NetWrix
Systems Management and Compliance

NetWrix Group Policy Change Reporter

Quick Start Guide

Contents

Introduction

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. Built-in Group Policy management tools don't have any auditing and change reporting capabilities and you just can't track who, what and when data for critical modifications. The uncontrolled and unaudited change process imposes major security and compliance risks for an IT infrastructure run by multiple IT professionals.

NetWrix Group Policy Change Reporter makes Group Policy change auditing task very easy and straightforward. This FREE product sends daily reports detailing every single change made to Group Policy configuration. The reports list newly created and deleted GPOs, GPO link changes, changes made to audit policy, password policy, software deployment, user desktops, and all other settings. The data includes Who, What and When information for all changes with previous and current values for all modified settings.

Reports can be used to:

- Audit and report on all day-to-day Group Policy management tasks.
- Streamline creation of compliance reports for your SOX, GLBA and HIPAA auditors - Download report sample.
- Provide bird's eye view of all Group Policy management processes to IT managers.

The product records all Group Policy modifications and archives them to enable historical reporting (full archiving capabilities are provided by commercial version). You can build summary of changes made to Group Policy during any period, to analyze any policy violations that took place in the past. For example, you can 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 many other examples.

Licensing

Group Policy Change Reporter comes in two versions: free and commercial. The table below outlines the differences between them.

Feature	Freeware Version	Commercial Version
Who and When fields for every change	No	Yes
Group Policy change reporting	Not detailed - only category names, without names and values	Yes
Long term archiving and reporting	Only for two days: today and yesterday	Any period of time
Technical support	Support forum	Phone, e-mail
Licensing	Free of charge	Per enabled AD account or site license, please see our pricing information or request a quote

The free version can be used by businesses and individuals for an **unlimited** time, at no charge. The commercial version can be evaluated free of charge for **20** days.

Getting Started

Follow the instructions below to install and configure Group Policy Change Reporter.

System Requirements

The product can be installed on any computer running Windows XP SP2 or higher. The computer must belong to the managed domain.

Supported Active Directory environments:

- Windows 2000
- Windows Server 2003, any forest mode (mixed, native, 2K3)
- Windows Server 2008

Additional software:

- .Net Framework 2.0 or later
- Windows Installer 3.1 or later
- Group Policy Management Console (GPMC). To obtain Group Policy Management Console, please follow this link: http://go.microsoft.com/fwlink/?LinkId=46570

Additional requirements:

- Disk space – enough for temporary data storage (the Group Policy snapshots will be saved there). Required space depends on the number of users in your Active Directory and is calculated as follows:

  NumUsers*1 Kb

  For example, if you have 5000 users in your domain, you need at least 5MB of storage (daily collected data); to keep 1000 users data for 2 months, you need about 60MB of space (1K * 1000 * 60).

- The size of Security event logs on your domain controllers must be large enough to hold events for at least 36 hours. Otherwise, you may get incomplete information about who made some of the modifications. It is recommended to use Group Policy to adjust event logs sizes (for that, use **Administrative Tools | Domain Controller Security Policy**; configure log size in **Computer Configuration\Windows Settings\Security Settings\Event Log** node). The product reports conditions when one or more logs have been overwritten since the last collection (*).

- SQL Server 2005 or 2008 with Reporting Services (SSRS) are required for advanced reporting (*). SQL Server Express Edition with Advanced Services is supported; it can be installed and configured automatically. The following article explains how to configure SQL Server 2005 Express Edition to allow remote connections: http://support.microsoft.com/default.aspx?scid=kb;EN-US;914277

(*) - feature is available in commercial version only.

Required rights and permissions

The account under which **Netwrix Active Directory Change Reporter** scheduled task will run requires the following:

1. Sufficient rights to query the entire Active Directory
2. **Content Manager** role for the **Home** folder on SSRS (*)
3. To collect and report on objects' security changes, this account must have **Manage auditing and security log** user right enabled (if the task is run under Domain Administrator account, this right will be enabled by default). Adjust Domain Controller Security Policy accordingly. (*)

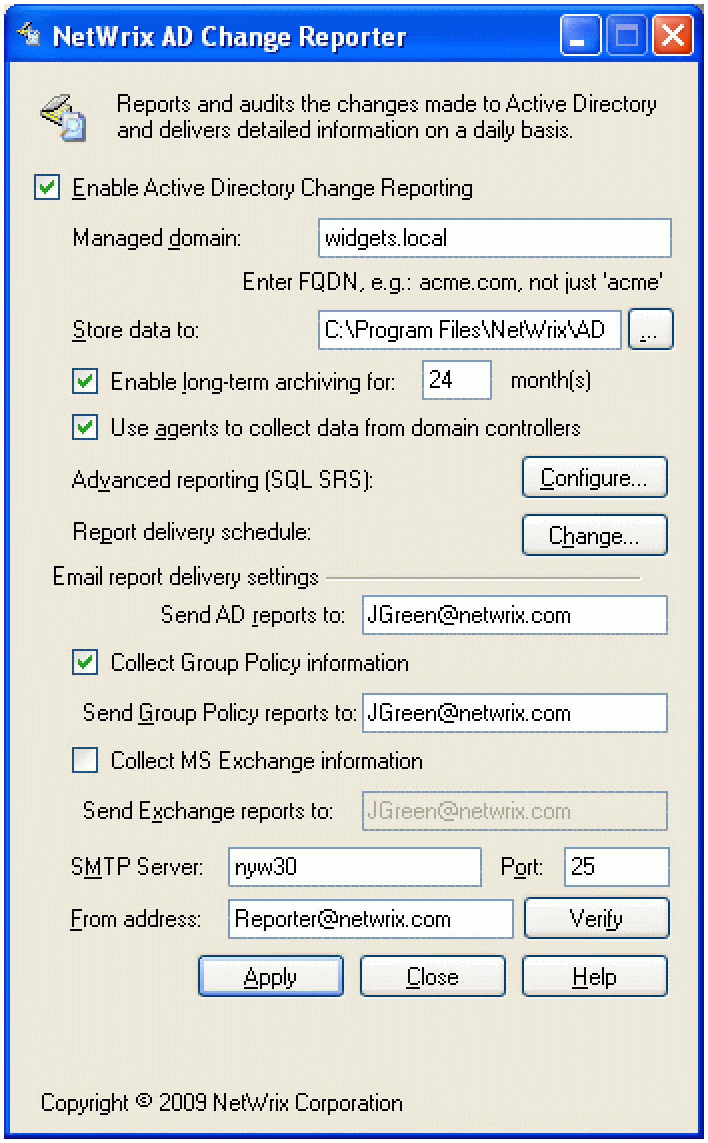
The account you will use to view the reports in SSRS Report Manager should have the **Browser** role for the Home folder on SSRS. (*)

If you plan to collect data using agents (recommended; for details, see the product Help), consider that agent service will be run under Local System account. (*)

(*) - requirement applies to commercial version only.

Installation and Configuration

To install the product, run the setup on the computer you have chosen. On the last step of the installation wizard, the configuration dialog box opens. To collect and report on Group Policy changes, verify that configuration settings are as follows:



NetWrix AD Change Reporter

Reports and audits the changes made to Active Directory and delivers detailed information on a daily basis.

☑ Enable Active Directory Change Reporting

Managed domain: widgets.local

Enter FQDN, e.g.: acme.com, not just 'acme'

Store data to: C:\Program Files\NetWrix\AD

☑ Enable long-term archiving for: 24 month(s)

☑ Use agents to collect data from domain controllers

Advanced reporting (SQL SRS):

Report delivery schedule:

Email report delivery settings

Send AD reports to: JGreen@netwrix.com

☑ Collect Group Policy information

Send Group Policy reports to: JGreen@netwrix.com

□ Collect MS Exchange information

Send Exchange reports to: JGreen@netwrix.com

SMTP Server: nyw30 Port: 25

From address: Reporter@netwrix.com

Copyright © 2009 NetWrix Corporation

- The **Enable Active Directory Change Reporting** check box is selected by default; when selected, the product generates the reports on AD changes and delivers them to the specified mailbox.
- Enter the Fully Qualified Name (FQDN) of the **Managed domain** which changes you want to track.

For example, *mydepartment.myorganizaton.domain.com*, not just *mydepartment* or anything else.

- In **Store data to** field, enter the path for the folder where NetWrix Active Directory Change Reporter will store the Active Directory snapshots that contain domain data for tracking and analysis. Default setting (installation folder path) should be changed to the storage folder in your production environment; make sure the storage size meets the requirements stated above.
- To enable historical reporting, set the archiving depth; for that, select **Enable long-term archiving for** check box, and specify how long it should be saved for (months) (*).
- If required, select **Use agents to collect data from domain controllers** (*); this is a recommended option. For details on using agents, refer to product Help.
- To provide for advanced reporting (*) based on SQL Server Reporting Services (SSRS), click **Configure...**. For more details, see the product Help.
- Under **Email report delivery settings**, enter the e-mail addresses to send AD change reports to (multiple addresses should be separated by comma).
- You can modify schedule for the Windows task called **Netwrix Active Directory Change Reporter** that performs the collection of changes to AD, and e-mails the reports. By default, this task will be launched at 3 AM daily. To modify the schedule, click **Change...**.
- Select the **Collect Group Policy information** check box.
- Supply the recipient's email address in the **Send Group Policy reports to:** field.
- Supply SMTP server settings (name, port, and From address).

(*) - feature is available in commercial version only.

When you have finished with these settings, click **Apply**. You will be prompted for the credentials to run data collection and report generation. The account you specify will be used to run the **Netwrix Active Directory Change Reporter** scheduled task (it can also be launched manually, as described later in this document).

- The account must be powerful enough to query the entire Active Directory.
- For advanced reporting to work properly, make sure that your user account and scheduled task account are assigned the Content Manager role for the SSRS Home folder.

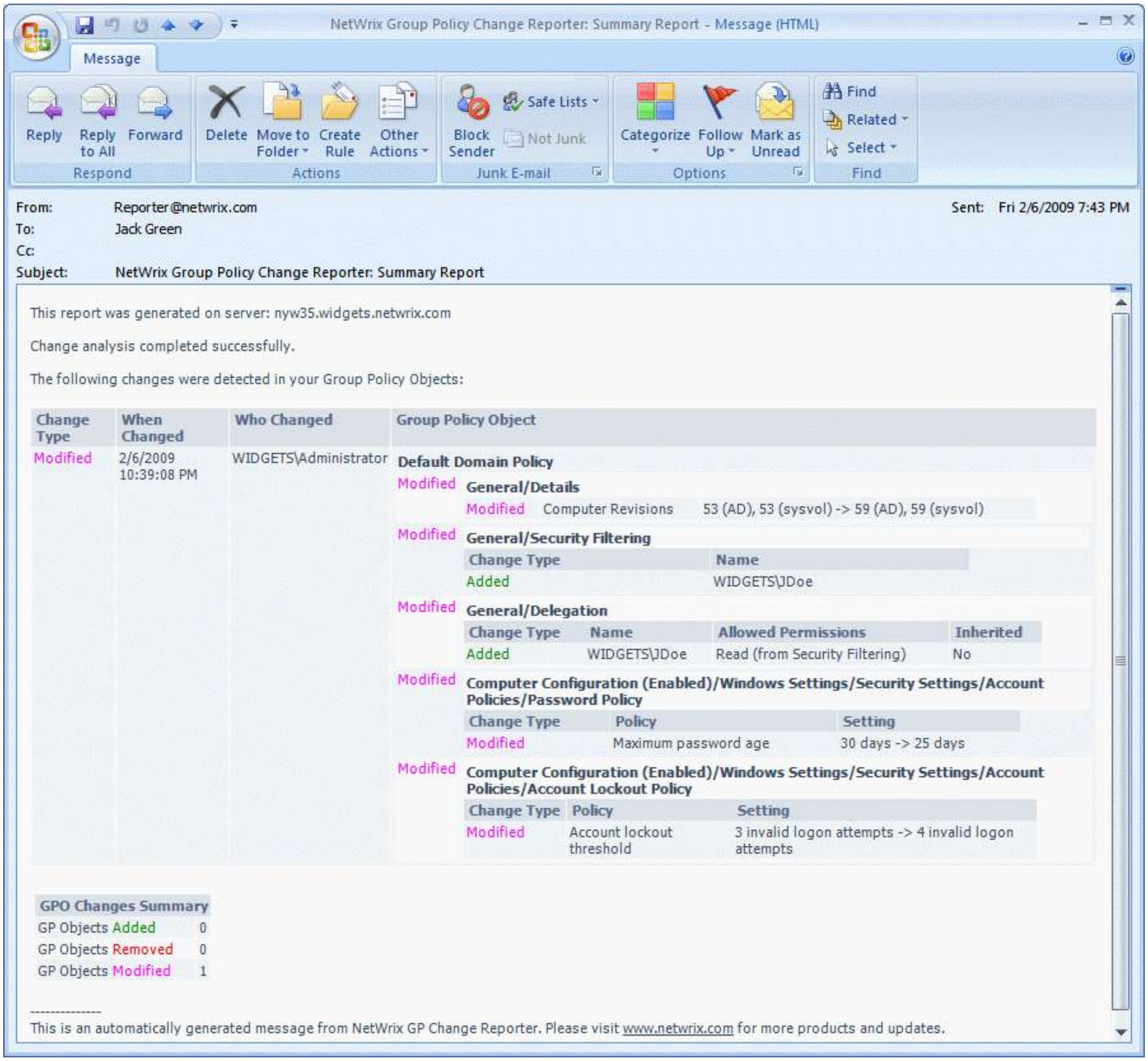
Note: The last requirement should be met if you are using the commercial version of the product.

The changes will take effect after you click **Apply** in the Configurator dialog. If necessary, you can later change configuration settings by invoking this dialog from the **Start** menu (select **NetWrix Active Directory Change Reporter** and then click **Configurator**).

Viewing the Reports

At the first run of the scheduled task, the message notifies you of the initial analysis completed. Next, you can make some changes to the Group Policy to see how they will be reported. After that, you can launch the scheduled task again, and then check the mailbox for the new report. The changes should be reported like shown in the figure below; if so, consider the product installation and configuration completed. If configured, reports on GP changes will be sent to the specified recipients, looking like the one below.

Important: Group Policy Management Console (GPMC) is required for generating the Group Policy change reports.



From: Reporter@netwrix.com
To: Jack Green
Cc:
Subject: NetWrix Group Policy Change Reporter: Summary Report
Sent: Fri 2/6/2009 7:43 PM

This report was generated on server: nyw35.widgets.netwrix.com

Change analysis completed successfully.

The following changes were detected in your Group Policy Objects:

Change Type	When Changed	Who Changed	Group Policy Object
Modified	2/6/2009 10:39:08 PM	WIDGETS\Administrator	Default Domain Policy

Modified **General/Details**

Modified	Computer Revisions	53 (AD), 53 (sysvol) -> 59 (AD), 59 (sysvol)

Modified **General/Security Filtering**

Change Type	Name
Added	WIDGETS\JDoe

Modified **General/Delegation**

Change Type	Name	Allowed Permissions	Inherited
Added	WIDGETS\JDoe	Read (from Security Filtering)	No

Modified **Computer Configuration (Enabled)/Windows Settings/Security Settings/Account Policies/Password Policy**

Change Type	Policy	Setting
Modified	Maximum password age	30 days -> 25 days

Modified **Computer Configuration (Enabled)/Windows Settings/Security Settings/Account Policies/Account Lockout Policy**

Change Type	Policy	Setting
Modified	Account lockout threshold	3 invalid logon attempts -> 4 invalid logon attempts

GPO Changes Summary	
GP Objects Added	0
GP Objects Removed	0
GP Objects Modified	1

This is an automatically generated message from NetWrix GP Change Reporter. Please visit www.netwrix.com for more products and updates.

Next Steps

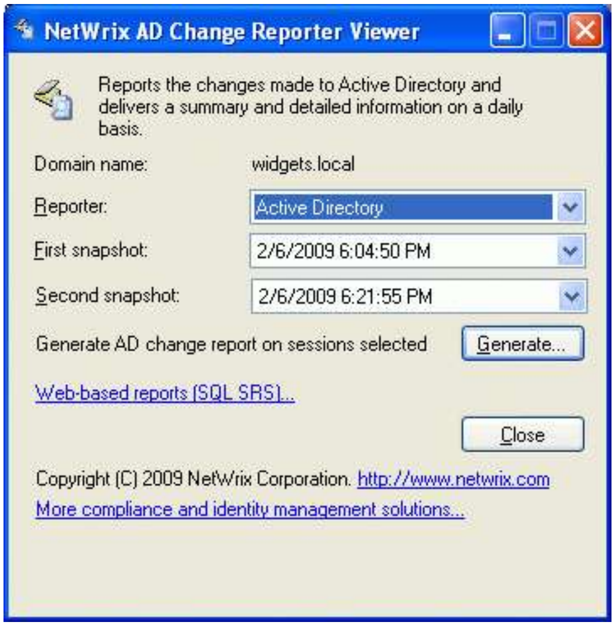
This section tells you how to manage Group Policy Change Reporter beyond the initial configuration. You can also refer to the product help.

Running an On-Demand Report

To get a report on changes to Group Policy right away, you can select the **Netwrix Active Directory ChangeReporter** in the list of the scheduled tasks, and select **Run** from its shortcut menu. The program will check for changes of Active Directory and Group Policy and automatically e-mail the report to the specified recipient(s).

Reporting on Changes That Occurred Between Two Snapshots

To view the changes that occurred between the particular snapshots, launch the **Report Viewer** from the Start menu.



NetWrix AD Change Reporter Viewer

Reports the changes made to Active Directory and delivers a summary and detailed information on a daily basis.

Domain name: widgets.local

Reporter: Active Directory

First snapshot: 2/6/2009 6:04:50 PM

Second snapshot: 2/6/2009 6:21:55 PM

Generate AD change report on sessions selected

Generate...
Web-based reports (SQL SRS)...
Close

Copyright (C) 2009 NetWrix Corporation. http://www.netwrix.com

More compliance and identity management solutions...

Use the **Reporter** drop-down list to select **Group Policy** as the source of data for reporting, then select the snapshots (by date) and click **Generate** to generate and save a report on changes between them (in the HTM format). The report will be opened in the web browser to show you the changes that occurred between selected snapshots.

Note: Actually, this report will be identical to the report on changes you received by email at the time of the second snapshot generation.

Using SSRS-based Reporting (Commercial Version Only)

With SQL Server Reporting Services deployed, you can also configure advanced reporting (SSRS-based). In this case, you can use the advantages of SSRS-based reporting:

- Use the wide variety of reports to analyze the operation of your network environment; dozens of reports will help you to stay compliant with standards and regulations your organization is subject to (SOX, HIPAA, PCI, GLBA, SAS70, and others).
- Change the report filters to fine-tune the data view according to your needs.
- Use one of popular formats: PDF, XLS, etc. to save the report.

- Apply grouping and sorting to report data, and so on.

To use this type of reporting, you can either click **Configure** when supplying configuration settings during the setup, or invoke the Configurator later on. For details, see the product Help.

Additional Functionality

With **NetWrix Active Directory Change Reporter** deployed in your network environment, you can also generate the reports on changes to Active Directory and Exchange Server objects, as well as revert unwanted Active Directory changes. For details, refer to Active Directory Change Reporter Quick Start Guide, Exchange Server Change Reporter Quick Start Guide, and AD Object Restore Wizard Quick Start Guide.

How It Works

Typical **Change Reporter** data flow is described below.

1. AD infrastructure and Group Policy settings are periodically collected and stored to the specified storage as configuration snapshots. A report displaying changes to Group Policy is sent to the specified e-mail recipient(s)

   Optionally, you can set up advanced reporting based on SQL Server Reporting Services as described in the product Help. Note that this functionality is available only in the commercial version of the product.

2. If SSRS-based reporting was configured for the product, then information about configuration changes is collected not only for a snapshot but is also automatically stored in the specified database and becomes available for report generation. You can view HTML reports in the SSRS Report Manager, or click the **More reports** link from the email report that you have received.

The **Change Reporter** collection and reporting workflow is usually as follows:

1. A user launches the Configurator and sets the parameters for automated data collection and reporting.

Note: Agents are recommended for data collection. Select the corresponding option in the Configurator to deploy the agents automatically (consider that agents usage is supported in commercial version only. For detailed information about agents, see the product Help.).

2. The Netwrix AD Change Reporter scheduled task is launched periodically (typically, every night, at 3 AM by default; it can also be launched manually when needed). This task collects configuration snapshots, and e-mails reports on changes and configuration to the specified recipients.
3. If SSRS-based reporting was configured, the task also stores information about configuration changes to the specified SQL server database (if automatic data import fails, you can use Database Importer to import data when necessary; see the product Help for details).
4. A user launches mail client to view the reports sent by e-mail; If SSRS-based reporting was configured, a user launches the web browser and views the reports in Report Manager.