TROUBLESHOOTING INCORRECT REPORTING OF THE "WHO CHANGED" PARAMETER

TECHNICAL ARTICLE

Product Version: 3.0

December/2011

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.

All rights reserved. Table of Contents

1. INTRODUCTION

1.1. Overview

NetWrix change auditing solutions track all changes made to monitored objects, and generate reports and real-time alerts that show *who* changed what, *when*, and *where*. However, incorrect audit settings on domain controllers may result in errors in change reports. The ‘Who changed’ column, containing the ‘System’ value instead of an account name, is the most common error found in reports. Problem reports usually have warning.txt or error.txt files attached that may help understand what caused the problem.

This article provides instructions on how to troubleshoot incorrect identification of the account under which changes were made. It is applicable to NetWrix Active Directory Change Reporter, NetWrix Exchange Change Reporter and NetWrix Group Policy Change Reporter.

> **Note:** This article covers troubleshooting of incorrect reporting of the ‘Who changed’ parameter for systems running Windows Server 2003 and Windows Server 2008 R2. 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 Incorrect Reporting of the “Who Changed” Parameter describes the most common issues, explains the reasons for these problems and provides instructions on how to solve them.
- A Appendix: Supporting Data contains a list of documentation on NetWrix products that this article applies to.

2. Troubleshooting Incorrect Reporting of the “Who Changed” Parameter

Below is a list of the most common problems causing incorrect reporting of the “Who Changed” parameter that users may encounter while using NetWrix change auditing products. Refer to the sections below for step-by-step instructions on how to troubleshoot these issues:

- Default Domain Audit Settings are not Configured Properly
- Configuration Container Audit Settings are not Configured Properly
- Directory Service Access and Account Management Events Auditing is not Enabled
- Failed to Open the Event Log
- Security Log Overwriting on a Domain Controller
- Auditing of Group Policy Preferences is not Supported

2.1. Default Domain Audit Settings are not Configured Properly

2.1.1. Problem Description

The daily summary report and the warning.txt file contain the following warning message:

```
Your default domain audit settings may prevent the 'Who Changed'
field from being reported correctly.
```

2.1.2. What Caused the Problem

Object-level Active Directory auditing settings are not configured for monitoring of *all* possible changes made to Active Directory by *any* user. Therefore, the daily summary reports can contain the ‘System’ value as a source of changes instead of an account name.

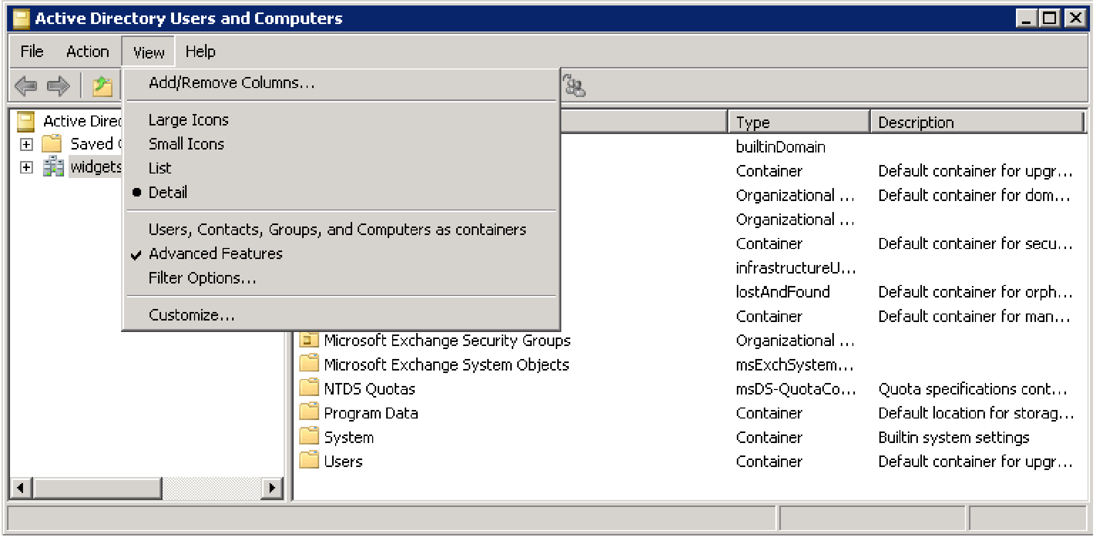
2.1.3. How to Fix

To monitor *all* possible changes made to Active Directory by *any* user, you must make sure that your Active Directory auditing settings are configured properly. To configure these settings, perform the following procedure on the problem domain controller(s):

Procedure 1. To configure Active Directory auditing settings

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**. In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** option is selected.

Figure 1: Active Directory Users and Computers Dialog



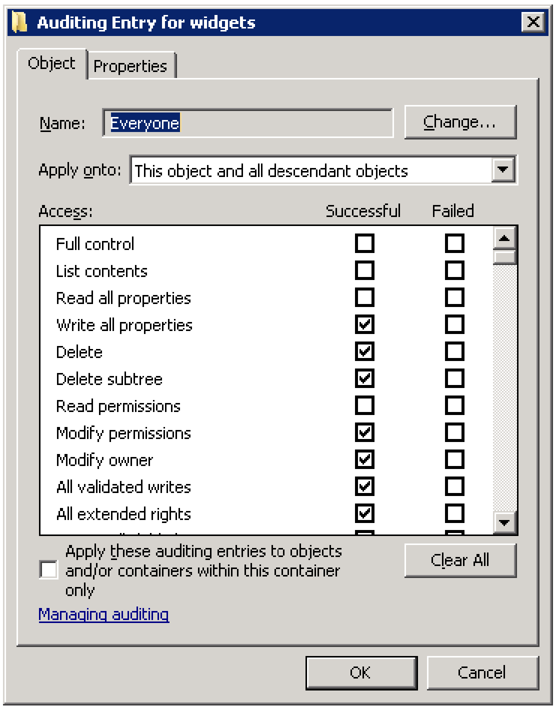
	Type	Description
	builtinDomain	
	Container	Default container for upgr...
	Organizational ...	Default container for dom...
	Organizational ...	
	Container	Default container for secu...
	infrastructureU...	
	lostAndFound	Default container for orph...
	Container	Default container for man...
Microsoft Exchange Security Groups	Organizational ...	
Microsoft Exchange System Objects	msExchSystem...	
NTDS Quotas	msDS-QuotaCo...	Quota specifications cont...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
Users	Container	Default container for upgr...

2. Right-click the **<Domain_Object_Name>** node and select **Properties**. In the **Properties** dialog, open the **Security** tab and click the **Advanced** button. The **Advanced Security Settings** dialog will open.

3. Select the **Auditing** tab and click the **Add** button. In the **Select user, Computer, Service account, or Group** dialog, type `Everyone` in the **Enter the object name to select** entry field and click **OK**.

4. In the **Audit Entry** dialog, make sure that the following access entries are deselected: Full Control, List Contents, Read All Properties and Read Permissions, and set the rest to **Successful**:

Figure 2: Audit Entry for company Dialog



Name: Everyone

Apply onto: This object and all descendant objects

Access:	Successful	Failed
Full control	□	□
List contents	□	□
Read all properties	□	□
Write all properties	☑	□
Delete	☑	□
Delete subtree	☑	□
Read permissions	□	□
Modify permissions	☑	□
Modify owner	☑	□
All validated writes	☑	□
All extended rights	☑	□

□ Apply these auditing entries to objects and/or containers within this container only

5. Make sure that the **Apply these auditing entries to objects and/or containers within his container only** check-box is deselected. Also, make sure that the **Apply onto** parameter is set to **This object and all descendant objects**.

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

2.2. Configuration Container Audit Settings are not Configured Properly

2.2.1. Problem Description

The daily summary report and the warning.txt file contain the following warning message:

```
Your configuration container audit settings may prevent the 'Who
Changed' field from being reported correctly.
```

2.2.2. What Caused the Problem

Object-level auditing of containers mentioned in the error report is not configured for monitoring of *all* possible changes made to Active Directory by *any* user.

2.2.3. How to Fix

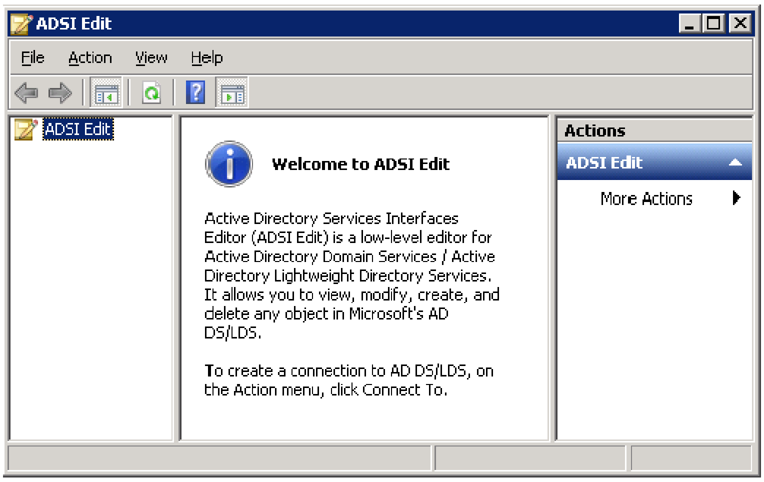
To monitor *all* possible changes made to Active Directory by *any* user, you must make sure that auditing of containers is configured properly. To do it, perform the following procedure on the problem domain controller(s):

> **Note:** To perform this procedure, you will need the ADSI Edit utility, which is a component of Windows Server Support Tools. If it has not been installed, download Windows Server Support Tools from the official website.

Procedure 2. To configure auditing of containers

1. Navigate to **Start → Programs → Administrative Tools → ADSI Edit**. The **ADSI Edit** dialog will open.

Figure 3: ADSI Edit dialog



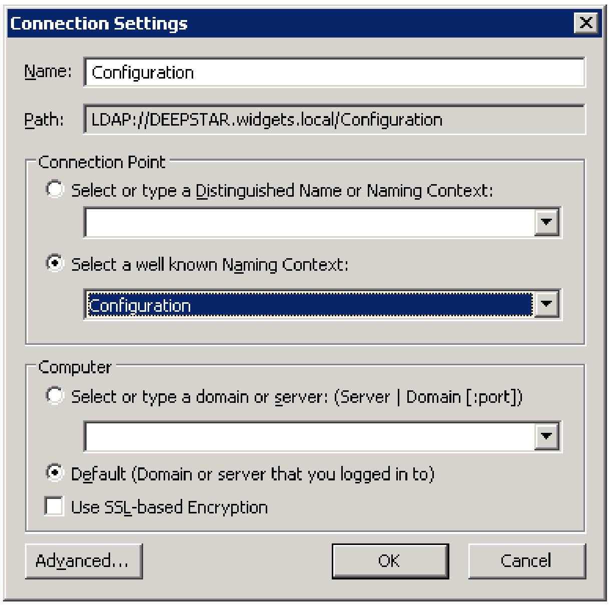
Welcome to ADSI Edit

Active Directory Services Interfaces Editor (ADSI Edit) is a low-level editor for Active Directory Domain Services / Active Directory Lightweight Directory Services. It allows you to view, modify, create, and delete any object in Microsoft's AD DS/LDS.

To create a connection to AD DS/LDS, on the Action menu, click Connect To.

2. Right click the **ADSI Edit** node and select the **Connect To** option. In the **Connection Settings** dialog, enable the **Select a well-known Naming Context** option and select **Configuration** from the drop-down list. Then click **OK**.

Figure 4: Connection Settings Dialog



Connection Settings

Name: Configuration

Path: LDAP://DEEPSTAR.widgets.local/Configuration

Connection Point

○ Select or type a Distinguished Name or Naming Context:

● Select a well known Naming Context:

Configuration

Computer

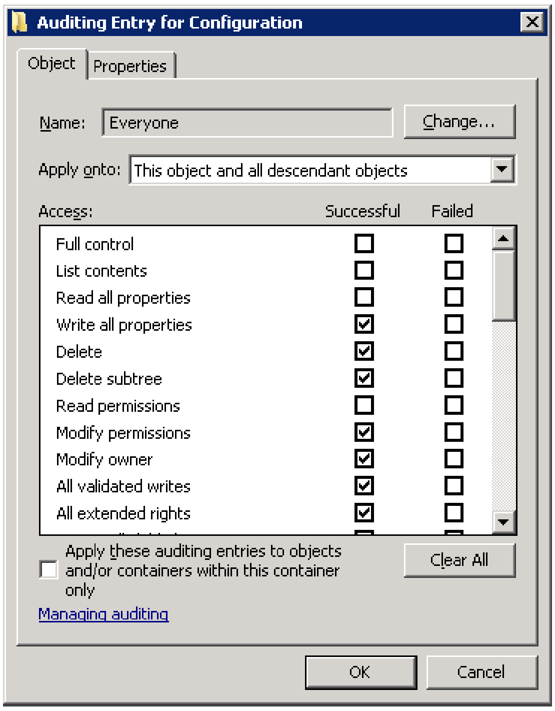
○ Select or type a domain or server: (Server | Domain [:port])

● Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

3. Expand the **Configuration <Domain_Name>** node. Right-click the **CN=Configuration, DC=…** node and select **Properties**.
4. In the **Properties** dialog select the **Security** tab and click the **Advanced** button. In the **Advanced Security Settings for Configuration** dialog open the **Auditing** tab and click the **Add** button.
5. In the **Select User, Computer, Service Account, or Group** dialog type `Everyone` in the **Enter the object name to select** entry field and click **OK.** The **Auditing Entry for Configuration** dialog will open.
6. Make sure that the following access entries are deselected: Full Control, List Contents, Read All Properties and Read Permissions, and set the rest to **Successful**:

Figure 5: Auditing Entry for Configuration Dialog



Auditing Entry for Configuration

Name: Everyone

Apply onto: This object and all descendant objects

Access:	Successful	Failed
Full control	□	□
List contents	□	□
Read all properties	□	□
Write all properties	☑	□
Delete	☑	□
Delete subtree	☑	□
Read permissions	□	□
Modify permissions	☑	□
Modify owner	☑	□
All validated writes	☑	□
All extended rights	☑	□

□ Apply these auditing entries to objects and/or containers within this container only

7. Make sure that the **Apply these auditing entries to objects and/or containers within his container only** check-box is deselected. Also, make sure that the **Apply onto** parameter is set to **This object and all descendant objects.**
8. Click **OK** to save the changes.

2.3. Directory Service Access and Account Management Events Auditing is not Enabled

2.3.1. Problem Description

The daily summary report and the error.txt file contain the following error message:

```
Auditing of Directory Service Access and successful Account
Management events is not enabled for this DC. Please adjust audit
policy settings (see the Troubleshooting section of the product
documentation for more information).
```

2.3.2. What Caused the Problem

The Local Security Policy Snap-in on the domain controller indicates that the **Audit Directory Service Access** and/or the **Audit Account Management** options are not set to **Success**. For instructions on how to set these options to **Success**, refer to Procedure 3 To set Audit Directory Service Access and Audit Account Management options to Success below.

If these settings are set to **Success** in the applied effective policy, but you keep receiving this error, the following reasons are possible:

- The effective policy applied to domain controllers is not configured properly.
- For some reason, the effective policy is not applied to the domain controller.
- The audit settings are configured using the Granular Audit Policies.

To solve these problems, please, contact NetWrix Technical Support.

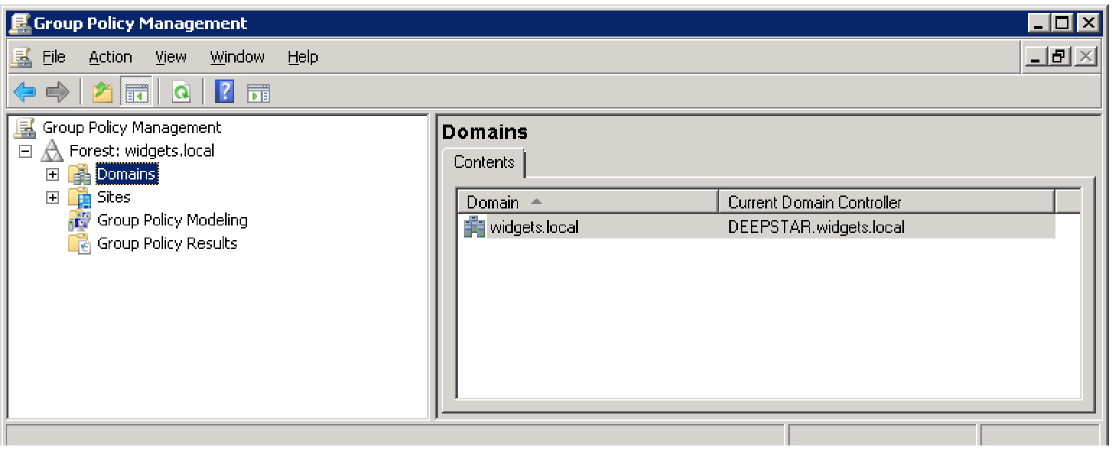
2.3.3. How to Fix

To set **Audit Directory Service Access** and **Audit Account Management** options to **Success**, perform the following procedure on the problem domain controllers:

Procedure 3. To set Audit Directory Service Access and Audit Account Management options to Success

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

Figure 6: Group Policy Management Dialog



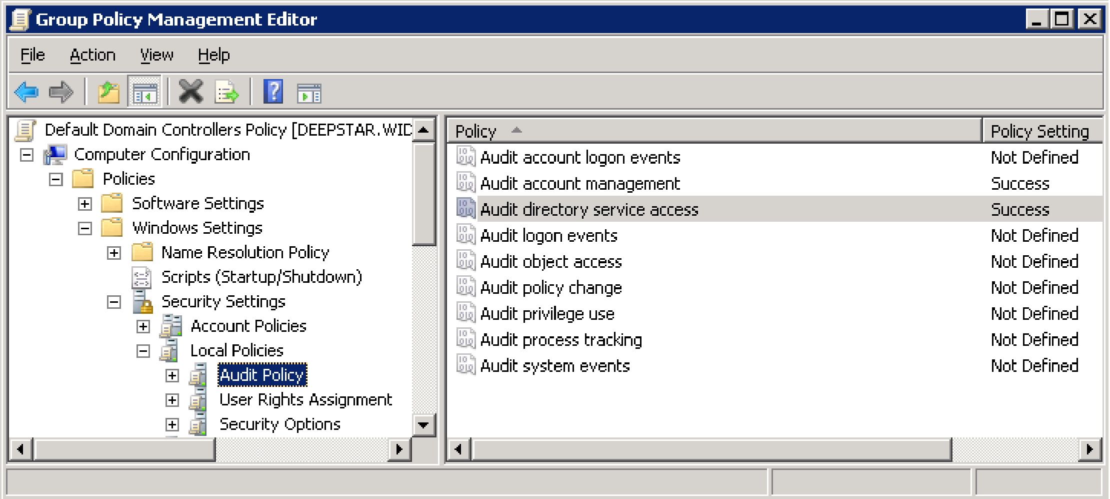
Domain	Current Domain Controller
widgets.local	DEEPSTAR.widgets.local

2. Navigate to **Domains → <Domain_Name> → Domain Controllers.** Right-click the effective policy applied to the domain controllers in the managed domain (**Default Domain Controllers Policy** by default) and select **Edit**.

3. In the **Group Policy Management editor** dialog navigate to **Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy**.

4. Ensure that the **Audit Active Directory Service Access** and **Audit Account Management** options are set to **Success** (or **Success** and **Failure**):

Figure 7: Group Policy Management Editor Dialog



Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Success
Audit directory service access	Success
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

5. Navigate to **Start → Run** and execute the `cmd` command. Type the `gpupdate` command and press **Enter**. The group policy will be updated.

2.4. Failed to Open the Event Log

2.4.1. Problem Description

The daily summary report and the error.txt file contain the following error message:

```
Failed to open the event log. Error details: The RPC server is
unavailable.
```

2.4.2. What Caused the Problem

Your NetWrix change auditing product could not collect events from the Security log of the domain controller. The domain controller is not accessible.

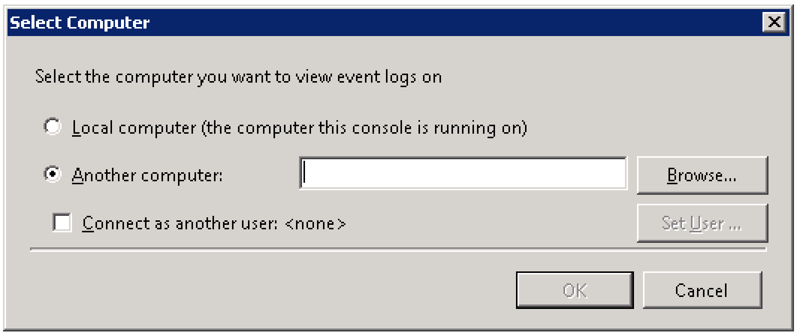
2.4.3. How to Fix

To check accessibility of a remote computer via the Event Viewer, perform the following procedure:

Procedure 4. To check accessibility of a remote computer

1. Log on to the computer where your NetWrix change auditing product is installed.
2. Navigate to **Start → Run.** Type `eventvwr` and click **OK.**
3. Right-click the **Event Viewer (Local)** node and select **Connect to Another Computer**. The **Select Computer** dialog will open:

Figure 8: Select Computer Dialog



Select Computer

Select the computer you want to view event logs on

○ Local computer (the computer this console is running on)

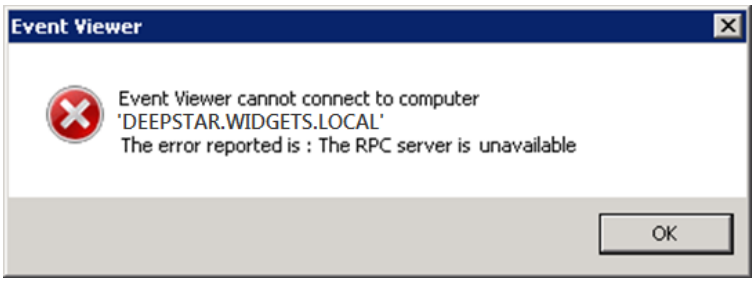
● Another computer:

☐ Connect as another user: <none>

4. Type the name of the domain controller reporting the error in the **Another Computer** entry field. Click **OK** to connect to the domain controller.
5. Do one of the following:

- If you have connected successfully, contact [NetWrix Technical Support]().
- If the following error message is returned:

Figure 9: Error Message



Event Viewer

Event Viewer cannot connect to computer 'DEEPSTAR.WIDGETS.LOCAL'
The error reported is : The RPC server is unavailable

a. Check whether the computer that you are trying to connect to is switched on and accessible (by executing the `Ping` command).

b. Ensure that Port 135 is opened on the remote computer (using the Telnet tool, for example).

c. Make sure that the domain controller is not blocked by a firewall.

d. Try to re-connect.

e. If you still cannot connect to the computer, please contact NetWrix Technical Support.

2.5. Security Log Overwriting on a Domain Controller

2.5.1. Problem Description

The daily summary report and the warning.txt file contain the following warning message:

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

2.5.2. What Caused the Problem

The problem occurs if the size of the Security log is not big enough to hold all events that occurred between data collections, and some events have been overwritten.

2.5.3. How to Fix

To prevent overwriting of the Security log, you must increase its size. To do this, perform Procedure 5 To increase the maximum size of the Security event log on the problem domain controller(s).

If increasing the maximum security log size does not resolve the problem, it may be necessary to enable the **Auto archiving Event Log** option. With this option, the Event Log will be archived and log overwrites will not occur on the domain controller(s).

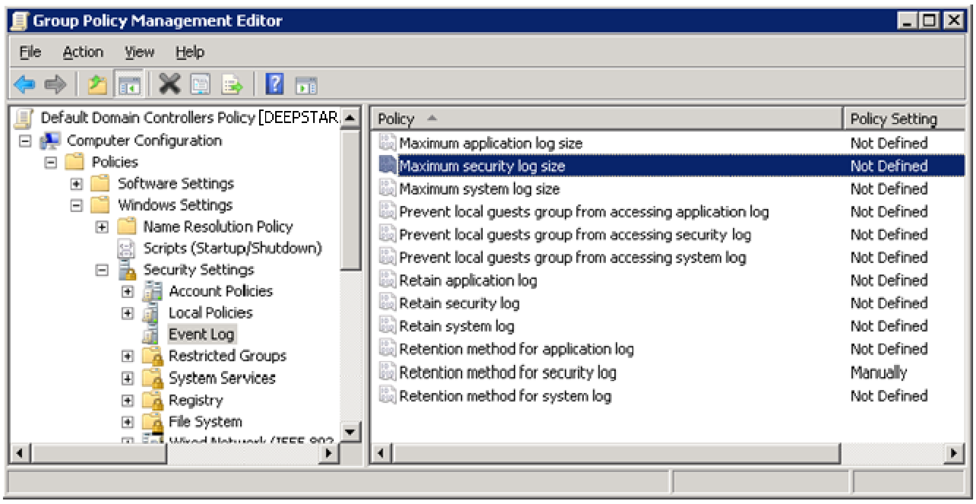
At first, verify the Event Log settings and the effective policy applied to the domain controllers in the managed domain (**Default Domain Controllers Policy** by default) by executing Procedure 6 To verify Event Log settings.

After verifying the Event Log settings, enable the **Auto archiving Event Log** option. To do this, perform Procedure 7 To enable Auto archiving centrally on all domain controllers on any of your domain controllers.

Procedure 5. To increase the maximum size of the Security event log

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **Group Policy Management**. The **Group Policy Management** dialog will open.
2. Navigate to **Domains** → **<Domain_Name>** → **Domain Controllers.** Right-click the effective policy applied to the domain controllers in the managed domain (**Default Domain Controllers Policy** by default) and select **Edit**.
3. Navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log**:

Figure 10: Group Policy Management Editor Dialog



Default Domain Controllers Policy [DEEPSTAR
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Manually
Retention method for system log	Not Defined

4. Ensure that **Retention method for security log** is set to **Not Defined** or **As Needed.**

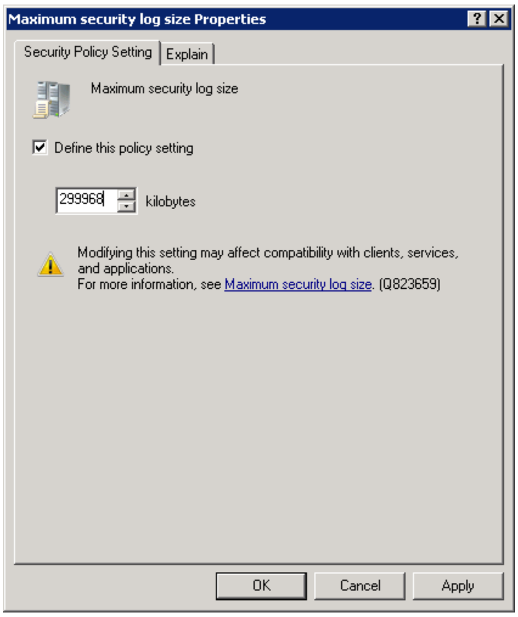
5. Double-click **Maximum security log size**. In the **Maximum security log size Properties** dialog, select the **Define this policy setting** option and set **Maximum security log size** according to the table below:

Table 1: Maximum security log size

Operational system of domain controllers	Maximum security log size
Both Windows Server 2003 and 2008/2008 R2	No more than 300 Mb
Only Windows Server 2008/2008 R2	From 300Mb or above depending on fillability of domain controller logs

Note: The Security log size on a domain controller running Windows Server 2003 operating system must not exceed 300 Mb. Please, refer to the following Microsoft article for details.

Figure 11: Maximum security log size Properties Dialog



Maximum security log size

☑ Define this policy setting

299968 kilobytes

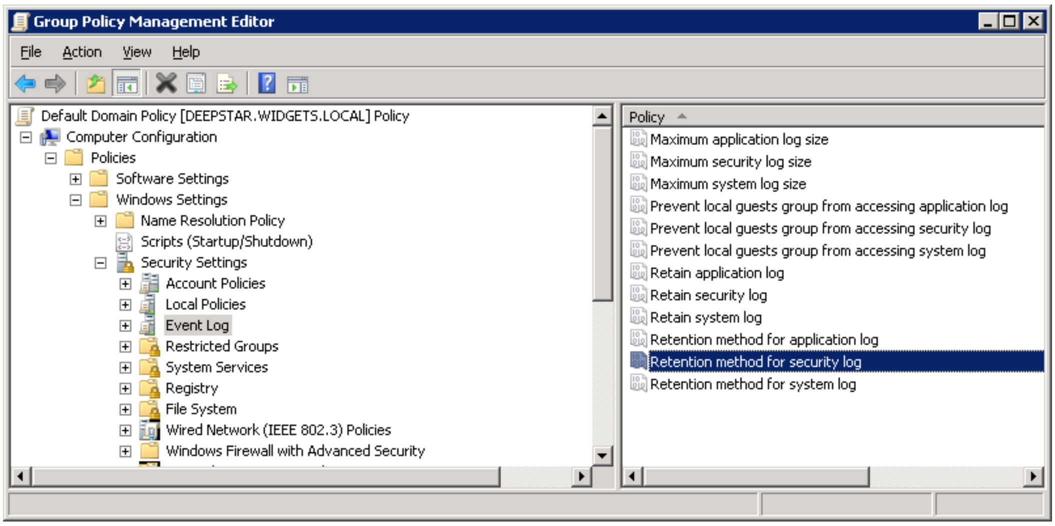
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Maximum security log size. (Q823659)

6. Click **OK** to save the changes.
7. Navigate to **Start** → **Run** and execute the `cmd` command. Type the `gpupdate` command and press **Enter**. The group policy will be updated.

Procedure 6. To verify Event Log settings

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **Group Policy Management**. In the **Group Policy Management** dialog navigate to **Domains** → **<Domain_Name>**. Right-click the effective policy of the domain (**Default Domain Policy** by default) and select **Edit**.
2. In the **Group Policy Management Editor** dialog navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log**.
3. Ensure that the **Retention Method for Security Log** parameter is set to **Manually**.

Figure 12: Group Policy Management Editor Dialog



Default Domain Policy [DEEPSTAR.WIDGETS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security

Policy
Maximum application log size
Maximum security log size
Maximum system log size
Prevent local guests group from accessing application log
Prevent local guests group from accessing security log
Prevent local guests group from accessing system log
Retain application log
Retain security log
Retain system log
Retention method for application log
Retention method for security log
Retention method for system log

4. Verify this setting for the domain controller Policy.

Procedure 7. To enable Auto archiving centrally on all domain controllers

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **Group Policy Management**. The **Group Policy Management** dialog will open.
2. Navigate to **Domains** → **<Domain_Name>** → **Domain Controllers.** Right-click the effective policy applied to the domain controllers in the managed domain (**Default Domain Controllers Policy** by default) and select **Edit**.
3. Navigate to **Computer Configuration** → **Policies**. Right-click **Administrative Templates: Policy definitions** and select **Add/remove templates**. In the **Add/Remove Templates** dialog click the **Add** button.
4. In the Policy **Templates** dialog navigate to the NetWrix product installation directory (the program may have been installed on another computer), select the Log Autobackup.adm file and click **Open.**
5. Click the **Close** button in the **Add/Remove Templates** dialog.

Note: If you have Windows Server 2003 or below installed, after step 4 click **View** in the Main menu, select **Filtering** and deselect the **Only show policy settings that can be fully managed** option.

6. Navigate to **Administrative Templates: Policy definitions → Classic Administrative Templates → System → Event Log**.
7. Double click **Automatically clear a full security event log and back up the log file**. Select the **Enabled** option and click **OK** to save changes.
8. Navigate to **Start → Run** and execute the `cmd` command. Type the `gpupdate` command and press **Enter**. The group policy will be updated.

2.6. Auditing of Group Policy Preferences is not Supported

2.6.1. Problem Description

The daily summary report and warning.txt file contains the following warning message:

```
Auditing of Group Policy Preferences is not supported on this
system. To resolve the issue install the product on a machine
running Windows Vista or higher.
```

2.6.2. What Caused the Problem

Some of the domain controllers in your environment run Windows Server 2008 or above. This operating system has a new Group Policy Preferences feature (please, refer to the Group Policy Preferences Overview article for details). Your NetWrix change auditing product is installed on a computer running Windows Server 2003 or below, and changes made to Group Policy Preferences will not be reported.

2.6.3. How to Fix

If you want to track changes made to Group Policy Preferences, you have to install your NetWrix change auditing product on a computer running Windows Vista or above.

2.7. If You have not Found a Solution

If none of the steps resolve the issue, or it is not described in this article, submit a ticket to NetWrix Technical Support Team.

You will have to provide Technical Support with the following information:

1. E-mail report containing the problem.
2. The warning.txt or *.errors.txt file, which is usually attached to the problem email report.
3. The entire contents from the Tracing subdirectory of the program installation directory. Please, archive the contents before sending.

A APPENDIX: SUPPORTING DATA

A.1 Related Documentation

The table below lists all documents available to support NetWrix Active Directory Change Reporter, Exchange Change Reporter and Group Policy Change Reporter:

Table 2: Products Documentation

Link	Overview
Active Directory Change Reporter	Active Directory Change Reporter documentation page
Exchange Change Reporter	Exchange Change Reporter documentation page
Group Policy Change Reporter	Group Policy Change Reporter documentation page