How to Configure NetWrix File Server Change Reporter to Monitor NetApp Filer CIFS Shares

Technical Article

April/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.

www.netwrix.com

Table of Contents

1. INTRODUCTION

1.1. Overview

This article is intended to help you configure NetWrix File Server Change Reporter and set up reporting on modifications and access events to the files, folders and shares of your NetApp® filer instance.

NetWrix File Server Change Reporter supports auditing of NetApp® filer CIFS shares since version 2.0. If you are running an older version, you can download the latest product edition from NetWrix File Server Change Reporter website.

Note: NetApp Filer is only configurable and available in the NetWrix File Server Change Reporter Standard configuration mode of the Enterprise Edition.

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 outlines its structure.
- Chapter 2 Management Accounts: lists all privileges and access rights required for NetWrix File Server Change Reporter access account and the NetApp management account.
- Chapter 3 NetApp Filer Command Prompt Overview: explains how to access the NetApp filer command line and lists the basic configuration commands.
- Chapter 4 Configuring NetApp Filer Settings: provides instructions on how to configure your NetApp filer to be monitored by NetWrix File Server Changer Reporter.
- Chapter 5 Configuring Audit Setting for the CIFS File Shares: explains how to configure audit settings for the CIFS file shares.
- Chapter 6 Configuring NetWrix File Server Change Reporter: provides instructions on how to configure NetWrix File Server Change Reporter to monitor NetApp filer CIFS shares.
- Chapter 7 Configuring Automatic Deletion of Security Log Auto Archives: explains how to enable automatic deletion of your security log archives.
- A Appendix: Related Documentation: lists all documentation published to support NetWrix File Server Change Reporter.

2. MANAGEMENT ACCOUNTS

This chapter explains the requirements to the NetWrix File Server Change Reporter access account and the NetApp filer management account. Please ensure that these accounts have the necessary access permissions and rights listed below.

2.1. File Server Change Reporter Access Account

On NetWrix File Server Change Reporter configuration, you are prompted to enter an account that will be used by the system for data collection and report generation. This must be a domain user account with the Domain Administrator rights, or with the following access permissions:

- Access to the file shares you are going to monitor ('read' access at least);
- Access to the security log shared folder ('read' access at least; 'write' access is required for automatic log deletion (for details, see Chapter 7 Configuring Automatic Deletion of Security Log Auto Archives).

2.2. NetApp Management Account

The NetApp management account is required to perform the operations related to the security log, and to validate audit settings against NetWrix File Server Change Reporter requirements.

This must be a domain or a NetApp filer local account with the following set of capabilities:

- login-http-admin;
- api-system-cli;
- api-options-get;
- cli-cifs.

These capabilities can be configured using the NetApp filer command prompt (for instructions on how to access the command prompt, refer to Chapter 3 NetApp Filer Command Prompt Overview):

Figure 1: Management Account Configuration

```
apphost01> useradmin user list fscr_user
Name: fscr_user
Info:
Rid: 131077
Groups: fscr_group
Full Name:
Allowed Capabilities: login-http-admin,api-system-cli,api-options-get,cli-cifs
Password min/max age in days: 0/4294967295
Status: enabled

apphost01>
```

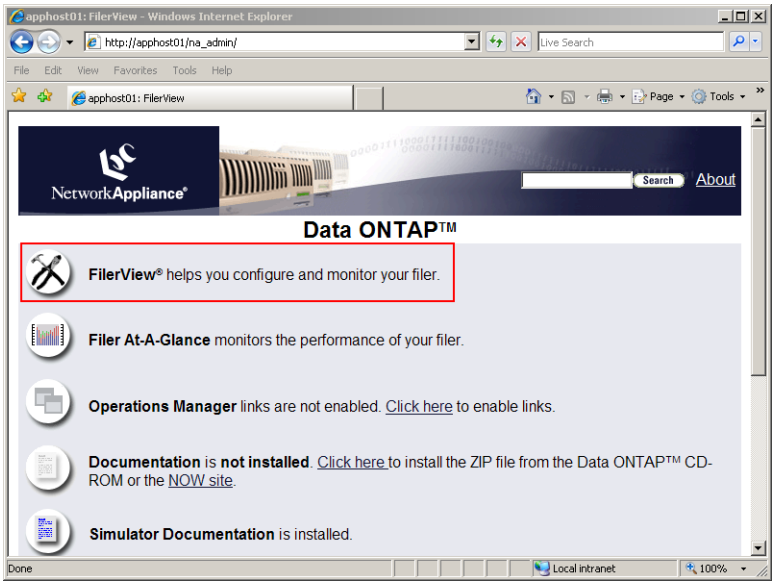
3. NetApp Filer Command Prompt Overview

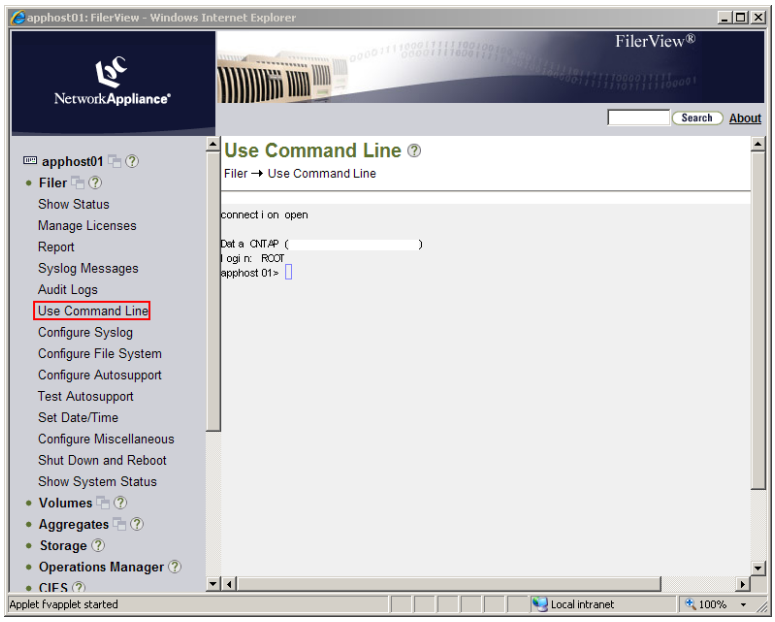
3.1. Accessing the Command Prompt

The NetApp filer command prompt is accessible through SSH/Telnet connection (depending on your NetApp filer settings), or via the web interface.

To access it via the web interface, open the NetApp filer web GUI, and navigate to **FilerView** > **Filer** > **Use Command Line**:

Figure 2: Accessing the Command Prompt





Note: The appearance of your NetApp filer instance may vary slightly from the screenshots used in this document.

3.2. Basic Configuration Commands

To perform the configuration procedures described in Chapter 4 Configuring NetApp Filer Settings of this document, the following commands must be used:

- To get an option value:

```
options <option_name>
```

- To set option value:

```
options <option_name> <option_value>
```

For example, to enable the `cifs.audit.enable` option, execute the following command:

```
options cifs.audit.enable on
```

Note: For a full list of commands and their detailed descriptions, please refer to NetApp command line reference document.

4. Configuring NetApp Filer Settings

This section explains how to configure the NetApp filer for audit by NetWrix File Server Change Reporter. The instructions in this section apply to the default VFiler. If you wish to audit several VFiler instances, you must perform these configuration steps for each of them.

The settings described in this chapter are performed via NetApp filer command line. For instructions on how to access NetApp Filer command line, and for description of some basic configuration commands, please refer to Chapter 3 NetApp Filer Command Prompt Overview.

Note: It is assumed that CIFS shares have already been set up on your NetApp filer.

4.1. Configuring Qtree Security

For auditing to function properly, the volume where the monitored file shares are located must have the security style set to 'ntfs':

Figure 3: Qtree Security

```
apphost01> qtree status
Volume   Tree     Style Oplocks  Status
-------- -------- ----- -------- ---------
vol0              ntfs  enabled  normal
vol0     test     ntfs  enabled  normal
vol1              unix  enabled  normal
vol2              ntfs  enabled  normal
apphost01>
```

4.2. Configuring Admin Web Access

NetWrix File Server Change Reporter uses the NetApp API to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to the MS Event Viewer compatible format.

NetWrix File Server Change Reporter supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

Make sure that `httpd.admin.enable` or `httpd.admin.ssl.enable` is set to 'on'. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option:

Figure 4: HTTPD.ADMIN Access

```
apphost01> options httpd.admin
httpd.admin.access           legacy
httpd.admin.enable           off
httpd.admin.hostsequiv.enable off
httpd.admin.max_connections  512
httpd.admin.ssl.enable       on
httpd.admin.top-page.authentication on
apphost01>
```

If non-default configuration for `httpd.admin.access` is set (i.e. 'limit access to trusted host only' or 'allow admin web access for specific Ethernet interfaces'), make sure that the Web Filer UI is accessible by the name of the audited file server.

For example, the audit share \\file_server\my_share\ must be viewed with the NetApp filer WebUI at http(s)://file_server/na_admin/.

4.3. Configuring CIFS Auditing

4.3.1. Configuring Audit Events Categories

To configure audit event categories, perform the following steps:

1. Set the following options to 'on':
   - `cifs.audit.enable`
   - `cifs.audit.file_access_events.enable`
2. Unless you are going to audit logon events, set the following options to 'off':
   - `cifs.audit.logon_events.enable`
   - `cifs.audit.account_mgmt_events.enable`

4.3.2. Configuring the Security Log

NetWrix File Server Change Reporter supports processing of auto-saved audit logs. In order to avoid overwriting of the security logs, the following settings are recommended:

- `cifs.audit.logsize` `300 000 000 (300 MB)`
- `cifs.audit.autosave.onsize.enable` `on`
- `cifs.audit.autosave.file.extension` `timestamp`

Also, you must disable the `cifs.audit.liveview.enable` option, since it interferes with the normal security log behavior and prevents NetWrix File Server Change Reporter from processing audit data properly.

Figure 5: Security Log Settings

```
apphost01> options cifs.audit
cifs.audit.account_mgmt_events.enable off
cifs.audit.autosave.file.extension timestamp
cifs.audit.autosave.file.limit 0
cifs.audit.autosave.onsize.enable on
cifs.audit.autosave.onsize.threshold 75%
cifs.audit.autosave.ontime.enable off
cifs.audit.autosave.ontime.interval 1d
cifs.audit.enable           on
cifs.audit.file_access_events.enable on
cifs.audit.liveview.enable   off
cifs.audit.logon_events.enable off
cifs.audit.logsize          300000000
cifs.audit.nfs.enable       off
cifs.audit.nfs.filter.filename
cifs.audit.saveas           /etc/log/adtlog.evt
apphost01>
```

Note: Due to Windows Server 2003 limitations, a security log larger than 300 MB cannot be processed. If you wish to have a log that exceeds 300 MB, NetWrix File Server Change Reporter must be installed on Windows Server 2008 / Windows Vista / Windows 7. However, even on these

Windows versions, it is not recommended to set security log size to a value that exceeds 300 MB, since this may slow down security log conversion and cause performance issues.

Make sure there is enough disk space allotted to the security logs archives. Depending on the file access activity, audit data may grow rapidly, and the location specified for the security log (and security log auto archives) must be large enough to hold data until it is processed by NetWrix File Server Change Reporter (by default, data collection runs every 24 hours). To set up old logs deletion, you can configure the `cifs.audit.autosave.file.limit` option by specifying the maximum number of files to be stored, or enable the built-in automatic log deletion option in NetWrix File Server Change Reporter (for instructions on how to do this, refer to Chapter 7 Configuring Automatic Deletion of Security Log Auto Archives).

4.3.3. Specifying the Security Log Shared Folder

NetWrix File Server Change Reporter accesses audit logs via a specified file share. This may be either the default administrative share (ETC$, C$, etc.), or a custom file share.

Use the `cifs shares` command to create a new file share or configure an existing share:

Figure 6: Cifs Shares Configuration

```
apphost01> cifs shares
Name          Mount Point                      Description
----          -----------                      -----------
ETC$          /etc                             Remote Administration
                        BUILTIN\Administrators / Full Control
C$            /                                Remote Administration
                        BUILTIN\Administrators / Full Control
share1        /vol/vol0/shares/share1
                        everyone / Full Control
```

Note: For a detailed description of the `cifs shares` command, please refer to NetApp command line reference document.

5. Configuring Audit Setting for the CIFS File Shares

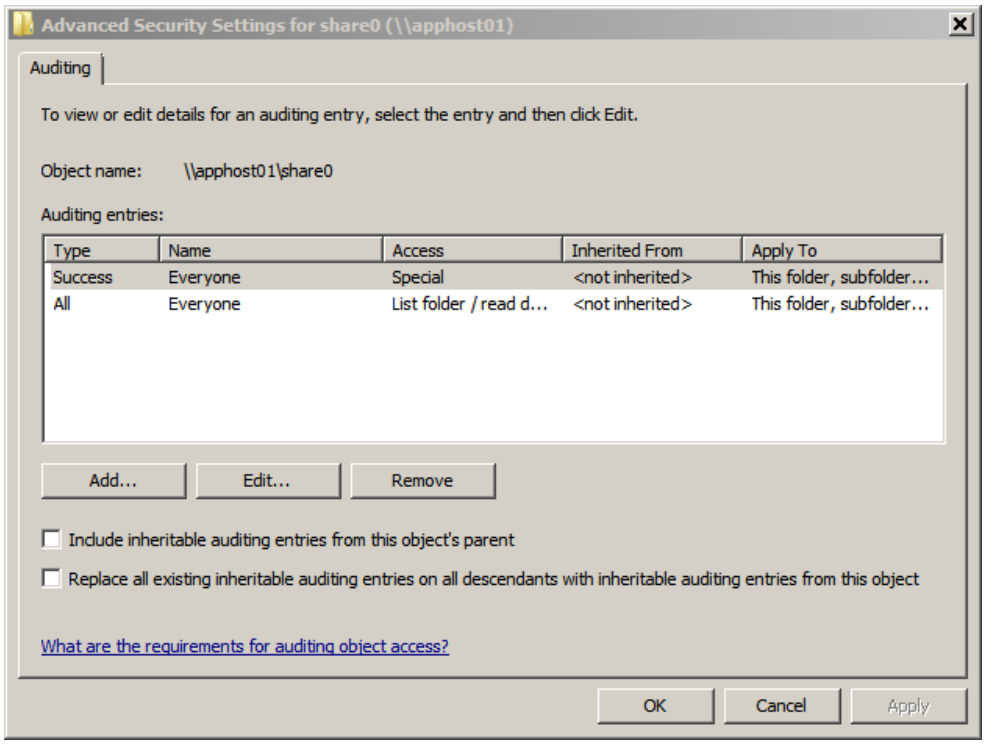
To configure audit settings for the CIFS file shares, perform the following steps on the monitored file share:

1. Navigate to the root share folder.
2. Right-click it and select **Properties** from the popup menu.
3. Open the **Security** tab.

Note: If there is no such tab, it means a wrong security style has been specified for the volume holding this file share. For instructions on how to configure the file share, please refer to Section 4.1 Configuring Qtree Security.

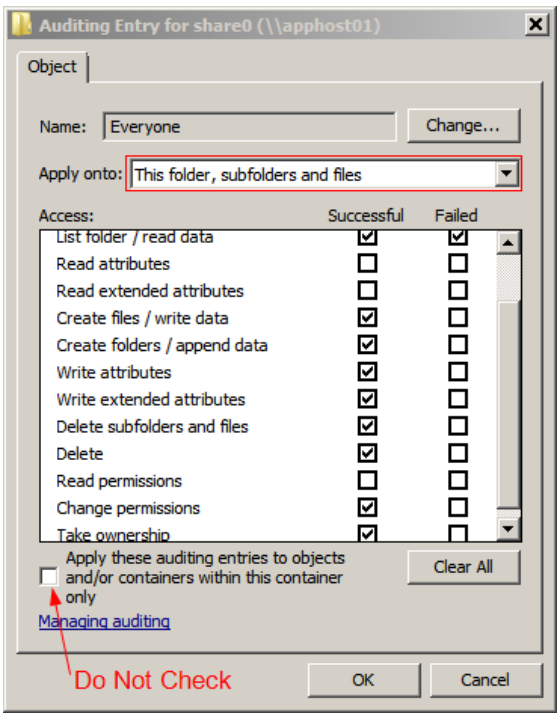
4. Click the **Advanced** button, and then select the **Auditing** tab.
5. Click **Edit**. The following dialog will be displayed:

Figure 7: Advanced Security Settings



6. Select the 'Success Everyone' entry, click **Edit** and make sure it is configured as shown in the figure below:

Figure 8: Auditing Entry Configuration



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

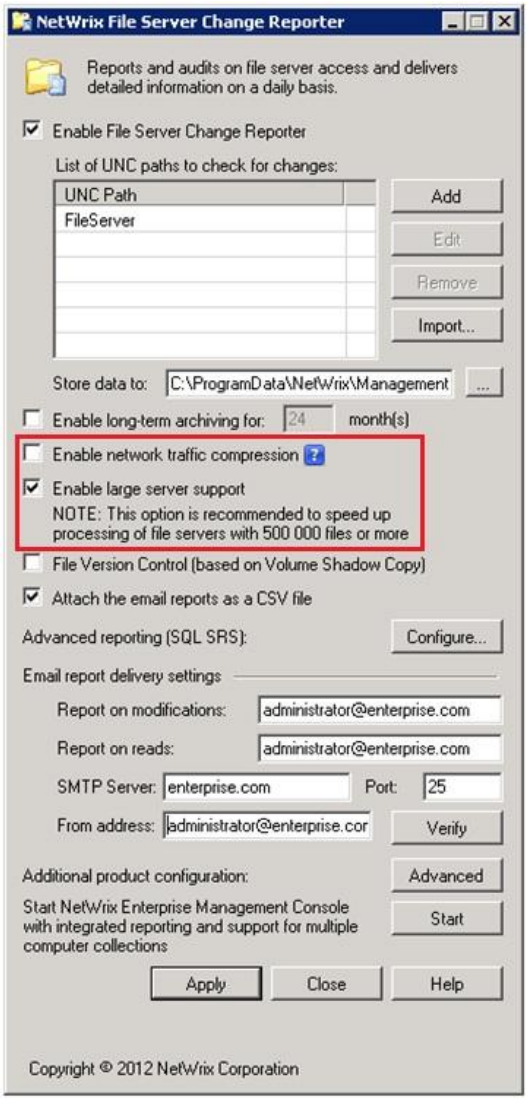
6. Configuring NetWrix File Server Change Reporter

This chapter explains how to configure NetWrix File Server Change Reporter to monitor NetApp Filer CIFS shares.

To do this, perform the following steps:

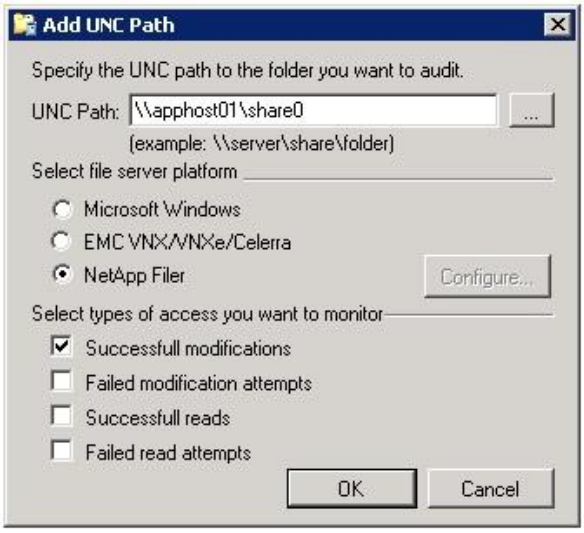
1. Launch NetWrix File Server Change Reporter Standard configuration mode (**Start** > **All Programs** > **NetWrix** > **File Server Change Reporter** > **File Server Change Reporter (Standard Edition)**).
2. Select the **Enable large server support** option, and deselect the **Enable network traffic compression** option:

Figure 9: NetWrix File Server Change Reporter Standard Configuration Main Window



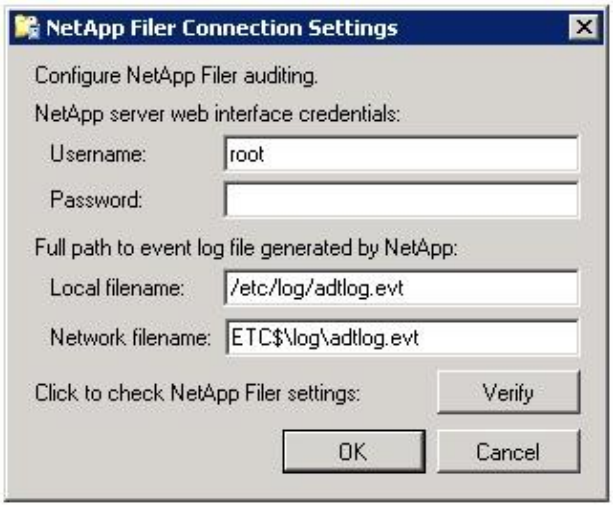
3. Click the **Add** button to add a UNC path. Specify the path and select NetApp Filer as the file server platform:

Figure 10: Add UNC Path Dialog



4. Click **Configure**. The following dialog will be displayed:

Figure 11: NetApp Filer Connection Settings



5. Specify the following parameters:

Table 1: NetApp Filer Parameters

Parameter	Description
Username	Specify the NetApp management account. For a detailed description of a management account, please refer to Section 2.2 NetApp Management Account .
Password	Enter the NetApp management account password.
Local filename	Specify the local path in the NetApp filer to the file where the event log files are to be saved. This file must be in .evt format. Example /etc/log/adtlog.evt.
Network filename	Specify the network path to the event log file. **NOTE**: The path must be entered without the server name, for example, \ETC$\log\adtlog.evt.

6. Click **Verify** to ensure that the values you have entered are correct. If errors are returned, check that:

- A valid filer DNS name or IP address were specified in the UNC Path;
- HTTP or HTTPS admin access has been enabled on the NetApp filer (for instructions on how to do this, please refer to Section 4.2 Configuring Admin Web Access);
- The Network filename you have specified is valid and the UNC path is accessible from the machine where NetWrix File Server Change Reporter is installed.

7. Configuring Automatic Deletion of Security Log Auto Archives

NetWrix File Server Change Reporter can be configured to automatically delete old EVT log files. To do this, perform the following steps:

1. Open the Registry Editor (go to **Start** > **Run** and type `regedit`).
2. Expand HKEY_LOCAL_MACHINE\SOFTWARE\NetWrix\File Server Change Reporter (for 64 bit operating systems the path is HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetWrix\File Server Change Reporter).
3. Set the 'CleanAutoBackupLogs' value to 1 and click **OK**.
4. Create a new DWORD value, if it does not exist.

With such configuration, log files older than 1 hour will be removed automatically. If the value is set to 0 or is not specified, log files will be kept forever.

A APPENDIX: RELATED DOCUMENTATION

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

Table 2: Product Documentation

Document Name	Overview
How to Configure NetWrix File Server Change Reporter to Monitor NetApp Filer CIFS Shares	The current document provides detailed instructions on how to configure NetWrix File Server Change Reporter and NetApp filer CIFS shares for auditing.
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.
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.
NetWrix File Server Change Reporter Troubleshooting Guide	The guide provides step-by-step instructions on troubleshooting incorrect reporting.
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 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.
Installing SQL Express on Windows Vista Technical Article	The article provides detailed instructions on how to install SQL 2005 with Advanced Services on Windows Vista.
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.