this check box if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this check box if your SMTP server requires SSL to be enabled.
Use Implicit SSL connection mode	Select this check box if the implicit SSL mode is used, which means that SSL connection is established before any meaningful data is sent.

6. On the **Specify Domain Name** step, specify your domain name in the FQDN format:
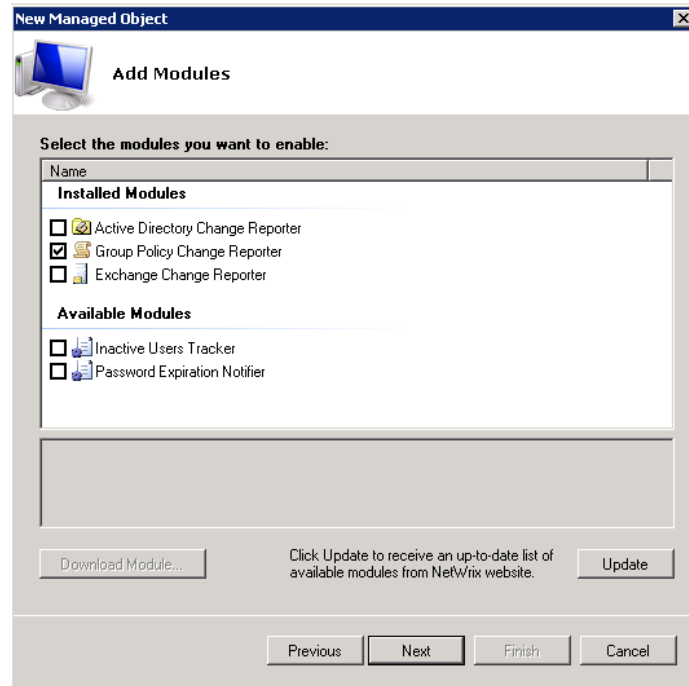
Figure 11:   New Managed Object: Specify Domain Name
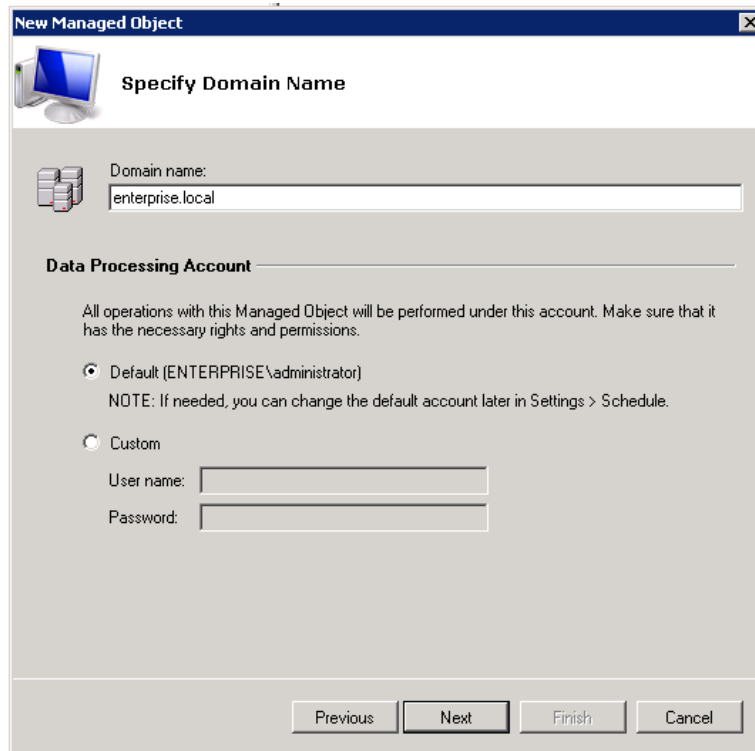
Make sure that the **Default** option is selected under **Data Processing Account** and click **Next** to continue.

7. On the **Add Modules** step, make sure that NetWrix Exchange Change Reporter is selected under **Installed Modules**:

*Figure 12:   New Managed Object: Add Modules*

Note: If you have installed other NetWrix change reporting products before, the list of **Installed Modules** may contain several options.

On this step, under **Available Modules**, there is a list of other NetWrix products that can have domain as a Managed Object type. To get more information on these products and download them, select the corresponding check box, or click a module and then click the **Download Module** button. You will be redirected to the product website page.

8. On the **Reports Settings** step, clear the **Enable Reports** check box:

Figure 13:   New Managed Object: Reports Settings
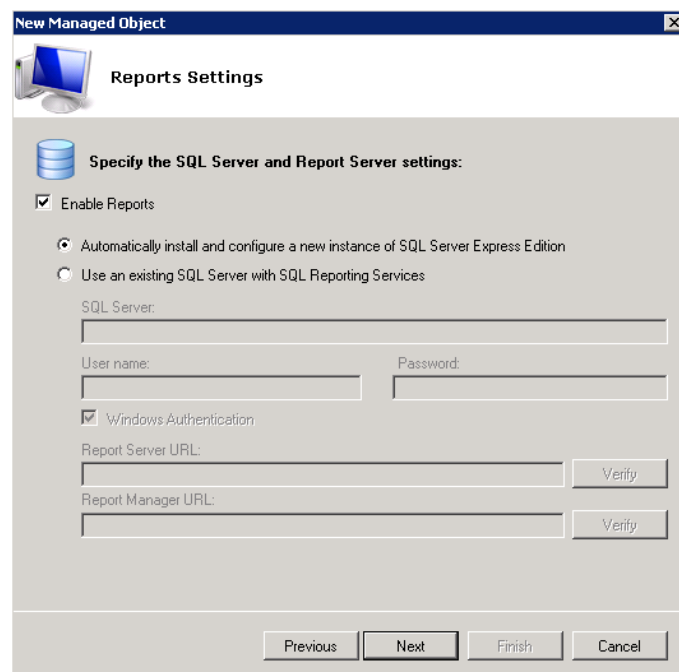
> **Note:**   The Reports functionality is not covered in this guide, as it only touches upon the basic product features. For instructions on how to configure and view SSRS-based reports, refer to NetWrix Active Directory Change Reporter Administrator's Guide.

9. On the **Specify Group Policy Change Reporter Change Summary Recipients** step, click the **Add** button to specify the Change Summary recipient(s):

*Figure 14:   New Managed Object: Specify Change Summary Recipients*
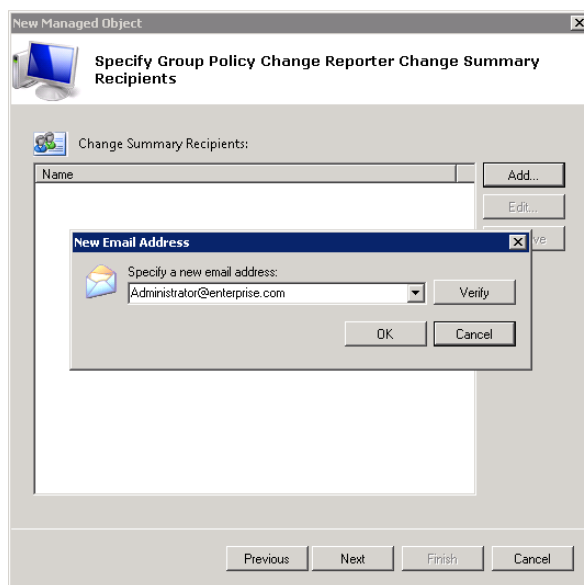
It is recommended to click the **Verify** button. The system will send a test message to the specified email address and will inform you if any problems are detected. Click **OK** to save the changes and then click **Next** to continue. If your audit settings have not been configured properly, you will receive a warning message. For detailed instructions on how to configure audit in your monitored Active Directory domain, refer to Chapter 6. Configuring Target Environment of NetWrix Active Directory Change Reporter Installation and Configuration Guide.

10. On the last step, review your Managed Object settings and click **Finish.** A confirmation message will be displayed.

The newly created Managed Object will appear under the Managed Objects node, and its details will be displayed in the right pane:

Figure 15:   The Managed Object Page
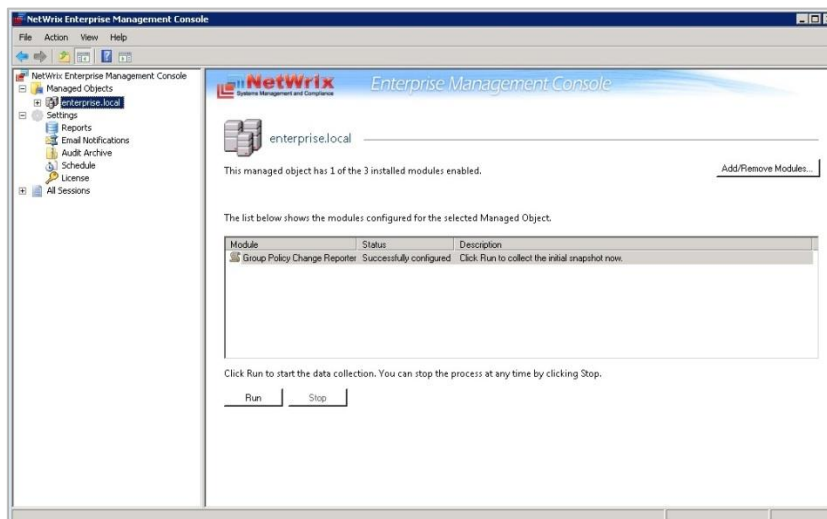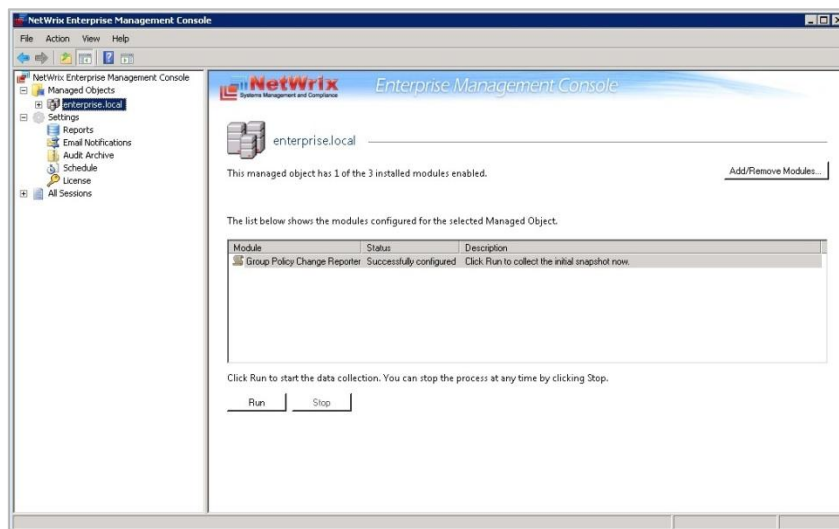
6. COLLECTING THE INITIAL SNAPSHOT

When you have added and configured a Managed Object, NetWrix Group Policy Change Reporter starts collecting data on changes that occurred in the target domain, and writes it to the Audit Archive, a local file-based storage. When the first data collection is performed, the initial snapshot of your monitored domain current state is created. NetWrix Group Policy Change reporter uses this information as a benchmark to generate change reports.

After you have configured a Managed Object, you can either wait for the system to run data collection automatically, or launch it manually from NetWrix Enterprise Management Console.

Procedure 4.   To launch a data collection task

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** node, and select your Managed Object.
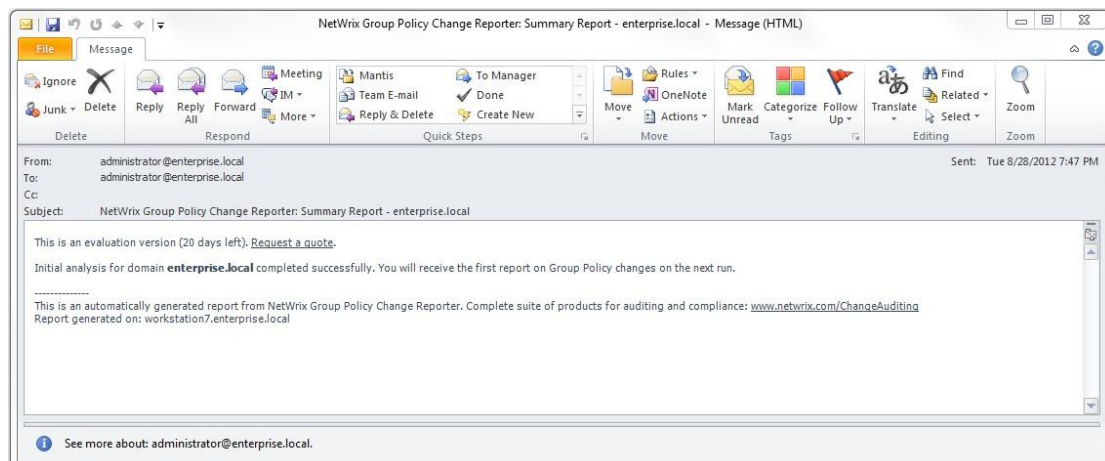
2. In the details pane, click **Run**.

Figure 16:   The Managed Object Page

> **Note:**   Depending on the size of your monitored environement, creation of an initial snapshot may take quite long.

After the initial data collection task has completed, an email notification is sent to the specified recipient(s) like in the example below:

Figure 17:   Initial Analysis Notification

7. MONITORING YOUR TARGET DOMAIN FOR CHANGES

7.1. Making Test Changes

Now that the product has collected a snapshot of your Managed Object current state, you can make test changes to your Group Policy configuration to see how these changes will be reported.

For example, you can change Password Policy settings.

> **Note:** Before making any test changes to your domain, ensure that you have the domain administrator's rights, and that the changes conform to your security policy.

7.2. Receiving a Change Summary

After you have made changes to the monitored domain, you can see how these changes are reported.

By default, NetWrix Group Policy Change Reporter emails a Change Summary to the specified recipient(s) daily at 3:00 AM. The Change Summary lists all changes that occurred in the last 24 hours and provides the WHAT, WHO, WHERE and WHEN details for every change.

If you do not wait until a scheduled Change Summary delivery, you can generate it manually. To do this, launch a data collection task manually as described in Procedure 4 To launch a data collection task earlier in this guide. After the task has completed, a Change Summary will be generated and sent to the specified email address:

Figure 18:   Change Summary Example
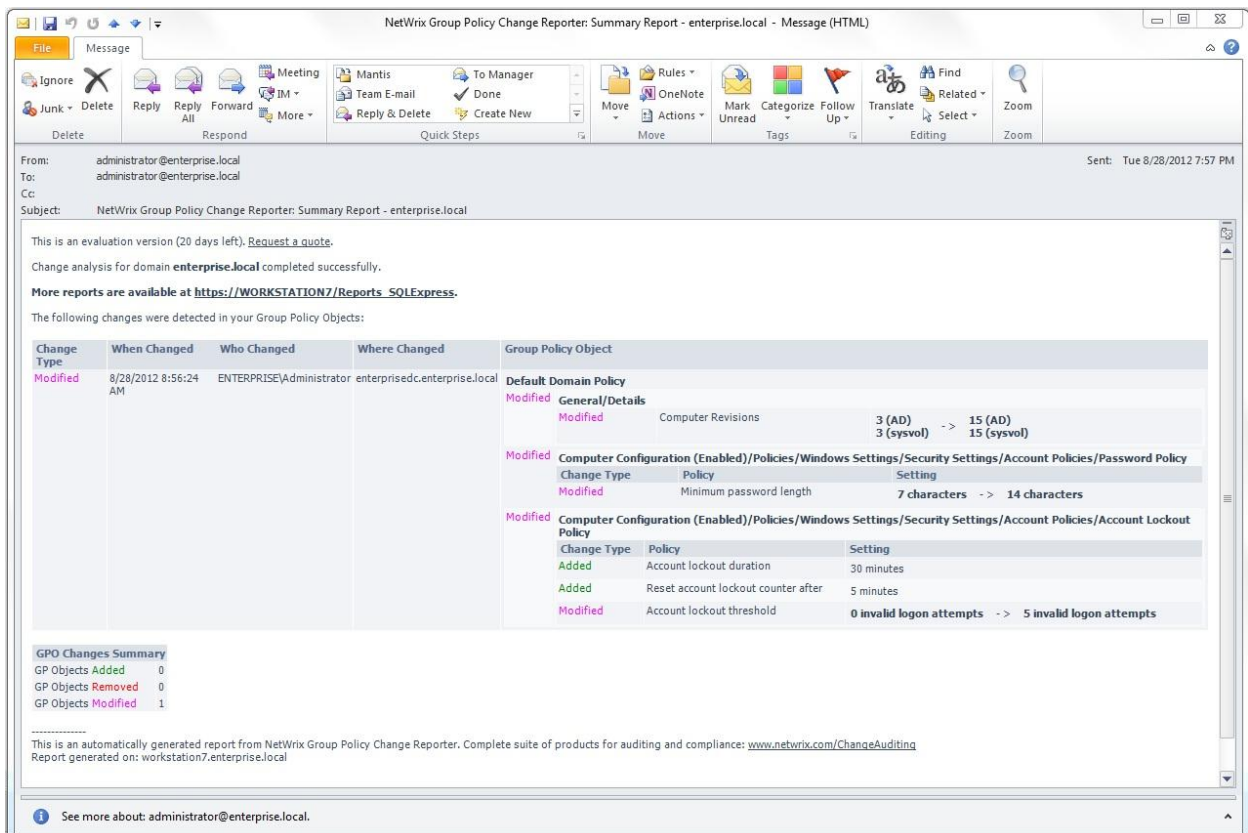
The above Change Summary example reflects the changes made to Default Domain Policy.

The Change Summary provides the following information for each change:

Table 5:   Change Summary Fields

Parameter	Description
Change Type	Shows the type of action that was performed on the Exchange object. The values are: • Added • Removed • Modified
When Changed	Shows the exact time when the change occurred.
Who Changed	Shows the name of the account under which the change was made.
Where Changed	Shows the name of the domain controller where the change was made.
Group Policy Object	Shows the Group Policy Object that was changed with details on its "before" and "after" values.

A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support the NetWrix Exchange Change Reporter:

Table 6: Product Documentation

Document Name	Overview
NetWrix Group Policy Change Reporter Quick-Start Guide	The current document. It is intended for the product evaluation purposes. The document provides instructions on how to start working with the program quickly and easily.
NetWrix Group Policy Change Reporter Administrator's Guide	Provides a detailed explanation of the NetWrix Group Policy Change Reporter features and step-by-step instructions on how to configure and use the product.
NetWrix Group Policy Change Reporter User Guide	Provides the information on different NetWrix Group Policy Change Reporter reporting capabilities, lists all available reports and explains how they can be viewed and interpreted.
NetWrix Active Directory Change Reporter Installation and Configuration Guide.	Provides detailed instructions on how to install and configure NetWrix Exchange Change Reporter.
NetWrix Active Directory Change Reporter Administrator's Guide	Provides a detailed explanation of the NetWrix Active Directory Change Reporter features and step-by-step instructions on how to configure and use the product.
NetWrix Active Directory Change Reporter Release Notes	Contains a list of the known issues that customers may experience with NetWrix Active Directory Change Reporter 7.2, and suggests workarounds for these issues.
NetWrix Active Directory Change Reporter Freeware Edition Quick-Start Guide	Provides instructions on how to install, configure and use NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter Freeware Edition.
Troubleshooting Incorrect Reporting of the "Who Changed" Parameter	Step-by-step instructions on how to troubleshoot incorrect reporting of the 'who changed' parameter.
Installing Microsoft SQL Server and Configuring the Reporting Services	This technical article provides instructions on how to install Microsoft SQL Server 2005/2008 R2/2012 Express and configure the Reporting Services.
How to Subscribe to SSRS Reports	This technical article explains how to configure a subscription to SSRS reports using the Report Manager.
Integration with Third Party SIEM Systems	This article explains how to enable integration with third-party Security Information and Event Management (SIEM) systems.