NETWRIX GROUP POLICY CHANGE REPORTER

USER 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

1. INTRODUCTION

1.1. Overview

This guide is intended for end users of NetWrix Group Policy Change Reporter. It contains information on different product reporting capabilities, lists all available report types and report output formats, and explains how these reports can be viewed and interpreted.

This guide can be used by auditors, company management or anyone who wants to view audit reports on the monitored environment.

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 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.
- Chapter 3 Change Summary shows a Change Summary example and explains what information a Change Summary contains.
- Chapter 4 Reports contains an overview of the Reports functionality, lists all reports available in NetWrix Group Policy Change Reporter and provides their descriptions. The chapter also explains how to view reports in a web browser or receive them by email.
- A Appendix: Related Documentation contains a list of all documentation published to support NetWrix Group Policy Change Reporter.

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.

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.

2.1. Key Benefits

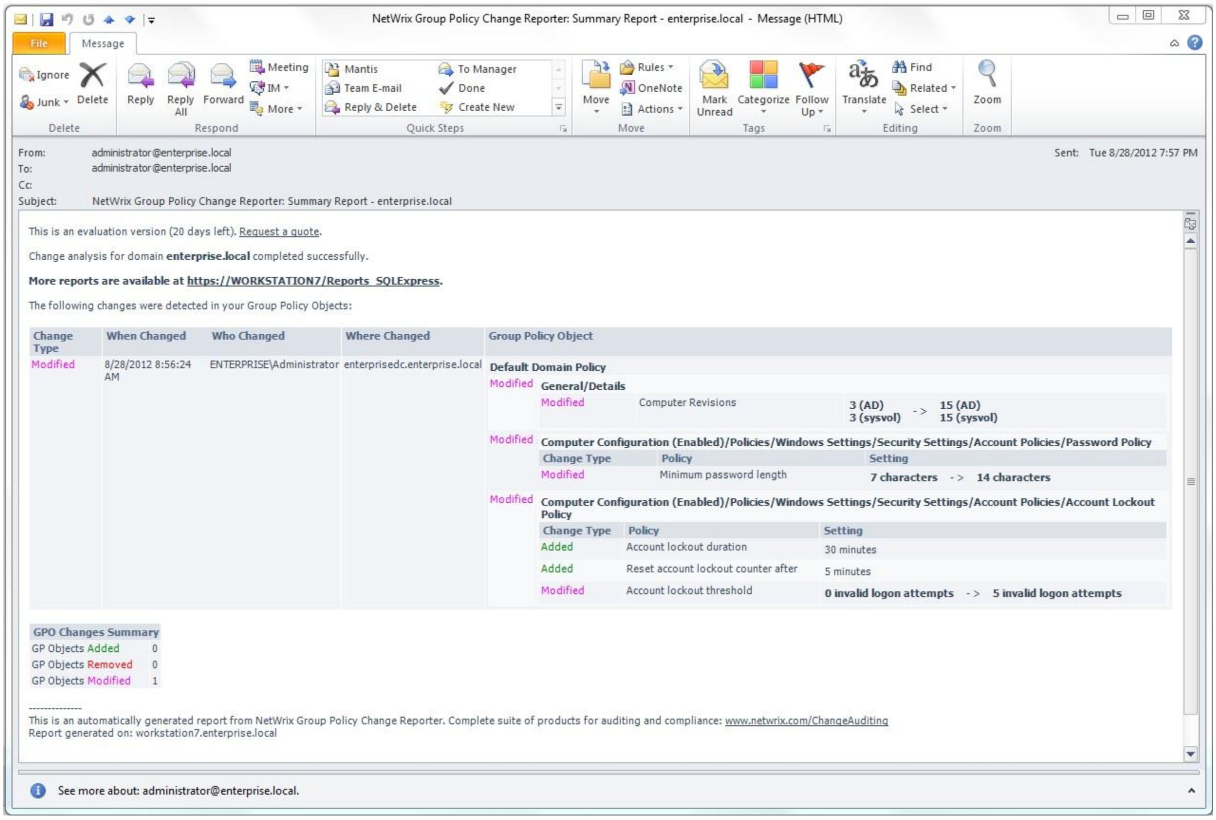
NetWrix Group Policy Change Reporter is a tool for automated auditing and reporting on changes to the monitored Group Policy objects. It allows you to do the following:

- **Monitor day-to-day administrative activities**: the product captures detailed information on all changes made to the monitored Group Policy objects, including the information on WHO changed WHAT, WHEN and WHERE. Audit reports and real-time email notifications facilitate review of daily activities.
- **Sustain compliance** by using in-depth change information. Audit data can be archived and stored for several years to be used for reports generation.
- **Integrate 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 Group Policy auditing and helping protect these investments.

3. Change Summary

Each day (at 3:00 AM by default), NetWrix Group Policy Change Reporter generates a Change Summary that contains the information on changes that occurred in the last 24 hours and emails it to the specified recipients:

Figure 1: Change Summary Example



From: administrator@enterprise.local
To: administrator@enterprise.local
Cc:
Subject: NetWrix Group Policy Change Reporter: Summary Report - enterprise.local

Sent: Tue 8/28/2012 7:57 PM

This is an evaluation version (20 days left). Request a quote.

Change analysis for domain **enterprise.local** completed successfully.

More reports are available at https://WORKSTATION7/Reports_SQLExpress.

The following changes were detected in your Group Policy Objects:

Change Type	When Changed	Who Changed	Where Changed	Group Policy Object
Modified	8/28/2012 8:56:24 AM	ENTERPRISE\Administrator	enterprisedc.enterprise.local	**Default Domain Policy**

Modified **General/Details**

Modified	Computer Revisions	**3 (AD) 3 (sysvol)** -> **15 (AD) 15 (sysvol)**

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

Change Type	Policy	Setting
Modified	Minimum password length	**7 characters** -> **14 characters**

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

Change Type	Policy	Setting
Added	Account lockout duration	30 minutes
Added	Reset account lockout counter after	5 minutes
Modified	Account lockout threshold	**0 invalid logon attempts** -> **5 invalid logon attempts**

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

This is an automatically generated report from NetWrix Group Policy Change Reporter. Complete suite of products for auditing and compliance: www.netwrix.com/ChangeAuditing
Report generated on: workstation7.enterprise.local

See more about: administrator@enterprise.local.

The Change Summary provides the following information for each change:

Table 1: Change Summary Fields

Parameter	Description
Change Type	Shows the type of action that was performed on the GP 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 from which the change was made.
Group Policy Object	Shows the Group Policy Object that was changed with details on its “before” and “after” values.

To receive daily Change Summary emails, ask your system administrator to add your email address to the Change Summary Recipients list.

4. Reports

NetWrix Group Policy Change Reporter allows generating reports based on Microsoft SQL Server Reporting Services (SSRS). The product provides a wide variety of predefined report templates that will help you stay compliant with various standards and regulations (such as HIPAA, FISMA, GLBA and SOX). You can use different output formats for your reports, such as PDF, XLS, and so on.

You can view reports through a web browser, or you can ask your system administrator to configure a subscription to the selected reports to receive them by email. For details on these options, refer to the following sections:

- 4.2 Viewing Reports in a Web Browser
- 4.3 Receiving Reports by Email

4.1. Reports List

NetWrix Group Policy Change Reporter provides predefined report templates. If none of these reports suits your needs, ask your system administrator to create custom report templates, or order them from NetWrix.

The table below lists all available reports and provides their descriptions:

Table 2: Reports List

Report Name	Description
Account Lockout Policy	
Account Lockout Policy Changes	Shows all changes made to account lockout policy settings. For example, changes to lockout threshold and duration. Unauthorized changes of account lockout settings may indicate attempts to compromise system security.
Lockout Duration Policy Changes	Shows modifications of account lockout duration setting.
Account Policies	
Account Policy Changes	Shows all changes to password policies, account lockout policies, and Kerberos policies.
Administrative Templates	
Administrative Template Changes	Administrative templates define policy settings in different categories, including desktops settings, services, and applications. The report shows all changes to the administrative templates.
Public Key Policy Changes	Public Key Policies enforce settings of the public key infrastructure, such as trusted certificate lists and enterprise certificate authority. The report shows changes to all public key policies.
Windows Components Policy Changes	Shows changes in standard system components and applications, such as shell, Windows Installer, Windows Update, Media Player, Internet Explorer, and others.
All Changes Reports	
All Group Policy Changes (Chart)	Shows all changes made to Group Policy objects, setting values, GPO links, and permissions. Filtered by date range.
All Group Policy Changes	Shows all changes made to Group Policy objects, setting values, GPO links, and permissions. Filtered by date range and user name who made changes.
Configuration	
Computer Configuration Windows Settings Changes	Shows all changes in Windows core operating system settings that can be enforced via Group Policy (Computer Configuration \ Windows Settings node).

User Configuration Changes	Shows all changes in Windows core operating system settings related to users: logon scripts, security settings, folder redirection, and others (User Configuration \ Windows Settings node).
Local Policies	
Audit Policy Changes	Audit policy defines what types of actions are logged to audit trails by the system. The report shows changes to all audit policies.
Interactive Logon Policy Changes	Shows changes to interactive logon rights.
Rename Administrator and Guest Policy Changes	Shows changes to the administrator and guest policy.
Security Options Policy Changes	Shows all changes to password policies.
User Rights Assignment Policy Changes	Shows changes to user rights assignment policy.
Password Policy	
All Password Policy Changes	Shows all changes to password policy
Password Age Policy Changes	Shows changes to minimum and maximum password age settings.
Password Complexity Policy Changes	Shows changes to password complexity requirements.
Password Encryption Policy Changes	Shows changes to the policy that defines whether passwords are stored using reversible encryption of not.
Password History Policy Changes	Shows changes to password history policy.
Policy	
Changes in GPO Links	Shows when GPOs are linked or unlinked to OUs and domains.
Internet Explorer Policy Changes	Shows all changes to the Internet Explorer settings on managed client workstations.
Logon and Logoff Script Policy Changes	Shows all changes to the logon and logoff script policy.
Network Policy Changes	Shows all changes to the network policy settings.
Printer Policy Changes	Shows all changes to the printer policy settings.
Registry Policy Changes	Shows all changes to policy-enforced registry permissions on managed servers.
Remote Installation Policy Changes	Shows all changes to the remote installation policy settings.
Restricted Groups Policy Changes	Shows all changes to the restricted groups policy settings.
Software Restriction Policy Changes	Shows all changes to the software restriction policy settings.
Startup and Shutdown Script Policy Changes	Shows all changes to the startup and shutdown script policy settings.
System Policy Changes	Shows all changes to the system policy settings.
System Services Policy Changes	Shows all changes to the system services policy settings.
Security Settings	
Security Policy Changes	Shows all changes made to security policies (for example, Local Policy, Account Policy, Password Policy and so on).
Software Installation	
Software Installation Policy Changes	This report shows all changes made to GPO software deployment settings.
Windows Settings	
Windows Settings Changes	Shows all changes to the Computer Configuration \ Windows Settings and User Configuration \ Windows Settings sections.
Wireless Network Policy Changes	Shows all changes to the wireless network policy changes.

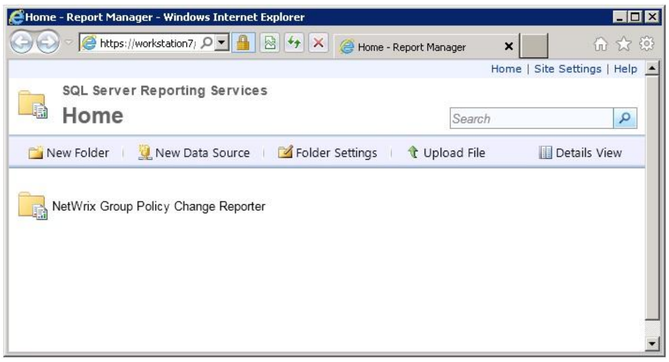
4.2. Viewing Reports in a Web Browser

To view reports in a web browser, ask your system administrator to provide you with the Report Manager URL.

Procedure 1. To view reports in a web browser

1. In your web browser, type the Report Manager URL in the address line and press **Enter.** The SQL Server Reporting Services **Home** page will open:

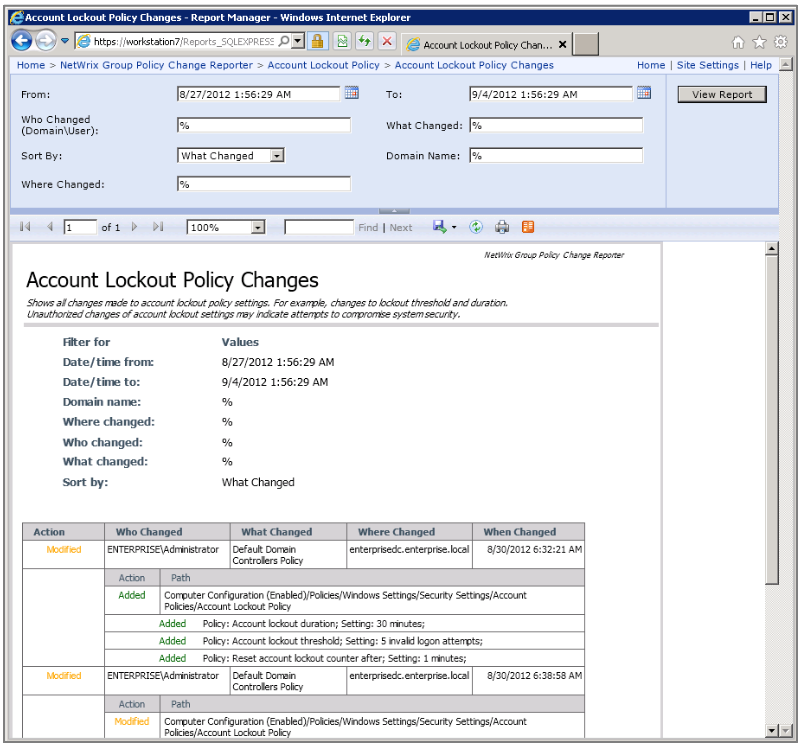
Figure 2: Report Manager: NetWrix Group Policy Change Reporter Page


Home - Report Manager - Windows Internet Explorer
https://workstation7/
Home - Report Manager
Home | Site Settings | Help
SQL Server Reporting Services
Home
Search
New Folder
New Data Source
Folder Settings
Upload File
Details View
NetWrix Group Policy Change Reporter

2. Click the **NetWrix Group Policy Change Reporter** folder and navigate to the report you want to generate.

3. Click the report name. The report will be displayed showing the changes that occurred in the last 24 hours. On this page, you can specify filters to the selected report and click the **View Report** button (**View Chart** for chart reports) to apply them:

Figure 3: Account Lockout Policy Changes Page (Web Browser)


Account Lockout Policy Changes - Report Manager - Windows Internet Explorer
https://workstation7/Reports_SQLEXPRESS
Account Lockout Policy Chan...
Home > NetWrix Group Policy Change Reporter > Account Lockout Policy > Account Lockout Policy Changes
Home | Site Settings | Help
View Report
1 of 1
100%
Find | Next
NetWrix Group Policy Change Reporter

From: 8/27/2012 1:56:29 AM

To: 9/4/2012 1:56:29 AM

Who Changed (Domain\User): %

What Changed: %

Sort By: What Changed

Domain Name: %

Where Changed: %

Account Lockout Policy Changes

Shows all changes made to account lockout policy settings. For example, changes to lockout threshold and duration. Unauthorized changes of account lockout settings may indicate attempts to compromise system security.

Filter for	Values
Date/time from:	8/27/2012 1:56:29 AM
Date/time to:	9/4/2012 1:56:29 AM
Domain name:	%
Where changed:	%
Who changed:	%
What changed:	%
Sort by:	What Changed

Action	Who Changed	What Changed	Where Changed	When Changed
Modified	ENTERPRISE\Administrator	Default Domain Controllers Policy	enterprisedc.enterprise.local	8/30/2012 6:32:21 AM
	Action	Path		
	Added	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy		
	Added	Policy: Account lockout duration; Setting: 30 minutes;		
	Added	Policy: Account lockout threshold; Setting: 5 invalid logon attempts;		
	Added	Policy: Reset account lockout counter after; Setting: 1 minutes;		
Modified	ENTERPRISE\Administrator	Default Domain Controllers Policy	enterprisedc.enterprise.local	8/30/2012 6:38:58 AM
	Action	Path		
	Modified	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy		

Note: Report filters may vary depending on the selected report.

4.3. Receiving Reports by Email

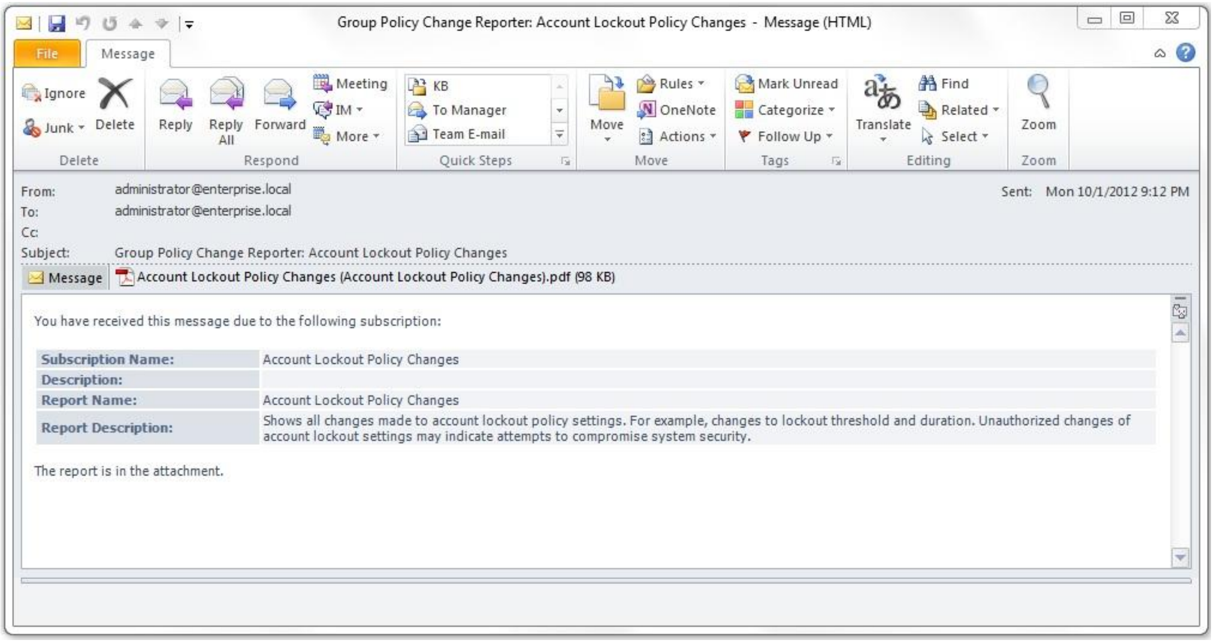
To receive reports by email, ask your system administrator to configure a subscription to the required reports. The administrator can set report filters, so that you only receive the information you need in the required output format: Excel, Word, or PDF.

Reports can be delivered on one of the following schedules:

- On a daily basis: reports will be delivered at the specified interval at 3:00 AM;
- On a weekly basis: reports will be delivered on the specified days of the week at 3:00 AM;
- On a monthly basis: reports will be delivered in the specified months on a selected date at 3:00 AM.

Reports will be delivered as email attachments in the selected format:

Figure 4: Report Delivered by Subscription



From: administrator@enterprise.local

Sent: Mon 10/1/2012 9:12 PM

To: administrator@enterprise.local

Cc:

Subject: Group Policy Change Reporter: Account Lockout Policy Changes

Message | Account Lockout Policy Changes (Account Lockout Policy Changes).pdf (98 KB)

You have received this message due to the following subscription:

Subscription Name:	Account Lockout Policy Changes
Description:	
Report Name:	Account Lockout Policy Changes
Report Description:	Shows all changes made to account lockout policy settings. For example, changes to lockout threshold and duration. Unauthorized changes of account lockout settings may indicate attempts to compromise system security.

The report is in the attachment.

A Appendix: Related Documentation

The table below lists all documents available to support NetWrix Group Policy Change Reporter:

Table 3: Product Documentation

Document Name	Overview
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 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 Quick-Start Guide	Provides an overview of the product functionality and instructions on how to install, configure and start using the product. This guide can be used for the product evaluation purposes.
NetWrix Active Directory Change Reporter Installation and Configuration Guide	Provides detailed instructions on how to install NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter, and explains how to configure the target AD domain for auditing.
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.