NETWRIX FILE SERVER CHANGE REPORTER

TROUBLESHOOTING GUIDE

January/2013

www.netwrix.com

Table of Contents

1. INTRODUCTION

1.1. Overview

NetWrix File Server Change Reporter detects and reports on access attempts and changes to files, folders, shares, as well as on changes to objects' properties including permissions. Reports include information on *what* changes were made, *who* made them, *when* and *where*. However, incorrect settings on file servers may result in errors in reports. For example, you can receive a report containing the "System" value instead of an account name in the "Who changed" column, or an empty report. Problem reports usually have a warning.txt file attached that may help understand what caused the problem, or, if email reports are disabled, you can find the problem's description in NetWrix Enterprise Management Console under your **Managed Object → Sessions** node.

This guide provides instructions on how to troubleshoot incorrect reporting issues you may encounter while using NetWrix File Server Change Reporter. For each issue there is a problem description or a message that can be found in the warning.txt file, an explanation of what caused the problem and instructions on how to solve it.

Note: This document applies to NetWrix File Server Change Reporter 3.3 and covers troubleshooting of incorrect reporting on file servers running Windows Server 2000 or later. For information on how to configure NetWrix File Server Change Reporter to monitor a NetApp filer or EMC VNX/VNXe/Celerra appliance, refer to one of the following technical articles respectively How to Configure NetWrix File Server Change Reporter to Monitor NetApp Filer CIFS Shares and How to Configure NetWrix File Server Change Reporter to Monitor EMC VNX/VNXe/Celerra CIFS Shares. If you have a different operating system, contact NetWrix Technical Support.

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 and defines its structure.
- Chapter 2 Troubleshooting Reporting Issues: describes the most common issues users may face when using NetWrix File Server Change Reporter and provides instructions on how to solve them.
- A Appendix: Related Documentation: contains a list of all documentation published to support NetWrix File Server Change Reporter.

2. Troubleshooting Reporting Issues

Below is a list of the most common problems causing incorrect or incomplete reporting that users may encounter while using NetWrix File Server Change Reporter. Refer to the sections below for step-by-step instructions on how to troubleshoot these issues:

- Default Audit Settings on Shares Issue
- Security Log Overflow Issue
- Disk Overfilling Issue on Monitored File Servers
- Incorrect Data in Reports Without Any Warnings

If none of the sections listed above help you resolve your issue, refer to section 2.5 If You Have Not Found a Solution.

2.1. Default Audit Settings on Shares Issue

2.1.1. Problem Description

You receive a report containing incorrect data or no data at all. In the attached warning.txt file or in Sessions you can find the following message and a list of file shares:

```
[WARNING]Your default audit settings on the following shares may
prevent the "Who Changed" and "When Changed" fields from being
reported correctly. Please refer to the Troubleshooting section of
the product documentation for more information.
```

2.1.2. What Caused the Problem

The problem occurs if the default audit settings on file shares prevent collection and storage of information required by NetWrix File Server Change Reporter.

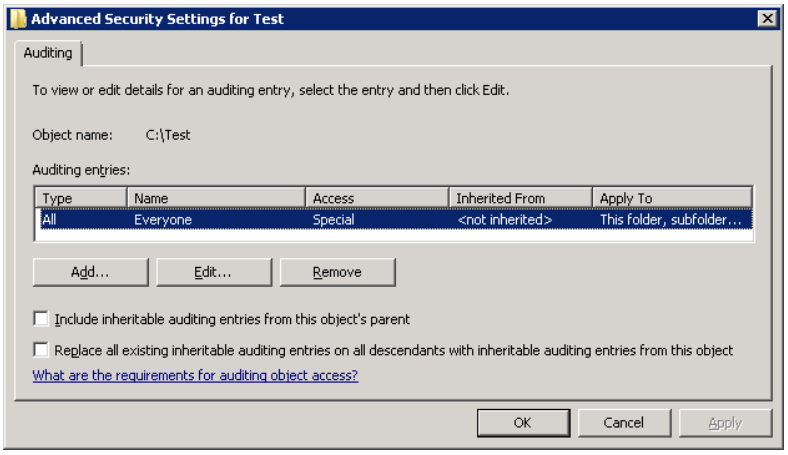
2.1.3. How to Fix

To configure audit on the file shares, perform the following procedure:

Procedure 1. To configure audit settings on file shares

1. Navigate to a file share specified in the warning message, right-click it and select **Properties** from the pop-up menu.
2. Open the Security tab and press the **Advanced** button. In the **Advanced Security Settings for <Shared_Folder_Name>** dialog, open the **Auditing** tab, select the **Everyone** entry and click the **Edit** button. The **Advanced Security Settings for <Shared_Folder_Name>** dialog will open:

Figure 1: Advanced Security Settings for < Shared_Folder_Name > Dialog



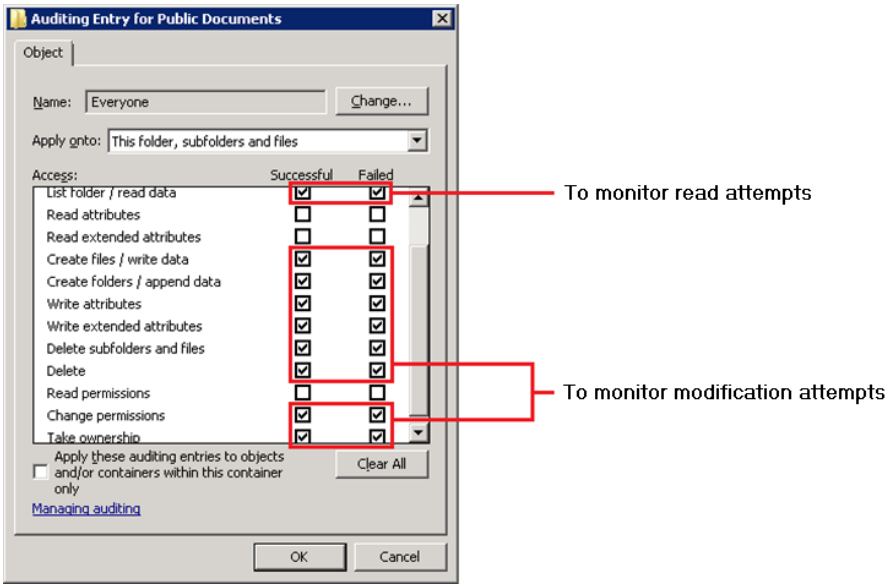
3. Select the **Everyone** group and click **Edit**.

   Note: You can specify any other required user group, but, in this case, reports will contain warnings about incorrect audit configuration. This will not affect the reporting functionality and the product will only monitor user accounts that belong to the selected group.

4. Access options must be selected depending on the access types that you have specified for monitoring in the product's configuration:

   - To monitor successful/failed modification attempts, select the following **Successful/Failed** check-boxes:
     - Create Files / Write Data
     - Create Folders / Append Data
     - Write Attributes
     - Write Extended Attributes
     - Delete Subfolders and Files
     - Delete
     - Change Permissions
     - Take Ownership
   - To monitor successful/failed read attempts, select the following **Successful/Failed** check-boxes:
     - List Folder / Read Data

Figure 2: Audit Entry for <Shared_Folder_Name> Dialog



5. Make sure that the **Apply onto** parameter is set to **This folder, subfolders and files** and the **Apply these auditing entries to objects and/or containers within this container only** check-box is *not* selected.

6. Click **OK** to save the changes.

After you have configured audit settings on the file shares, make sure that you have specified the types of events you want to monitor in the Audit object access policy. If you have not configured the Audit object access policy on the managed file server(s) before, perform the following procedure:

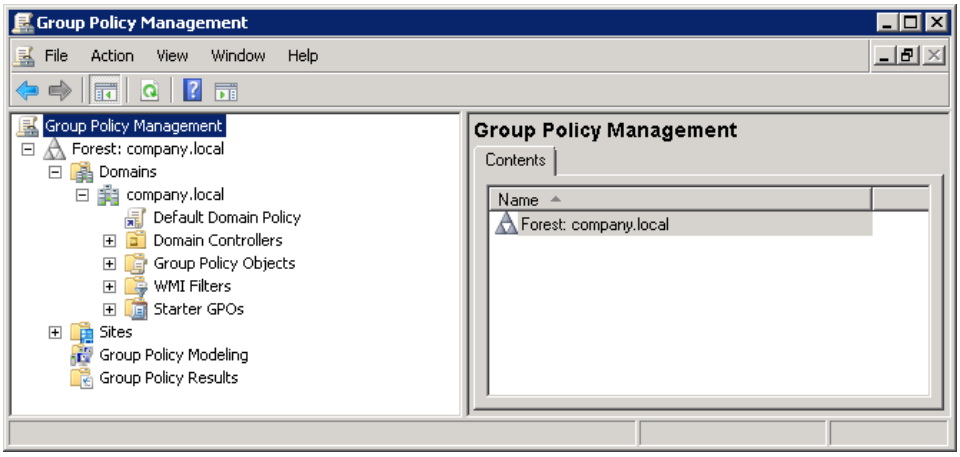
> **Note:** For Microsoft Windows file servers running Windows Vista or later, you can configure the granular audit policy. Via the granular audit policy you can manage auditing at a detailed level, which helps you avoid saving unnecessary data to your event logs. To configure the granular audit policy on your server, refer to the following technical article: How to Configure Granular Audit Policy on a File Server Monitored by NetWrix File Server Change Reporter

Procedure 2. To configure Audit object access policy

> **Note:** This procedure provides instructions on how to configure Audit object access for all monitored file servers using the Group Policy. Alternatively, you can configure it separately for each of your file servers in the local policies.

1. Navigate to **Start → Programs → Administrative Tools → Group Policy Management**. The Group Policy Management console will open:

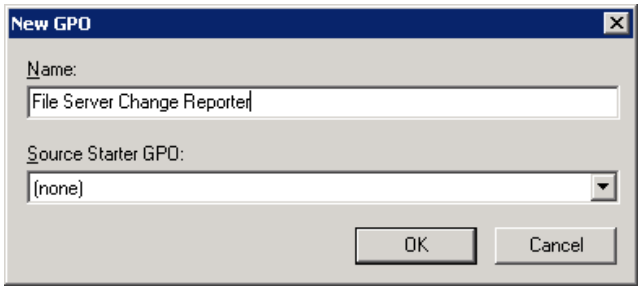
Figure 3: Group Policy Management Console



2. Expand the **Domains** node, right-click the **<Company_Domain_Name>** node, select **New Organizational Unit** and specify the unit's name (for example, File Servers).

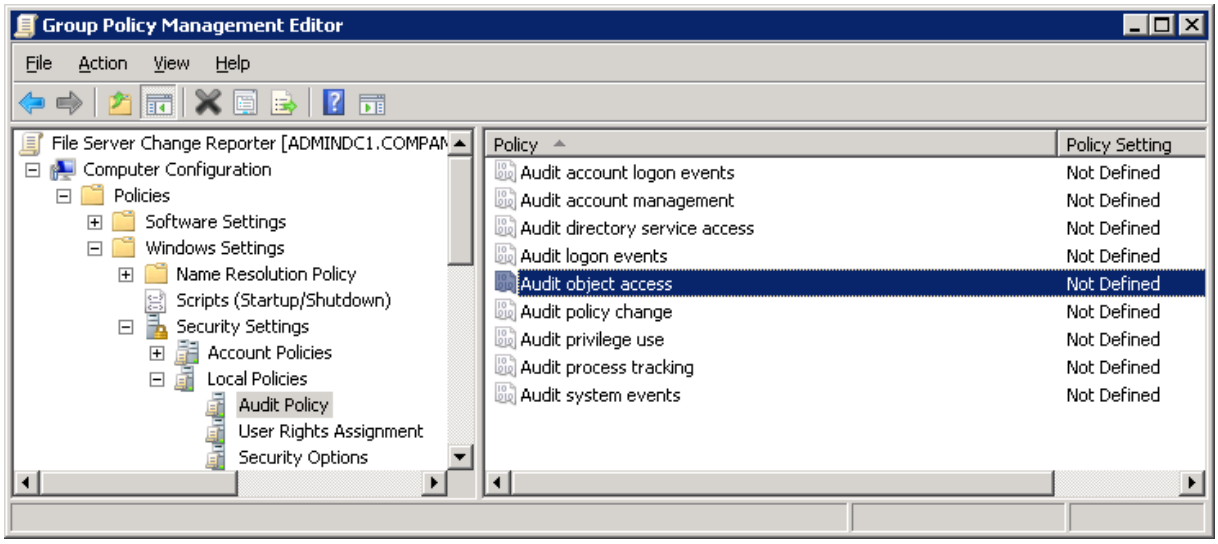
3. Right-click the newly created Organizational Unit and select **Create a GPO in this domain and Link it here…** option. In the **New GPO** dialog type 'File Server Change Reporter' in the **Name** entry field and click **OK**:

Figure 4: New GPO Dialog



4. Right-click the newly created File Server Change Reporter GPO and select the **Edit** option. In the **Group Policy Management Editor** dialog, navigate to **Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy**:

Figure 5: Group Policy Management Editor Dialog



5. In the right pane, double-click **Audit object access.** Select the **Success** check box to monitor successful read/modification attempts and the **Failure** check box to monitor failed read/modification attempts:

Figure 6: Audit object access Properties Dialog

6. Click **OK** to save the changes.
7. Navigate to **Start → Control Panel → Administrative Tools → Active Directory Users and Computers**. Click the **Computers** node and move your monitored file server(s) from the right pane to the newly created **File Servers** organizational unit.
8. On the file server, navigate to **Start → Run** and execute the `cmd` command. Type the `gpupdate/force` command and press **Enter**. The Group Policy will be updated.
9. Using the **Resultant Set of Policy** (RSoP) snap-in, ensure that your settings are not overridden by other Group Policies. To do this, navigate to **Start → Run** and execute the `cmd` command. Type the `rsop.msc` command and press **Enter**.

2.2. Security Log Overflow Issue

2.2.1. Problem Description

You receive a report containing incorrect data or no data at all. In the attached warning.txt file or in Sessions you can find the following warning message:

```
[WARNING] Security log overwrites occurred on this computer since
the last collection. Please increase the maximum size of the
Security event log.
```

2.2.2. What Caused the Problem

The problem can be caused by one of the following:

- The size of the Security event log of the monitored computer exceeds the maximum value (for details, refer to Table 1: Security Event Log Requirements for Windows Operating Systems) and NetWrix File Server Change Reporter cannot read

information from the log. Perform Procedure 3 To change the maximum size of the Security event log to resolve the issue.

- The size of the Security event log of the monitored computer is set correctly (for details, refer to Table 1: Security Event Log Requirements for Windows Operating Systems), but it is not enough to keep all events until the next data collection. Perform Procedure 4 To configure automatic archiving of the Security event log to resolve the issue.

2.2.3. How to Fix

The maximum size of the Security event log on the target computer must be set based on its operating systems. The table below can help you choose the Security event log maximum size:

Table 1: Security Event Log Requirements for Windows Operating Systems

Operating System on the computer		Network Traffic Compression option is enabled*	Security log auto archiving is enabled	Security Event Log Maximum Size
where NetWrix File Server Change Reporter is installed	which is monitored by NetWrix File Server Change Reporter			
Windows 2000/XP/2003/Vista/7/ 2008/2008 R2	Windows 2000/XP/2003	Yes/No	Yes/No	300 MB
Windows 2000/XP/2003	Windows Vista/7/2008/2008 R2	No	No	300 MB
Windows 2000/XP/2003	Windows Vista/7/2008/2008 R2	No	Yes	Configuration is not supported
Windows 2000/XP/2003	Windows Vista/7/2008/2008 R2	Yes	Yes/No	4 GB
Windows Vista/7/2008/2008 R2	Windows Vista/7/2008/2008 R2	Yes/No	Yes/No	4 GB

* *For information on this option, refer to NetWrix File Server Change Reporter Administrator's Guide.*

If you monitor computers with NetApp filer or EMC VNX/VNXe/Celerra data storage systems installed, the following Security event log size is recommended:

Table 2: Security Event Log Requirements for Data Storage Systems

Operating System where NetWrix File Server Change Reporter is installed	Data Storage System	Security Event Log Maximum Size
Windows 2000/XP/2003	NetApp filer EMC VNX/VNXe/Celerra	300 MB
Windows Vista/7/2008/2008 R2	NetApp filer	4 GB (300 MB is recommended)
Windows Vista/7/2008/2008 R2	EMC VNX/VNXe/Celerra	4 GB

Procedure 3. To change the maximum size of the Security event log on the monitored computer

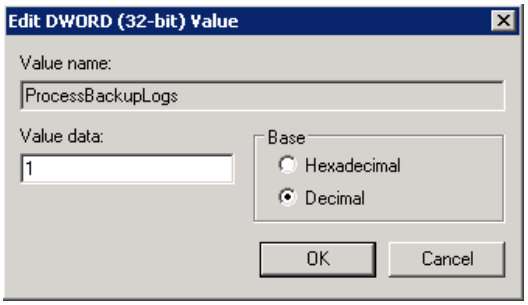
Note: Perform the following steps on the file server where the error occurred. You must be a member of the Administrators group to make these changes.

1. Navigate to **Start → Programs → Administrative Tools → Event Viewer**. In the Event Viewer dialog expand the **Windows Logs** node, right-click **Security** and select **Properties** from the pop-up menu. The **Log Properties - Security** dialog will open.
2. Set the **Maximum log size** to a selected value and enable the **Overwrite events as needed** option.
3. Click **OK** to save the changes.

Procedure 4. To configure automatic archiving of the Security event log

1. On the monitored computer, do one of the following depending on its operating system:
   - If you have Windows Server 2003 installed:
     1. Navigate to **Start → Run,** type the "`regedit`" command and click **OK**.
     2. Navigate to HKLM → SYSTEM → CurrentControlSet → Services → Eventlog → Security. Double-click AutoBackupLogFiles, set the "AutoBackupLogFiles" (DWORD) value to 1 and "Retention" (DWORD) value to 0xFFFFFFFF (do not overwrite).
     3. Click **OK** to save the changes.
   - If you have Windows Server 2008 installed:
     1. Navigate to **Start → Programs → Administrative Tools → Event Viewer**. In the Event Viewer dialog expand the **Windows Logs** node, right-click **Security** and select **Properties** from the pop-up menu. The **Log Properties - Security** dialog will open.
     2. Select the **Archive the log when full, do not overwrite events** option.
     3. Click **OK** to save the changes.
2. Then navigate to **Start → Run,** type the "`regedit`" command and click **OK.**
3. Navigate to **HKEY_LOCAL_MACHINE → SOFTWARE → NetWrix → File Server Change Reporter** (for 32-bit OS) or **HKEY_LOCAL_MACHINE → SOFTWARE → Wow6432Node → NetWrix → File Server Change Reporter** (for 64-bit OS).
4. Double-click **ProcessBackupLogs.** The **Edit DWORD Value** dialog will open.
5. Type '1' in the **Value data** entry field:

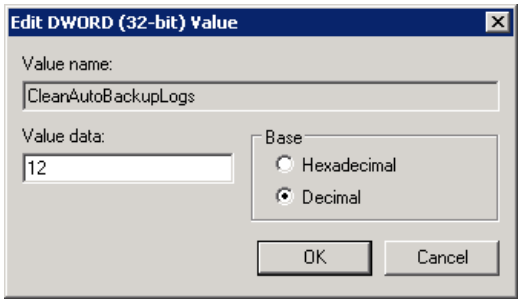
Figure 7: Edit DWORD Value Dialog



6. Click **OK** to save the changes.
7. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.

   Note: If there is no such registry key, create it manually (type DWORD).
8. Type an integer, for example 12, that defines the time (in hours) after which archives will be deleted. Make sure that the **Decimal** radio-button is selected, and click **OK**:

Figure 8: Edit DWORD Value Dialog



Archives older than 12 hours will be deleted automatically after every data collection.

Note: If you do not set the **CleanAutoBackupLogs** registry entry to a value other than 0, you must remove old automatic backups manually, or you may run out of space on a file server's system drive.

9. Click **OK** to save the changes.

Note: In addition to configuration of the settings described above, it is recommended to specify only the essential events for monitoring. This can significantly decrease audit data flow.

2.3. Disk Overfilling Issue on Monitored File Servers

2.3.1. Problem Description

The disk on a monitored file server is overfilled with Security event log auto archives.

2.3.2. What Caused the Problem

Disk overfilling can be caused by the following reasons:

- Removal of processed auto archives is not configured.
- The maximum size of the Security event log does not meet the requirements of Table 1: Security Event Log Requirements for Windows Operating Systems, so NetWrix File Server Change Reporter cannot process auto archives and remove them.
- The disk where auto archives are stored is too small to contain all archives accumulated between two NetWrix File Server Change Reporter data processing tasks.

2.3.3. How to Fix

To solve the problem, check the state of the audit archives automatic removal option (for more information on how to do this, refer to Procedure 4 To configure automatic archiving of the Security event log). Enable it, if it is disabled. If the automatic removal option is enabled, check the audit archives creation date (the current location of the Security event log can be found by viewing the log's properties in the Event Viewer):

- If archives are stored longer than it is defined by the limiting CleanAutoBackupLogs parameter, make sure that Security event log is reachable by NetWrix File Server Change Reporter and the log's size meets the requirements listed in Table 1: Security Event Log Requirements for Windows Operating Systems.

- If archives are not stored longer than it is defined by the limiting CleanAutoBackupLogs parameter, it means that audit archives fill the free disk space before NetWrix File Server Change Reporter removes them. To resolve the problem, do either of the following:
    - Change the location of the Event Viewer log files. Move them to a disk with more free space available. Audit archives will be accumulated on the disk and removed after the data collection.

      NOTE: For information on how to do this for Windows 2000 and Windows Server 2003, refer to the following Microsoft technical article. For Windows Server 2008, log location can be changed under the log properties. It is recommended to reboot your server after this.
    - Configure NetWrix File Server Change Reporter data processing task to run more frequently and decrease the value of the CleanAutoBackupLogs parameter. If the task runs frequently enough to prevent the Security event log from being filled up, you can disable the automatic archiving option (the disk will not be overfilled, but this can cause audit data loss).

      NOTE: If you have other NetWrix change reporting products installed, when configuring the CleanAutoBackupLogs parameter, remember that other NetWrix products must have an opportunity to process audit archives before they are removed.

2.4. Incorrect Data in Reports Without Any Warnings

2.4.1. Problem Description

You receive reports containing no information or the 'System' value in the 'Who changed' column with no warning.txt file attached.

2.4.2. What Caused the Problem

The problem can be caused by one of the following:

- The Security event log is not populated with new events.
- The Security event log was relocated.

2.4.3. How to Fix

If you change the location of the Security event log and do not reboot your file server, the system services may not update their setting according to the new configuration. Therefore, you must reboot your file server.

If you have not relocated the Security event log, perform one of the following to resolve the issue:

- Open the Security event log using the Event Viewer. If the log is corrupted or contains events with ID 521, this may indicate that there is not enough free disk space to store new information. Provide more disk space and clear the log (for additional information, refer to Section 2.3 Disk Overfilling Issue on Monitored File Server).
- Make sure that either the **Overwrite events as needed** retention method is selected, or the Security log automatic archiving option is enabled (for information on how to do this, refer to Procedure 4 To configure automatic

archiving). Using the **Resultant Set of Policies** (RSoP) snap-in, verify that these settings are not overridden by Group Policies. To do this, navigate to **Start → Run** and execute the `cmd` command. Type the `rsop.msc` command and press **Enter.**

2.5. If You Have Not Found a Solution

If your issue has not been covered in this troubleshooting guide, please try to find a solution to it in the Knowledge Base available on the NetWrix website. Otherwise, you can submit a ticket to NetWrix Technical Support Team.

NetWrix Technical Support Team usually requests the following information:

1. The problematic email report.
2. The warning.txt file, which is usually attached to the problematic email report.
3. All contents of the \Tracing sub-directory of the program installation folder.

A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support NetWrix File Server Change Reporter:

Table 3: Product Documentation

Document Name	Overview
NetWrix File Server Change Reporter Troubleshooting Guide	The current document provides step-by-step instructions on troubleshooting of incorrect reporting.
NetWrix File Server Change Reporter Administrator's Guide	The guide provides detailed instructions on how to configure and use NetWrix File Server Change Reporter
NetWrix File Server Change Reporter Quick Start Guide for the Enterprise Edition	The guide provides instructions on how to start working with the program quickly and easily.
How to Perform File System Backup and Restore with NetWrix File Server Change Reporter	The technical article provides instructions on how to roll back to a previously saved back-up point using NetWrix File Server Change Reporter.
Installing Microsoft SQL Server and Configuring the Reporting Services	The technical article provides instructions on how to install Microsoft SQL Server 2005/2008/2008 R2 Express and configure the Reporting Services.
How to Configure NetWrix File Server Change Reporter to Monitor NetApp Filer CIFS Shares	The technical article provides detailed instructions on how to configure NetWrix File Server Change Reporter and NetApp filer CIFS shares for auditing.
How to Configure NetWrix File Server Change Reporter to Monitor EMC VNX/VNXe/Celerra CIFS Shares	The technical article provides detailed instructions on how to configure NetWrix File Server Change Reporter and the EMC VNX/VNXe/Celerra CIFS shares for auditing.
Subscription to SQL Server Reports	The article provides step-by-step instructions on how to configure subscription to SSRS reports.
NetWrix File Server Change Reporter Quick Start Guide (Freeware Edition)	The document is intended for evaluation of the product Freeware Edition. It provides instructions on how to start working with the program quickly and easily.
How to Configure Granular Audit Policy on a File Server Monitored by NetWrix File Server Change Reporter	The technical article provides instructions on how to configure granular Audit policy on a file server monitored by NetWrix File Server Change Reporter.
NetWrix File Server Change Reporter Release Notes	The document provides a list of known issues that customers may experience while using the release version 3.3.