

# NETWRIX GROUP POLICY CHANGE REPORTER

# **QUICK-START GUIDE**

Product Version: 7.2 November 2012

Copyright © 2012 NetWrix Corporation. All Rights Reserved.

#### 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.

© 2012 NetWrix Corporation.

All rights reserved.

# Table of Contents

| 1. | INTRODUCTION   |
|----|--|
|    | 1.1. Overview  |
|    | 1.2. How This Guide is Organized 4                   |
|    | 1.3. Free Pre-Sales Support 4                        |
| 2. | PRODUCT OVERVIEW                                     |
|    | 2.1. Key Features and Benefits                       |
|    | 2.2. Product Workflow                                |
|    | 2.3. Product Editions                                |
| 3. | INSTALLING NETWRIX EXCHANGE CHANGE REPORTER          |
|    | 3.1 Installation Prerequisites                       |
|    | 3.1.1. Hardware Requirements                         |
|    | 3.1.2. Software Requirements                         |
|    | 3.1.3. Supported Environments                        |
|    | 3.2. Installing NetWrix Group Policy Change Reporter |
| 4. | Configuring Target AD Domain 11                      |
| 5. | CONFIGURING MANAGED OBJECT                           |
| 6. | COLLECTING THE INITIAL SNAPSHOT                      |
| 7. | MONITORING YOUR TARGET DOMAIN FOR CHANGES            |
|    | 7.1. Making Test Changes21                           |
|    | 7.2. Receiving a Change Summary                      |
| A  | Appendix: Related Documentation                      |

# **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 <u>NetWrix Group Policy Change Reporter Administrator's Guide</u>.

## 1.2. How This Guide is Organized

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

- Chapter <u>1 Introduction</u> is the current chapter. It explains the purpose of this document, defines its audience and outlines its structure.
- Chapter <u>2 Product Overview</u> 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 <u>3 Installing NetWrix Exchange Change Reporter</u> lists hardware and software requirements, and instructions on the installation of NetWrix Group Policy Change Reporter.
- Chapter <u>4 Configuring Target AD Domain</u> explains how to adjust audit settings in your target AD domain and prepare it for monitoring.
- Chapter <u>5 Configuring Managed Object</u> explains how to configure a Managed Object, which is an AD domain with Group Policy configuration that you monitor for changes.
- Chapter <u>6 Collecting the Initial Snapshot</u> explains how to run data collection to perform the initial analysis of your domain current state.
- Chapter <u>7 Monitoring Your Target Domain for Changes</u> provides instructions on how to make test changes to the monitored domain and see how they are reported by the product.
- <u>Appendix: Related Documentation</u> 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, <u>contact NetWrix</u> <u>support specialists</u>.

# 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 <u>Summary: Limitations of Native Active Directory Auditing Tools</u>.

Powered by the <u>NetWrix AuditAssurance</u><sup>™</sup> 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. <u>AuditAssurance</u><sup>™</sup> 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.

<u>Table 1:</u> below outlines the difference between the 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,<br>grouping and sorting, and dozens of<br>predefined report templates   | No                                      | Yes   |
| Custom reports  | No                                      | Yes<br>Create manually, or<br><u>order from NetWrix</u> |
| Predefined reports for SOX, HIPAA, GLBA, and FISMA compliance   | No                                      | Yes   |
| Report Subscriptions  | No                                      | Yes   |
| Integration with Microsoft System Center<br>Operations Manager Pack (SCOM) (via<br><u>NetWrix SCOM Management Pack for</u><br><u>Group Policy Change Reporter</u> ) | No                                      | Yes   |
| Long-term archiving of audit data   | No<br>Data is only stored for<br>4 days | Yes<br>Any period of time                               |
| Daily Change Summary email reflecting the changes made during the last day  | Yes                                     | Yes   |
| A single installation handles multiple<br>Managed Objects, each with its own<br>individual settings   | No                                      | Yes   |
| Integrated interface for all NetWrix<br>products, which provides centralized<br>configuration and settings management   | No                                      | Yes   |
| Reports can be viewed directly from<br>NetWrix Enterprise Management Console  | No                                      | Yes   |

 Table 1:
 NetWrix Group Policy Change Reporter Editions

| Technical Support | <u>Support Forum</u><br><u>Knowledge Base</u> | Full range of options:<br>Phone, email,<br><u>submission of support</u><br><u>tickets, Support</u><br>Forum, Knowledge<br><u>Base</u> |
|-------------------|---|---|
| Licensing         | Free of charge                                | Per server<br><u>Request a quote</u>  |

# 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:

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

Table 2: NetWrix Group Policy Change Reporter Hardware Requirements

#### 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    | <ul> <li>Windows XP SP2 (both 32-bit and 64-bit<br/>systems) and above</li> </ul>                                     |
| Additional software | <ul> <li>.NET Framework <u>2.0</u>, <u>3.0</u> or <u>3.5</u></li> <li>Windows Installer 3.1 or later</li> </ul>       |
|                     | <ul> <li>Microsoft Management Console 3.0 or later</li> </ul>   |
|                     | Group Policy Management Console   |
|                     | <ul> <li>IIS 5.1 or later (IIS 7.0 or later requires IIS 6<br/>Management Compatibility - all components)*</li> </ul> |

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. <u>Download</u> 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 <u>NetWrix Active Directory Change Reporter Installation and Configuration Guide</u> for the detailed step-by-step instructions.

#### Procedure 2. To configure target AD domain automatically

 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

| 🐔 Active Directory Audi                                    | t Configuration                                       | ×           |
|--|---|-------------|
| Select an effective policy,<br>controllers of domain "corp | to be applied to the do<br>blocal", from the list bel | main<br>ow: |
| Default Domain Controller                                  | s Policy  | •           |
|  | ОК  | Cancel      |

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:

| 5 Audit Policy Settings Report  | ×       |
|---|---------|
| Domain Controller: rootdc1.corp.local<br>Audit account management: Not Defined<br>Audit directory service access: Not Defined | <u></u> |
|   |         |
|   |         |
|   |         |
|   |         |
|   |         |
|   |         |
|   |         |
|   | -       |
|   | Close   |

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

| 🐔 Active Directory Audit Configuration 🛛 🗙 |  |  |  |  |
|--|--|--|--|--|
|  | Event Log Retention Settings   |  |  |  |
|  | Step 1: Detect current event log capacity and retention settings.<br>A detailed report will be displayed without changing anything. If<br>you do not have admin rights you can ask the administrator to<br>make changes as per the documentation and click 'Next' to skip<br>step 2 below. |  |  |  |
|  | Detect Step 2: Click 'Adjust' to automatically make necessary modifications to event log retention settings. Adjust  |  |  |  |
| ∕∕ ⊗,                                      | If you have already configured these settings, you can skip this step by clicking Next.  |  |  |  |
|  | < Back Next > Cancel   |  |  |  |

- 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

| 률 NetWrix Enterprise Management Consol   |   |  |  |  |  |
|--|---|--|--|--|--|
| Tile Action View Help  |   |  |  |  |  |
| 🗇 🔿 🙍 📊 👔 🖬  |   |  |  |  |  |
| <ul> <li>WetWrix Enterprise Management Console</li> <li>Managed Objects</li> <li>Settings</li> <li>All Sessions</li> </ul> | Enterprise Management Console   |  |  |  |  |
|  | Managed Objects —<br>Start by configuring one or several Managed Objects. Managed Objects can be grouped into folders.  |  |  |  |  |
|  | Create New Managed Object<br>This wizard helps you create a Managed Object. You can enable different modules for your Managed Objects depending on the type of<br>audit data you want to collect. |  |  |  |  |
|  | Create New Folder Create a folder to group your Managed Objects.  |  |  |  |  |
|  |   |  |  |  |  |
|  |   |  |  |  |  |
|  |   |  |  |  |  |

- 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.

| Select Manag<br>Installed Ma | ed Object ty<br>anaged Obje | pe from the list:<br>ct Types |      |  |
|------------------------------|-----------------------------|-------------------------------|------|--|
| Domain                       |                             |                               |      |  |
| Available M                  | anaged Obj                  | ect Types                     |      |  |
| Organizational<br>Unit       | Computer<br>Collection      | William Wirtual<br>Center     |      |  |
| Active Directory             | domain                      |                               | <br> |  |
|                              |                             |                               |      |  |

New Managed Object: Select Managed Object Type

Figure 8:

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.
- In the dialog that opens, specify the default Data Processing Account (in the 5. 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.

| New Manage                     | ed Object                                  |
|--------------------------------|--|
|                                | Default Account                            |
| Specify I                      | the default data processing account        |
| User nan                       | ne: Specify Account                        |
| This acc<br>you can<br>wizard. |  |
|                                | OK Cancel      Previous Next Finish Cancel |

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

| New Managed Object  | ×       |
|---|---------|
| Configure Email Settings  |         |
| Specify the SMTP server settings for email delivery. Reports and alerts sent using this server. | will be |
| SMTP server name:   |         |
| lenterprise.local   |         |
| Port: 25  |         |
| Sender address:   |         |
| administrator@enterprise.local  | Verify  |
|   |         |
| liser name:   |         |
|   |         |
| ,<br>Password:  |         |
|   |         |
| Confirm password:   |         |
|   |         |
| Use Secure Sockets Layer encrypted connection (SSL)   |         |
| 🔲 Use Implicit SSL connection mode 🛛 👔  |         |
|   |         |
| Previous Next Finish  | Cancel  |

The following parameters must be specified:

| Parameter  | Description  |
|--|--|
| SMTP server name                                       | Enter your SMTP server name.   |
| Port   | Enter your SMTP server port number.  |
|  | Enter the address that will appear in the "From" field in reports and Change Summaries.  |
| Sender address   | To check the email address, click <b>Verify</b> . 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<br>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.                       |

Table 4: Email Settings Parameters

6. On the Specify Domain Name step, specify your domain name in the FQDN format:

Figure 11: New Managed Object: Specify Domain Name

| New Manag | jed Object  | x |
|-----------|---|---|
|           | Specify Domain Name   |   |
| đ         | Domain name:<br>enterprise.local  |   |
| Data P    | rocessing Account   |   |
| All<br>ha | operations with this Managed Object will be performed under this account. Make sure that it<br>s the necessary rights and permissions.<br>Default (ENTERPRISE\administrator)<br>NOTE: If needed, you can change the default account later in Settings > Schedule. |   |
| c         | Custom  |   |
|           | User name:  |   |
|           | Password:   |   |
|           | ,   |   |
|           |   |   |
|           |   |   |
|           |   |   |
|           | Previous Next Finish Cancel   |   |

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  |
|---|
| New Managed Object  |
| Add Modules   |
| Select the modules you want to enable:  |
| Name  |
| Installed Modules   |
| Active Directory Change Reporter     Since Policy Change Reporter     Active Directory Change Reporter     Active Directory Change Reporter     Available Modules |
| Inactive Users Tracker     Imactive Users Tracker     Imactive Users Tracker     Imactive Users Tracker   |
|   |
| Download Module Click Update to receive an up-to-date list of available modules from NetWrix website. Update  |
| Previous Next Finish Cancel   |

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

| New Ma | anaged Object   | ×    |
|--------|---|------|
| Ą      | Reports Settings  |      |
|        | Specify the SQL Server and Report Server settings:  |      |
| 💌 Er   | nable Reports   |      |
| œ      | $^\circ$ Automatically install and configure a new instance of SQL Server Express Edition |      |
| 0      | Use an existing SQL Server with SQL Reporting Services                                    |      |
|        | SQL Server:   |      |
|        | ]   |      |
|        | User name: Password:  | _    |
|        |   |      |
|        | Windows Authentication  |      |
|        | Heport Server URL:  | iu I |
|        | Report Manager URL:   |      |
|        | Verif   | y I  |
|        |   |      |
|        |   |      |
|        |   |      |
|        | Previous Next Finish Cano   | el   |

- **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 <u>NetWrix Active Directory Change Reporter Administrator's Guide</u>.
- 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

| New Manage | d Object 🛛 🗶   |
|------------|--|
|            | Specify Group Policy Change Reporter Change Summary<br>Recipients                                    |
| C Name     | Add Edit w Email Address Specify a new email address: Administrator@enterprise.com Uterify UK Cancel |
|            |  |
|            | Previous Next Finish Cancel  |

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 <u>NetWrix Active Directory</u> <u>Change Reporter Installation and Configuration Guide</u>.

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:

|   | ole   |                             |  |                    |
|---|---|-----------------------------|--|--------------------|
| File Action View Help   |   |                             |  |                    |
| (= =) 2 🗊 🖬 🖬   |   |                             |  |                    |
| NetWrix Enterprise Management Console     Managed Objects     Optimize_local     Settions | In NetWrix<br>Systeme Management and Compliance | Enterprise I                | lanagement Console                             |                    |
| Email Notifications   | enterprise.loca                                 | (                           |  |                    |
| Schedule     Schedule     Schedule     Sessions   | This managed object has 1 of                    | the 3 installed modules er  | abled.   | Add/Hemove Modules |
|   | The list below shows the mode                   | ules configured for the sel | ected Managed Object.                          |                    |
|   | Module  | Status                      | Description                                    | 1                  |
|   | Group Policy Change Report                      | er Successfully configured  | Click Run to collect the initial snapshot now. |                    |
|   |   |                             |  |                    |
|   | Click Run to start the data coll Run Stop       | ection. You can stop the p  | rocess at any time by clicking Stop.           |                    |

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.

| 🖉 NetWrix Enterprise Management Console   |  |                          |  | _ 🗆 🗙 |
|---|--|--------------------------|--|-------|
| File Action View Help   |  |                          |  |       |
| 💠 🧼 🖄 📅 🛛 📅   |  |                          |  |       |
| NetWrix Enterprise Management Console     Managed Objects     Settings     Settings     Reports     Email NetRicitons     Email NetRicitons | Event Management and Complexes                                   | Enterprise I             | Management Console                             |       |
| Audi Archive     Audi Archive     Audi Archive     Dicense     All Sessions   | This managed object has 1 of the The list below shows the module | Add/Remove Modules       |  |       |
|   | Module   | Statur                   | Description                                    |       |
|   | Group Policy Change Reporter                                     | Successfully configured  | Click Run to collect the initial snapshot now. |       |
|   | Click Run to start the data collect                              | tion. You can stop the p | vracess at any time by clicking Stop.          |       |

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

|  | A CONTRACT OF A |  |  |                            |                                 | The second                   |             |                | 927 RE 20470 00 |      |   |
|--|---|--|--|----------------------------|---------------------------------|------------------------------|-------------|----------------|-----------------|------|---|
| Junk + Delete  | Reply Reply All Forward More *  | Mantis and American A | <ul> <li>➡ To Manager</li> <li>✓ Done</li> <li>➡ Create New</li> </ul> | Move                       | Rules *<br>OneNote<br>Actions * | Mark Unread                  | Categorize  | Follow<br>Up * | Translate       | Zoom |   |
| Delete   | Respond   | Quick S  | Steps  | <b>F</b> 2                 | Move                            |                              | Tags        | 5              | Editing         | Zoom |   |
| ibject: Netwrb   | x Group Policy Change Reporter: Summ  | ary Report - enterprise.ioo  | cal  |                            |                                 |                              |             |                |                 |      | ć |
| This is an evaluation<br>Initial analysis for do   | x Group Pointy Change Reporter: Summ<br>i version (20 days left). <u>Request a quot</u> -<br>omain <b>enterprise.local</b> completed suc  | e.<br>cessfully. You will receive f  | cai<br>the first report on Group                                       | Policy cha                 | nges on the nex                 | t run.                       |             |                |                 |      | C |
| This is an evaluation<br>Initial analysis for do<br><br>This is an automatica<br>Report generated on | x croup youry Change Reporter: Summ<br>version (20 days left). <u>Request a quot</u><br>omain <b>enterprise.Jocal</b> completed suc<br>ally generated report from NetWrix Gro<br>1: workstation7.enterprise.local   | any keport - enterprise of<br>å.<br>cessfully. You will receive f<br>up Policy Change Reporter   | the first report on Group<br>rr. Complete suite of pro                 | Policy cha<br>Jucts for au | nges on the nex                 | t run.<br>pliance: <u>ww</u> | w.netwrix.c | om/Chan        | geAuditing      |      |   |
| This is an evaluation<br>Initial analysis for do   | x uroup routy Change Reporter: Summ<br>version (20 days left). <u>Request a quot</u><br>omain <b>enterprise.local</b> completed suc<br>ally generated report from NetWrix Gro<br>workstation7.enterprise.local  | any keport - enkerprise.iod<br>å<br>cessfully. You will receive f<br>up Policy Change Reporter   | cai<br>the first report on Group<br>rr. Complete suite of pro          | Policy cha<br>Jucts for au | nges on the nex                 | t run.<br>pliance: <u>ww</u> | w.netwrix.c | om/Chan        | aeAuditina      |      |   |

# 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 <u>Procedure 4</u>. 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:

|                          | 👁 🗸 🗠   |   | NetWrix Group P   | olicy Change Re                  | eporter: Summar            | y Report - enter                                | prise.local - Message (HTN                                 | AL)   |                                    |
|--------------------------|---|---|---|----------------------------------|----------------------------|---|--|---|------------------------------------|
| ile Mes                  | ssage   |   |   |                                  |                            |   |  |   | 24                                 |
| Ignore 🗙<br>Junk + Delet | te Reply Reply<br>All   | Forward More *                                | Mantis     A       Amage: Amag | To Manager<br>Done<br>Create New | →<br>→<br>Move             | Pules ▼<br>MOneNote Actions ▼                   | Mark Categorize Follow<br>Unread • Up •                    | Translate<br>↓ Select →                             | Zoom                               |
| Delete                   | F   | Respond                                       | Quick Ste   | ps                               | Gi.                        | Move  | Tags 5   | Editing   | Zoom                               |
| m: ac<br>ac<br>iject: N  | dministrator@enterpri<br>dministrator@enterpris<br>letWrix Group Policy | se.local<br>se.local<br>Change Reporter: Summ | ary Report - enterprise.local   |                                  |                            |   |  |   | Sent: Tue 8/28/2012 7:5            |
|                          |   |   |   |                                  |                            |   |  |   |                                    |
| is is an evalu           | uation version (20 da   | ys left). <u>Request a quote</u>              | é.  |                                  |                            |   |  |   |                                    |
| iange analysi            | is for domain <b>enter</b>  | prise.local completed su                      | ccessfully.   |                                  |                            |   |  |   |                                    |
| ore reports              | are available at ht   | tps://WORKSTATION                             | //Reports SQLExpress.   |                                  |                            |   |  |   |                                    |
|                          |   | dia and care ballar (                         | the second s  |                                  |                            |   |  |   |                                    |
| s tollowing o            | changes were detecte  | a in your Group Policy C                      | bjects:   |                                  |                            |   |  |   |                                    |
| nange                    | When Changed  | Who Changed                                   | Where Changed   | Group Po                         | olicy Object               |   |  |   |                                    |
| pe                       |   |   |   | 1                                |                            |   |  |   |                                    |
| arried                   | 8/28/2012 8:56:24<br>AM   | ENTERPRISE(Administ                           | ator enterprisedc.enterprise  | e.local Default I                | Domain Policy              |   |  |   |                                    |
|                          |   |   |   | Modified                         | General/Deta               | ils   |  |   |                                    |
|                          |   |   |   |                                  | Modified                   | Computer F                                      | levisions  | 3 (AD) -> 15 (/<br>3 (sysyol) -> 15 (/              | AD)<br>sysyol)                     |
|                          |   |   |   | Modified                         |                            | 6 I. I.   | II Disks here i  | 5 (5)5101) IS (.                                    |                                    |
|                          |   |   |   | nouncu                           | Computer Cor               | Inguration (Ena                                 | abled)/Policies/Windows                                    | Settings/Security Setting                           | s/Account Policies/Password Policy |
|                          |   |   |   |                                  | Modified                   | Minimu  | m password length  | 7 characters  | 14 characters                      |
|                          |   |   |   | 11. 11. 1                        |                            |   |  | 7 characters ~ 7                                    | 14 characters                      |
|                          |   |   |   | Modified                         | Computer Cor<br>Policy     | figuration (Ena                                 | abled)/Policies/Windows                                    | Settings/Security Setting                           | s/Account Policies/Account Lockout |
|                          |   |   |   |                                  | Change Type                | Policy  | 9  | Setting   |                                    |
|                          |   |   |   |                                  |                            |   |  |   |                                    |
|                          |   |   |   |                                  | Added                      | Account locko                                   | ut duration 3  | 30 minutes  |                                    |
|                          |   |   |   |                                  | Added                      | Account locko<br>Reset account                  | ut duration 3<br>lockout counter after 5                   | 30 minutes<br>5 minutes                             |                                    |
|                          |   |   |   |                                  | Added<br>Added<br>Modified | Account locko<br>Reset account<br>Account locko | ut duration 3<br>lockout counter after 5<br>ut threshold 6 | 30 minutes<br>5 minutes<br>9 invalid logon attempts | -> 5 invalid lagon attampts        |

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:

| Parameter           | Description   |
|---------------------|---|
|                     | Shows the type of action that was performed on the Exchange object. The values are:             |
| Change Type         | • 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. |

Table 5:Change Summary Fields

## A APPENDIX: RELATED DOCUMENTATION

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

| Document Name  | Overview   |
|--|--|
| NetWrix Group Policy Change Reporter<br>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<br>Administrator's Guide                        | Provides a detailed explanation of the<br>NetWrix Group Policy Change Reporter<br>features and step-by-step instructions on how<br>to configure and use the product.   |
| <u>NetWrix Group Policy Change Reporter</u><br><u>User Guide</u>                     | Provides the information on different NetWrix<br>Group Policy Change Reporter reporting<br>capabilities, lists all available reports and<br>explains how they can be viewed and<br>interpreted.              |
| NetWrix Active Directory Change<br>Reporter Installation and Configuration<br>Guide. | Provides detailed instructions on how to install and configure NetWrix Exchange Change Reporter.   |
| NetWrix Active Directory Change<br>Reporter Administrator's Guide                    | Provides a detailed explanation of the<br>NetWrix Active Directory Change Reporter<br>features and step-by-step instructions on how<br>to configure and use the product.                                     |
| NetWrix Active Directory Change<br>Reporter Release Notes                            | Contains a list of the known issues that<br>customers may experience with NetWrix<br>Active Directory Change Reporter 7.2, and<br>suggests workarounds for these issues.                                     |
| NetWrix Active Directory Change<br>Reporter Freeware Edition Quick-Start<br>Guide    | Provides instructions on how to install,<br>configure and use NetWrix Active Directory<br>Change Reporter, NetWrix Group Policy<br>Change Reporter and NetWrix Exchange<br>Change Reporter Freeware Edition. |
| Troubleshooting Incorrect Reporting of<br>the "Who Changed" Parameter                | Step-by-step instructions on how to troubleshoot incorrect reporting of the 'who changed' parameter.   |
| Installing Microsoft SQL Server and<br>Configuring the Reporting Services            | This technical article provides instructions on<br>how to install Microsoft SQL Server 2005/2008<br>R2/2012 Express and configure the Reporting<br>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<br>Systems   | This article explains how to enable integration<br>with third-party Security Information and<br>Event Management (SIEM) systems.   |

Table 6: Product Documentation