



# Filtering out System Messages in the Who Changed Column

NetWrix File Server Change Reporter  
Technical Article

# Table of Contents

Applies To.....	1
Summary .....	1
Steps to Resolve .....	2
Default Audit Settings on Shares Result in Incorrect Report .....	2
Security Log Overflow Occurred.....	5
Additional Information.....	7

## Contacting NetWrix Support

If you have any questions please feel free to contact the [NetWrix support team](#).

NetWrix provides unlimited phone and email support for customers who purchase the commercial version (including evaluation). In addition, on the [NetWrix Support Forum](#), a limited support is provided for customers who use the freeware version.

## Disclaimer

The information in this publication is furnished for information use only, does not constitute a commitment from NetWrix Corporation of any features or functions discussed and is subject to change without notice. NetWrix Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

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.

© 2011 NetWrix Corporation. All rights reserved.

[www.netwrix.com](http://www.netwrix.com)

## Applies To

NetWrix File Server Change Reporter 3.2 or later (hereafter *FSCR*)

## Summary

One of the most frequent issues reported to technical support is that the Who Changed column in the FSCR reports contains *System* as originator of changes. This is a very common error resulted from current auditing settings that must be changed on file servers monitored by the product.

As a rule, the problematic reports have the *warning.txt* file attached. This file contains error messages that usually give an idea where the problem is located.

## Steps to Resolve

This section discusses some typical error messages you may encounter in the *warning.txt* file and provides the solution procedures.

### Default Audit Settings on Shares Result in Incorrect Report

In the *warning.txt* file, you may encounter the following error message and a list of file shares:

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.

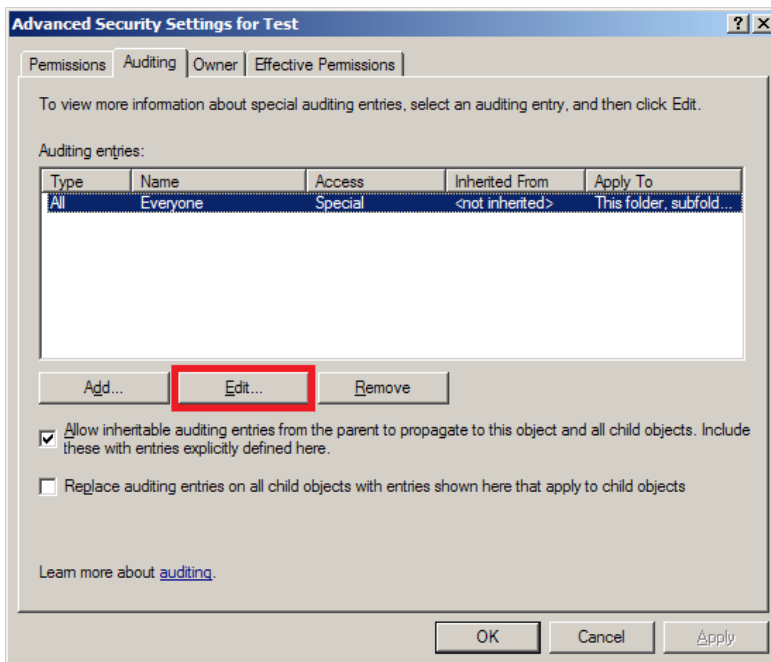
#### Cause

This issue occurs when auditing is not configured for monitored file servers.

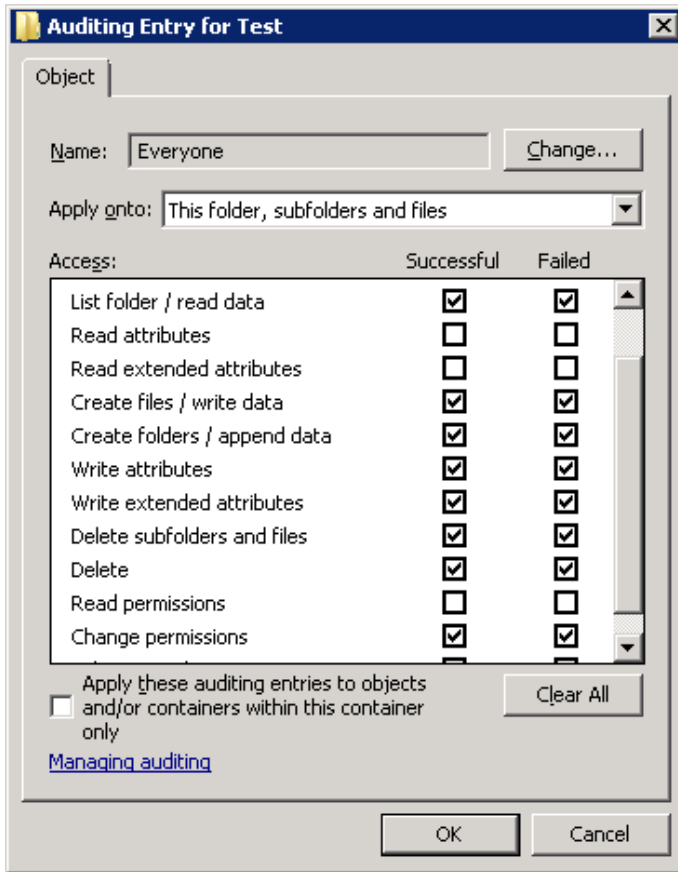
#### Solution

To resolve this issue, complete the following steps:

1. Right-click the file share in question, and on the shortcut menu, click **Properties**.
2. In the **Properties** dialog box, open the **Security** tab, and click **Advanced**.



3. In the **Advanced Security Settings** dialog box, under **Auditing entries**, select the Everyone group, and then click **Edit**.

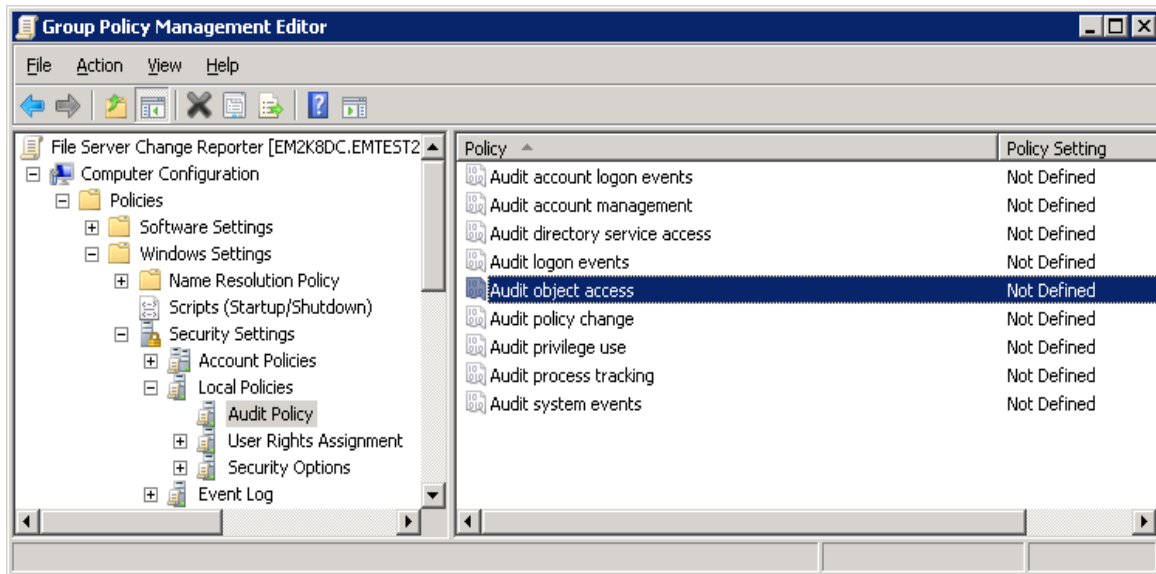


4. In the **Auditing Entry** dialog box, from the **Apply onto** list, select **This folder, subfolders and files**.
5. Ensure that the **Apply these auditing entries ...** check box is cleared, while the **Successful** and **Failed** check boxes next to the following access options are selected:
  - List Folder / Read Data (required only for monitoring access attempts)
  - Create Files / Write Data (these access options and the following ones are required for monitoring changes)
  - Create Folders / Append Data
  - Write Attributes
  - Write Extended Attributes
  - Delete Subfolders and Files
  - Delete
  - Change Permissions
  - Take Ownership
6. Click **OK**.

In Group Policy enforced on the managed file servers, it is necessary to set the *Audit object access* policy setting to **Success and Failure**.

To perform this, it is recommended to create a Group Policy Object and link it to your server OU, using the following steps:

1. Open Group Policy Management console.
2. In the console tree, select the Organizational Unit where your file server resides, and on the **Action** menu, click **Create a GPO in this domain and Link it here ...**
3. In the **New GPO** dialog box, in the **Name** text box, type (for example) `File Server Change Reporter`, and click **OK**.
4. Select the newly created File Server Change Reporter GPO, and on the **Action** menu, click **Edit**.
5. In the Group Policy Management Editor console tree, expand **Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies**, and then click **Audit Policy**.



6. In the details pane, double-click **Audit object access**.
7. On the **Security Policy Setting** tab of the **Audit object access Properties** dialog box, select all check boxes, and click **OK**.



8. Click **OK**

## Security Log Overflow Occurred

In the *warning.txt* file, you may encounter the following warning message:

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

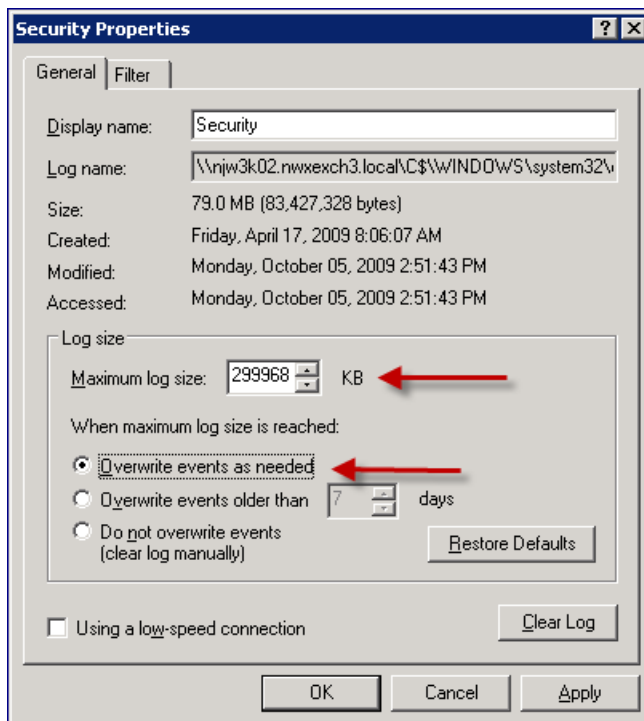
### Cause

This issue occurs when the maximum size of the Security event log is not enough to store all necessary information.

### Solution


To resolve this issue, increase the maximum size of the Security Event log for the problematic file servers by performing the following steps:

1. On the file server where this error occurred, open Event Viewer.
2. Right-click the **Security log** and click **Properties**
3. In the **General** tab, set the **Maximum log size** to a recommended value (for more information, see NetWrix KB article at [http://www.netwrix.com/kb\\_5017000000ijCg](http://www.netwrix.com/kb_5017000000ijCg), select the **Overwrite events as needed** option, and click **OK**.



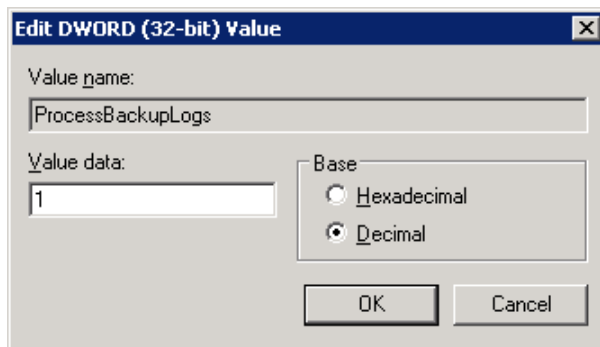
 You must be a member of the Administrators group to perform this procedure.

If this procedure does not help you resolve this issue, enable the automatic archiving the Security Event log when full. For information about how to configure this option, see NetWrix KB article at [http://www.netwrix.com/kb\\_50170000000ijCl](http://www.netwrix.com/kb_50170000000ijCl) or refer to documentation on Event Viewer you are actually using on the file server.

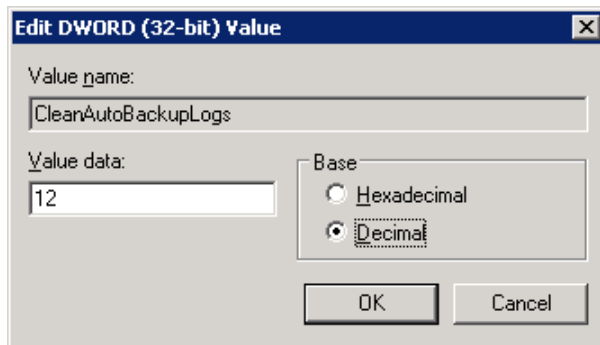
 Depending on the level of access activity on your file servers and the enforced audit policies, the Security log auto-backup files may fill up the free space on your disk drive faster than FSCR can remove them. In this case, you may need to provide more space on the system drive of your file server.

In addition, on the computer where FSCR is installed, perform the following steps:

1. Open Registry Editor.
2. Expand the **HKLM\SOFTWARE\NetWrix** node (on 64-bit systems, expand **HKLM\Software\Wow6432Node\NetWrix**), and click **File Server Change Reporter**.
3. Change the following values:
  - Set the **ProcessBackupLogs** value to 1 and click **OK**:



- Set the **CleanAutoBackupLogs** value to any integer, such as 12, and click **OK** — in this scenario, the archives older than 12 hours will be automatically deleted:



 If you did not set the **CleanAutoBackupLogs** value to any integer, remove old automatic backups manually. Otherwise, you may run out of space on your hard drive.



## Additional Information

Last updated: February 4, 2011

These are typical steps used to fix the *System* message in the **Who Changed** column. If the procedures described in this article do not help you resolve this issue, submit a ticket to NetWrix support team at:

[http://www.netwrix.com/support\\_ticket.html](http://www.netwrix.com/support_ticket.html)

Provide the following information:

1. The problematic email report (attach it to email).
2. The *warning.txt* file that is usually attached to the problematic email.
3. All files in the **Tracing** sub-directory of the program installation folder.

For more information, refer to the FSCR documentation at

<http://www.netwrix.com/pdfviewer.html?product=fscr&type=QuickStart>