NETWRIX CHANGE NOTIFIER FOR FILE SERVERS

QUICK-START GUIDE

Product version: 3.3.231

February 2014

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

Netwrix Change Notifier for File Servers tracks all changes to the monitored Windows-based CIFS file shares and emails daily Change Summaries listing all changes that occurred in the last 24 hours.

1.2. Supported Environments

Netwrix Change Notifier for File Servers supports auditing of Windows-based file servers running Windows 2000 and above.

1.3. Licensing

Netwrix Change Notifier for File Servers is a freeware product with an unlimited license.

1.4. How It Works

The product data collection and reporting workflow is as follows:

1. An administrator sets the parameters for automated data collection and specifies which file shares to monitor.
2. A dedicated scheduled task which is launched daily collects audit data and emails Change Summaries to the specified recipients. You can also use the Change Viewer tool to generate and view on-demand summaries.

The product reports the following types of events:

- Successful modifications
- Successful reads

2. Install Netwrix Change Notifier for File Servers

2.1. Deployment Options

Netwrix Change Notifier for File Servers can be installed on any computer in the domain where the monitored file servers are located.

If you want to monitor file servers located in different domains, the monitored servers must have accounts with the same name and password as the account under which the product is run. Both accounts must have the local administrator permissions.

2.2. Hardware Requirements

Before installing Netwrix Change Notifier File Servers, make sure that your hardware meets the following requirements:

Table 1: Netwrix Change Notifier Hardware Requirements

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2GHz	Intel Core 2 Duo 2x 64 bit, 3GHz
Memory*	512 MB RAM	4 GB RAM
Disk space	• 50MB physical disk space for product installation. • Additional space is required for the Audit Archive and depends on the average number of changes per day.	Two physical drives with a total of 20GB free space

* **These are rough estimations. The actual required memory size depends on the average number of changes per day in the monitored environment.**

2.3. Software Requirements

This section lists the minimum software requirements for Netwrix Change Notifier for File Servers. Make sure that this software has been installed before proceeding with the installation.

Table 2: Netwrix Change Notifier Software Requirements

Component	Requirement
Operating System	• Windows 7 and above
Additional software	• .NET Framework 3.5 • Windows Installer 3.1 or above

2.4. Installing Netwrix Change Notifier for File Servers

To install Netwrix Change Notifier File Servers, download and run the Netwrix_Change_Notifier_for_File_Servers.msi file. Follow the instructions of the installation wizard. When prompted, accept the license agreement and specify the installation folder.

3. Configure Rights and Permissions

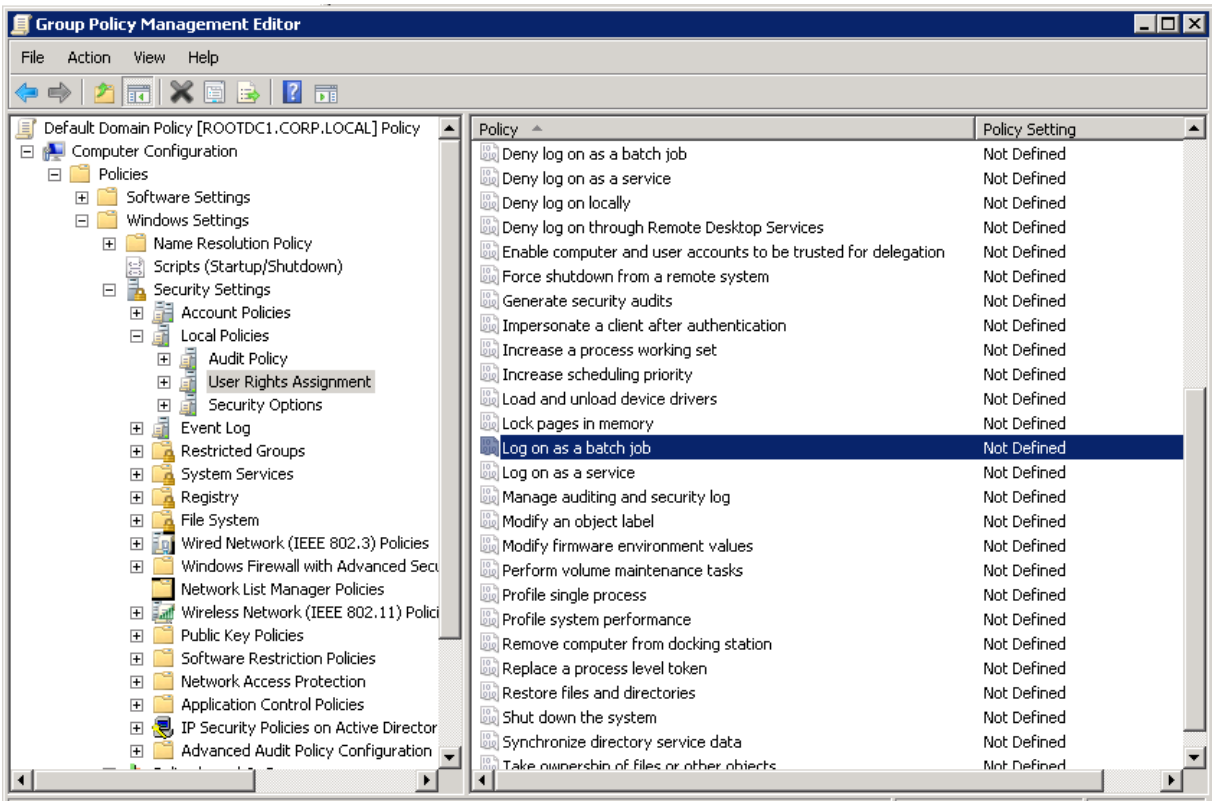
The account under which Netwrix Change Notifier for File Servers collects data from the monitored servers must have the following rights and permissions:

- The account must be a member of the **Local Administrators group** on the computer where the product is installed
- The **Log on as a batch job** policy must be defined for this account (see Procedure 1 To define the Log on as a batch job policy)
- The account must be assigned the **Manage auditing and security log** right (see Procedure 2 To assign the "Manage auditing and security log" right)
- The account must have the read access to the monitored shares.

Procedure 1. To define the Log on as a batch job policy

1. Open the **Group Policy Management** console on any domain controller in the monitored domain: navigate to **Start → Administrative Tools → Group Policy Management**.
2. In the left pane, navigate to **Forest: <domain_name> → Domains → <domain_name>**, right-click **Default Domain Policy** and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment** and locate the **Log on as a batch job** policy:

Figure 1: Group Policy Management Editor



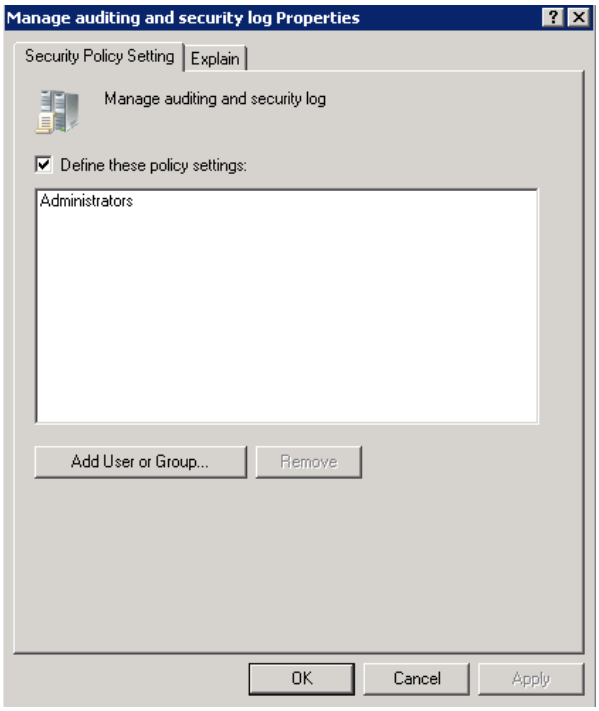
4. Double-click this policy, select **Define these policy settings** and click **Add User or Group**. Specify the account that you want to define this policy for.

5. Navigate to **Start → Run** and type `cmd`. Input the gpupdate /force command and click **Enter** to update the group policy.

Procedure 2. To assign the "Manage auditing and security log" right

1. Open the Group Policy Management console on any domain controller in the domain where the monitored servers are located: navigate to **Start → Group Policy Management**.
2. In the left pane, navigate to **Forest: <domain_name> → Domains → <domain_name> → Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**) node and select **Edit** from the popup menu.
3. In the Group Policy Management Editor, in the left pane, navigate to **Computer Configuration → Policies → Windows Settings → Security Settings** and select **Local Policies**.
4. On the right, double-click the **User Rights Assignment** policy.
5. Locate the **Manage auditing and security log** right and double-click it. The Manage auditing and security log Properties dialog will be displayed:

Figure 2: Manage Auditing and Security Log Properties Dialog



6. Select the **Define these policy settings** option and click the **Add User or Group** button. In the dialog that appears, type in the name of the user that you want to grant this right to and click **OK**.
7. Open the command line interface: navigate to **Start** and type "`cmd`".
8. Type the "`gpupdate /force`" command and press **Enter**. The group policy will be updated.

4. Configure Audit Settings

For Netwrix Change Notifier for File Servers to collect data on changes, you must perform the following procedures:

- Configure Object Access Audit
- Configure Audit Settings on File Shares

4.1. Configure Object Access Audit

For Netwrix Change Notifier for File Servers to collect data on changes, you must define the audit policy settings for the Object Access event category.

To perform this procedure, you must be logged on as a member of the Administrator's group, or you must be granted the **Manage auditing and security log** right.

To enable audit settings centrally on all monitored servers, it is recommended to create a Group Policy Object and assign it to the organizational unit where your file servers are located. For instructions on how to create a Group Policy Object, refer to the following Microsoft article: Create a new Group Policy object.

Procedure 3. To configure object access auditing

1. In the Group Policy Object, navigate to **Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy** node.
2. Locate the **Audit object access** policy. Double-click this policy, select the **Define these policy settings** option and select **Success**.

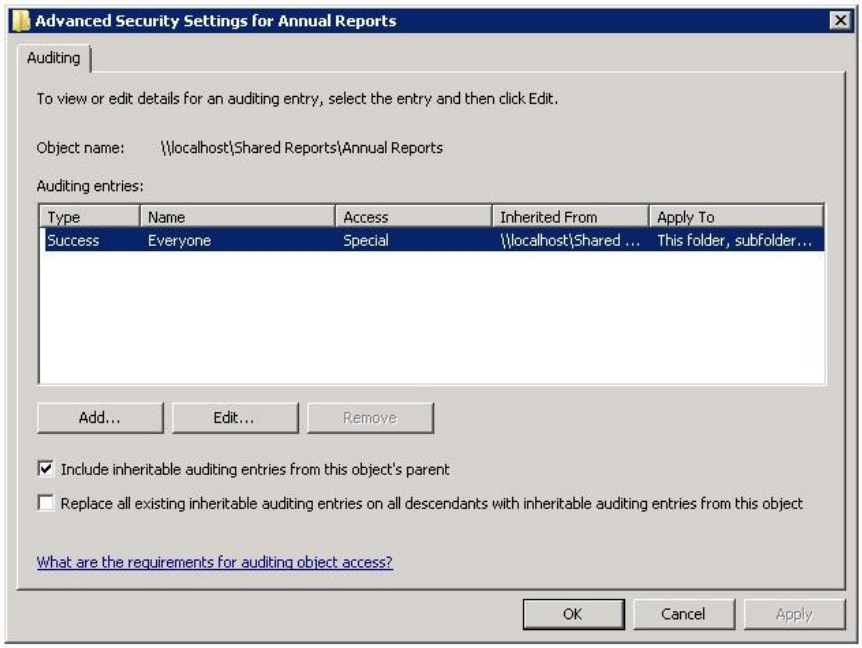
Alternatively, you can use the local policy as described in the following Microsoft article: Define or modify auditing policy settings for an event category.

4.2. Configure Audit Settings on File Shares

Procedure 4. To configure the default audit settings on file shares

1. Navigate to the required file share, right-click it and select **Properties** from the pop-up menu. The **<Share_Name> Properties** form will open.
2. Select the **Security** tab and click **Advanced**. The **Advanced Security Settings for <Share_Name>** form will open.
3. Navigate to the **Auditing** tab, select the **Everyone** group (or another user-defined group of the selected users granted special permissions) and click **Edit**. The **Advanced Security Settings for <Share_Name>** form will open as a separate dialog:

Figure 3: Advanced Security Settings



Note: You can specify any other required user group, but in this case the current version of Netwrix Change Notifier for File Servers will send you email reports with warnings about the audit configuration. This will not affect the reporting functionality and the product will only monitor user accounts that belong to the selected group.

4. Select the **Everyone** group and click the **Edit** button. The **Auditing Entry for <Share_Name>** dialog will appear.
5. Select the **Success** check-box for the following Access option: List Folder / Read Data.

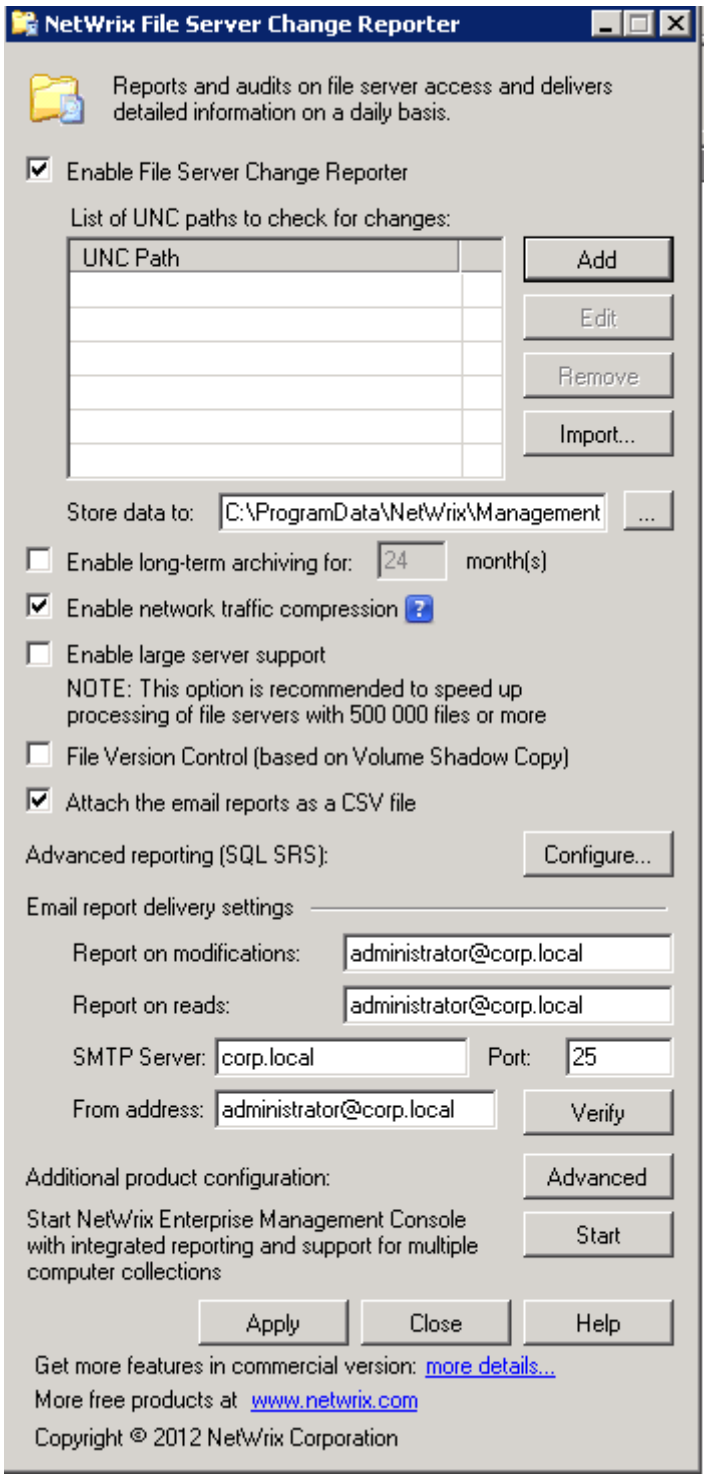
5. Configure Netwrix Change Notifier for File Servers

After you have installed Netwrix Change Notifier for File Servers, you need to enable and configure file servers audit.

Procedure 5. To configure file servers audit

1. Navigate to **Start → All Programs → Netwrix Freeware → Netwrix Change Notifier for File Servers.** The product configuration dialog will open:

Figure 4: Netwrix Change Notifier for File Servers Dialog



2. Specify the following settings and parameters:

Table 3: Netwrix Change Notifier for File Servers Settings

Parameter	Instruction
Enable File Server Change Reporter	Enable this option to activate File Servers audit.
List of UNC paths to check for changes:	Click the Add button and specify the UNC path to the file share you want to audit. In the **Select file server platform**, make sure the Microsoft Windows option is selected. **Note:** Auditing of EMC and NetApp Filer appliances is not supported. In the **Select types of access you want to monitor** section, select **Successful modifications** and **Successful reads**. **Note:** Reporting on failed reads and modifications attempts is not supported.
Enable long-term archiving for:	This option is not supported.
Enable network traffic compression	Select this option to enable agent-based data collection to reduce server load.
Enable large server support	This option is not supported.
File Version Control	This option is not supported.
Attach the email reports as a CSV file	Select this option if you want audit information to be attached to the Change Summary emails, instead of being sent in the message body.
Advanced reporting (SQL SRS)	This option is not supported.
Report on modifications:	Specify the email address where reports on successful modifications must be sent.
Report on reads:	Specify the email address where reports on successful read attempts must be sent.
SMTP Server	Specify the SMTP server name for email delivery.
Port	Specify your SMTP server port number.
From address	Specify the address that will appear in the “From” field in the Change Summary emails.
Additional product configuration	Click the **Advanced** button to modify the default Change Summary delivery schedule (3:00 AM) and enable SMTP authentication and an implicit SSL connection mode.
Start Netwrix Enterprise Management Console	This option is not supported.

3. Save your configuration by clicking the **Apply** button. The **Scheduled Task Credentials** dialog will be displayed.
4. Specify the account under which the product will collect audit data. Make sure that the account has the required rights and permissions (see Chapter 3 Configure Rights and Permissions).
5. Enter and confirm the account password and click **OK**.

Note: To change the settings later, launch the product configuration dialog from the **Start** menu.

6. Monitor Your File Servers for Changes

When the product has been configured, it starts collecting data on file server changes. By default, the data collection task is launched daily at 3:00 AM. If required, you can launch the product scheduled task manually or modify its schedule.

6.1. Launch the Product Task Manually

Procedure 6. To launch the product scheduled task manually:

1. Launch **Task Scheduler**.
2. In the left pane, expand the **Task Scheduler Library** node. In the right pane, select the task called ***Netwrix Management Console - File Server Change Reporter - <your_computer_collection_name>*** (where <your_domain_name> is the name of the domain you specified in the configuration settings).
3. Right-click the task and select **Run** from the drop-down list. Alternatively, use the **Run** option from the **Actions** menu.

6.2. Modify the Product Task Schedule

Procedure 7. To modify the product task schedule:

1. Launch Netwrix Change Notifier for File Servers.
2. In the main configuration dialog, click the **Advanced** button at the bottom.
3. In the dialog that opens, modify the default schedule, click **OK**, and click **Apply** in the main window to save the changes.

6.3. View a Change Summary

After the first data collection task has finished, an email will be delivered to the specified address notifying you that the initial analysis has been completed.

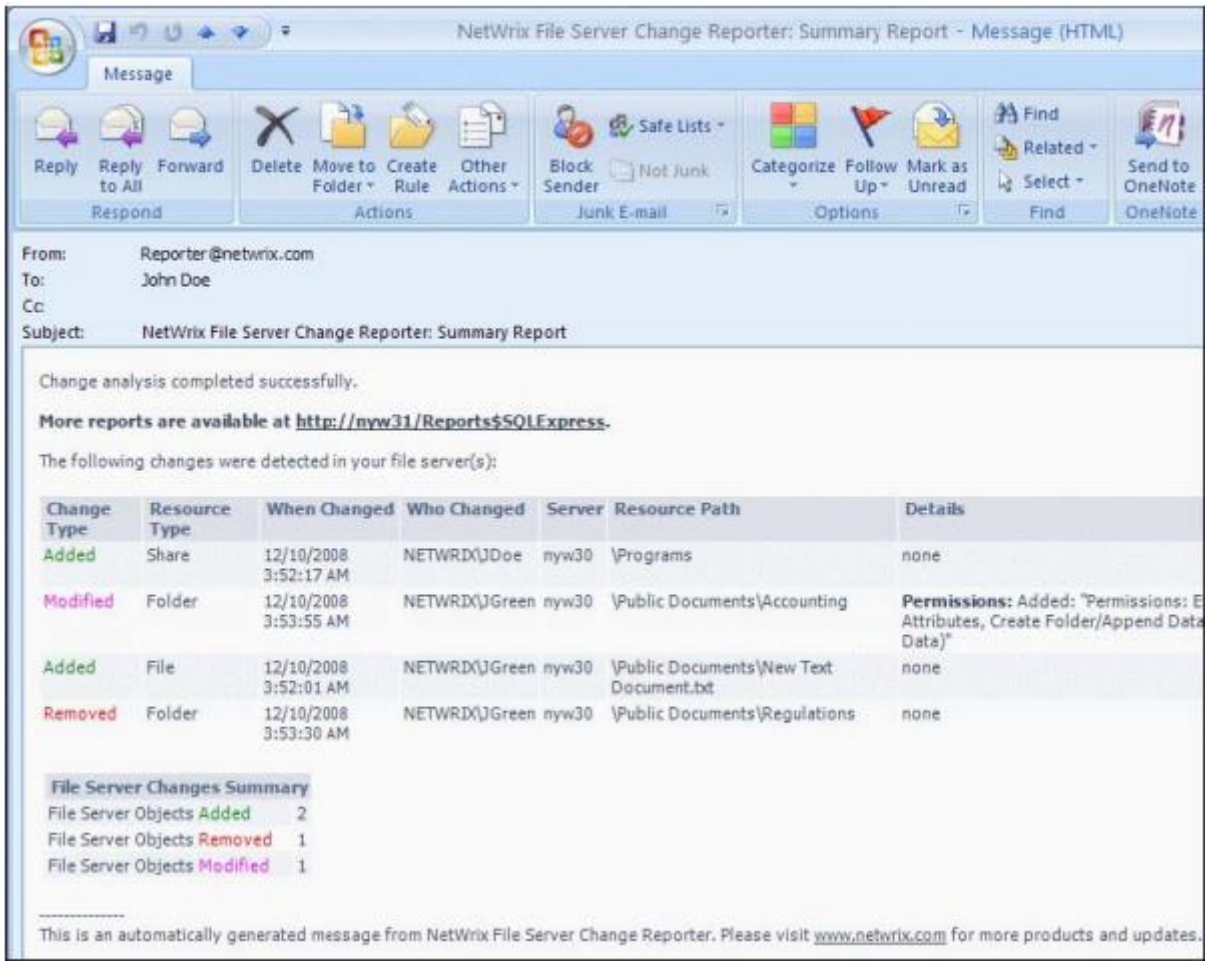
After that, you can make test changes to your environment to see how they are reported.

When the task is launched the next time (either automatically or manually), it detects the changes made since the last data collection, generates and delivers the Change Summary to the specified recipients. A Change Summary contains the following information:

- Change type (Added/Removed/Modified)
- Resource type (share, file or folder)
- Server: the server that hosts the monitored share
- Resource path: the path to the monitored share
- Details (the modified properties and their before and after values)

Below is an example of the Netwrix Change Notifier for File Servers Change Summary:

Figure 5: Netwrix Change Notifier Change Summary Example



6.4. Generating an On-Demand Change Summary

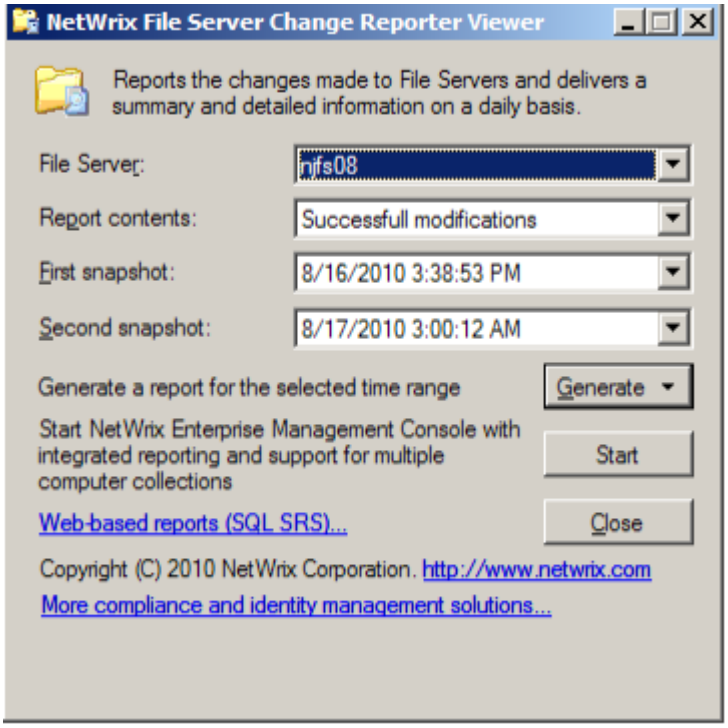
You can generate Change Summaries for a specific period of time using the Report Viewer tool.

Note: The product allows you to generate a summary of changes collected within the last 2 days only.

Procedure 8. To generate an on-demand Change Summary

1. Navigate to **Start → All Programs → Netwrix Freeware → Netwrix Change Notifier for File Servers → Report Viewer.** The following dialog is displayed:

Figure 6: Report Viewer Dialog



2. Select the file server from the drop-down list, the type of data, and the time range you want to generate the report on.
3. Click **Generate**. The **Save as** window appears allowing you to name your report and select the location for it. Click **Save**.
4. The Change Summary is saved locally in the HTML format and displayed in your default web browser.