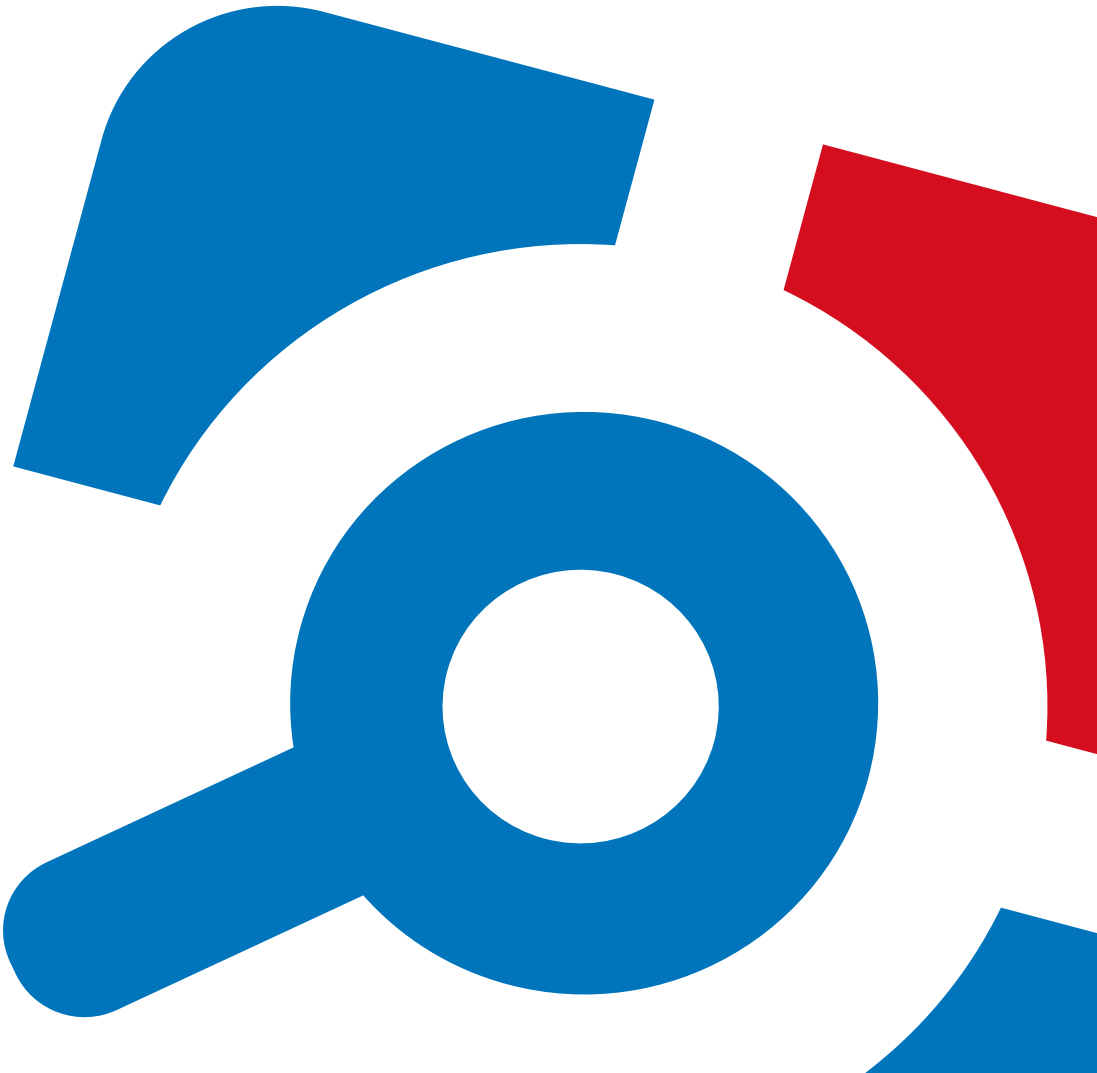
netwrix

Netwrix Auditor

Installation and Configuration Guide

Version: 8.0
5/17/2016



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, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

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. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. 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

This guide is intended for administrators who are going to install and configure Netwrix Auditor.

The guide provides detailed instructions on how best to deploy and set up the product to audit your IT infrastructure. It lists all product requirements, necessary rights and permissions and guides you through the installation and audit configuration processes.

1.1. Netwrix Auditor Overview

Netwrix Auditor is an IT auditing platform that delivers complete visibility into changes and data access in hybrid cloud IT environments by providing actionable audit data about *who* changed *what*, *when* and *where* each change was made, and *who* has access to *what*. Netwrix Auditor helps organizations prevent security breaches caused by insider attacks, pass compliance audits with far less effort and expense, and keep tabs on what privileged users are doing in the environment.

Netwrix Auditor enables auditing of the broadest variety of IT systems, including Active Directory, Exchange, file servers, SharePoint, SQL Server, VMware and Windows Server. It also supports monitoring of privileged user activity in all other systems, even if they do not produce any logs, by enabling video recording of user screen activity and later search and replay. More than 160,000 IT departments worldwide rely on Netwrix Auditor to secure IT infrastructure, prove compliance and increase operational efficiency. The product has earned over 70 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

Major benefits:

- **Change auditing and alerting:** Netwrix Auditor detects all configuration, content and security changes across your entire IT infrastructure. Reports and real-time alerts include the critical who, what, when and where details, including before and after values, enabling quick and effective response.
- **AuditIntelligence interactive search:** Netwrix Auditor enables you to easily search through audit data and fine-tune sorting and filtering criteria so you can quickly hone in on exactly the information you need.
- **Configuration assessment:** State-in-time™ reports show configuration settings at any point in time, such as group membership or password policy settings as they were configured a year ago.
- **Access auditing:** Monitoring of and reporting on successful and failed access to systems and data helps keep sensitive data safe.
- **Predefined reports and diagrams:** Netwrix Auditor includes more than 150 predefined reports and diagrams. Reports can be exported to a range of formats, including PDF and XLS, and stakeholders can subscribe to reports to stay informed automatically by email.

- **AuditArchive™:** Netwrix Auditor's scalable two-tiered storage system (file-based + SQL database) holds consolidated audit data for more than 10 years.
- **Unified platform:** Many vendors require multiple standalone tools that are hard to integrate, but Netwrix Auditor is a unified platform that can audit the entire IT infrastructure.

The table below provides an overview of each Netwrix Auditor solution:

Application	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain structure that can be used to assess its state at present or at any moment in the past. The product provides logon activity summary, reports on interactive and non-interactive logons including failed logon attempts. Also, Netwrix Auditor for Active Directory helps detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a built–in Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.
Netwrix Auditor for Exchange	Netwrix Auditor for Exchange detects and reports on all changes made to Microsoft Exchange configuration and permissions. In addition, it tracks mailbox access events in the managed Exchange organization, and notifies the users whose mailboxes have been accessed by non–owners.
Netwrix Auditor for Office 365	Netwrix Auditor for Office 365 detects and reports on all changes made to Microsoft Exchange Online configuration and permissions. In addition, it tracks mailbox access events in the managed Exchange Online organization, and notifies the users whose mailboxes have been accessed by non–owners.
Netwrix Auditor for Windows File Servers	Netwrix Auditor for Windows File Servers detects and reports on all changes made to Windows–based file servers, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for EMC	Netwrix Auditor for EMC detects and reports on all changes made to EMC Celerra, VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.

Application	Features
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7-modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for SharePoint	Netwrix Auditor for SharePoint detects and reports on read access and changes made to SharePoint farms, servers and sites, including modifications of content, security settings and permissions.
Netwrix Auditor for SQL Server	Netwrix Auditor for SQL Server detects and reports on all changes to SQL Server configuration and database content.
Netwrix Auditor for VMware	Netwrix Auditor for VMware detects and reports on all changes made to ESX servers, folders, clusters, resource pools, virtual machines and their virtual hardware configuration.
Netwrix Auditor for Windows Server	Netwrix Auditor for Windows Server detects and reports on all changes made to Windows–based server configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. Netwrix Auditor collects Windows event logs and syslog events from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data. In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.

2. System Requirements

This section lists the requirements for the systems that are going to be audited with Netwrix Auditor, and for the computer where the product is going to be installed. It also contains the information on the SQL Server versions supported by the Audit Database. Refer to the following sections for detailed information:

- Requirements for Audited Systems
- Requirements to Install Netwrix Auditor
- Supported Microsoft SQL Server Versions

2.1. Requirements for Audited Systems

The table below provides the requirements for the systems that can be audited with Netwrix Auditor:

Audited System	Supported Versions
Active Directory	Domain Controller OS versions: • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2
Exchange	• Microsoft Exchange 2007 • Microsoft Exchange 2010 SP1 and above • Microsoft Exchange 2013
Exchange Online	Exchange Online version provided within Microsoft Office 365
Windows File Servers	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8/ 8.1, and Windows 10 • Windows Server OS (32 and 64-bit): Windows Server 2008 SP2/2008 R2, Windows Server 2012/2012 R2
EMC	• EMC VNX/VNXe/Celerra families (CIFS configuration only) • EMC Isilon 7.2.0.0 - 7.2.0.4, 7.2.1.0 - 7.2.1.2 (CIFS configuration only)
NetApp	• NetApp Data ONTAP 7 (CIFS configuration only) • NetApp Data ONTAP 8 in 7-mode (CIFS configuration only) • NetApp Clustered Data ONTAP 8.2.1 - 8.2.3, 8.3, 8.3.1, 8.3.2 (CIFS

Audited System	Supported Versions
	configuration only)
SharePoint	• Microsoft SharePoint Foundation 2010 and SharePoint Server 2010 • Microsoft SharePoint Foundation 2013 and SharePoint Server 2013
SQL Server	• Microsoft SQL Server 2005 • Microsoft SQL Server 2008 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014
VMware	• VMware ESXi 4.x and above • vSphere vCenter 4.x and above
Windows Server	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8/ 8.1, and Windows 10 • Windows Server OS (32 and 64-bit): Windows Server 2008 SP2/2008 R2, Windows Server 2012/2012 R2
Cisco	Cisco ASA 5500 Series Adaptive Security Appliance Software Release 8.0
DNS	Windows Server OS (32 and 64-bit): Windows Server 2008 SP2/2008 R2, Windows Server 2012/2012 R2
Event Log	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8/ 8.1, and Windows 10 • Windows Server OS (32 and 64-bit): Windows Server 2008 SP2/2008 R2, Windows Server 2012/2012 R2 • Any Linux system using Syslog (event collection rules must be created manually)
IIS	IIS 7.0 and above
User Activity	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8/ 8.1, and Windows 10 • Windows Server OS (32 and 64-bit): Windows Server 2008 SP2/2008 R2, Windows Server 2012/2012 R2

2.2. Requirements to Install Netwrix Auditor

This section provides the requirements for the computer where Netwrix Auditor is going to be installed. Refer to the following sections for detailed information:

- Hardware Requirements
- Software Requirements
- Deployment Options

2.2.1. Hardware Requirements

Before installing Netwrix Auditor, make sure that your hardware meets the following requirements:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2 GHz	Intel Core 2 Duo 2x 64 bit, 3 GHz
RAM	2 GB	8 GB
Disk space	• Full installation—1 TB The disk space required for Netwrix Auditor to function properly depends on the average number of changes per day in the audited environment, the Audit Database location and the Long-Term Archive retention settings. **NOTE:** Netwrix Auditor informs you if you are running out of space on a system disk where the Long-Term Archive is stored by default. You will see events in the **Netwrix Auditor System Health** log once the free disk space starts approaching minimum level. When the free disk space is less than 3 GB all Netwrix services will be stopped. • Client installation—200 MB	
Screen resolution	1280 x 1024	1920 x 1080 and higher

2.2.2. Software Requirements

The table below lists the minimum software requirements for the Netwrix Auditor installation:

Component	Full installation	Client installation (only Netwrix Auditor client)
Operating system	• Windows Desktop OS (64-bit): Windows 7 SP1, Windows 8/8.1 • Windows Server OS (64-bit): Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2	• Windows Desktop OS (32 and 64-bit): Windows 7 SP1, Windows 8/8.1, and Windows 10 • Windows Server OS (32 and 64-bit): Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2
Framework	• .Net Framework 3.5 SP1	

2.2.3. Deployment Options

This section provides recommendations on how best to deploy Netwrix Auditor. Review these recommendations and choose the most suitable option depending on the IT infrastructure you are going to audit with Netwrix Auditor.

Install Netwrix Auditor Administrator Console on...	To audit...
Any computer in your network	• Exchange Online
Any computer in the audited domain or domain where your audited system resides. It is not recommended to install Netwrix Auditor on a domain controller.	• Active Directory* • Exchange* • File Servers • SharePoint* **NOTE:** The computer where Netwrix Auditor Administrator Console is installed must be able to access the Central Administration website on the audited SharePoint Farm by its name and port number. Netwrix Auditor for SharePoint Core Service must be installed on the computer where SharePoint Central Administration is installed. • SQL Server • VMware • Windows Server*

Install Netwrix Auditor Administrator Console on...	To audit...
	• Cisco • DNS* • Event Log • Group Policy* • IIS * If you want to audit several domains or systems that reside in different domains, you must establish two-way trust relationships between these domains and the domain where Netwrix Auditor Administrator Console is installed.

NOTE: The Netwrix Auditor client can be installed on any workstation provided that a user who runs the product is granted all necessary permissions to access audit data. See Configure Netwrix Auditor User Rights and Permissions for more information.

2.3. Supported Microsoft SQL Server Versions

Microsoft SQL Server provides Reporting Services that enables creating reports based on data stored in the Audit Database. Netwrix Auditor uses Reporting Services to run data searches and generate reports on changes to the audited environment and on the point-in-time configuration.

If you want to be able to generate reports and run searches in the Netwrix Auditor client, SQL Server must be deployed on the same computer where Netwrix Auditor is installed, or on a computer that can be accessed by the product.

The following SQL Server versions are supported:

Version	Edition
SQL Server 2008	Express Edition with Advanced Services Standard or Enterprise Edition **NOTE:** SQL Server Reporting Services 2008 is not supported. In this case you have to install and configure Reporting Services 2008 R2 and above manually.
SQL Server 2008 R2	Express Edition with Advanced Services Standard or Enterprise Edition

Version	Edition
SQL Server 2012	Express Edition with Advanced Services Standard or Enterprise Edition
SQL Server 2014	Express Edition with Advanced Services Standard or Enterprise Edition

The following SQL Server Reporting Services versions are supported: 2008 R2 and above.

NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

SQL Server is not included in the product installation package and must be installed manually or automatically through the **Audit Database Settings** wizard. This wizard automatically installs SQL Server 2014 Express Edition with Advanced Services and configures Reporting Services.

For your convenience, Netwrix provides instructions on the manual installation of Microsoft SQL Server with Advanced Services. See Install Microsoft SQL Server for more information. For full installation and configuration details, refer to the documentation provided by Microsoft.

NOTE: If you install Netwrix Auditor on a read-only domain controller, SQL Server installation will fail (both manual or automatic through the **Audit Database Settings** wizard). This is a known issue, for details refer to the following Microsoft Knowledge base article: You may encounter problems when installing SQL Server on a domain controller. To fix the issue, install Netwrix Auditor on another computer, or install SQL Server manually on a different computer that can be accessed by the product.

You can also configure Netwrix Auditor to use an existing SQL Server instance.

NOTE: If you have more than one Netwrix Auditor Server running in your network, make sure to configure them to use different SQL Server instances. The same SQL Server instance cannot be used to store audit data collected by several Netwrix Auditor Servers.

3. Install Netwrix Auditor

This chapter provides step-by-step instructions on how to install Netwrix Auditor and its Compression Services. Refer to the following sections for detailed information:

- Install the Product
- Install Netwrix Auditor Core Services

It also includes advanced scenarios such as:

- Install Netwrix Auditor Client through Group Policy
- Install Netwrix Auditor in Silent Mode

3.1. Install the Product

To install Netwrix Auditor

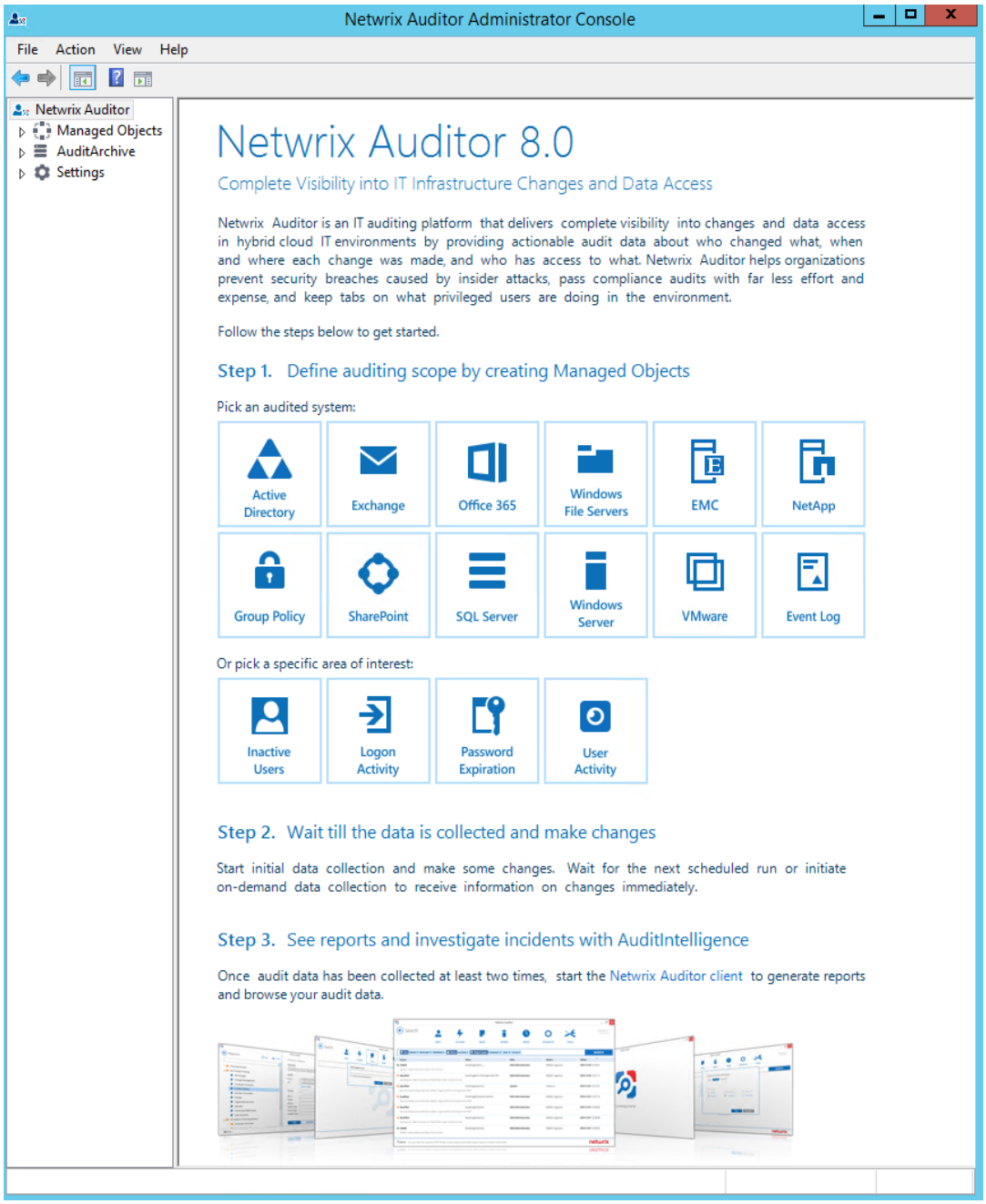
1. Download Netwrix Auditor 8.0.

   NOTE: Before installing Netwrix Auditor, make sure that the **Windows Firewall** service is started. If you use a third-party firewall, see Configure Ports for Inbound Connections. Also, you must be a member of the local **Administrators** group to run the Netwrix Auditor installation.

2. Unpack the installation package. The following window will be displayed on successful operation completion:

3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, you will be prompted to select the installation type:
   - **Full installation**—Select if you are going to install Netwrix Auditor for the first time. In this case both Netwrix Auditor Administrator Console and the Netwrix Auditor client will be installed.
   - **Client installation**—Select if you have been already auditing your IT infrastructure with Netwrix Auditor and now you want to install the client console on a remote machine to provide access to your audit results (e.g., generate reports and search your audit data).
5. On the **Destination Folder** step, specify the installation folder.
6. Click **Install**.

After a successful installation, Netwrix Auditor shortcuts will be added to the **Start** menu/screen and Netwrix Auditor Administrator Console will open.



NOTE: Netwrix recommends to install Netwrix Auditor on a workstation, not a domain controller. See Deployment Options for more information. But if you want to install Netwrix Auditor on a read-only domain controller anyway, prior to running the installation, perform the following steps:

1. On a writable domain controller, create the following groups using the **Active Directory Users and Computers** snap-in: **Netwrix Auditor Administrators** and **Netwrix Auditor Client Users**.
2. Add a user who is going to install Netwrix Auditor to these groups.
3. Wait for the changes to be replicated on a read-only domain controller.

3.2. Install Netwrix Auditor Core Services

To audit SharePoint farms and user activity, Netwrix Auditor provides Core Services that must be installed in the audited environment to collect audit data. Both Core Services can be installed either automatically (on the **New Managed Object** wizard completion), or manually.

Refer to the following sections below for manual installation instructions:

- Install Netwrix Auditor for SharePoint Core Service
- Install Netwrix Auditor User Activity Core Service

3.2.1. Install Netwrix Auditor for SharePoint Core Service

Prior to the Netwrix Auditor for SharePoint Core Service installation, review the following prerequisites and make sure that:

- Netwrix Auditor for SharePoint Core Service is going to be installed on the computer that hosts SharePoint Central Administration in the audited SharePoint farm.
- The **SharePoint Administration (SPAdminV4)** service is started on the target computer. See Configure SharePoint Farm for Auditing for more information.
- The user that is going to run the Core Service installation:
  - Is a member of the **local Administrators** group on SharePoint server, where the Core Service will be deployed.
  - Is granted the **SharePoint_Shell_Access** role on SharePoint SQL Server configuration database. See Assign SharePoint_Shell_Access Role for more information.

NOTE: During the Netwrix Auditor for SharePoint Core Service installation / uninstallation your SharePoint sites may be unavailable.

To install Netwrix Auditor for SharePoint Core Service manually

1. Navigate to *%Netwrix Auditor installation folder%\SharePoint Auditing\SharePointPackage* and copy **SpaPackage_<version>.msi** to the computer where Central Administration is installed.
2. Run the installation package.
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.

3.2.2. Install Netwrix Auditor User Activity Core Service

By default, the Core Service is installed automatically on the audited computers upon the **New Managed Object** wizard completion. If, for some reason, installation has failed, you must install the Core Service manually on each of the audited computers.

Before installing Netwrix Auditor User Activity Core Service to audit user activity, make sure that:

- The Data Processing Account has access to the administrative shares. See Configure Data Processing Account Rights and Permissions for more information.

To install Netwrix Auditor User Activity Core Service to audit user activity

1. Navigate to *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Video Recording* and copy the **UACoreSvcSetup.msi** file to the audited computer.
2. Run the installation package.
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.
4. On the **Core Service Settings** page, specify the host server (i.e., the name of the computer where Netwrix Auditor is installed) and the server TCP port.

3.3. Install Netwrix Auditor Client through Group Policy

The Netwrix Auditor client can be deployed on multiple computers through Group Policy. This can be helpful if you want to grant access to audit data to a significant number of employees and, therefore, have to run Netwrix Auditor installation on multiple computers.

NOTE: You must be a member of the local **Administrators** group to run the Netwrix Auditor installation.

3.3.1. Extract MSI File

1. Download the product installation package.
2. Open the command prompt: navigate to **Start** → **Run** and type "*cmd*".
3. Enter the following command to extract the msi file into %Temp% folder:

   ```
   Netwrix_Auditor.exe -d%Temp%
   ```

   where %Temp% can be replaced with any folder you want to extract the file to.
4. Navigate to this directory and locate **Netwrix_Auditor_client.msi**.

3.3.2. Create and Distribute Installation Package

1. Create a shared folder that will be used for distributing the installation package.

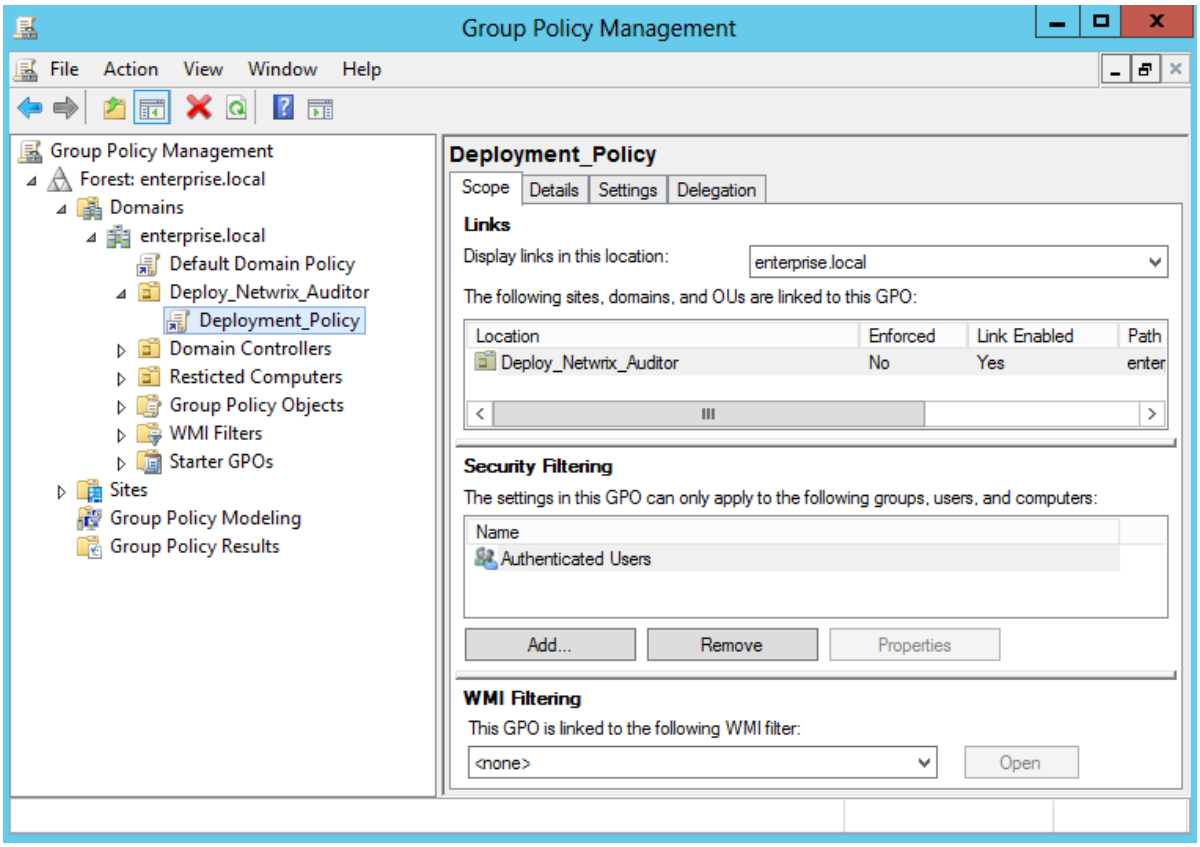
NOTE: Make sure that the folder is accessible from computers where the Netwrix Auditor clients are going to be deployed. You must grant the **Read** permissions on this folder to these computer accounts.

2. Copy **Netwrix_Auditor_client.msi** to the shared folder.

3.3.3. Create a Group Policy to Deploy Netwrix Auditor

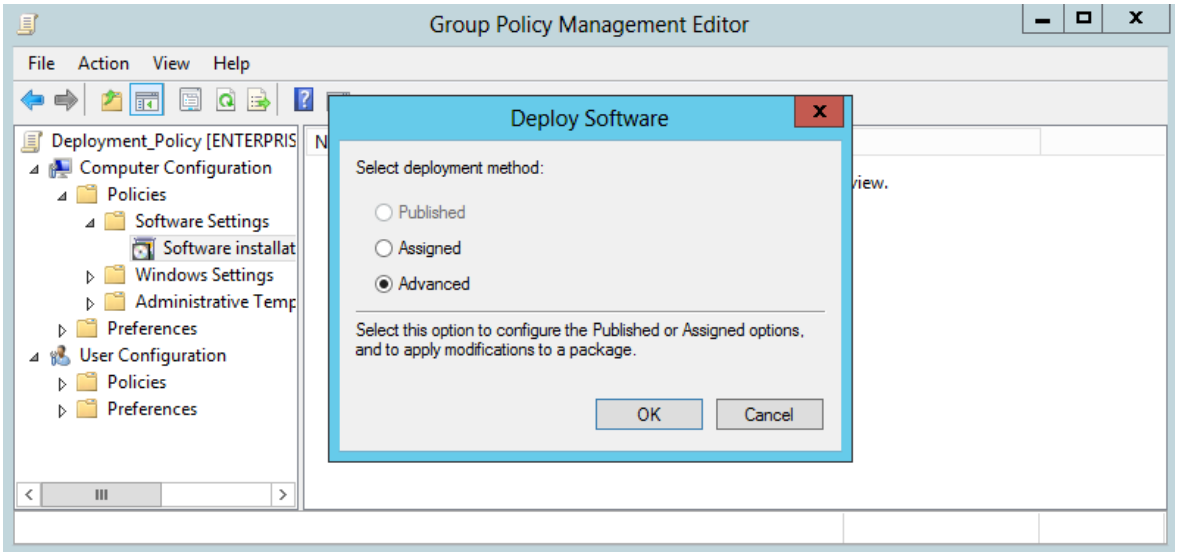
NOTE: It is recommended to create a dedicated organizational unit using **Active Directory Users and Computers** and add computers where you want to deploy the Netwrix Auditor client.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domain** → **<domain_name>**, right-click **<OU_name>** and select **Create a GPO in this domain and Link it here**.

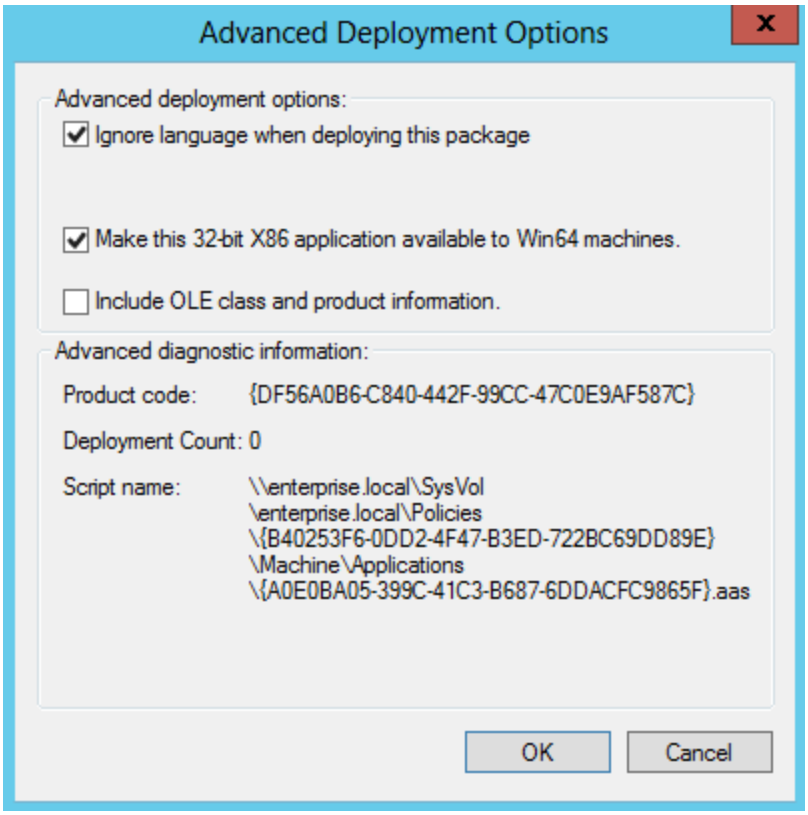


3. Right-click the newly created GPO and select **Edit** from the pop-up menu.
4. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Software Settings** → **Software installation.**
5. In the right page, right-click and select **New** → **Package**.
6. In the dialog that opens, locate **Netwrix_Auditor_client.msi** and click **Open**.

7. In the **Deploy Software** dialog, select **Advanced**.



8. In the **Netwrix Auditor Properties** dialog, select the **Deployment** tab and click **Advanced**.
9. In the **Advanced Deployment Options** dialog, select the **Ignore language when deploying this package** checkbox.



10. Close the **Netwrix Auditor Properties** dialog.
11. Reboot computers where you want to deploy the Netwrix Auditor client.

The product will be automatically installed on computers affected by the newly created Group Policy after reboot.

3.4. Install Netwrix Auditor in Silent Mode

Silent installation provides a convenient method for deploying Netwrix Auditor without UI.

To install Netwrix Auditor in a silent mode

1. Download the product installation package.
2. Open the command prompt: navigate to **Start** → **Run** and type "*cmd*".
3. Enter the following command to extract the msi file into the %Temp% folder:

   ```
   Netwrix_Auditor.exe -d%Temp%
   ```

   where %Temp% can be replaced with any folder you want to extract the file to.
4. Enter the following command:

   ```
   msiexec.exe /i "path to netwrix_auditor_setup.msi" /qn install_all=0
   ```

Command Line Option	Description
`/i`	Run installation.
`/q`	Specify the user interface (UI) that displays during installation. You can append other options, such as `n` to hide the UI.
`install_all`	Specify components to be installed: • 0—Install the Netwrix Auditor client only. • 1—Full installation

4. Configure IT Infrastructure for Audit

Netwrix Auditor relies on native logs for collecting audit data. Therefore, successful change and access auditing requires a certain configuration of native audit settings in the audited environment and on the computer where Netwrix Auditor resides. Configuring your IT Infrastructure may also include enabling certain built-in Windows services, etc. Proper audit configuration is required to ensure audit data integrity, otherwise your change reports may contain warnings, errors or incomplete audit data.

The table below lists the native audit settings that must be adjusted to ensure collecting comprehensive and reliable audit data.

Audited system	Required configuration

Active Directory (including Group Policy)	***In the audited environment:***
	• The ADSI Edit utility must be installed on any domain controller in the audited domain. See Install ADSI Edit for more information.
	• The following policies must be set to *"Success"* for the effective domain controllers policy:
	  • **Audit account management**
	  • **Audit directory service access**
	• The **Audit logon events** policy must be set to *"Success"* (or *"Success"* and *"Failure"*) for the effective domain controllers policy.
	• The Advanced audit policy settings can be configured instead of basic.
	• The **Maximum Security event log** size must be set to 4GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*.
	OR
	Auto archiving must be enabled to prevent audit data loss if log overwrites occur.
	• The Object-level audit settings must be configured for the **Domain**, **Configuration** and **Schema** partitions.
	• The AD **tombstoneLifetime** attribute must be set to *"730"*.
	
	On the computer where Netwrix Auditor is installed:

Audited system	Required configuration
	• Customize the retention period for the backup logs if necessary (by default, it is set to *"50"*).

Exchange	***In the audited environment:***
	• The ADSI Edit utility must be installed on any domain controller in the audited domain. See Install ADSI Edit for more information.
	• The following policies must be set to *"Success"* for the effective domain controllers policy:
	  • **Audit account management**
	  • **Audit directory service access**
	• The **Audit logon events** policy must be set to *"Success"* (or *"Success"* and *"Failure"*) for the effective domain controllers policy.
	• The Advanced audit policy settings can be configured instead of basic.
	• The **Maximum Security event log** size must be set to 4GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*.
	  OR
	  Auto archiving must be enabled to prevent audit data loss if log overwrites occur.
	• The Object-level audit settings must be configured for the **Domain**, **Configuration** and **Schema** partitions.
	• The AD **tombstoneLifetime** attribute must be set to *"730"*.
	• The **Administrator Audit Logging** settings must be configured (only required for Exchange 2010 and 2013).
	• In order to audit mailbox access, the **Logons** logging level must be set to *"Minimum"* via the Exchange Management Shell.
	  NOTE: This is only required if you disable Netwrix Auditor Mailbox Access Core Service when auditing mailbox access on Exchange 2007 and 2010.
	• In order to audit mailbox access, native audit logging must be enabled for user, shared, equipment, linked, and room mailboxes.
	  • Access types: administrator , delegate user
	  • Actions: Update, Move, MoveToDeletedItems, SoftDelete, HardDelete,

Audited system	Required configuration
	FolderBind, SendAs, SendOnBehalf, Create ***On the computer where Netwrix Auditor is installed:*** • Customize the retention period for the backup logs, if necessary (by default, it is set to *"50"*).

Exchange Online	***In the audited environment:***
	• Native audit logging must be enabled for user, shared, equipment, linked, and room mailboxes.
	  • Access types: administrator , delegate user
	  • Actions: Update, Move, MoveToDeletedItems, SoftDelete, HardDelete, FolderBind, SendAs, SendOnBehalf, Create
	
	NOTE: This is only required for auditing non-owner mailbox access within your Exchange Online organization.

Window File Servers	***In the audited environment:***
	• For a security principal (e.g., **Everyone**), the following options must be set to *"Success"* and *"Fail"* in the **Advanced Security** → **Auditing** settings for the audited shared folders:
	  • List Folder / Read Data (Files only)
	  • Create Files / Write Data
	  • Create Folders / Append Data
	  • Write Attributes
	  • Write Extended Attributes
	  • Delete Subfolders and Files
	  • Delete
	  • Change Permissions
	  • Take Ownership
	• The **Audit object access** policy must set to *"Success"* and *"Failure"*.
	• The following **Advanced audit policy** settings can be configured if you want to narrow the scope of events collected by the product:
	  • The **Audit: Force audit policy subcategory settings (Windows Vista**

Audited system	Required configuration
	or later) security option must be enabled. • For **Windows Server 2008 / Windows Vista** — The **Object Access** category must be disabled while the **Handle Manipulation** and **File System** subcategories must be enabled. • For **Windows Server 2008 R2 / Windows 7 and above**—The **Audit File System** and **Audit Handle Manipulation** advanced audit policies must be set to *"Success"* and/or *"Failure"*. • The **Security event log maximum size** must be set to 4GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*. • The **Remote Registry** service must be started. • The following inbound Firewall rules must be enabled: • Remote Event Log Management (NP-In) • Remote Event Log Management (RPC) • Remote Event Log Management (RPC-EPMAP) • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (DCOM-In) • Windows Management Instrumentation (WMI-In) • Network Discovery (NB-Name-In) • File and Printer Sharing (NB-Name-In) • File and Printer Sharing (Echo Request - ICMPv4-In) • File and Printer Sharing (Echo Request - ICMPv6-In)
EMC Isilon	***In the audited environment:*** • **CIFS** Network Protocol support is required. • Create a shared directory */ifs/.ifsvar/audit/* on your cluster. **NOTE:** Use **SMB (CIFS)** protocol for sharing. • The following filters for auditing protocol operations that succeeded/failed must be enabled for audited access zones on your cluster: • Audit Success: read, write, delete, set_security, rename • Audit Failure: read, create, write, delete, set_security, rename

Audited system	Required configuration

EMC Celerra/ VNX/VNXe	***In the audited environment:***
	• **CIFS** Network Protocol support is required.
	• **Security Event Log Maximum Size** must be set to 4GB.
	• The **Audit object access** policy must be set to *"Success"* and *"Failure"* in the Group Policy of the OU where the audited EMC VNX/VNXe/Celerra appliance belongs to.
	• Audit settings must be configured for CIFS File Shares. For a security principal (e.g., **Everyone**), the following options must be set to *"Success"* and *"Fail"* in the **Advanced Security** → **Auditing** settings for the audited shared folders:
	  • List Folder / Read Data (Files only)
	  • Create Files / Write Data
	  • Create Folders / Append Data
	  • Write Attributes
	  • Write Extended Attributes
	  • Delete Subfolders and Files
	  • Delete
	  • Change Permissions
	  • Take Ownership

NetApp Filer	***In the audited environment:***
	• CIFS Network Protocol support is required.
	• Qtree Security must be configured. The volume where the audited file shares are located must be set to the *"ntfs"* or *"mixed"* security style.
	• On **Data ONTAP 7** and **Data ONTAP 8 in 7-mode**:
	  • The `httpd.admin.enable` or the `httpd.admin.ssl.enable` option must be set to *"on"*. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option.
	  • The `cifs.audit.liveview.enable` option must be set to *"off"*.
	  • The `cifs.audit.enable` and the `cifs.audit.file_access_events.enable` options must be set to *"on"*.
	  • Unless you are going to audit logon events, the `cifs.audit.logon_`

Audited system	Required configuration

`events.enable` and the `cifs.audit.account_mgmt_events.enable` options must be set to *"off"*.

- The Security log must be configured:
  - `cifs.audit.logsize 300 000 000 (300 MB)`
  - `cifs.audit.autosave.onsize.enable on`
  - `cifs.audit.autosave.file.extension timestamp`

- On **Clustered Data ONTAP 8**:
  - `External Web Services: true`.

    For security reasons, it is recommended to enable only SSL access.
  - Firewall policy for data interfaces must be modified to allow ONTAPI protocol connections.
  - Audit settings must be configured as follows:

```
                    Auditing State: true
              Log Destination Path: /logs
  Categories of Events to Audit: file-ops, cifs-
                                    logon-logoff
                     Log Format: evtx
```

  - `vserver audit modify -rotate-size 300MB`

- The Security Log shared folder must be configured if you are not going to detect in automatically via Netwrix Auditor Administrator Console.
- Audit settings must be configured for CIFS File Shares. For a security principal (e.g., **Everyone**), the following options must be set to *"Success"* and *"Fail"* in the **Advanced Security** → **Auditing** settings for the audited shared folders:
  - List Folder / Read Data (Files only)
  - Create Files / Write Data
  - Create Folders / Append Data
  - Write Attributes
  - Write Extended Attributes
  - Delete Subfolders and Files
  - Delete
  - Change Permissions

Audited system	Required configuration
	• Take Ownership
SharePoint	***In the audited environment:*** • The **Audit Log Trimming** setting must be set to *"Yes"* and **Specify the number of days of audit log data to retain** must be set to 7 days. • The **Editing users and permissions** option must be enabled. • For auditing read access events only: The **Opening or downloading documents, viewing items in lists, or viewing item properties** option must be enabled. • The **SPAdminV4** service must be enabled (required for the Netwrix Auditor Core Service for SharePoint installation).
SQL Server	No configuration is required
VMware	No configuration is required

Windows Server (including DNS)	***In the audited environment:***
	• The **Remote Registry** and the **Windows Management Instrumentation (WMI)** service must be started.
	• The **Audit Security Group Management, Audit User Account Management, Audit Handle Manipulation, Audit Other Object Access Events** and **Audit Registry** policy must be set to *"Success"*.
	• The **Security event log maximum size** must be set to 4 GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*.
	• The following inbound Firewall rules must be enabled:
	  • Remote Event Log Management (NP-In)
	  • Remote Event Log Management (RPC)
	  • Remote Event Log Management (RPC-EPMAP)
	  • Windows Management Instrumentation (ASync-In)
	  • Windows Management Instrumentation (DCOM-In)
	  • Windows Management Instrumentation (WMI-In)
	  • Network Discovery (NB-Name-In)
	  • File and Printer Sharing (NB-Name-In)

Audited system	Required configuration
	• Remote Service Management (NP-In) • Remote Service Management (RPC) • Remote Service Management (RPC-EPMAP) **NOTE:** If the audited servers are behind the Firewall, for configuration details refer to the following Netwrix Knowledge Base articles: How to audit servers located in another subnet behind firewall and Ports required to monitor servers over the firewall.
Event Log (including Cisco)	*In the audited environment:* • For Windows-based platforms: the **Remote Registry** service must be running and its **Startup Type** must be set to *"Automatic"*. • For Syslog-based platforms: the Syslog daemon must be configured to redirect events.
IIS	*In the audited environment:* • The **Remote Registry** service must be running and its **Startup Type** must be set to *"Automatic"*. • The **Microsoft-IIS-Configuration/Operational log** must be enabled and its **maximum size** must be set to 4 GB. The retention method of the log must be set to *"Overwrite events as needed"*.

Logon Activity	*In the audited environment:*
	• The following policies must be set to *"Success"* and *"Failure"* for the effective domain controllers policy:
	  • **Audit Logon Events**
	  • **Audit Account Logon Events**
	• The **Audit system events** policy must be set to *"Success"* for the effective domain controllers policy.
	• The Advanced audit policy settings can be configured instead of basic.
	• The **Maximum Security event log** size must be set to 4GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"* or *"Archive the log when full"*.
	• The following Windows Firewall inbound rules must be enabled:
	  • **Remote Event Log Management (NP-In)**

Audited system	Required configuration
	• **Remote Event Log Management (RPC)** • **Remote Event Log Management (RPC-EPMAP).**
User Activity	***In the audited environment:*** • The **Windows Management Instrumentation** and the **Remote Registry** service must be running and their **Startup Type** must be set to *"Automatic"*. • The **File and Printer Sharing** and the **Windows Management Instrumentation** features must be allowed to communicate through Windows Firewall. • Local TCP Port 9003 must be opened for inbound connections. • Remote TCP Port 9004 must be opened for outbound connections. ***On the computer where Netwrix Auditor is installed:*** • The **Windows Management Instrumentation** and the **Remote Registry** services must be running and their **Startup Type** must be set to *"Automatic"*. • The **File and Printer Sharing** and the **Windows Management Instrumentation** features must be allowed to communicate through Windows Firewall. • Local TCP Port 9004 must be opened for inbound connections.

Refer to the following topics for detailed instructions depending on the system you are going to audit:

- Configure Domain for Auditing Active Directory
- Configure Infrastructure for Auditing Exchange
- Configure Infrastructure for Auditing Exchange Online
- Configure Windows File Servers for Auditing
- Configure EMC Isilon for Auditing
- Configure EMC Celerra/VNX for Auditing
- Configure NetApp Filer for Auditing
- Configure SharePoint Farm for Auditing
- Configure Windows Server for Auditing
- Configure Infrastructure for Auditing Event Log
- Configure Domain for Auditing Group Policy
- Configure Infrastructure for Auditing IIS

- Configure Infrastructure for Auditing Logon Activity
- Configure Computers for Auditing User Activity

4.1. Configure Domain for Auditing Active Directory

You can configure your Active Directory domain for auditing in one of the following ways:

- Automatically when creating a Managed Object

  If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

- Automatically through the **Active Directory Audit Configuration** wizard integrated in Netwrix Auditor Administrator Console

  With this wizard you can configure audit settings for Active Directory, Exchange and Group Policy. On each step, the wizard checks your audit settings and provides a report on their current values. If any of your current settings conflict with the configuration required for the product to function properly, these conflicts will be listed. In this case, you can choose whether you want to adjust your audit settings automatically and override your current settings, or if you want to configure them manually. For detailed instructions, refer to Netwrix Auditor Administrator's Guide.

- Manually. To configure your domain for auditing manually, perform the following procedures:

  - Configure Basic Domain Audit Policies or Configure Advanced Audit Policies. Either local or advanced audit policies must be configured to track changes to accounts and groups, and to identify workstations where changes were made.
  - Configure Object-Level Auditing
  - Configure Security Event Log Size and Retention Settings
  - Adjust Active Directory Tombstone Lifetime

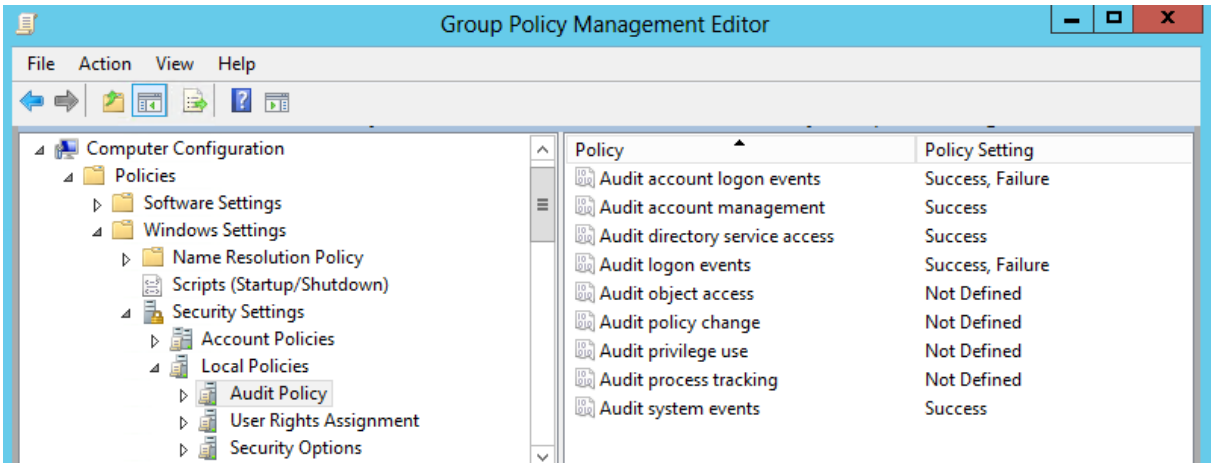
  NOTE: Netwrix recommends you to exclude read-only domain controllers from the Active Directory auditing scope. See Netwrix Auditor Administrator Guide for more information.

4.1.1. Configure Basic Domain Audit Policies

Basic audit policies allow tracking changes to user accounts and groups and identifying originating workstations. You can configure advanced audit policies for the same purpose too. See Configure Advanced Audit Policies for more information.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers 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** → **Audit Policy.**
4. Configure the following audit policies.

Policy	Audit Events
Audit account management	*"Success"*
Audit directory service access	*"Success"*
Audit logon events	*"Success"* and *"Failure"*



NOTE: The **Audit logon events** policy is only required to collect the information on the originating workstation, i.e., the computer from which a change was made. This functionality is optional and can be disabled. See Netwrix Auditor Administrator's Guide for more information.

5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

4.1.2. Configure Advanced Audit Policies

You can configure advanced audit policies instead of basic domain policies to collect Active Directory changes with more granularity. Either basic or advanced audit policies must be configured to track changes to accounts and groups, and to identify workstations where changes were made.

Perform the following procedures:

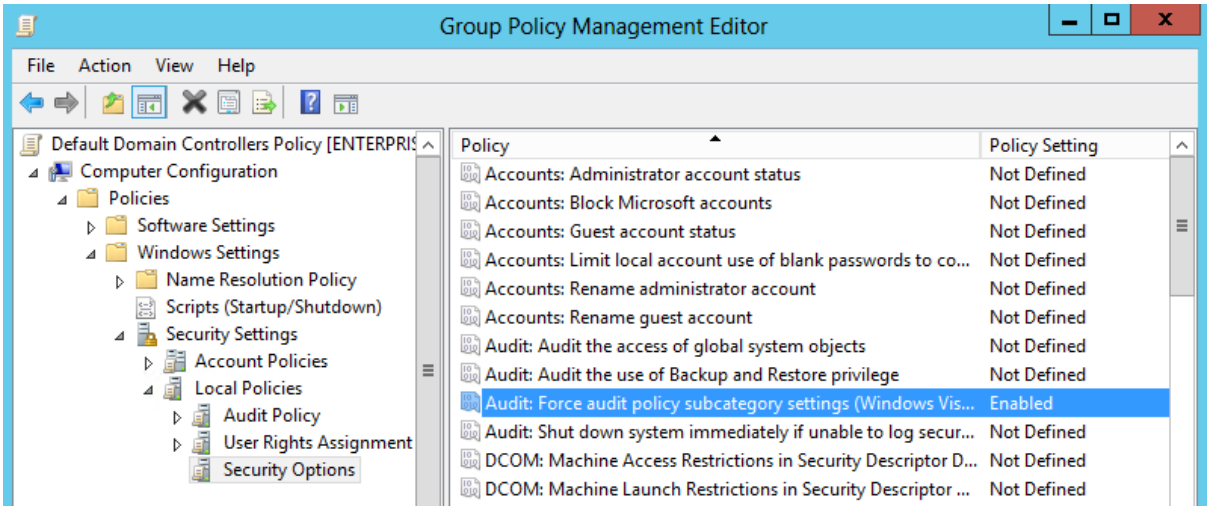
- To configure security options
- To configure advanced audit policies

To configure security options

NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** option.

To do it, perform the following steps:

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers 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** → **Security Options**.
4. Locate the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** and make sure that policy setting is set to *"Enabled"*.



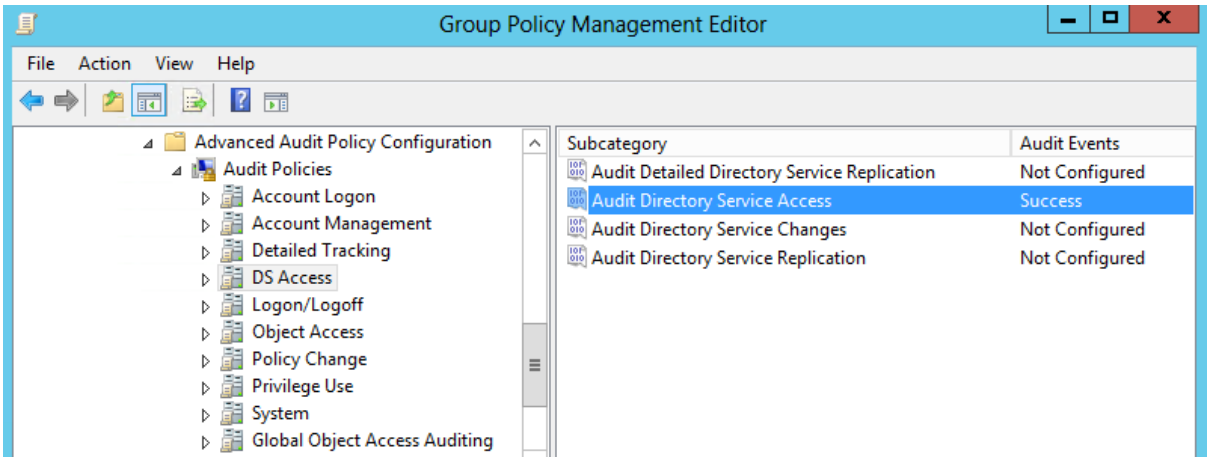
5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

To configure advanced audit policies

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**

2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers 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** → **Advanced Audit Policy Configuration** → **Audit Policies**.
4. Configure the following audit policies.

Policy Subnode	Policy Name	Audit Events
Account Management	• **Audit Computer Account Management** • **Audit Distribution Group Management** • **Audit Security Group Management** • **Audit User Account Management**	*"Success"*
DS Access	**Audit Directory Service Access**	*"Success"*
Logon/Logoff	• **Audit Logoff** • **Audit Logon** **NOTE:** These policies are only required to collect the information on the originating workstation, i.e., the computer from which a change was made.	*"Success"*



5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

4.1.3. Configure Object-Level Auditing

Object-level Active Directory auditing must be configured so that the "Who" and "When" information appears in audit reports. If, in addition to the Domain partition, you also want to audit changes to AD configuration and schema, you must enable object-level auditing for these partitions.

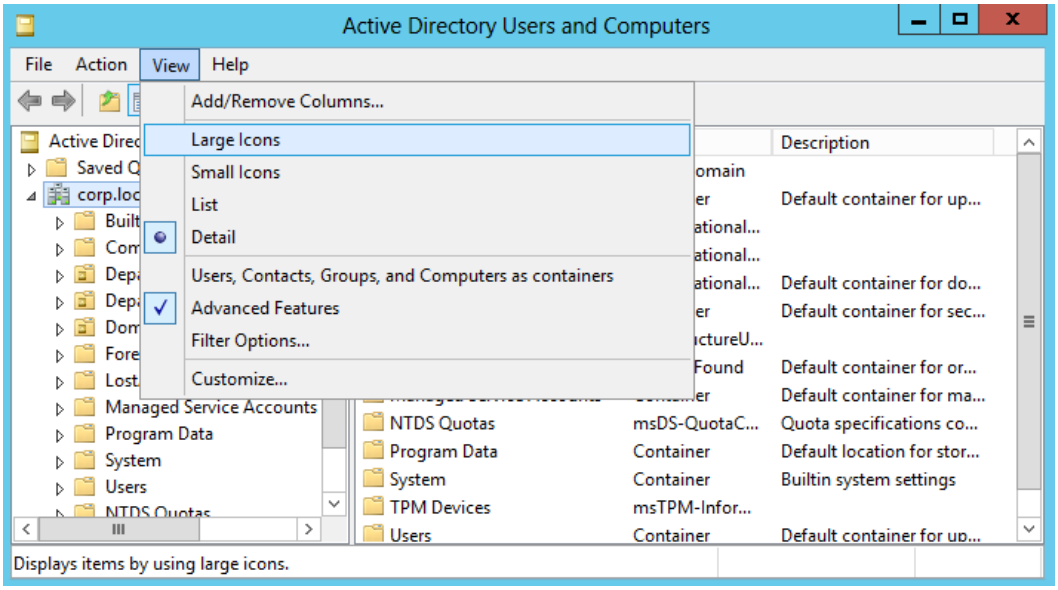
NOTE: Auditing of the Configuration partition is enabled by default. Refer to Netwrix Auditor Administrator's Guide for detailed instructions on how to enable auditing of changes to the Schema partition in the target AD domain.

Perform the following procedures to configure object-level auditing for the Domain, Configuration and Schema partitions:

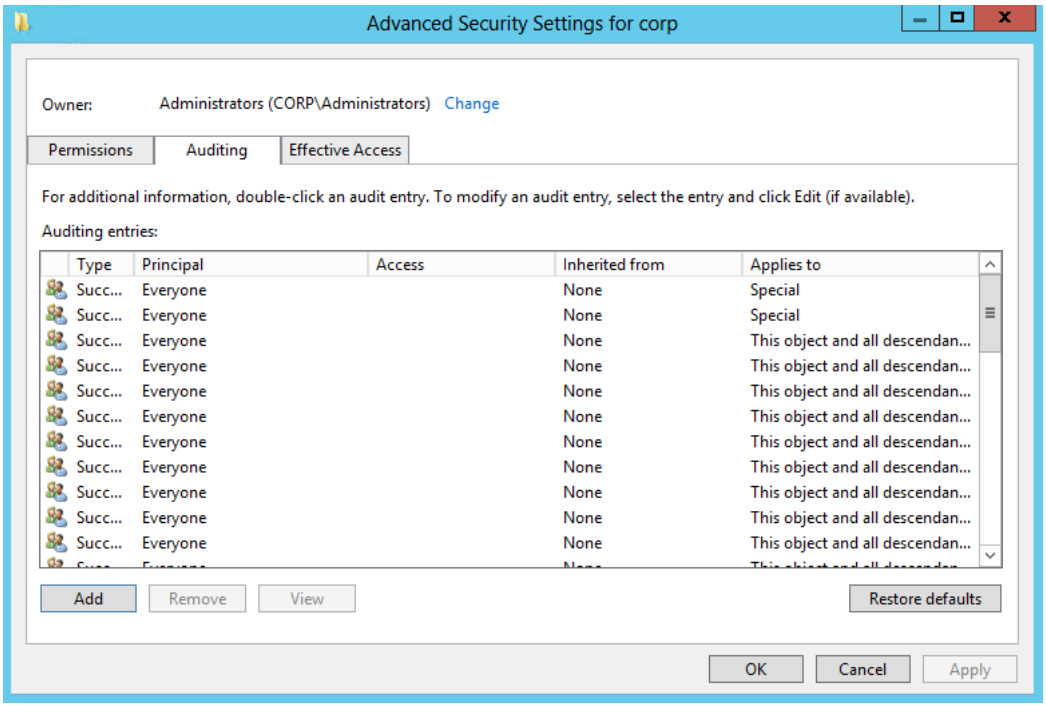
- To configure object-level auditing for the Domain partition
- To enable object-level auditing for the Configuration and Schema partitions

To configure object-level auditing for the Domain partition

1. Open the **Active Directory Users and Computers** console on any domain controller in the target domain: navigate to **Start**→ **Administrative Tools** → **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** are enabled.



3. Right-click the **<domain_name>** node and select **Properties.** Select the **Security** tab and click **Advanced**. In the **Advanced Security Settings for <domain_name>** dialog, select the **Auditing** tab.

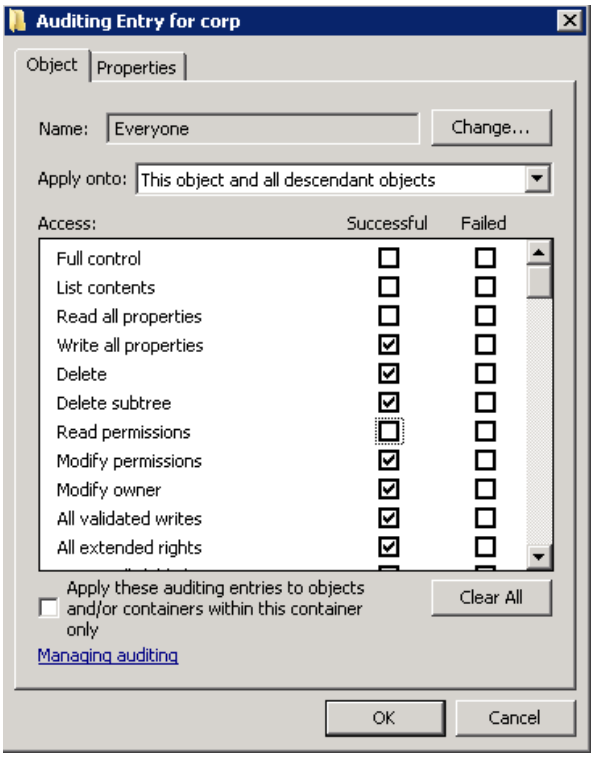


4. Do one of the following depending on the OS:

   - On pre-Windows Server 2012 versions:

     a. Click **Add**. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

     b. In the **Audit Entry** dialog that opens, set the *"Successful"* flag for all access entries except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.



c. Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared. Also, make sure that the **Apply onto** parameter is set to *"This object and all descendant objects"*.

- On Windows Server 2012 and above

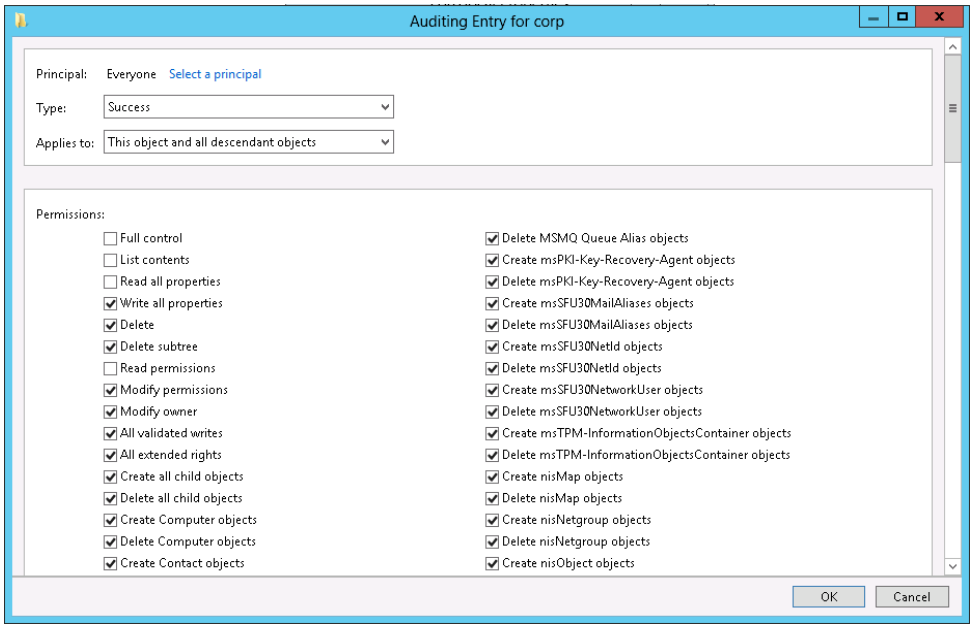
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

b. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

c. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.

d. Under **Permissions**, select all checkboxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

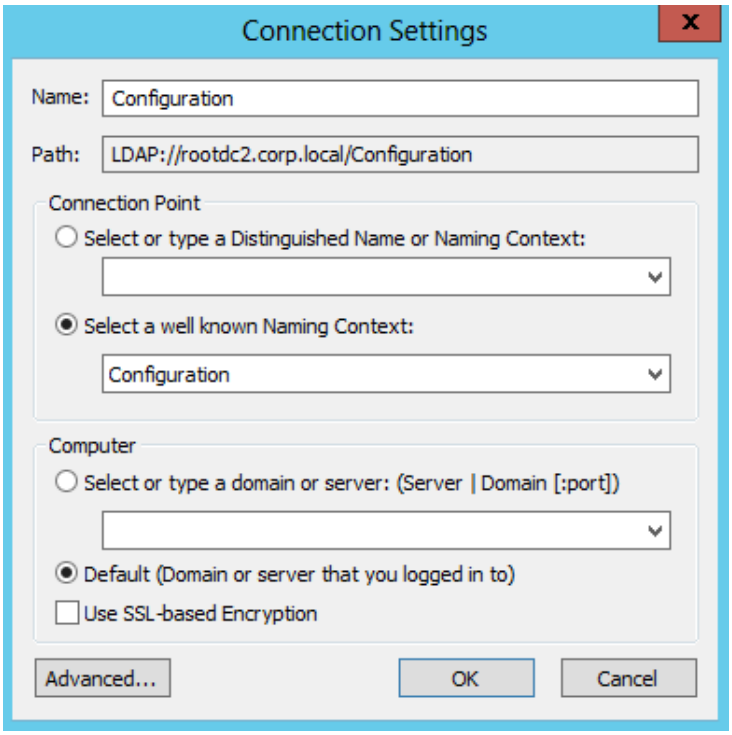
e. Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.



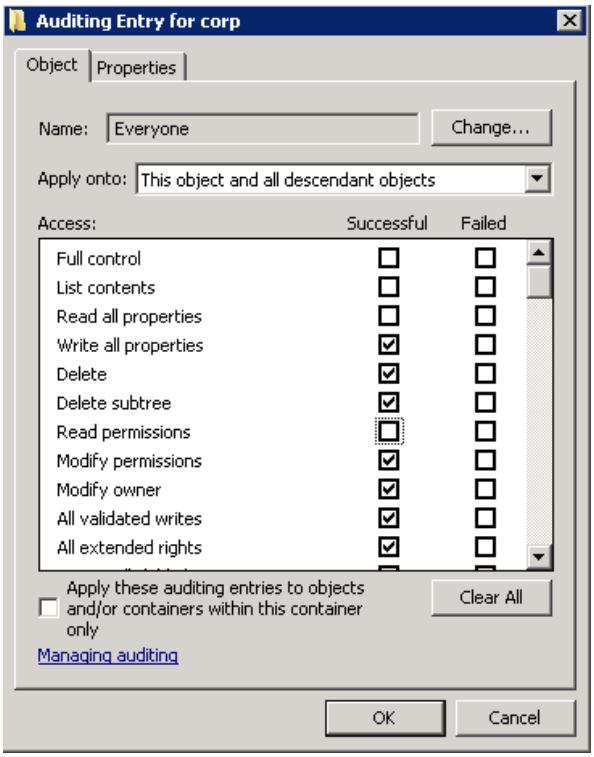
To enable object-level auditing for the Configuration and Schema partitions

NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2008 and above, this component is installed together with the AD DS role, or it can be downloaded and installed along with Remote Server Administration Tools. Refer to Install ADSI Edit for detailed instructions on how to install the ADSI Edit utility.

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **ADSI Edit**.
2. Right-click the **ADSI Edit** node and select **Connect To**. In the **Connection Settings** dialog, enable **Select a well-known Naming Context** and select **Configuration** from the drop-down list.



3. Expand the **Configuration <Your_Root_Domain_Name>** node. Right-click the **CN=Configuration, DC=<name>,DC=<name>...** node and select **Properties.**
4. In the **CN=Configuration, DC=<name>, DC=<name> Properties** dialog select the **Security** tab and click **Advanced**. In the **Advanced Security Settings for Configuration** dialog, open the **Auditing** tab.
5. Do one of the following depending on the OS:
   - On pre-Windows Server 2012 versions:
     a. Click **Add**. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.
     b. In the **Audit Entry** dialog that opens, set the *"Successful"* flag for all access entries except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.



c. Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared. Also, make sure that the **Apply onto** parameter is set to *"This object and all descendant objects"*.

- On Windows Server 2012 and above

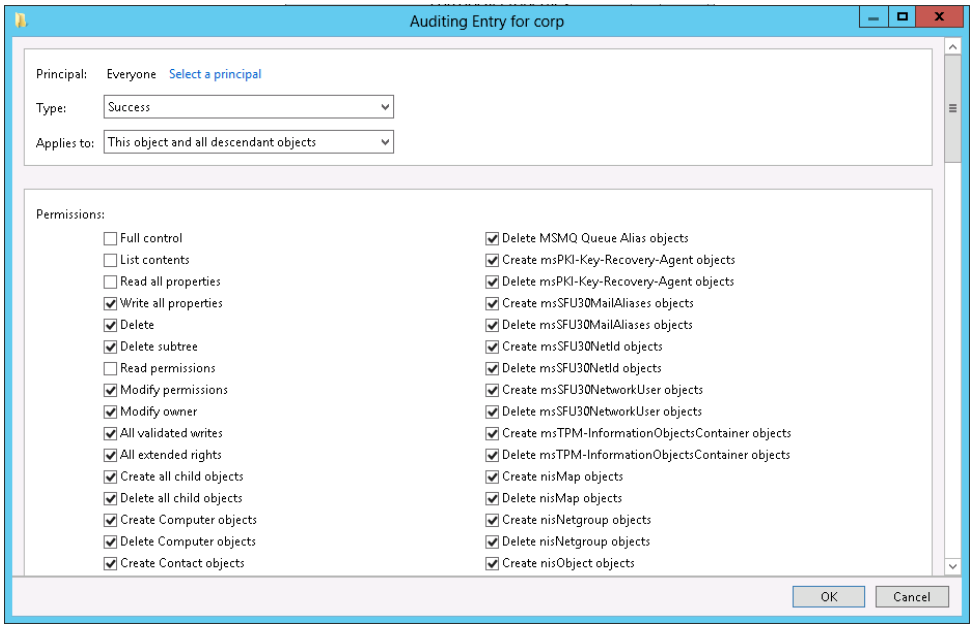
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

b. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

c. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.

d. Under **Permissions**, select all checkboxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

e. Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.



6. Repeat these steps for the Schema container if necessary.

4.1.4. Configure Security Event Log Size and Retention Settings

Defining the **Security** event log size is essential for change auditing. If your **Security** log size is insufficient, overwrites may occur before data is written to the Long-Term Archive and the Audit Database, and some audit data may be lost. To prevent overwrites, you must increase the maximum size of the **Security** event log.

The retention method of the **Security** event log must be set to *"Overwrite events as needed"* (unless it is set to *"Archive the log when full"*). In this case, events will be written into the log even if it reaches its maximum size (new events will overwrite the oldest events in the log). Alternatively, you can enable auto archiving for the **Security** event log to prevent audit data loss if log overwrites occur.

To adjust your **Security** event log size and retention settings, perform the following procedures:

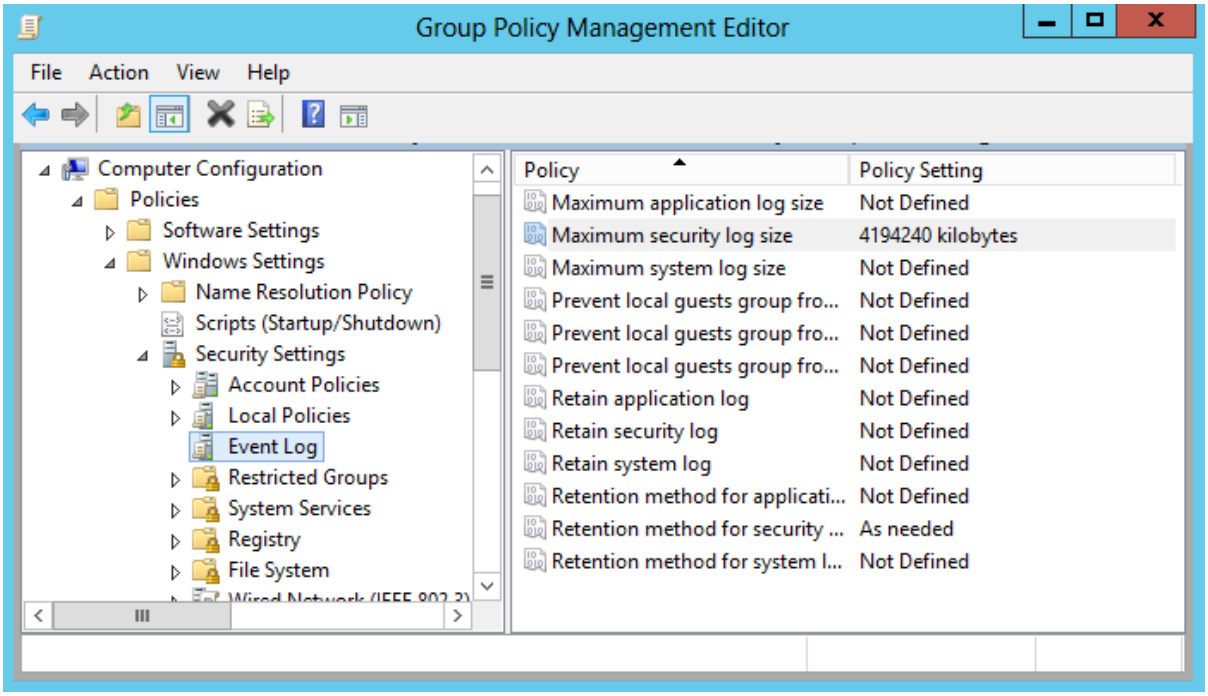
- To increase the maximum size of the Security event log and set its retention method
- To enable Auto archiving centrally on all domain controllers
- To configure the retention period for the backup logs

To increase the maximum size of the Security event log and set its retention method

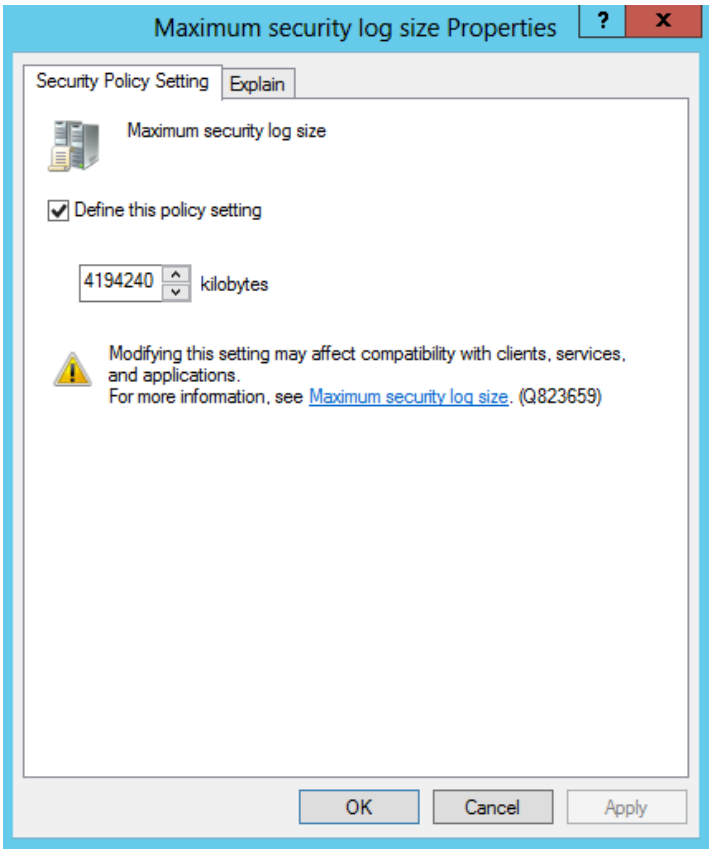
1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain**

Controllers Policy), and select **Edit** from the pop-up menu.

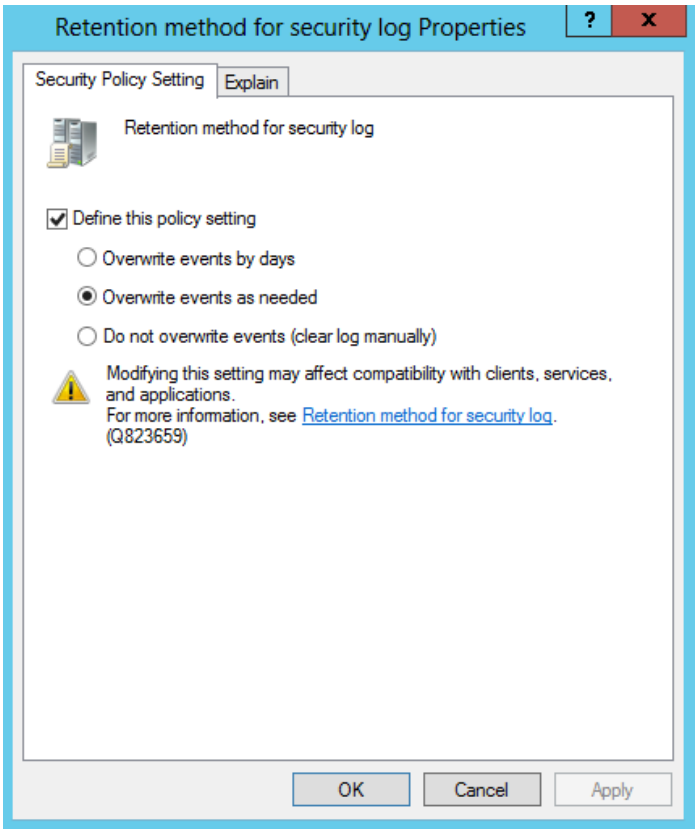
3. Navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log** and double-click the **Maximum security log size** policy.



4. In the **Maximum security log size Properties** dialog, select **Define this policy setting** and set maximum security log size to *"4194240"* kilobytes (4GB).



5. Select the **Retention method for security log** policy. In the **Retention method for security log Properties** dialog, check **Define this policy** and select **Overwrite events as needed**.



6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

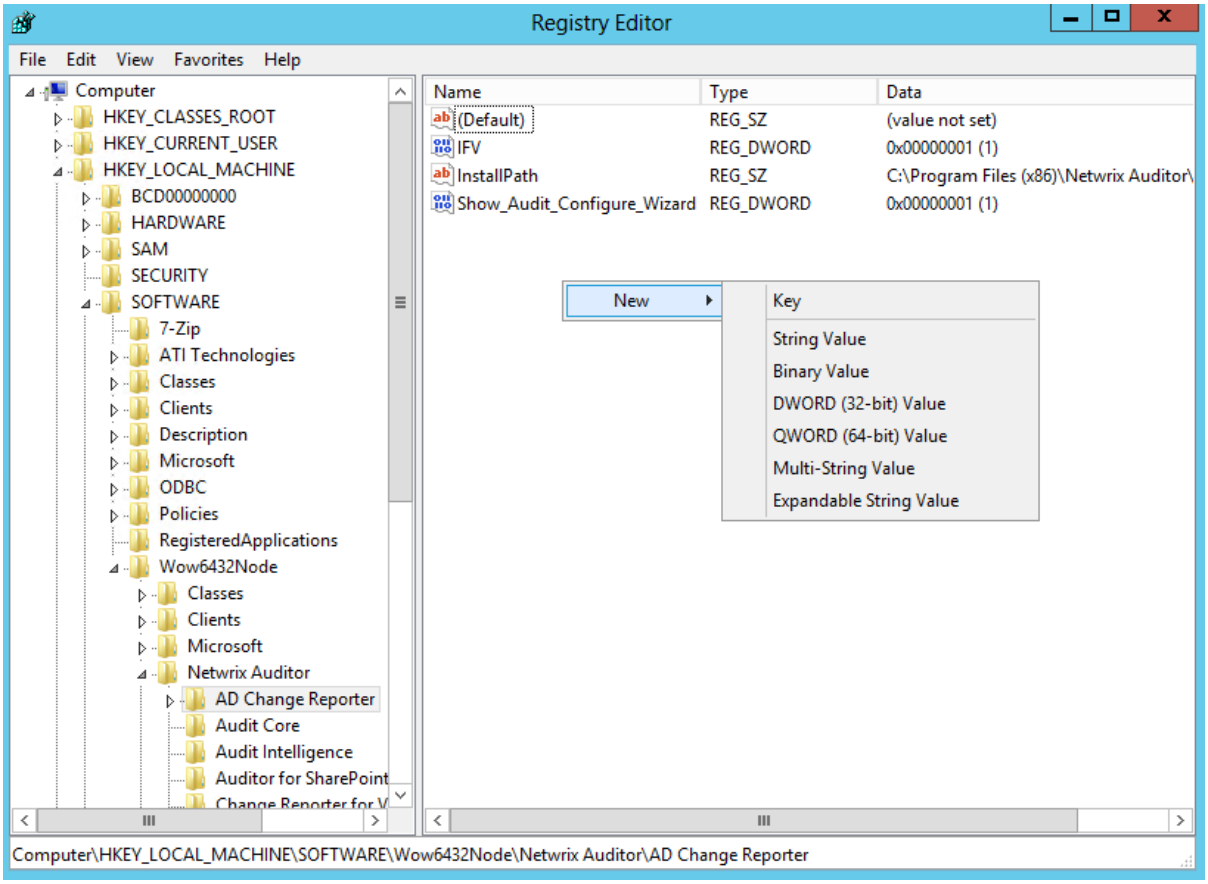
To enable Auto archiving centrally on all domain controllers

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. Navigate to **Computer Configuration** → **Policies**. Right-click **Administrative Templates: Policy definitions** and select **Add / Remove templates**. Click **Add** in the dialog that opens.
4. In the **Policy Templates** dialog, navigate to *%Netwrix Auditor installation folder%/Active Directory Auditing*, select the **Log Autobackup.adm** file (if the product is installed on a different computer, copy this file to the domain controller), and click **Open**.
5. Navigate to **Administrative Templates: Policy definitions** → **Classic Administrative Templates** → **System** → **Event Log**. Select **Automatically clear a full security event log and back up the log file** and set it to *"Enable"*.
6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

To configure the retention period for the backup logs

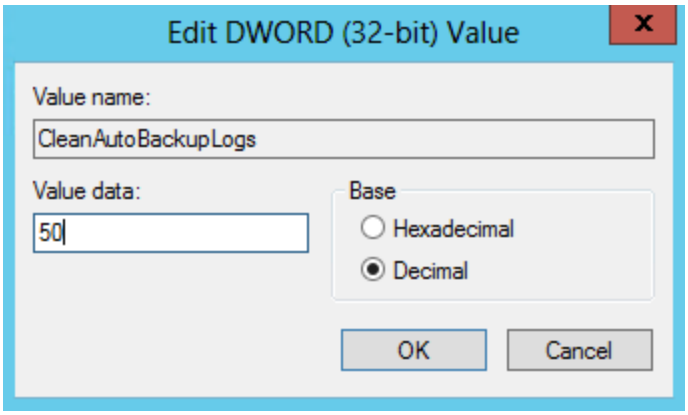
1. On the computer where Netwrix Auditor is installed, open **Registry Editor**: navigate to **Start→ Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE → SOFTWARE → Wow6432Node → Netwrix Auditor → AD Change Reporter**.
3. In the right-pane, right-click and select **New→DWORD (32-bit Value)**.

   NOTE: For the backup logs retention functionality to work properly, you need to specify the **CleanAutoBackupLogs** name for the newly created registry value.



4. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.

   This value defines the time period (in hours) after which security event logs archives will be automatically deleted from the domain controllers. By default, it is set to *"50"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.



NOTE: If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old automatic backups manually, or you may run out of space on your hard drive.

4.1.5. Adjust Active Directory Tombstone Lifetime

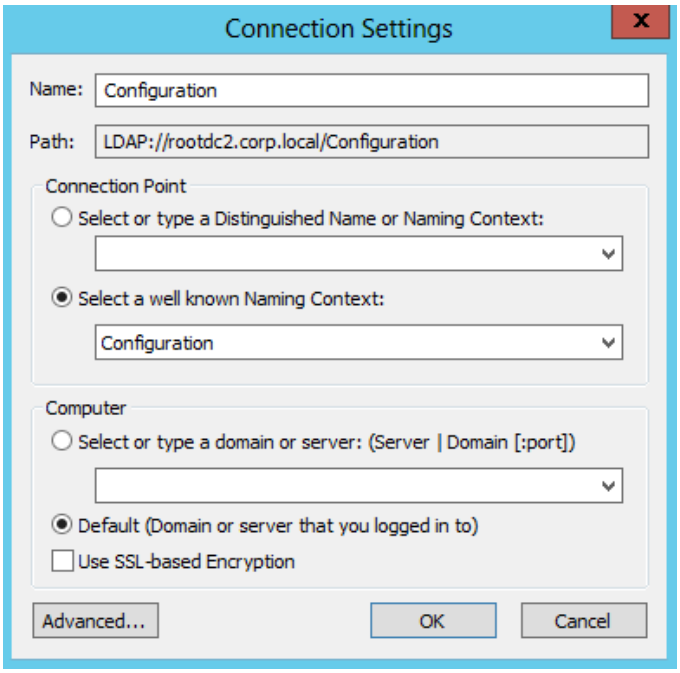
You can restore deleted Active Directory objects and their attributes using the Active Directory Object Restore tool integrated with Netwrix Auditor. The tool finds the information on deleted objects in the product snapshots (this data is stored in the Long-Term Archive, a local file-based storage of audit data) and AD tombstones.

To be able to restore deleted Active Directory objects longer, increase the Active Directory tombstone lifetime property (set by default to 180 days). Netwrix recommends to set it to 2 years (730 days). You can specify any number of days, but a selected value should not exceed the Long-Term Archive retention period. Take into consideration that increasing tombstone lifetime may affect Active Directory performance and operability.

To change the tombstone lifetime attribute

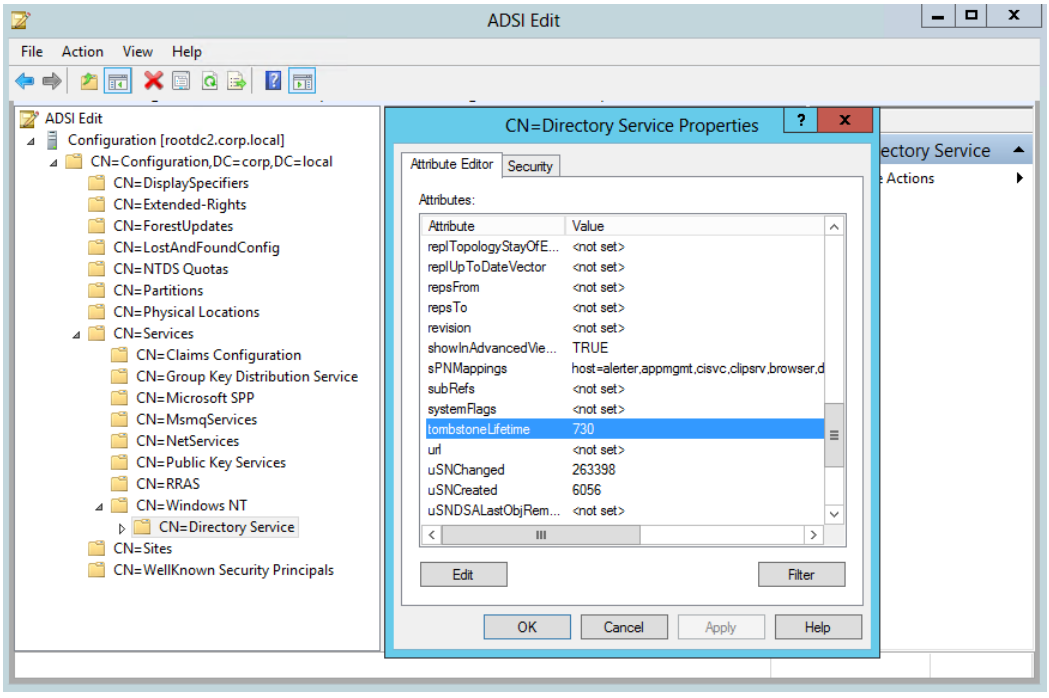
NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2008 and above, this component is installed together with the AD DS role, or it can be downloaded and installed along with Remote Server Administration Tools. Refer to Install ADSI Edit for detailed instructions on how to install the ADSI Edit utility.

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **ADSI Edit**.
2. Right-click the **ADSI Edit** node and select **Connect To**. In the **Connection Settings** dialog, enable **Select a well-known Naming Context** and select **Configuration** from the drop-down list.



3. Navigate to **Configuration <Your_Root_Domain_Name** → **CN=Configuration,DC=<name>,DC=<name>** → **CN=Services** → **CN=Windows NT** → **CN=Directory Service**. Right-click it and select **Properties** from the pop-up menu.

4. In the **CN=Directory Service Properties** dialog, locate the **tombstoneLifetime** attribute in the **Attribute Editor** tab.



5. Click **Edit**. Set the value to *"730"* (which equals 2 years).

4.2. Configure Infrastructure for Auditing Exchange

You can configure your infrastructure for auditing Exchange in one of the following ways:

- Automatically when creating a Managed Object

  If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

- Automatically through the **Active Directory Audit Configuration** wizard integrated in Netwrix Auditor Administrator Console

  With this wizard you can configure audit settings for Active Directory, Exchange and Group Policy. On each step, the wizard checks your audit settings and provides a report on their current values. If any of your current settings conflict with the configuration required for the product to function properly, these conflicts will be listed. In this case, you can choose whether you want to adjust your audit settings automatically and override your current settings, or if you want to configure them manually. For detailed instructions, refer to Netwrix Auditor Administrator's Guide.

- Manually. You need to adjust the same audit settings as those required for auditing Active Directory. See Configure Domain for Auditing Active Directory for more information.

  If your Exchange organization is running Exchange 2010 or 2013, you must also configure the Administrator Audit Logging (AAL) settings. If you want to audit non-owner access in addition to Exchange auditing, configure mailbox audit. See Configure Exchange for Auditing Mailbox Access for more information.

4.2.1. Configure Exchange Administrator Audit Logging Settings

If the audited AD domain has an Exchange organization running Exchange 2010 or 2013, you must configure the Exchange Administrator Audit Logging (AAL) settings. To do this, perform the following procedure on any of the audited Exchanges (these settings will then be replicated to all Exchanges in the domain).

To configure Exchange Administrator Audit Logging settings

1. On the computer where the audited Exchange is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**.
2. Execute the following command depending on your Exchange version:

- Exchange 2010

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets *
```

- Exchange 2013

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets * -LogLevel Verbose
```

3. On the computer where Netwrix Auditor is installed, browse to the *%Netwrix Auditor installation folder%/Active Directory Auditing* folder, locate the **SetAALExcludedCmdlets.ps1** file and copy it to Exchange.
4. In **Exchange Management Shell**, in the command line, execute this file by specifying the path to it:

```
<Path_To_ SetAALExcludedCmdlets_File>\SetAALExcludedCmdlets.ps1
```

This file contains a list of cmdlets that must be excluded from Exchange logging to reduce server load.

4.2.2. Configure Exchange for Auditing Mailbox Access

Perform the following procedures:

- To configure mailbox access auditing for Exchange 2007 and 2010
- To configure mailbox access auditing for Exchange 2013

To configure mailbox access auditing for Exchange 2007 and 2010

Netwrix Auditor allows auditing non-owner mailbox access on Exchange, and provides utilities that let you dispense with native Exchange auditing. These utilities log information on all types of non-owner activities in mailboxes of other users (opening messages and folders, sending emails, etc.). If the **Use Core Service to collect detailed audit data** option is disabled, only the access event itself is logged.

If you do not use Network traffic compression for data collection, you must configure native auditing on the audited Exchange:

1. On the computer where the audited Exchange is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**.
2. Execute the following command:

```
Set-EventLogLevel "MSExchangeIS\9000 Private\Logons" -Level Low
```

3. Navigate to **Start** → **Run** and type *"services.msc"*. In the **Services** snap-in, locate the **Microsoft Exchange Information Store** service and restart it.

To configure mailbox access auditing for Exchange 2013

Netwrix Auditor automatically configures auditing settings for Exchange 2013. In case of failure, you must configure native auditing on each audited Exchange server manually. You can configure auditing for:

- All user, shared, linked, equipment, and room mailboxes
- Selected mailboxes

Perform the steps in the table below to start auditing your mailboxes.

Audit...	Steps...
All mailboxes	1. On the computer where the audited Exchange is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**. **NOTE:** If you have already configured Netwrix Auditor to audit mailbox access, you can find the full list of audited Exchange servers on the computer where Netwrix Auditor resides. Navigate to **C:\ProgramData\Netwrix Auditor\Non-owner Mailbox Access Reporter for Exchange\Default.xml** 2. Execute the following command: `Get-MailboxDatabase -Server {0} | foreach { Get-Mailbox -RecipientTypeDetails UserMailbox, SharedMailbox, EquipmentMailbox, LinkedMailbox, RoomMailbox | Set-Mailbox -AuditEnabled $true -AuditAdmin Update,Copy,Move, MoveToDeletedItems,SoftDelete,HardDelete,FolderBind, SendAs,SendOnBehalf,MessageBind,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete,HardDelete, FolderBind,SendAs,SendOnBehalf,Create }` Where the *{0}* character must be replaced with your audited server **FQDN name** (e.g., *stationexchange.enterprise.local*). **NOTE:** If you are going to audit multiple Exchange servers, repeat these steps for each audited Exchange.
Selected mailbox	1. On the computer where the audited Exchange is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**. 2. Execute the following command: `Set-Mailbox -Identity {0} -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete, FolderBind,SendAs,SendOnBehalf,MessageBind,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete, HardDelete,FolderBind,SendAs,SendOnBehalf,Create` Where the *{0}* character must be replaced with one of the following: • `Display Name. Example: "Michael Jones"` • `SMTP address. Example: mail.enterprise.local.com` • `Domain\User. Example: enterprise.local\MJones`

Audit...	Steps...
	• GUID. Example: {c43a7694-ba06-46d2-ac9b-205f25dfb32d} • (DN) Distinguished name. Example: CN=MJones,CN=Users,DC=enterprisedc1,DC=enterprise,DC=local • User Principal Name. Example: MJones@enterprise.local

NOTE: If you are going to audit multiple individual mailboxes, repeat these steps for each mailbox on each Exchange server.

4.3. Configure Infrastructure for Auditing Exchange Online

You can configure your Exchange Online for auditing in one of the following ways:

- Automatically when creating a Managed Object. If you select to configure audit on the target Exchange Online automatically, your current audit settings will be checked on each data collection and adjusted if necessary.
- Manually. Special manual configuration steps only required if you are going to audit non-owner mailbox access within your Exchange Online organization. In this case, you need to create a remote Shell session to Exchange Online. For detailed instructions on how to create a remote session, read the following Microsoft article: Connect to Exchange Online using remote PowerShell.

Perform the steps in the table below to start auditing mailbox access your Exchange Online organization.

To...	Do...
Audit all mailboxes	1. On the local computer, navigate to **Start** → **Programs** → **Windows Power Shell**. 2. Connect to your Exchange Online. 3. Execute the following command: `Get-Mailbox -RecipientTypeDetails UserMailbox,SharedMailbox,EquipmentMailbox,LinkedMailbox, RoomMailbox | Set-Mailbox -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete, FolderBind,SendAs,SendOnBehalf,MessageBind,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete, HardDelete,FolderBind,SendAs,SendOnBehalf,Create`
Audit selected mailbox	1. On the local computer, navigate to **Start** → **Programs** → **Windows Power Shell**.

To...	Do...

2. Connect to Exchange Online.
3. Execute the following command:

```
Set-Mailbox -Identity {0} -AuditEnabled $true –AuditAdmin
Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete,
FolderBind,SendAs,SendOnBehalf,MessageBind,Create
–AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete,
HardDelete,FolderBind,SendAs,SendOnBehalf,Create
```

Where the *{0}* character must be replaced with one of the following:

- `Display Name. Example: "Michael Jones"`
- `SMTP address. Example: mail.enterprise.local.com`
- `Domain\User. Example: enterprise.local\MJones`
- `Email address. Example: analyst@enterprise.onmicrosoft.com`
- `GUID. Example: {c43a7694-ba06-46d2-ac9b-205f25dfb32d}`
- `LegacyExchangeDN. Example: /o=EnterpriseDev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT) /cn=Recipients/cn=97da560450c942aba81b2da46c60858a-analyst`
- `SamAccountName. Example: MANAG58792-1758064122`
- `(DN) Distinguished name. Example: CN=MJones,CN=Users,DC=enterprisedc1,DC=enterprise,DC=local`
- `User ID or User Principal Name. Example: MJones@enterprise.onmicrosoft.com`

NOTE: If you are going to audit multiple individual mailboxes, repeat these steps for each mailbox.

4.4. Configure Windows File Servers for Auditing

If you have multiple file shares frequently accessed by a significant number of users, it is reasonable to audit objects modification only. Tracking all access events may result in too much data written to the audit logs, whereas only some part of it may be of any interest. Note that audit flags must be set on every file share you want to audit.

If you are going to audit an entire file server, consider the following:

- If you specify a single computer name, Netwrix Auditor will audit all shared folders on this computer. Note that Netwrix Auditor does not track content changes on folders whose name ends with the $ symbol (which are either hidden or administrative/system folders). In order for the report functionality to work properly, you need to configure audit settings for each share folder on the computer separately. Otherwise, reports will contain limited data and warning messages.
- For your convenience, if your file shares are stored within one folder (or disk drive), you can configure audit settings for this folder only. As a result, you will receive reports on all required access types applied to all file shares within this folder. It is not recommended to configure audit settings for system disks.

You can configure your file shares for auditing in one of the following ways:

- Automatically when creating a Managed Object

  If you select to automatically configure audit in the target environment, your current audit settings will be periodically checked and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments.

- Manually. To configure your file servers for auditing manually, perform the following procedures:
  - Configure Object-Level Access Auditing
  - Configure Audit Object Access Policy or Configure Advanced Audit Policy
  - Configure Event Log Size and Retention Settings
  - Enable Remote Registry Service
  - Configure Windows Firewall Inbound Connection Rules

4.4.1. Configure Object-Level Access Auditing

Netwrix Auditor can be configured to audit all access types, review the table below and select options that you want to track:

Access Type	Description
Successful modifications	Commonly used option to track important data. Helps find out *who* created, modified, moved, renamed or removed files and *when* these changes were done.
Failed modification attempts	Used to track suspicious activity on your file server. Helps find out *who* tried to change or delete files, etc., but failed to do it. Investigate incidents with AuditIntelligence and figure out *why* that user tried to do it.
Successful reads	Used to supervise important files with confidential information for

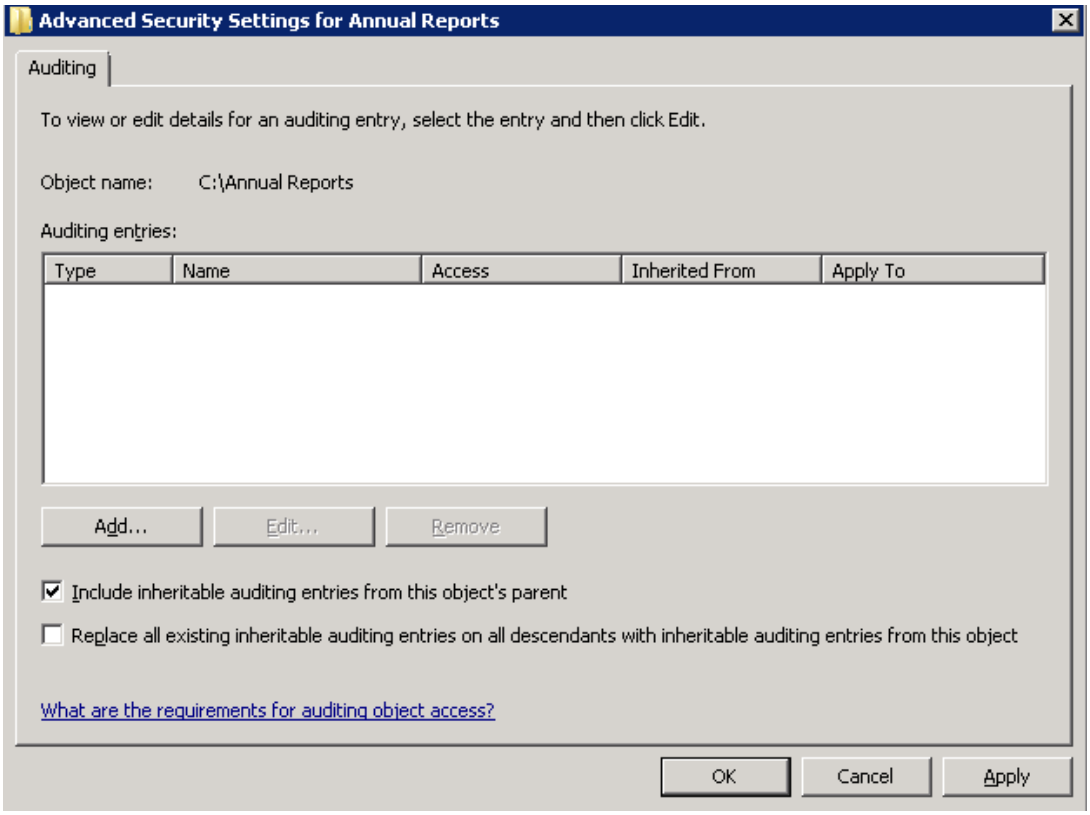
Access Type	Description
	privileged users only. Browse your audit data in the Netwrix Auditor client and discover *who* accessed important files besides your trusted users. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.
Failed read attempts	Used to track suspicious activity. Helps find out *who* was trying to read files, but failed to do it. Investigate your incidents with AuditIntelligence and figure out *why* that user tried to do it. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.

Perform one of the following procedures depending on the OS:

- To configure Object-level access auditing on pre-Windows Server 2012 versions
- To configure Object-level access auditing on Windows Server 2012 and above

To configure Object-level access auditing on pre-Windows Server 2012 versions

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. In a separate **Advanced Security Settings for <Share_Name>** dialog, click **Add** to add a principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.

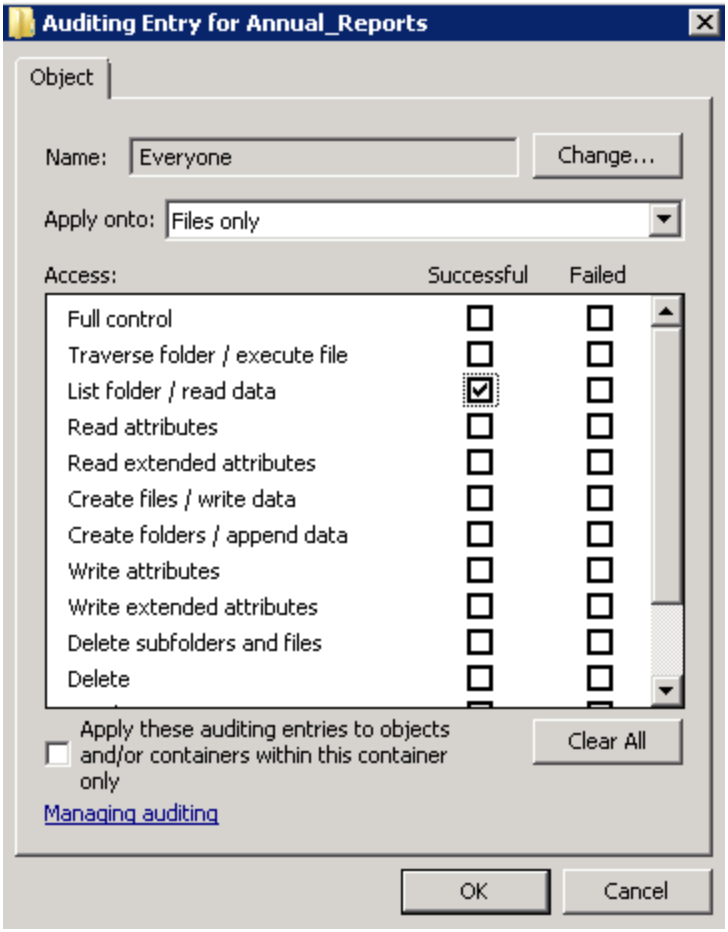
   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the reports or data searches performed in the Netwrix Auditor client and the product will only audit user accounts that belong to the selected group.

5. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modifications as well as failed reads and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful modifications
   - Failed read attempts
   - Failed modification attempts

Auditing Entry
Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

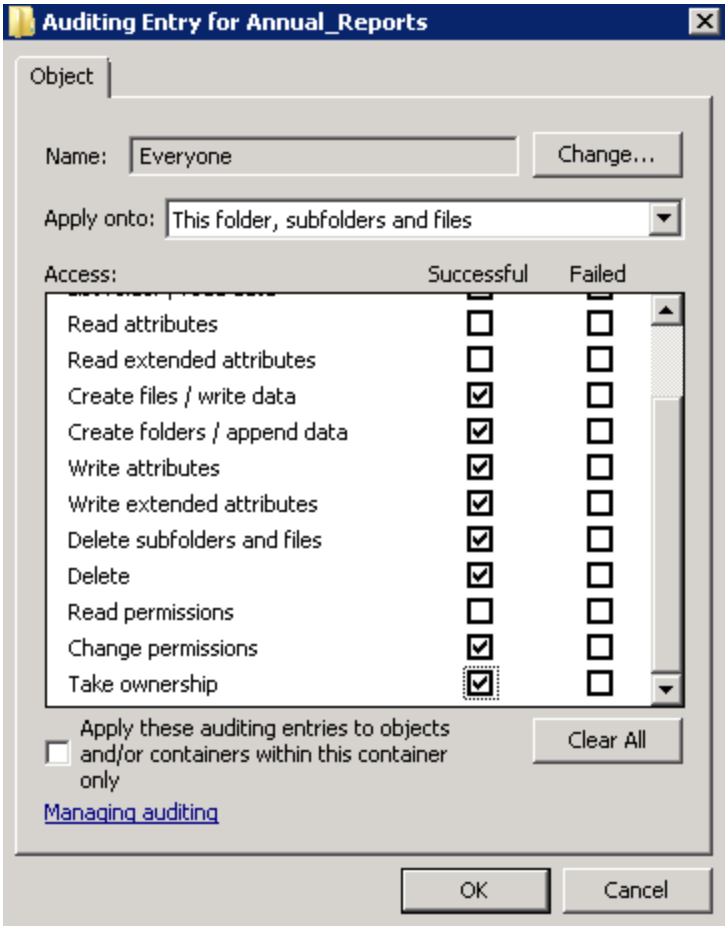


- Apply onto—Select *"Files only"*.
- Check *"Successful"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful modifications

The Auditing Entry below shows Advanced Permissions for auditing successful modifications only:

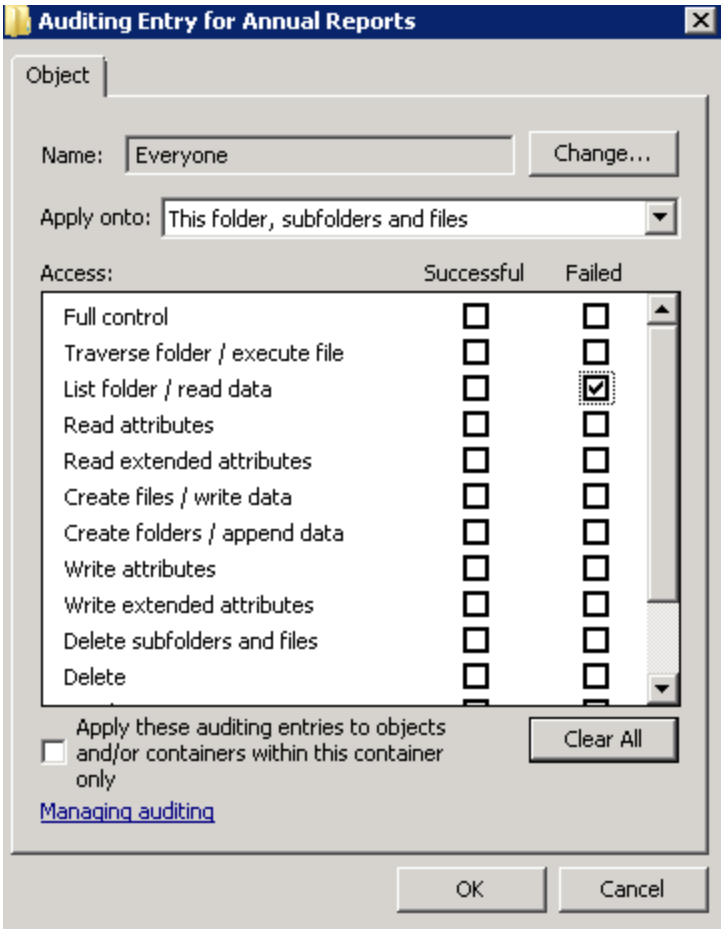
Auditing Entry



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Successful"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Auditing Entry
Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts only:

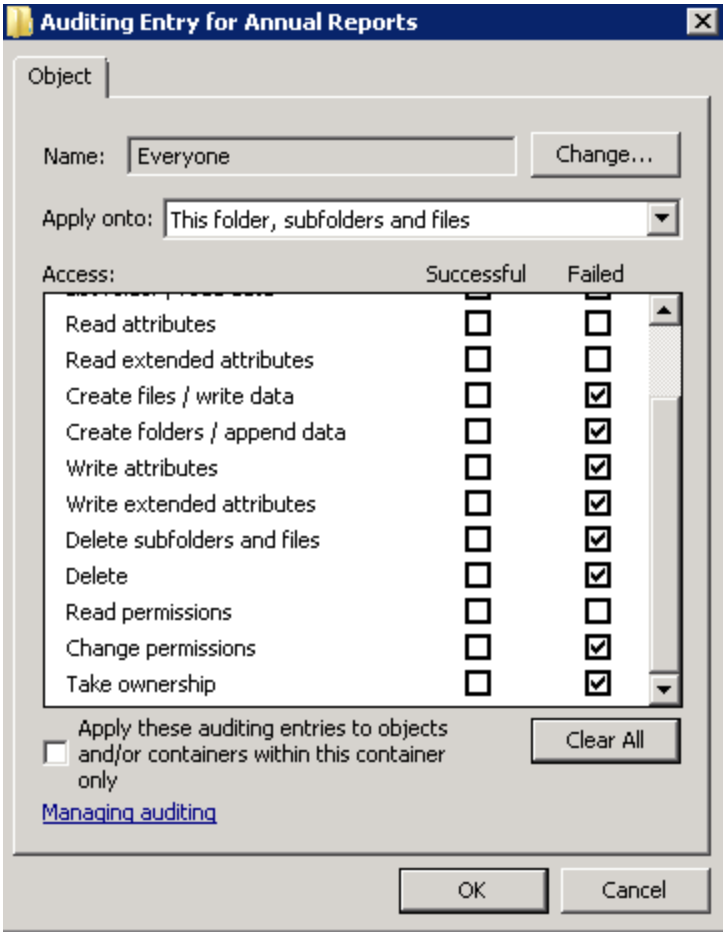


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed modification attempts

The Auditing Entry below shows Advanced Permissions for auditing failed modification attempts only:

Auditing Entry

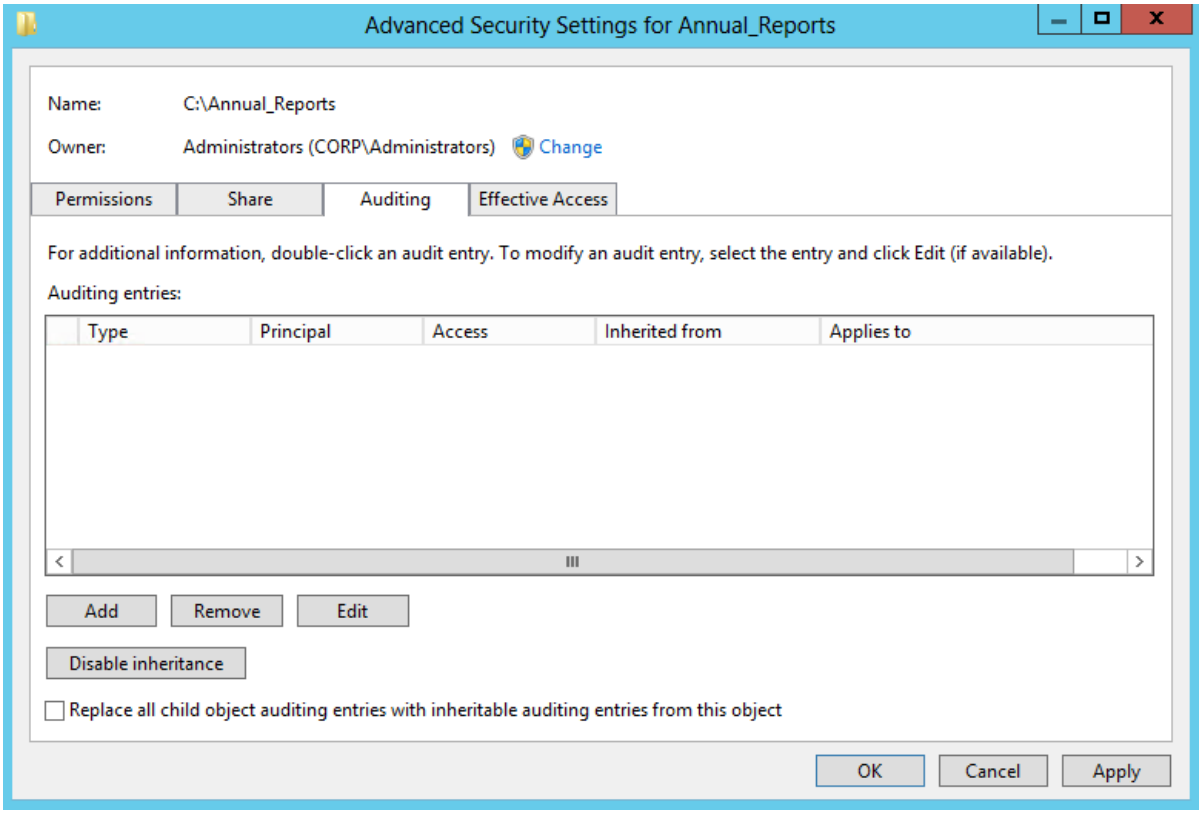


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

NOTE: If no data is present in reports, or the **Who** field contains the *"system"* value, refer to Netwrix Knowledge Base articles.

To configure Object-level access auditing on Windows Server 2012 and above

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab.



4. Click **Add** to add a new principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.
5. In the **Auditing Entry for <Folder_Name>** dialog, click the **Select a principal link** and specify **Everyone**.

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. The product will audit only user accounts that belong to the selected group.

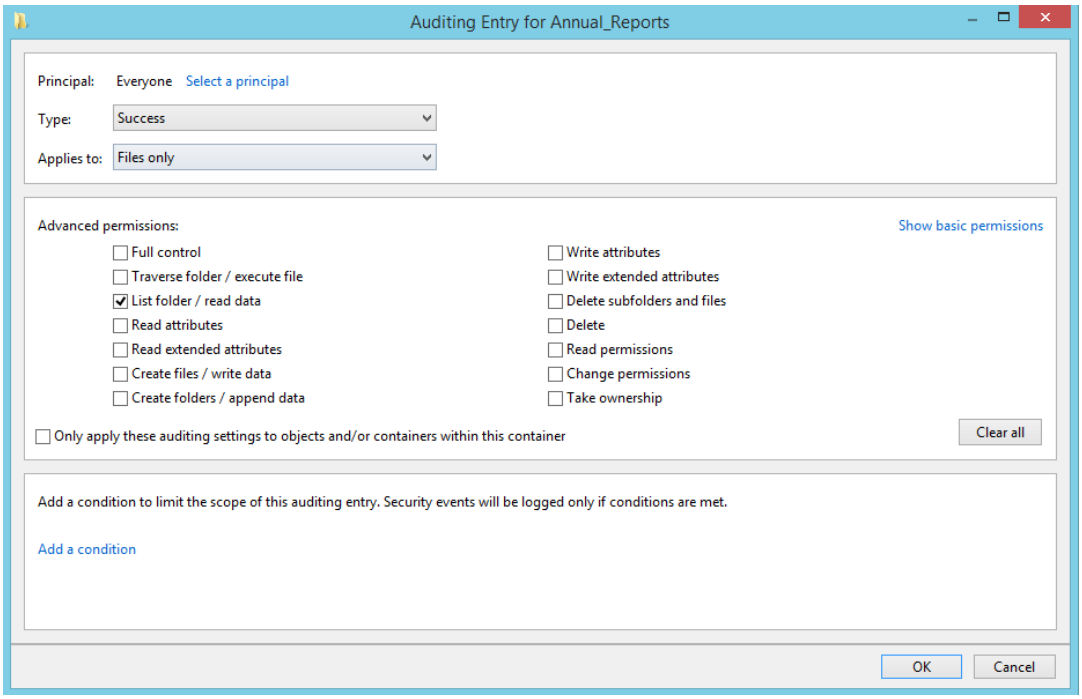
6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

- Successful reads
- Successful modifications
- Failed read attempts
- Failed modification attempts

Auditing Entry

Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

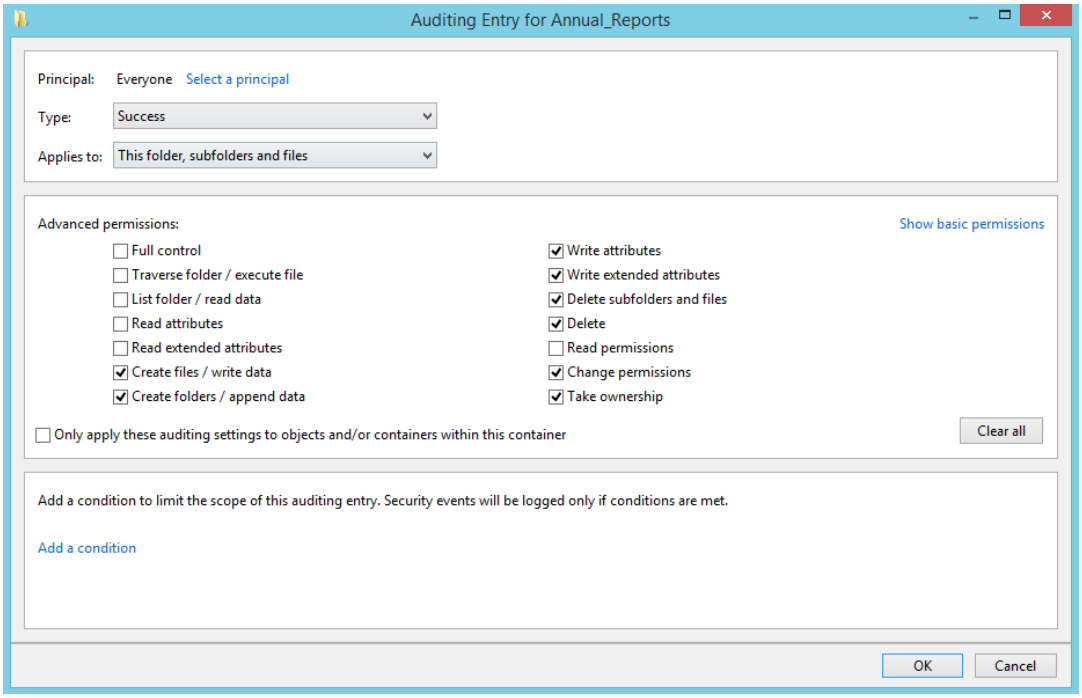


- Type—Set to *"Success"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful modifications

The Auditing Entry below shows Advanced Permissions for auditing successful modifications only:

Auditing Entry

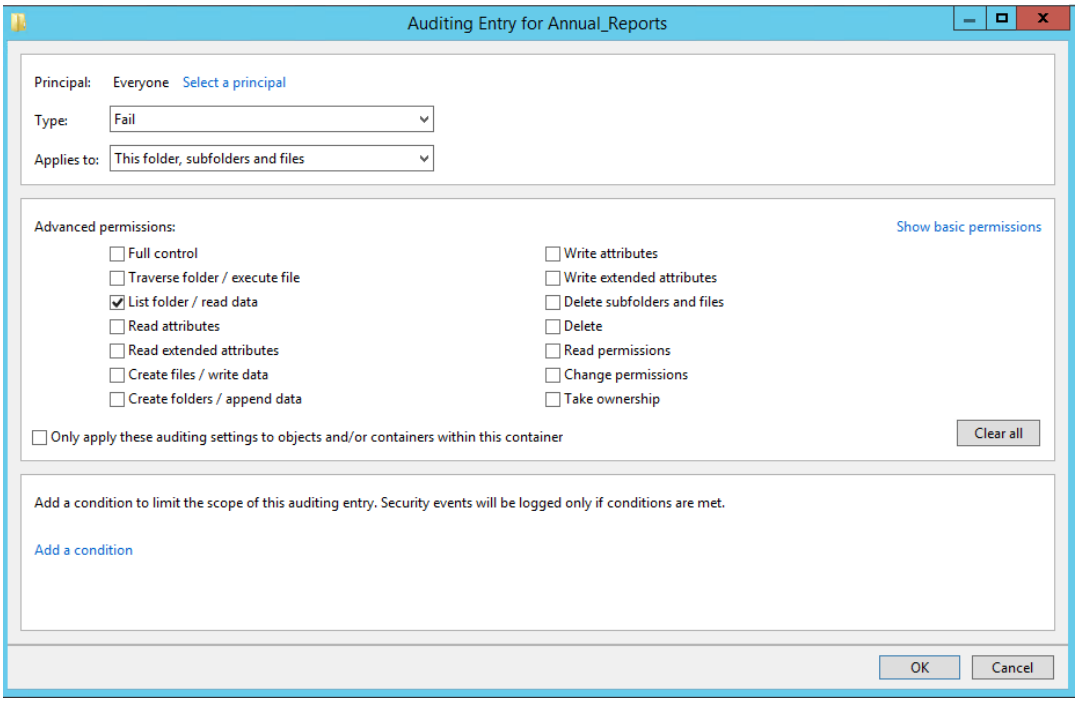


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts:

Auditing Entry

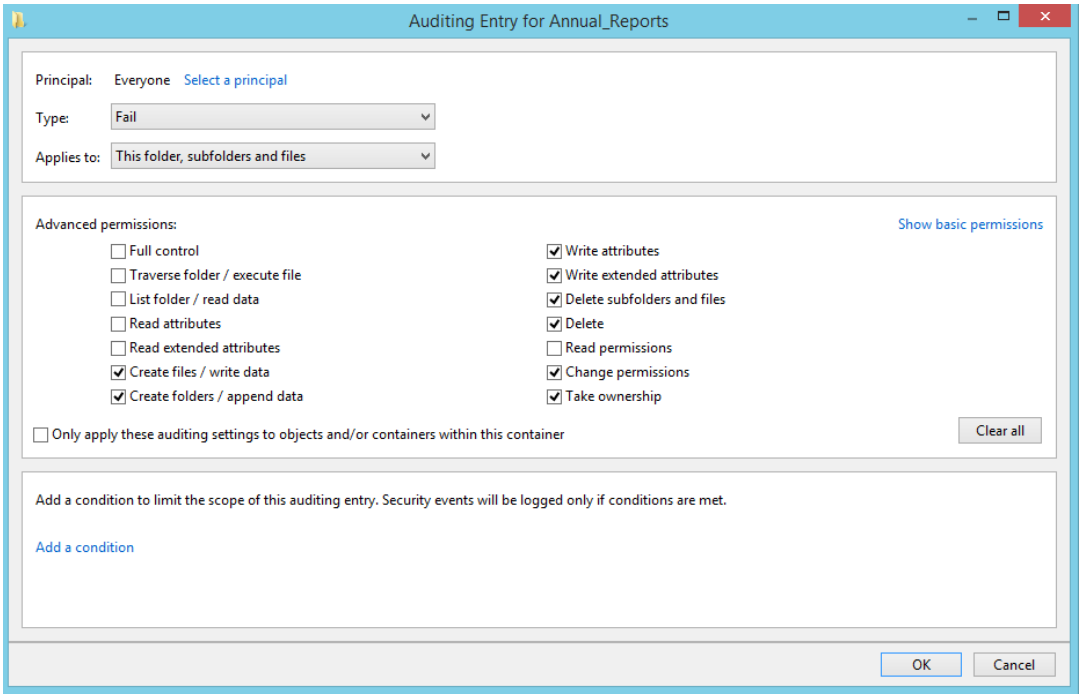


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed modification attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read and modification attempts:

Auditing Entry



- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

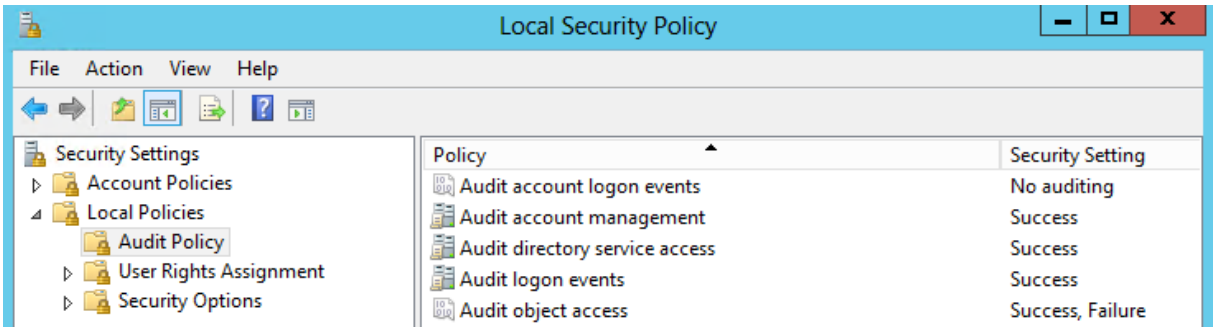
NOTE: If no data is present in reports, or the **Who** field contains the *"system"* value, refer to Netwrix Knowledge Base articles.

4.4.2. Configure Audit Object Access Policy

You can choose whether to configure the **Audit object access** legacy policy or to configure advanced policies. See Configure Advanced Audit Policy for more information.how to

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Administrative Tools** →**Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **Audit Policy**.

Policy Subnode	Policy Name	Audit Events
Audit Policy	**Audit object access**	*"Success"* and *"Failure"*



4.4.3. Configure Advanced Audit Policy

Configuring advanced audit will help you limit the range of events tracked and recorded by the product, thus preventing your AuditArchive and the Security event log from overfilling. Perform procedures below instead of Configure Audit Object Access Policy.

Perform the following procedures:

- To configure security options
- To configure advanced audit policy on Windows Server 2008 / Windows Vista
- To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

To configure security options

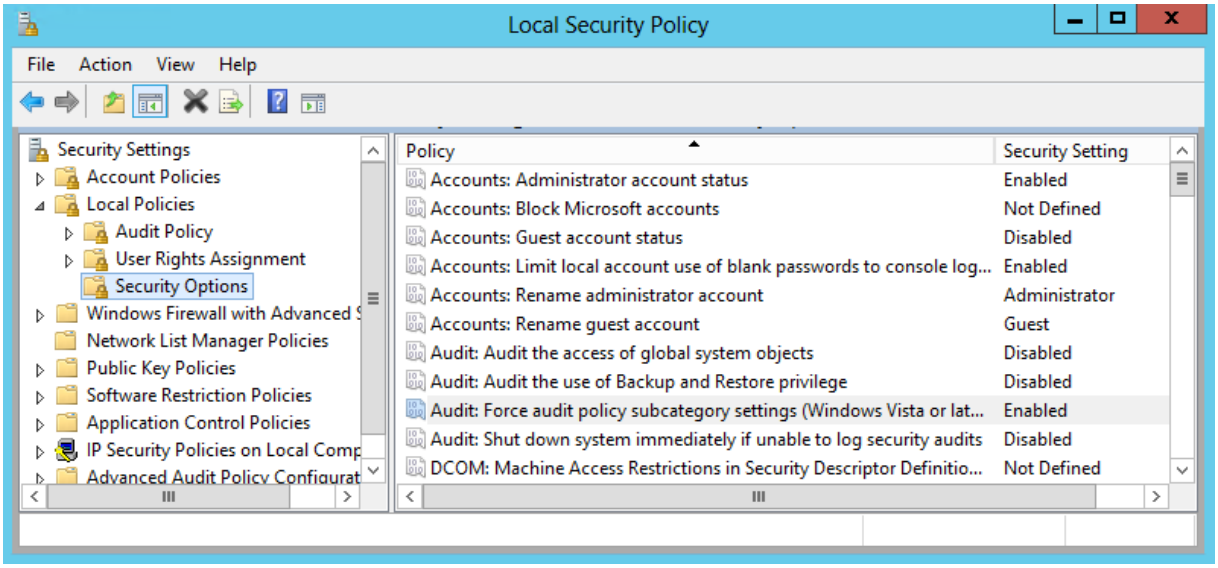
NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** option.

To do it, perform the following steps:

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **All Programs** →

Administrative Tools → **Local Security Policy**.

2. Navigate to **Security Settings** → **Local Policies** → **Security Options** and locate the **Audit: Force audit policy subcategory settings (Windows Vista or later)** policy.



3. Double-click the policy and enable it.

To configure advanced audit policy on Windows Server 2008 / Windows Vista

In Windows Server 2008 / Windows Vista, audit policies are not integrated with the Group Policies and can only be deployed using logon scripts generated with the native Windows **auditpol.exe** command line tool. Therefore, these settings are not permanent and will be lost after server reboot.

NOTE: The procedure below explains how to configure Advanced audit policy for a single server. If you audit multiple servers, you may want to create logon scripts and distribute them to all target machines via Group Policy. Refer to Microsoft Knowledge Base article: How to use Group Policy to configure detailed security auditing settings for more information.

1. On an audited file server, navigate to **Start** → **Run** and type *"cmd"*.
2. Disable the **Object Access** category by executing the following command in the command line interface:

```
auditpol /set /category:"Object Access" /success:disable /failure:disable
```

3. Enable the following audit subcategories:
   - Handle Manipulation {0CCE9223-69AE-11D9-BED3-505054503030}
   - File System {0CCE921D-69AE-11D9-BED3-505054503030}
4. Execute the following commands in the command line interface:

```
auditpol /set /subcategory:"File System" /success:enable /failure:enable
```

```
auditpol /set /subcategory:"Handle Manipulation" /success:enable
/failure:enable
```

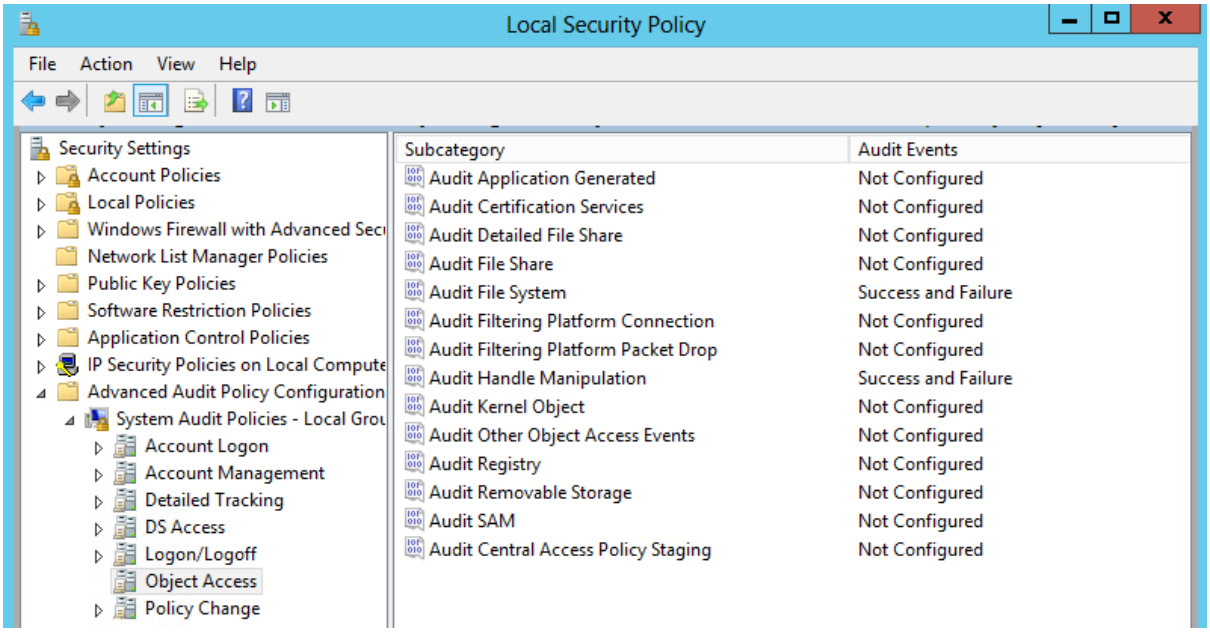
NOTE: It is recommended to disable all other subcategories unless you need them for other purposes. You can check your current effective settings by executing the following command: `auditpol /get /category:"Object Access"`.

To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

In Windows Server 2008 R2 and Windows 7 and above, Advanced audit policies are integrated with Group Policies, so they can be applied via Group Policy Object or Local Security Policies. The procedure below describes how to apply Advanced policies via Local Security Policy console.

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Administrative Tools** → **Local Security Policy**.
2. In the left pane, navigate to **Security Settings** → **Advanced Audit Policy Configuration** → **System Audit Policies**→ **Object Access**.
3. Configure the following audit policies.

Policy Name	Audit Events
• **Audit File System** • **Audit Handle Manipulation**	*"Success"* and/or *"Failure"* depending on the type of events you want to track.



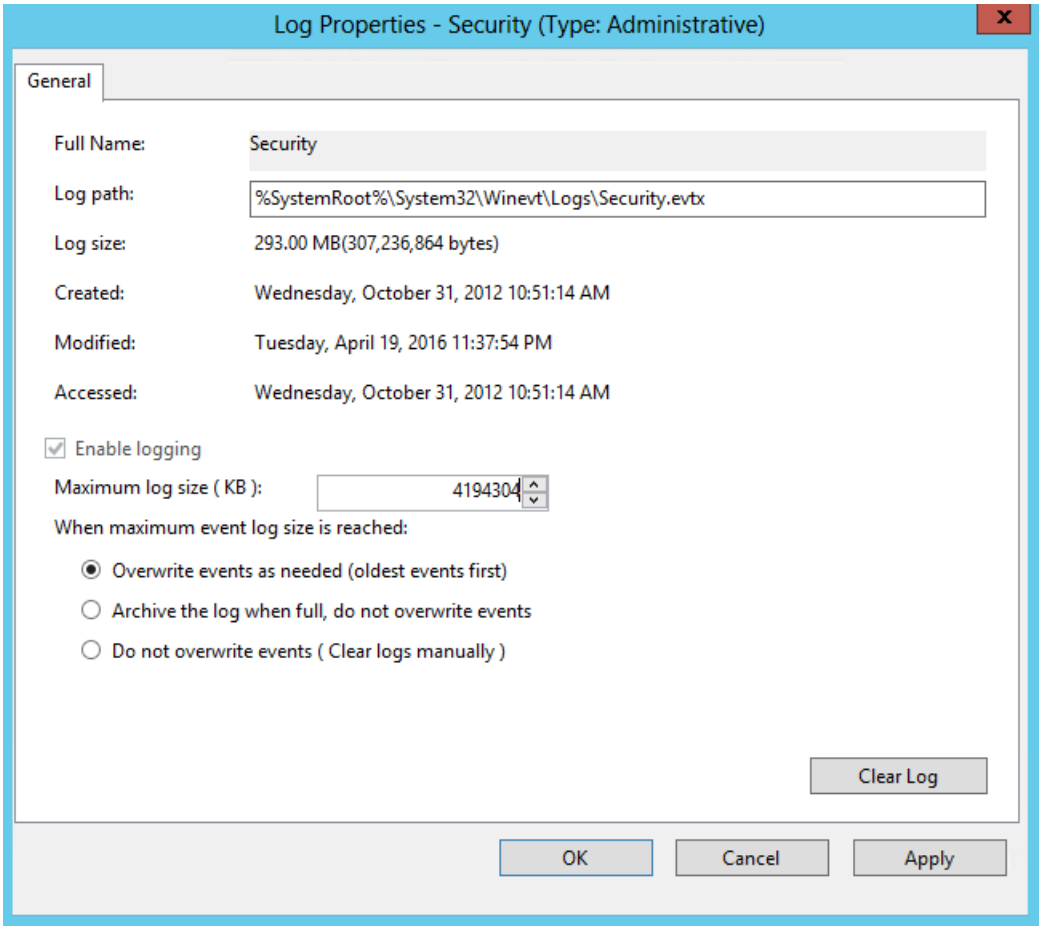
NOTE: You can check your current effective settings by executing the following command: `auditpol /get /category:"Object Access"`.

4.4.4. Configure Event Log Size and Retention Settings

The procedure below describes one of the possible ways to adjust event log settings. If you have multiple target computers, you need to perform this procedure on each of them.

NOTE: If you move security log files from the default system folder to a non-default one, you must reboot your target server for the reports and search functionality to work properly.

1. On a target server, navigate to **Start** → **Programs** → **Administrative Tools** → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Security** and select **Properties**.



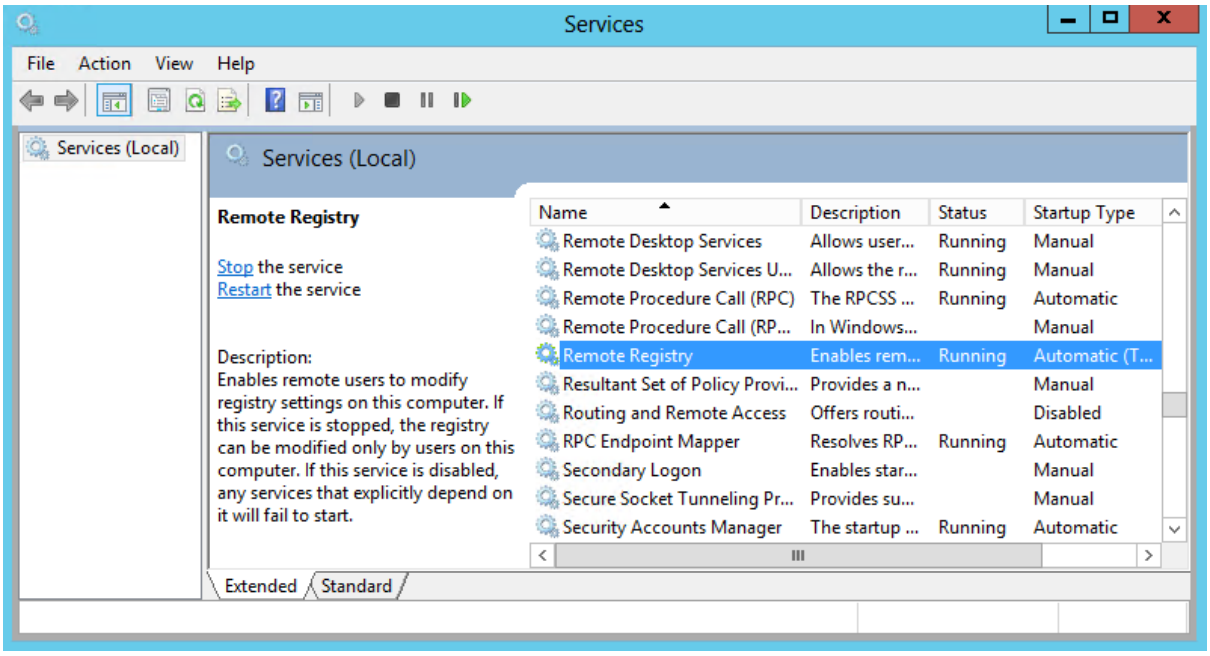
3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field, specify the size—4GB.
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

NOTE: Make sure the **Maximum security log size** group policy does not overwrite your log settings. To check this, start the **Group Policy Management** console, proceed to the GPO that affects your server, and navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log**.

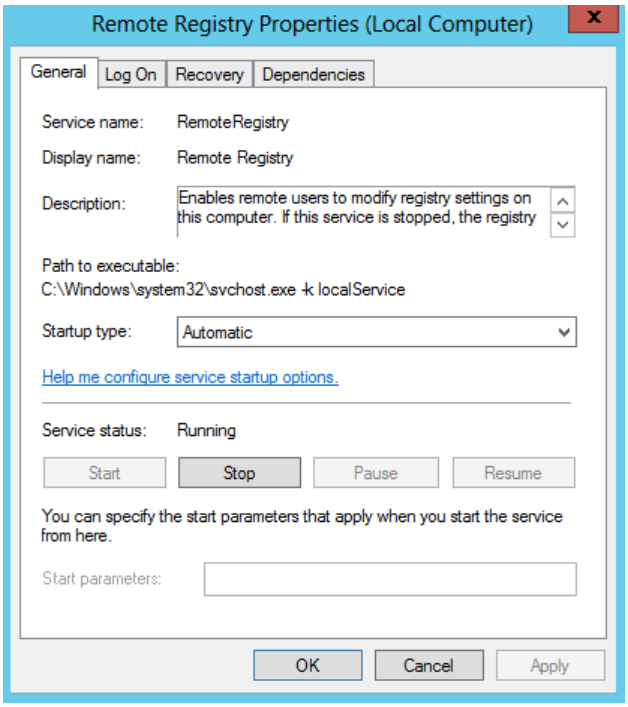
4.4.5. Enable Remote Registry Service

To enable the Remote Registry service

1. Navigate to **Start** → **Administrative Tools** → **Services**.



2. In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.

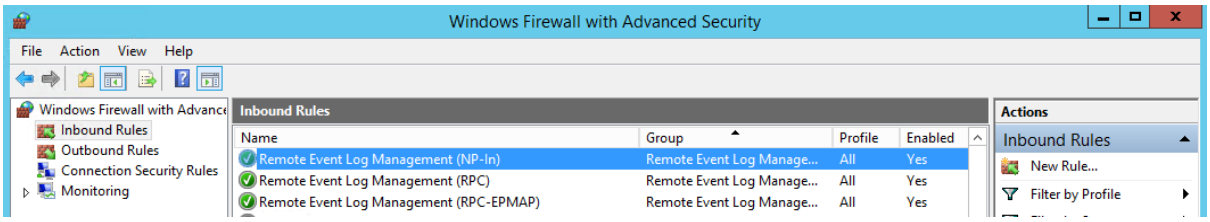


4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.

4.4.6. Configure Windows Firewall Inbound Connection Rules

NOTE: Also, you can configure Windows Firewall settings through Group Policy settings. To do this, edit the GPO affecting your firewall settings. Navigate to **Computer Configuration** → **Administrative Templates** → **Network** → **Network Connections** → **Windows Firewall**, select **Domain Profile** or **Standard Profile**. Then, enable the **Allow inbound remote administration exception**.

1. On each audited server, navigate to **Start** → **Control Panel** and select **Windows Firewall**.
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.



4. Enable the following inbound connection rules:
   - **Remote Event Log Management (NP-In)**
   - **Remote Event Log Management (RPC)**
   - **Remote Event Log Management (RPC-EPMAP)**
   - **Windows Management Instrumentation (ASync-In)**
   - **Windows Management Instrumentation (DCOM-In)**
   - **Windows Management Instrumentation (WMI-In)**
   - **Network Discovery (NB-Name-In)**
   - **File and Printer Sharing (NB-Name-In)**
   - **File and Printer Sharing (Echo Request - ICMPv4-In)**
   - **File and Printer Sharing (Echo Request - ICMPv6-In)**

4.5. Configure EMC Celerra/VNX for Auditing

You can configure your file shares for auditing in one of the following ways:

- Automatically when creating a Managed Object—Partially. Only audit settings for file shares will be configured. If you select to automatically configure audit in the target environment, your current audit settings will be periodically checked and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments.

- Manually. To configure EMC Celerra/VNX/VNXe for auditing, perform the following procedures:

  - Configure Security Event Log Maximum Size to avoid overwriting of the security logs; it is recommended to set security log size to a maximum (4GB).

    By default, the security log is set to overwrite events that are older than 10 days, and its size is set to 512 KB. The default location for the security.evt log is **C:\security.evt**, which corresponds to the root partition of the Data Mover. To be able to increase the security log size, you must move it from the Data Mover root folder.

  - Configure Audit Object Access Policy. Set the **Audit object access** policy set to *"Success"* and *"Failure"* in the Group Policy of the OU where your EMC VNX/VNXe/Celerra appliance belongs to. For more information on VNX/VNXe/Celerra GPO support, refer to documentation provided by EMC.

  - Configure Audit Settings for CIFS File Shares on EMC VNX/ VNXe/ Celerra

4.5.1. Configure Security Event Log Maximum Size

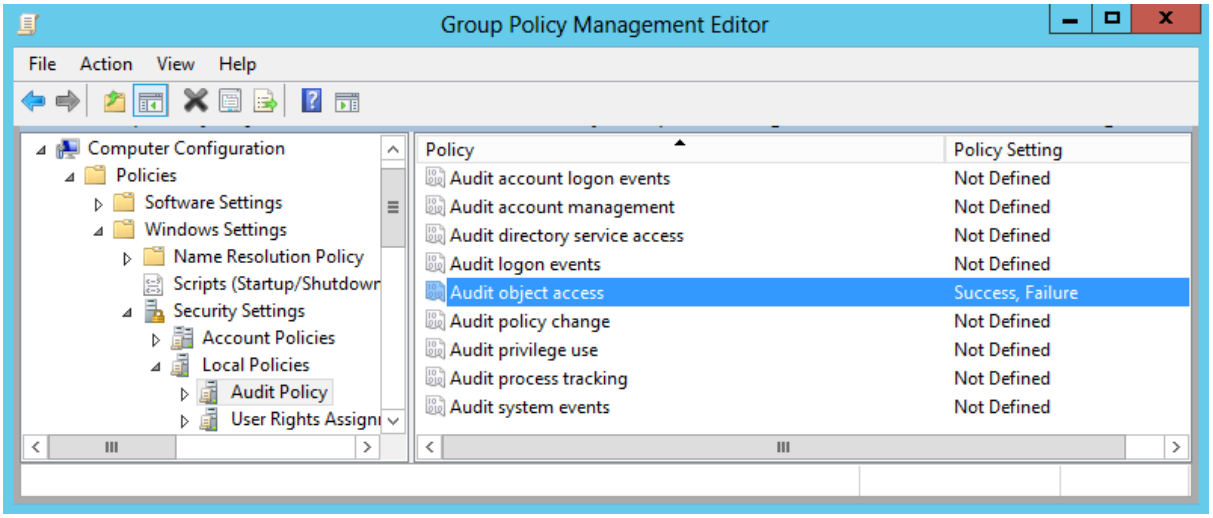
1. On your file server, create a new file system where the security log will be stored.
2. Mount this file system on a mount point, e.g., **/events**.
3. Make sure that it is accessible via the **\\<file_server_name>\C$\events** UNC path.
4. On the computer where Netwrix Auditor is installed, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
5. Navigate to **File** → **Connect Network Registry** and specify the file server name.
6. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security** and set the **File** value to *"C:\events\security.evt"*.
7. Set the **MaxSize** value to *"4 000 000 000 (decimal)"*.
8. Restart the corresponding Data Mover for the changes to take effect.

4.5.2. Configure Audit Object Access Policy

NOTE: Netwrix recommends you to avoid linking a GPO to the top level of the domain due to the potential impact. Instead, create a new organization unit for your file servers within your domain and assign GPO there. For detailed instructions on how to create a new OU, refer to the following Microsoft article: Create a New Organizational Unit.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>**, right-click **<OU_name>** and select **Create a GPO in this domain and Link it here**.
3. Enter the name for the new GPO.
4. Right-click the newly created GPO and select **Edit**.
5. 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** → **Audit Policy.**

Policy Subnode	Policy Name	Audit Events
Audit Policy	**Audit object access**	*"Success"*and*"Failure"*



6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

4.5.3. Configure Audit Settings for CIFS File Shares on EMC VNX/ VNXe/ Celerra

Netwrix Auditor can be configured to audit all access types, review the table below and select options that you want to track:

Access Type	Description
Successful modifications	Commonly used option to track important data. Helps find out *who* created, modified, moved, renamed or removed files and *when* these

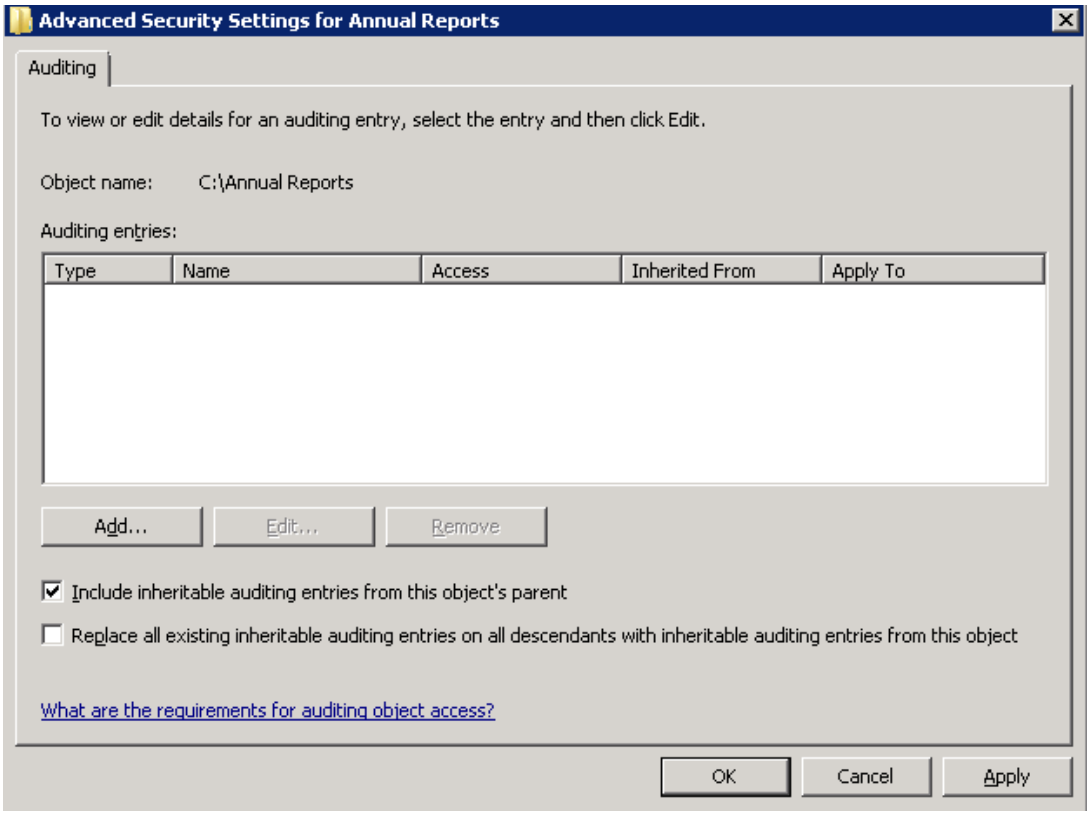
Access Type	Description
	changes were done.
Failed modification attempts	Used to track suspicious activity on your file server. Helps find out *who* tried to change or delete files, etc., but failed to do it. Investigate incidents with AuditIntelligence and figure out *why* that user tried to do it.
Successful reads	Used to supervise important files with confidential information for privileged users only. Browse your audit data in the Netwrix Auditor client and discover *who* accessed important files besides your trusted users. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.
Failed read attempts	Used to track suspicious activity. Helps find out *who* was trying to read files, but failed to do it. Investigate your incidents with AuditIntelligence and figure out *why* that user tried to do it. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.

To configure audit settings for the CIFS file shares, perform the following procedure on the audited file share:

- To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions
- To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. In a separate **Advanced Security Settings for <Share_Name>** dialog, click **Add** to add a principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.

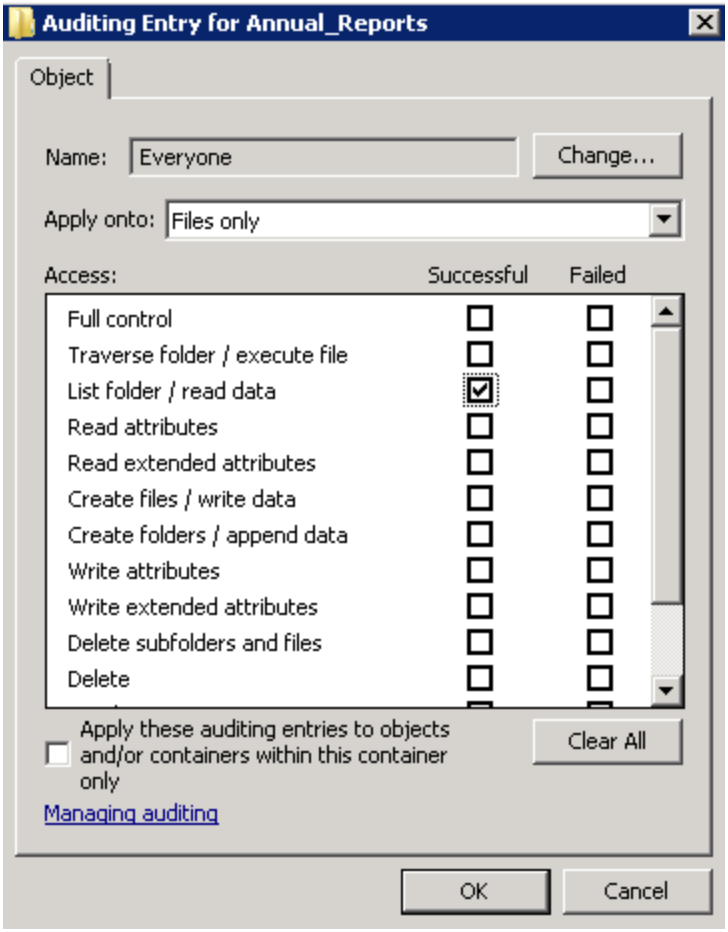
   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the reports or data searches performed in the Netwrix Auditor client and the product will only audit user accounts that belong to the selected group.

5. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modifications as well as failed reads and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful modifications
   - Failed read attempts
   - Failed modification attempts

Auditing Entry
Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

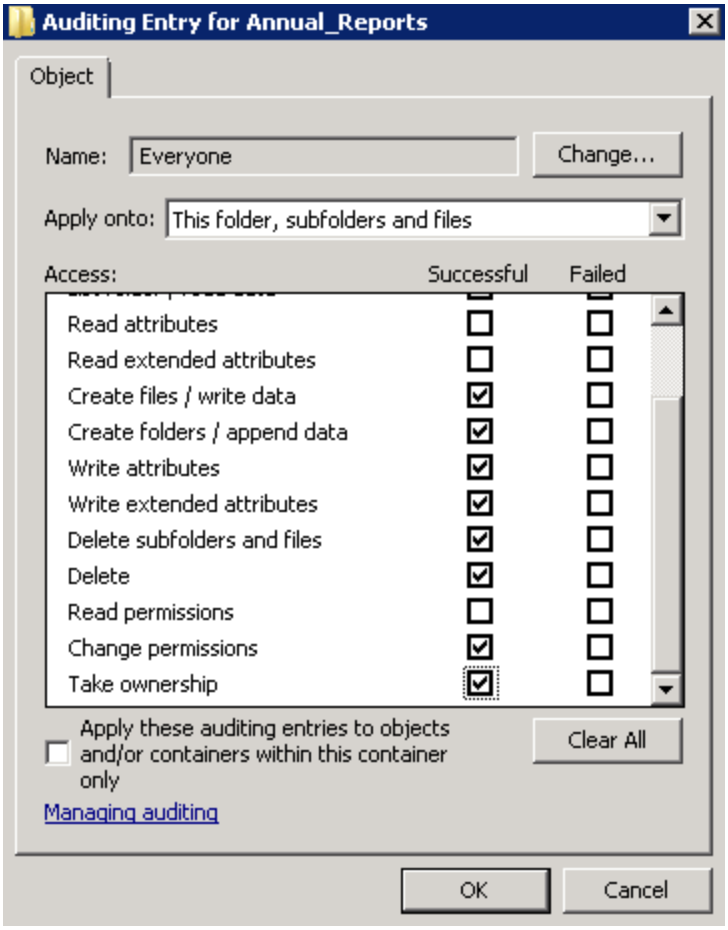


- Apply onto—Select *"Files only"*.
- Check *"Successful"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful modifications

The Auditing Entry below shows Advanced Permissions for auditing successful modifications only:

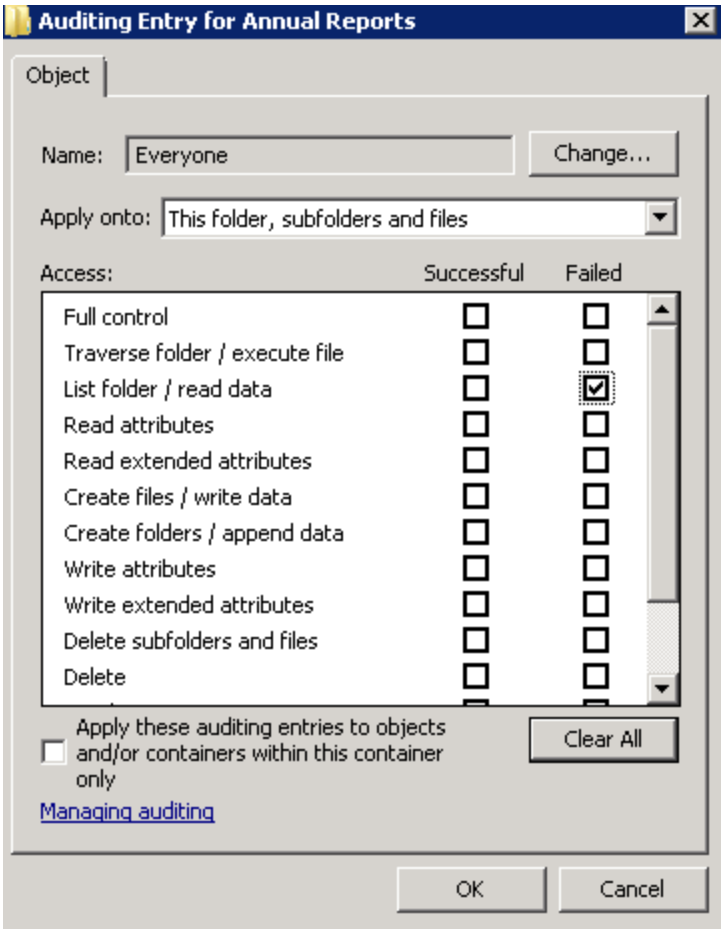
Auditing Entry



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Successful"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Auditing Entry
Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts only:

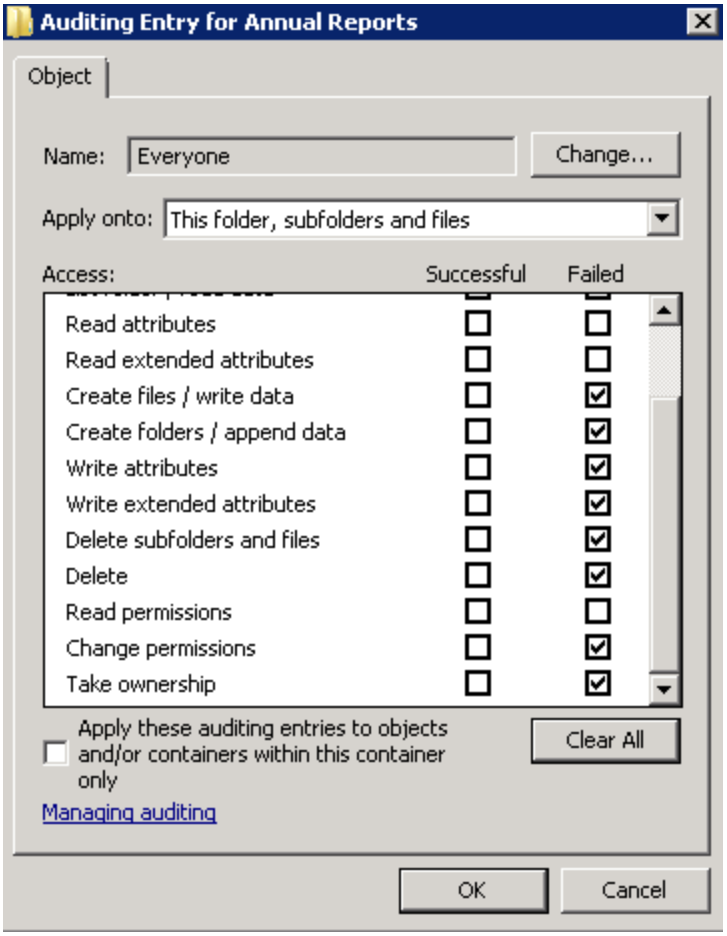


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed modification attempts

The Auditing Entry below shows Advanced Permissions for auditing failed modification attempts only:

Auditing Entry

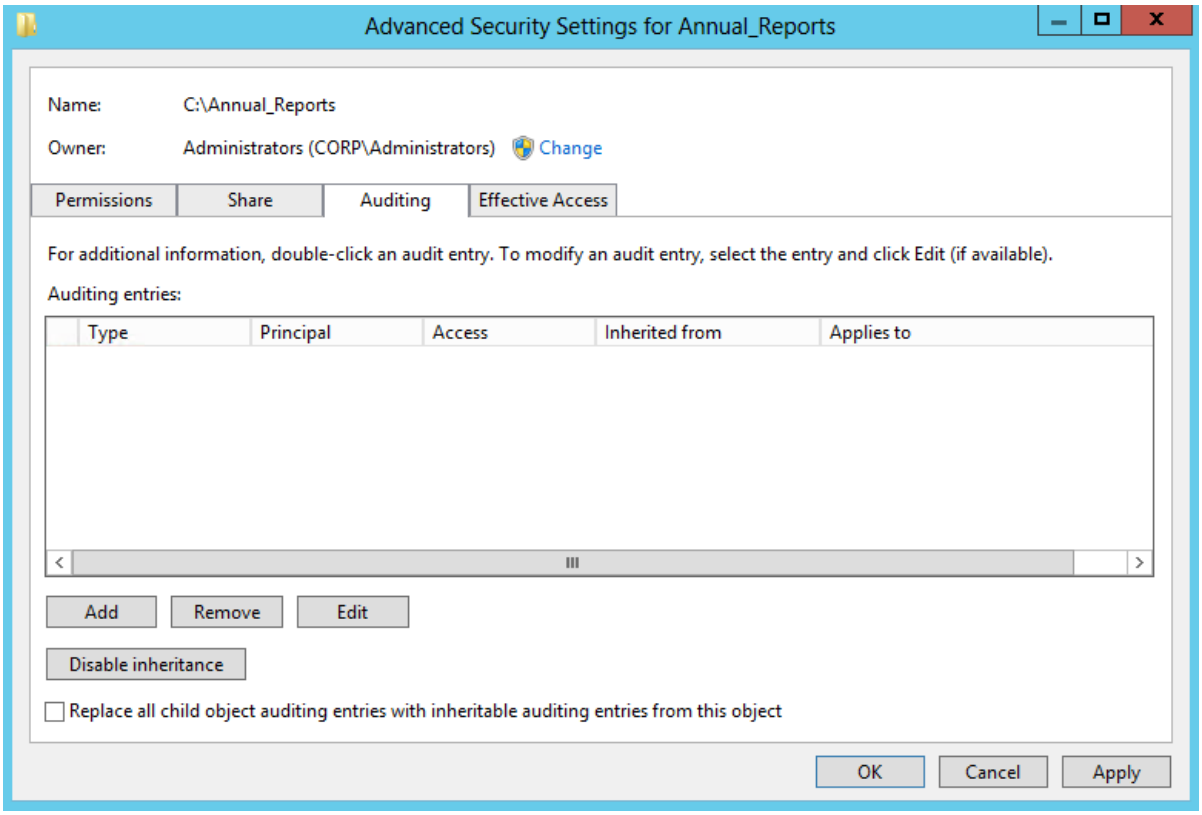


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

NOTE: If no data is present in reports, or the **Who** field contains the *"system"* value, refer to Netwrix Knowledge Base articles.

To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab.



4. Click **Add** to add a new principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.
5. In the **Auditing Entry for <Folder_Name>** dialog, click the **Select a principal link** and specify **Everyone**.

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. The product will audit only user accounts that belong to the selected group.

6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will

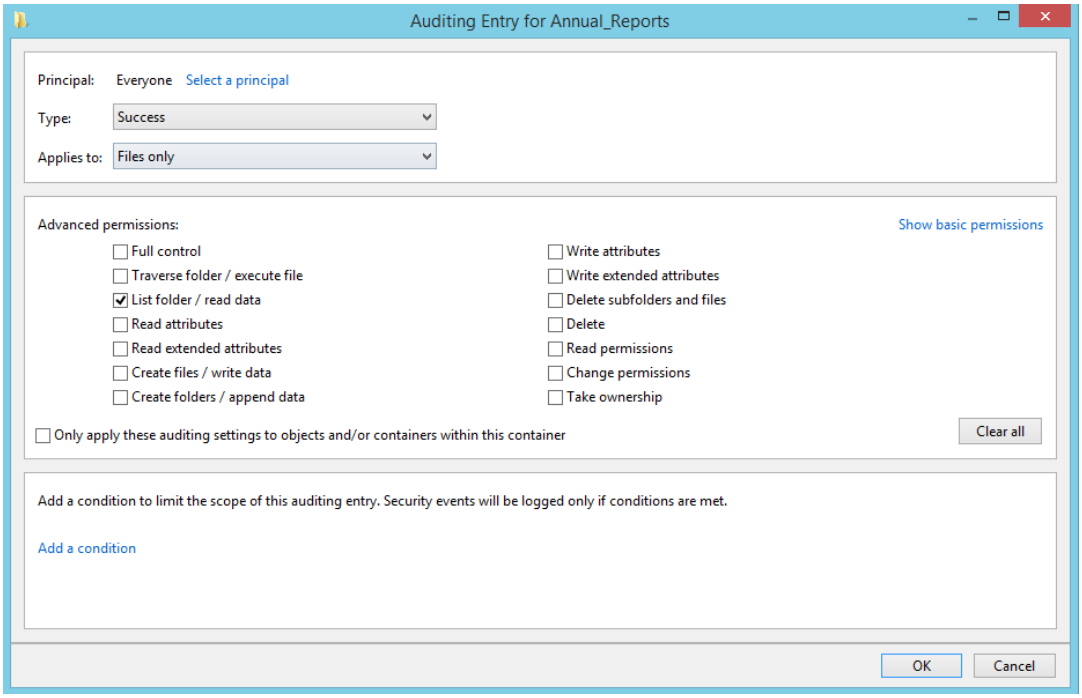
contain limited data and warning messages. Review the following for additional information:

- Successful reads
- Successful modifications
- Failed read attempts
- Failed modification attempts

Auditing Entry

Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

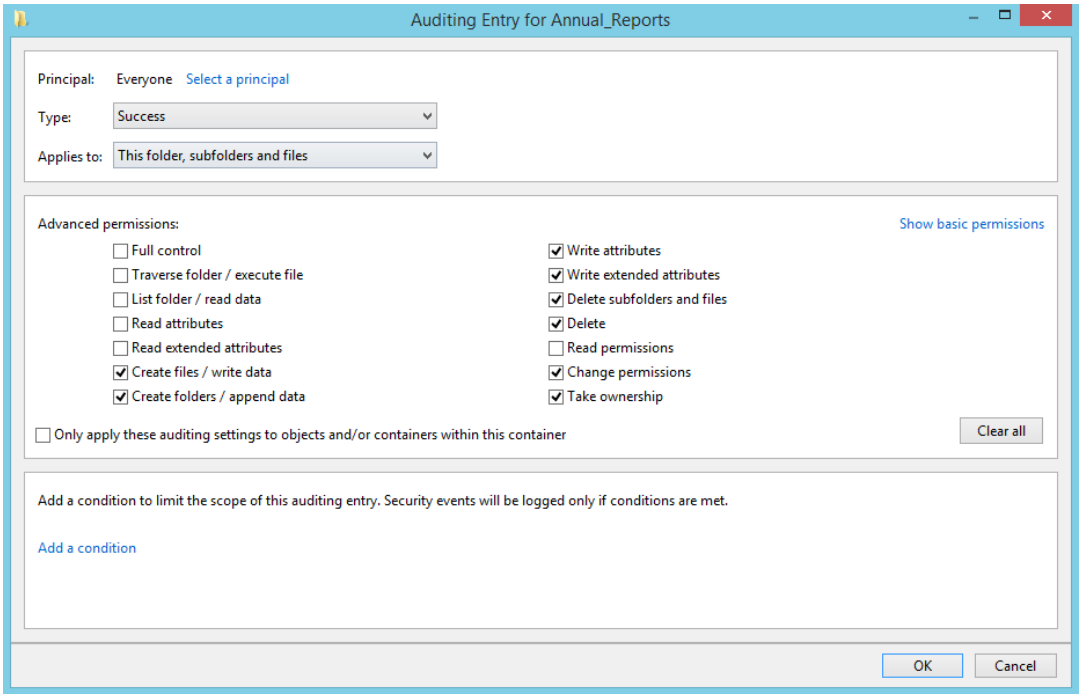


- Type—Set to *"Success"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful modifications

The Auditing Entry below shows Advanced Permissions for auditing successful modifications only:

Auditing Entry

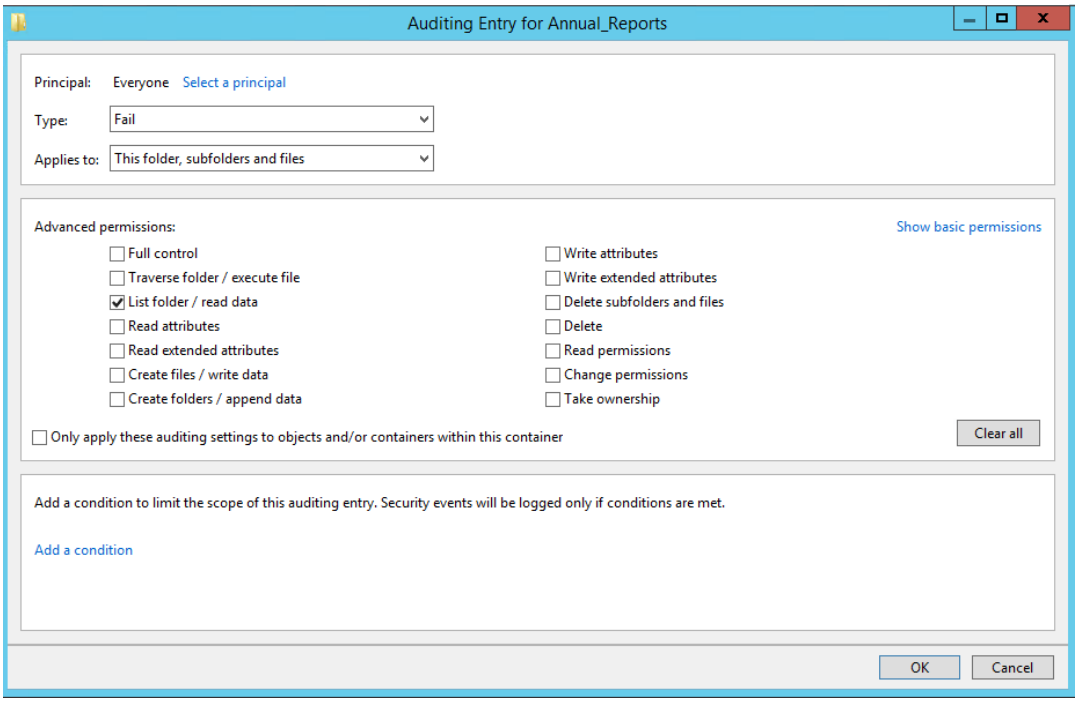


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts:

Auditing Entry

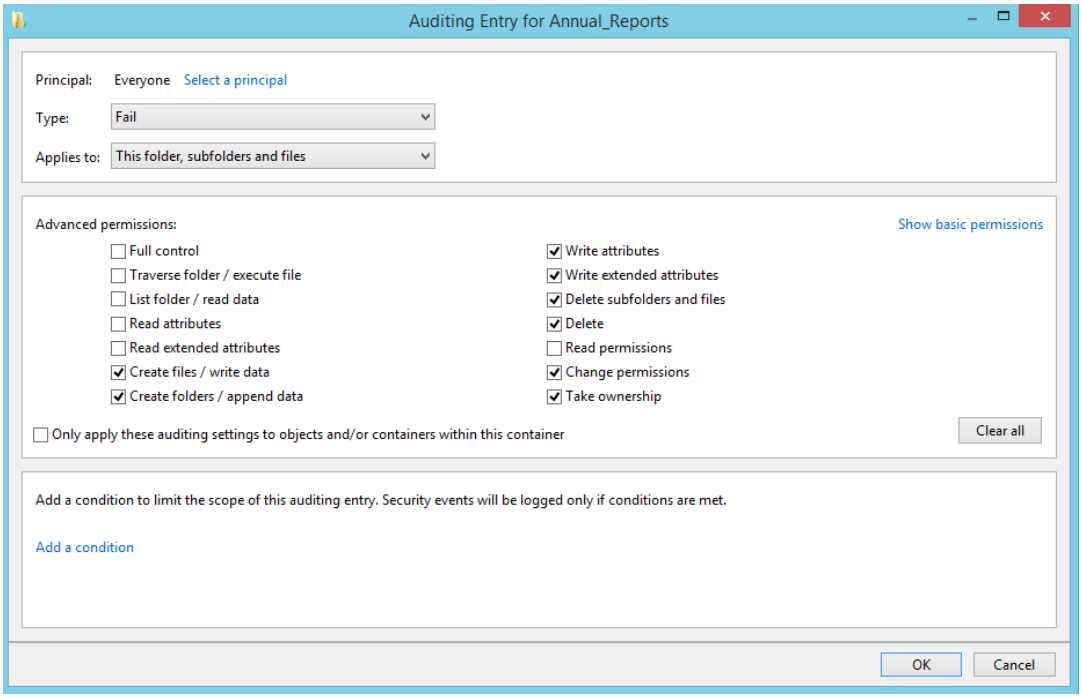


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed modification attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read and modification attempts:

Auditing Entry



- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

NOTE: If no data is present in reports, or the **Who** field contains the *"system"* value, refer to Netwrix Knowledge Base articles.

4.6. Configure EMC Isilon for Auditing

NOTE: The following EMC Isilon versions supported:

To configure your EMC Isilon appliance for auditing perform the following procedures:

- Configure EMC Isilon in Normal and Enterprise Modes
- Configure EMC Isilon in Compliance Mode

4.6.1. Configure EMC Isilon in Normal and Enterprise Modes

You can configure your cluster for auditing in one of the following ways:

- Using the **configure_ifs.sh** shell script that comes with Netwrix Auditor. See To configure EMC Isilon cluster in Normal and Enterprise mode via shell script for more information.
- Manually. See To configure EMC Isilon cluster in Normal and Enterprise mode manually for more information.

To configure EMC Isilon cluster in Normal and Enterprise mode via shell script

1. On the computer where Netwrix Auditor Administrator Console resides, navigate to *C:\Program Files (x86)\Netwrix Auditor\File Server Auditing* and copy the **configure_ifs.sh** shell script to */ifs/data* catalog on your cluster.
2. Navigate to your cluster command prompt through the **SSH** connection.
3. Log in to your cluster as a root user.
4. Run the shell script by executing the following command:

   ```
   sh /ifs/data/configure_ifs.sh -z zone1 -a 15
   ```

   where

   `zone1` is the name of the audited access zone on your file server.

   `15` is a combination of the bitwise flags. The table below shows the example combination of 4 flags:

   ```
   Successful modifications              1
   Failed modification attempts          2
   Successful reads                      4
   Failed read attempts                  8
   Total:                                15
   ```

To configure EMC Isilon cluster in Normal and Enterprise mode manually

1. Navigate to your cluster command prompt through the **SSH** connection.
2. Log in to your cluster as a root user.

3. Grant full access to the catalog */ifs/.ifsvar/audit/* for **BUILTIN\Administrators**:

   ```
   chmod -R +a group "BUILTIN\Administrators" allow dir_gen_all,object_
   inherit,container_inherit,inherited /ifs/.ifsvar/audit/
   ```

   ```
   chmod -a group "BUILTIN\Administrators" allow dir_gen_all,object_
   inherit,container_inherit,inherited /ifs/.ifsvar/audit/
   ```

   ```
   chmod +a group "BUILTIN\Administrators" allow dir_gen_all,object_
   inherit,container_inherit /ifs/.ifsvar/audit/
   ```

4. Create a shared folder named **netwrix_audit$** on a system zone. This folder points to */ifs/.ifsvar/audit/*:

   ```
   /usr/likewise/bin/lwnet share add "netwrix_
   audit$"="c:\\ifs\\.ifsvar\\audit\\"
   ```

   ```
   isi smb shares modify netwrix_audit$ --new-zone=system
   ```

5. Add the **BUILTIN\Administrators** group in the share permissions for **netwrix_audit$** folder with *"full access"* rights:

   ```
   isi smb shares permission create --share=netwrix_audit$ --
   group="BUILTIN\Administrators" --permission-type=allow --permission=full --
   zone=system
   ```

6. Enable protocol auditing for a selected zone (for example, *"zone1"*):

   ```
   isi audit settings modify --add-audited-zones=zone1 --protocol-auditing-
   enabled=true
   ```

   Enable filters for auditing protocol operations that succeeded/failed for audited access zones on your cluster.

To enable filter...	Execute command...
Successful modifications Audit Success: • write • delete • set_security • rename	`isi zone zones modify zone1 --audit-success=write,delete,set_security,rename`
Failed modification attempts Audit Failure: • create • write	`isi zone zones modify zone1 --audit-failure=create,write,delete,set_security,rename`

To enable filter...	Execute command...
• delete • set_security • rename	
Successful reads Audit Success: read	`isi zone zones modify zone1 --audit-success=read`
Failed read attempts Audit Failure: • create • read	`isi zone zones modify zone1 --audit-failure= create, read`

7. Create the *"netwrix_audit"* role and add the required privileges to this role. For example:

```
isi auth roles create --name=netwrix_audit
isi auth roles modify netwrix_audit --add-priv-ro="ISI_PRIV_LOGIN_PAPI,ISI_PRIV_AUTH,ISI_PRIV_AUDIT,ISI_PRIV_IFS_BACKUP"
isi auth roles modify netwrix_audit --add-group="BUILTIN\Administrators"
```

4.6.2. Configure EMC Isilon in Compliance Mode

You can configure your cluster for auditing in one of the following ways:

- Using the **configure_ifs.sh** shell script that comes with Netwrix Auditor. See To configure EMC Isilon cluster in Compliance mode via shell script for more information.
- Manually. See To configure EMC Isilon cluster in Compliance mode manually for more information.

To configure EMC Isilon cluster in Compliance mode via shell script

1. On the computer where Netwrix Auditor Administrator Console resides, navigate to *C:\Program Files (x86)\Netwrix Auditor\File Server Auditing* and copy the **configure_ifs.sh** shell script to */ifs/data* catalog on your cluster.
2. Navigate to your cluster command prompt through the **SSH** connection.
3. Log in to your cluster as a compadmin user.
4. Run the shell script by executing the following command:

```
sh /ifs/data/configure_ifs.sh -z zone1 -a 15
```

where

`zone1` is the name of the audited access zone on your file server.

`15` is a combination of the bitwise flags. The table below shows the example combination of 4 flags:

```
Successful modifications              1
Failed modification attempts          2
Successful reads                      4
Failed read attempts                  8
Total:                                15
```

5. Create a shared folder named **netwrix_audit$** on a system zone. This folder points to */ifs*:

```
isi smb shares create --name=netwrix_audit$ --path=/ifs/ --zone=system --
browsable=true
```

6. Add the **BUILTIN\Administrators** group in the share permissions for **netwrix_audit$** folder with *"full access"* rights:

```
isi smb shares permission create --share=netwrix_audit$ --
group=BUILTIN\Administrators --permission-type=allow --permission=full --
zone=system
```

7. Grant your Data Processing Account *"read access"* rights to the catalog */ifs/.ifsvar/audit* :

```
isi zone modify system --add-user-mapping-rules="Enterprise\Administrator
++ compadmin [group]"
```

Where `Enterprise\Administrator` is your Data Processing Account name.

To configure EMC Isilon cluster in Compliance mode manually

1. Navigate to your cluster command prompt through the **SSH** connection.
2. Log in to your cluster as a compadmin user.
3. Create a shared folder named **netwrix_audit$** on a system zone. This folder points to */ifs*:

```
isi smb shares create --name=netwrix_audit$ --path=/ifs/ --zone=system --
browsable=true
```

4. Add the **BUILTIN\Administrators** group in the share permissions for **netwrix_audit$** folder with *"full access"* rights:

```
isi smb shares permission create --share=netwrix_audit$ --
group=BUILTIN\Administrators --permission-type=allow --permission=full --
zone=system
```

5. Grant your Data Processing Account *"read access"* rights to the catalog */ifs/.ifsvar/audit* :

```
isi zone modify system --add-user-mapping-rules="Enterprise\Administrator
++ compadmin [group]"
```

Where `Enterprise\Administrator` is your Data Processing Account name.

6. Configure protocol auditing for selected zone (for example, *"zone1"*).

```
isi audit settings modify --add-audited-zones=zone1 --protocol-auditing-
enabled=true
```

Enable filters for auditing protocol operations that succeeded/failed for audited access zones on your cluster.

To enable filter...	Execute command...
Successful modifications Audit Success: • write • delete • set_security • rename	`isi zone zones modify zone1 --audit-success=write,delete,set_security,rename`
Failed modification attempts Audit Failure: • create • write • delete • set_security • rename	`isi zone zones modify zone1 --audit-failure=create,write,delete,set_security,rename`
Successful reads Audit Success: read	`isi zone zones modify zone1 --audit-success=read`
Failed read attempts Audit Failure: • create • read	`isi zone zones modify zone1 --audit-failure= create, read`

7. Create the *"netwrix_audit"* role and add the required privileges to this role. For example:

```
isi auth roles create --name=netwrix_audit
```

```
isi auth roles modify netwrix_audit --add-priv-ro="ISI_PRIV_LOGIN_PAPI,ISI_
PRIV_AUTH,ISI_PRIV_AUDIT,ISI_PRIV_IFS_BACKUP"
```

```
isi auth roles modify netwrix_audit --add-group="BUILTIN\Administrators"
```

4.7. Configure NetApp Filer for Auditing

You can configure your file shares for auditing in one of the following ways:

- Automatically when creating a Managed Object

  NOTE: For NetApp Data ONTAP 7 and 8 in 7-mode, configure audit automatically. For NetApp Clustered Data ONTAP 8 only audit settings for file shares can be configured automatically.

  If you select to automatically configure audit in the target environment, your current audit settings will be periodically checked and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments.

- Manually. To configure your NetApp appliance for auditing, perform the following procedures:
  - Configure NetApp Data ONTAP 7 and 8 in 7-mode for Auditing or Configure NetApp Clustered Data OnTap 8 for Auditing
  - Configure Audit Settings for CIFS File Shares

4.7.1. Configure NetApp Data ONTAP 7 and 8 in 7-mode for Auditing

To configure NetApp filer appliances for auditing, perform the following procedures:

- Prerequisites
- Configure Qtree Security
- Configure Admin Web Access
- Configure Event Categories

4.7.1.1. Prerequisites

NOTE: CIFS must be set up on your NetApp filer in advance.

The instructions in this section apply to the default VFiler. To audit several VFiler instances, you must perform these configuration steps for each of them.

NOTE: Currently, Netwrix Auditor can be configured to audit non-default VFiler using HTTP only.

The following commands are used:

- To get an option value:

  ```
  options <option_name>
  ```

- To set option value:

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

4.7.1.2. Configure Qtree Security

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Set the volume where the audited file shares are located to the *"ntfs"* or *"mixed"* security style:

```
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>
```

4.7.1.3. Configure Admin Web Access

Netwrix Auditor uses the NetApp API to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to an Event Viewer compatible format. Netwrix Auditor supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Make sure that the `httpd.admin.enable` or `httpd.admin.ssl.enable` option is set to *"on"*. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option.

```
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>
```

4.7.1.4. Configure Event Categories

Perform the following procedures to configure event categories:

- To configure audit event categories
- To configure Security log
- To configure logs retention period
- To specify the Security log shared folder

To configure audit event categories

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Set the `cifs.audit.enable` and `cifs.audit.file_access_events.enable` options to *"on"*.
3. Unless you are going to audit logon events, set the `cifs.audit.logon_events.enable` and `cifs.audit.account_mgmt_events.enable` options to *"off"*.

   NOTE: It is recommended to turn off logon auditing in order to reduce the number of events generated.

To configure Security log

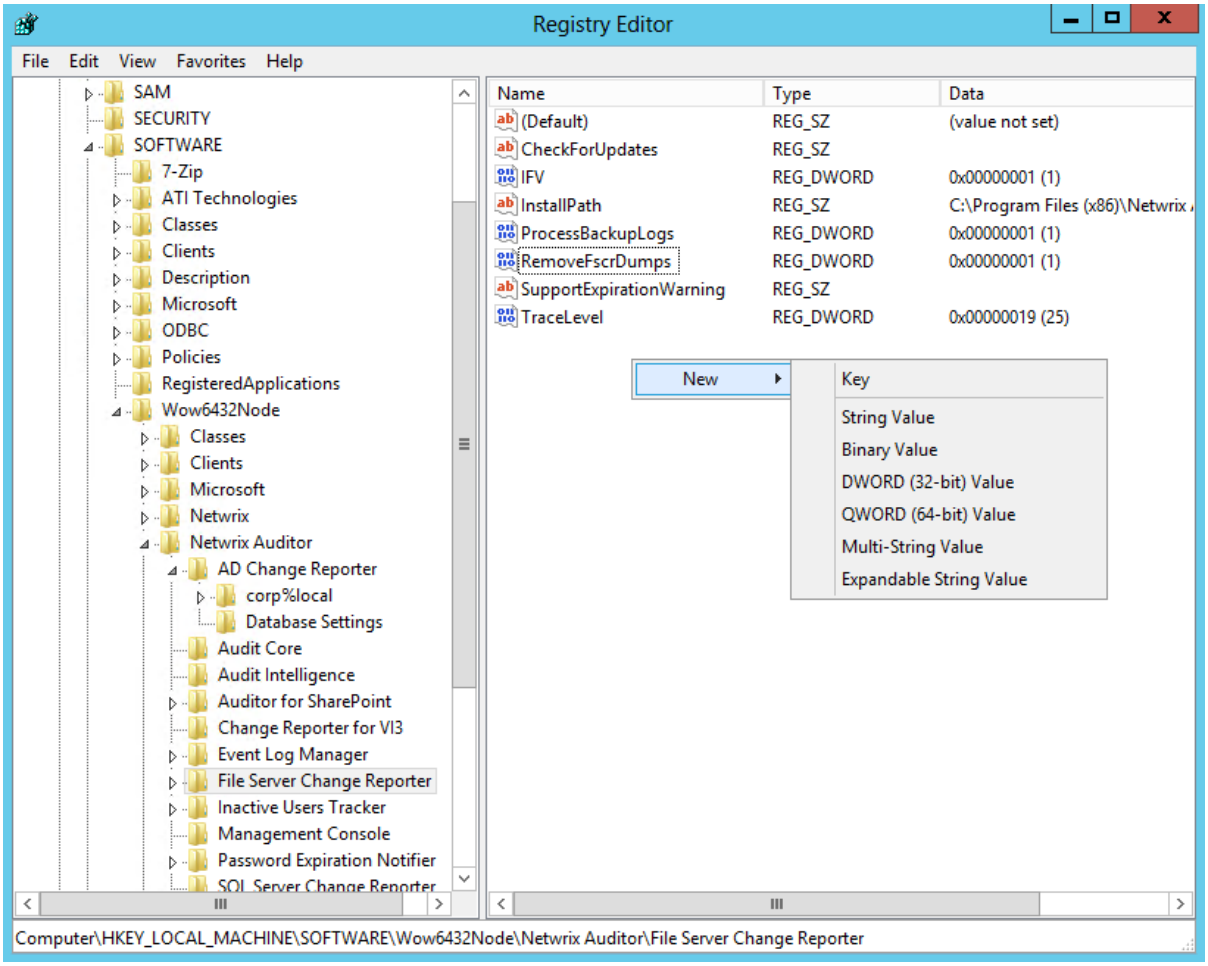
1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. In order to avoid overwriting of the security logs, set the following values:
   - `cifs.audit.logsize 300 000 000 (300 MB)`
   - `cifs.audit.autosave.onsize.enable on`
   - `cifs.audit.autosave.file.extension timestamp`
3. Disable the `cifs.audit.liveview.enable` option since it interferes with the normal Security log behavior and prevents Netwrix Auditor from processing audit data properly.
4. 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 set retention in Netwrix Auditor.
5. Perform any test actions with a file share to ensure the log is created.

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 Auditor (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 logs retention.

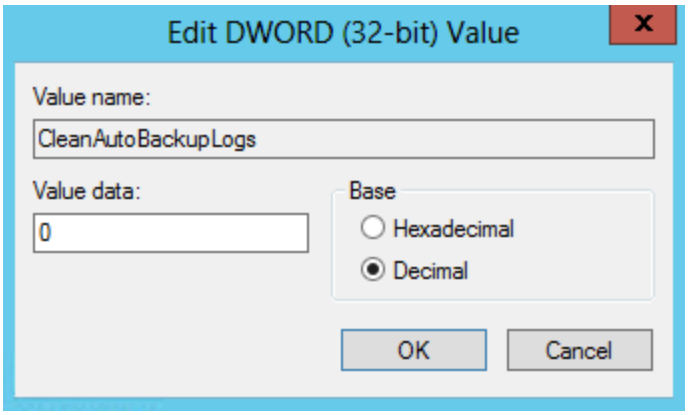
To configure logs retention period

1. On the computer where Netwrix Auditor Administrator Console is installed, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **File Server Change Reporter**.
3. In the right-pane, right-click and select **New** → **DWORD (32-bit Value)**.

   NOTE: For the backup logs retention functionality to work properly, you need to specify the **CleanAutoBackupLogs** name for the newly created registry value.



4. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.
5. This value defines the time period (in hours) after which security event logs archives will be automatically deleted. By default, it is set to *"0"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.



6. **NOTE:** If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old logs manually, or you may run out of space on your hard drive.

To specify the Security log shared folder

Netwrix Auditor accesses audit logs via a specified file share. This may be either the default administrative share (ETC$, C$, etc.), or a custom file share.

NOTE: Perform the procedure below if you are not going to detect file shares automatically via Netwrix Auditor Administrator Console.

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Use the `cifs shares` command to create a new file share or configure an existing share.

```
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
```

3. Perform any test actions with a file share to ensure the log is created.

4.7.2. Configure NetApp Clustered Data ONTAP 8 for Auditing

To configure Clustered Data ONTAP for auditing, perform the following procedures:

- Prerequisites
- Configure ONTAPI Web Access

- Configure Firewall Policy
- Configure Event Categories and Log

4.7.2.1. Prerequisites

Netwrix assumes that you are aware of Clustered Data ONTAP basic installation and configuration steps. If not, refer to the following administration and management guides.

Clustered Data ONTAP version	Related documentation
Clustered Data ONTAP 8.2	• Clustered Data ONTAP® 8.2 File Access and Protocols Management Guide • Clustered Data ONTAP® 8.2 System Administration Guide for SVM Administrators
Clustered Data ONTAP 8.3	• Clustered Data ONTAP® 8.3 System Administration Guide for Cluster Administrators • Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS

Perform the steps below before proceeding with Clustered Data ONTAP configuration:

1. Configure CIFS server and make sure it functions properly.

   NOTE: NFS file shares are not supported.

2. Configure System Access Control List (SACL) on your file share. See Configure Audit Settings for CIFS File Shares for more information.
3. Set the **Security Style** for **Volume** or **Qtree** where the audited file shares are located to the *"ntfs"* or *"mixed"*.
4. Configure audit manually. Review the **Auditing NAS events on SVMs with FlexVol volumes** section in Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS.

   NOTE: The current version of Netwrix Auditor do not supports auditing of Infinite Volumes.

4.7.2.2. Configure ONTAPI Web Access

Netwrix Auditor uses ONTAPI to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to an MS Event Viewer compatible format. Netwrix Auditor supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

1. Navigate to your cluster command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your current web access settings. Make sure that External Web Services are allowed. For example:

```
cluster1::> system services web show
       External Web Services: true
                      Status: online
          HTTP Protocol Port: 80
         HTTPs Protocol Port: 443
               TLSv1 Enabled: true
               SSLv3 Enabled: true
               SSLv2 Enabled: false
```

3. Enable ONTAPI access on the SVM where CIFS server is set up and configured. The example command output shows correct web access settings where `vs1` is your SVM name.

```
cluster1::>  vserver  services web show -vserver vs1
Vserver      Type     Service     Description                Enabled
                      Name
----------   -------  --------    -----------------------    ------
vs1             data  ontapi      Remote Administrative API  true
                                  Support
```

4. Enable **HTTP/HTTPS** access. For example:

```
cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled true
```

5. Enable only **SSL** access (HTTPS in Netwrix Auditor Administrator Console). For example:

```
cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled true -ssl-o
nly true
```

6. Make sure that the builtin **vsadmin** role or a custom role (e.g., fsa_role) assigned to your Data Processing Account can access ONTAPI. For example:

```
cluster2::> vserver services web access show -vserver vs2
Vserver           Type      Service Name    Role
--------------    -------   ------------    ---------------
vs2               data      ontapi          fsa_role
vs2               data      ontapi          vsadmin
vs2               data      ontapi          vsadmin-protocol
vs2               data      ontapi          vsadmin-readonly
vs2               data      ontapi          vsadmin-volume
5 entries were displayed.
```

4.7.2.3. Configure Firewall Policy

Configure firewall to make file shares and Clustered Data ONTAP HTTP/HTTPS ports accessible from the computer where Netwrix Auditor Administrator Console is installed. Your firewall configuration depends on network settings and security policies in your organization. Below is an example of configuration:

1. Navigate to your cluster command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your current firewall configuration. For example:

```
cluster1::> system services firewall show
Node           Enabled       Logging
-------------  ------------  -------
cluster1-01    true          false
```

3. If firewall disabled, complete the configuration. If not, allow HTTP/HTTPS. For example:

```
cluster1::> system services firewall policy modify -policy pol1 -service
http -action allow -ip-list 192.168.1.0/24
```

```
cluster1::> system services firewall policy modify -policy pol1 -service
https -action allow -ip-list 192.168.1.0/24
```

where `pol1` is your Firewall policy name and `-ip-list 192.168.1.0/24` is your subnet where Netwrix Auditor Administrator Console resides.

4.7.2.4. Configure Event Categories and Log

Perform the following procedures to configure audit:

- To configure auditing state, event categories and log format
- To configure Security log size
- To configure logs retention period

To configure auditing state, event categories and log format

1. Configure audit settings in the context of Cluster or Storage Virtual Machine. Navigate to command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your audit settings. For example, for ONTAPI 8.3:

```
vs1::> vserver audit show -instance

                          Auditing State: true
                    Log Destination Path: /logs
           Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                   Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
```

```
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
       Log Rotation Schedule: Hour: -
     Log Rotation Schedule: Minute: -
                Rotation Schedules: -
          Log Files Rotation Limit: 0
```

3. Check the following options:

Option	Setting
`Auditing State`	true
`Categories of Events to Audit`	file-ops **NOTE:** Only required if you use ONTAP 8.3. You cannot select event categories if you use Clustered Data ONTAP 8.2.
`Log Format`	*"XML"* or *"EVTX"*

4. Update your audit settings if required. For example:

```
vs1::> vserver audit modify
```

To configure Security log size

1. Navigate to your Storage Virtual Machine command prompt through the **SSH/Telnet** connection.
2. Set the log file size limit. For example:

```
vserver audit modify -rotate-size 300MB
```

300MB is the recommended maximum log size proceeding from performance evaluations. 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 Auditor (by default, data collection runs every 24 hours). You can customize your security log by configuring log rotation schedule. For detailed information, review the **Planning the auditing configuration** section in Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS.

3. Perform any test actions with a file share to ensure the log is created.

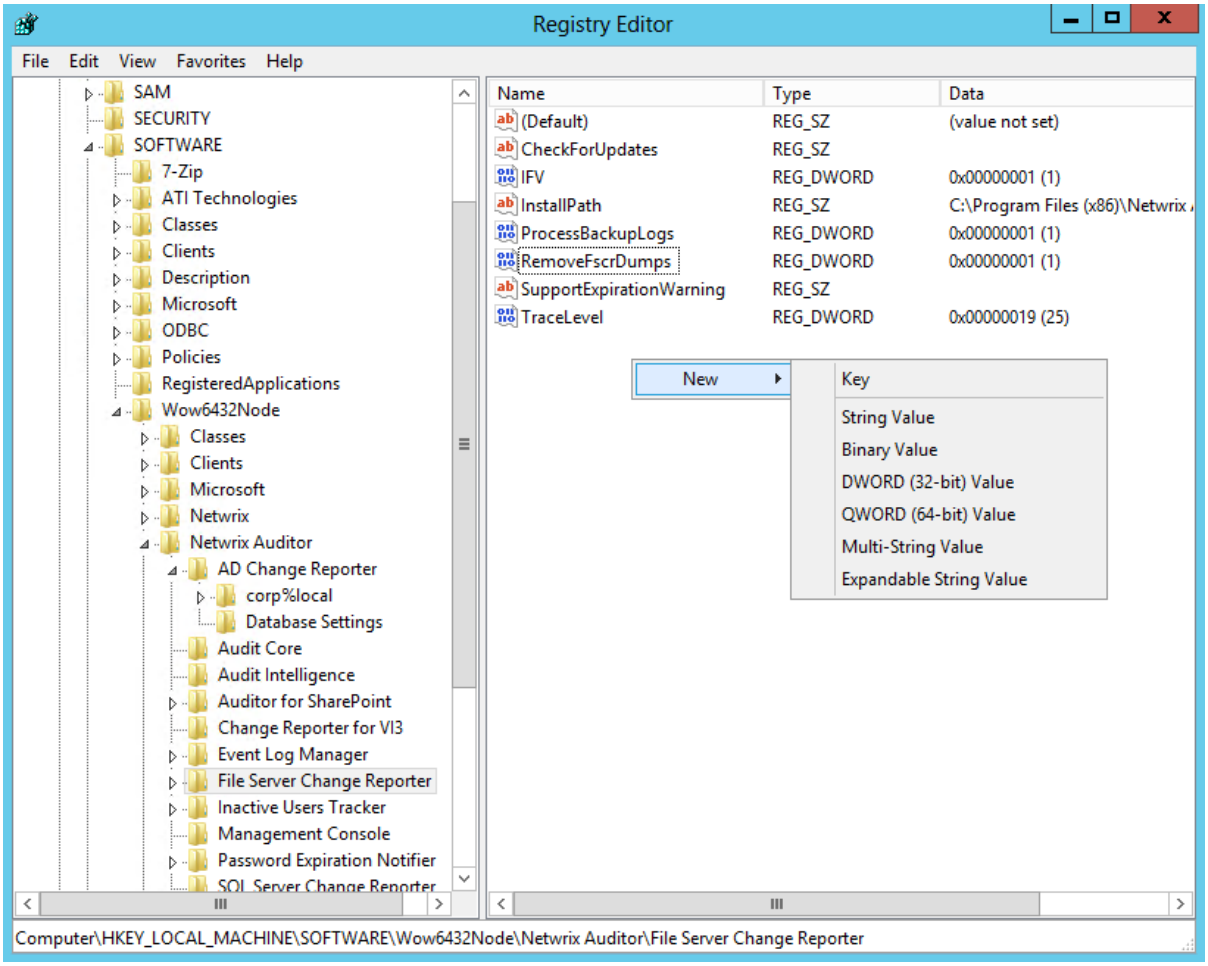
To configure logs retention period

1. On the computer where Netwrix Auditor Administrator Console is installed, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **File**

Server Change Reporter.

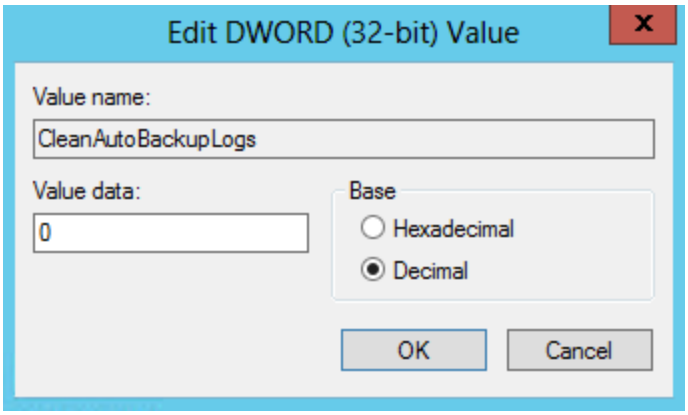
3. In the right-pane, right-click and select **New** → **DWORD (32-bit Value)**.

   NOTE: For the backup logs retention functionality to work properly, you need to specify the **CleanAutoBackupLogs** name for the newly created registry value.



4. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.

5. This value defines the time period (in hours) after which security event logs archives will be automatically deleted. By default, it is set to *"0"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.



6. **NOTE:** If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old logs manually, or you may run out of space on your hard drive.

To specify the Security log shared folder

Netwrix Auditor accesses audit logs via a specified file share. This may be either the default administrative share (ETC$, C$, etc.), or a custom file share.

NOTE: Perform the procedure below if you are not going to detect file shares automatically via Netwrix Auditor Administrator Console.

1. Navigate to your Storage Virtual Machine command prompt through the **SSH/Telnet** connection.
2. Review the local path to audit logs. For example:

```
vs1::> vserver audit show -instance

                    Auditing State: true
               Log Destination Path: /logs
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                         Log Format: evtx
                Log File Size Limit: 100MB
       Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
       Log Rotation Schedule: Hour: -
     Log Rotation Schedule: Minute: -
                 Rotation Schedules: -
           Log Files Rotation Limit: 0
```

3. Review the list of available file shares on your SVM. For example:

```
vs1::> vserver cifs share show
Vserver    Share     Path      Properties    Comment    ACL
---------  --------  --------  ----------    ---------  -----------------
vs1        admin$    /         browsable     -          -
vs1        c$        /         oplocks       -          BUILTIN\Administrators
                                                        / Full Control
                               browsable
                               changenotify
vs1        ipc$      /         browsable     -          -
```

4. Perform any test actions with a file share to ensure the log is created.

4.7.3. Configure Audit Settings for CIFS File Shares

Netwrix Auditor can be configured to audit all access types, review the table below and select options that you want to track:

Access Type	Description
Successful modifications	Commonly used option to track important data. Helps find out *who* created, modified, moved, renamed or removed files and *when* these changes were done.
Failed modification attempts	Used to track suspicious activity on your file server. Helps find out *who* tried to change or delete files, etc., but failed to do it. Investigate incidents with AuditIntelligence and figure out *why* that user tried to do it.
Successful reads	Used to supervise important files with confidential information for privileged users only. Browse your audit data in the Netwrix Auditor client and discover *who* accessed important files besides your trusted users. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.
Failed read attempts	Used to track suspicious activity. Helps find out *who* was trying to read files, but failed to do it. Investigate your incidents with AuditIntelligence and figure out *why* that user tried to do it. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.

Do one of the following depending on the OS:

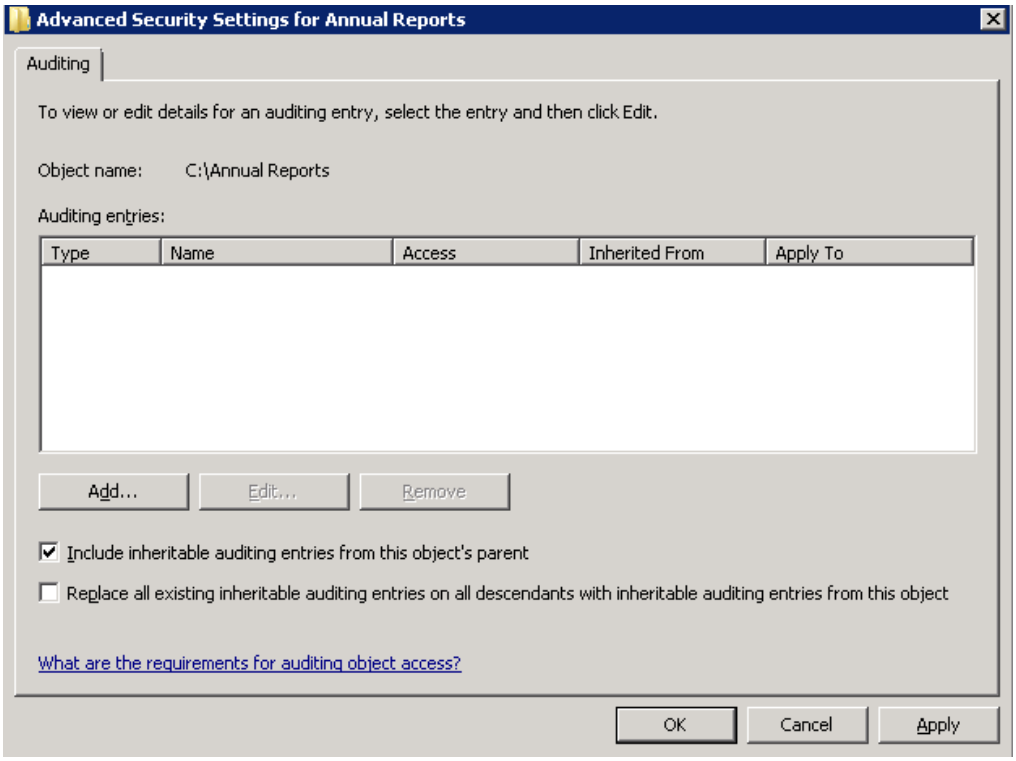
- To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions
- To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions

1. Navigate to the root share folder, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

   NOTE: If there is no such tab, it means a wrong security style has been specified for the volume holding this file share.

3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. In a separate **Advanced Security Settings for <Share_Name>** dialog, click **Add** to add a principal. You can also select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.

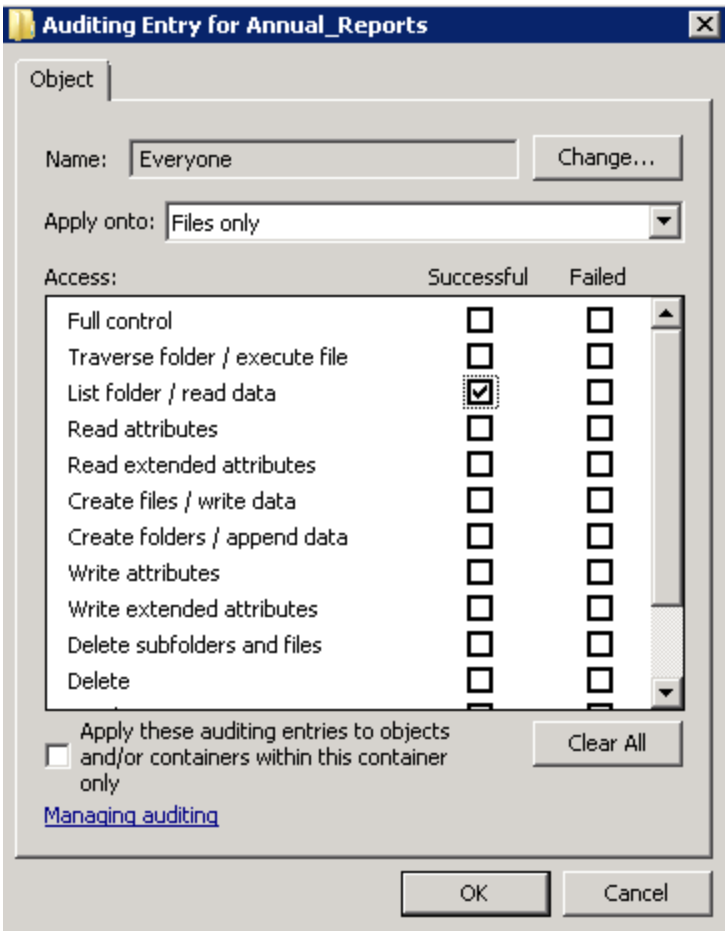
NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the Reports functionality and the product will only audit user accounts that belong to the selected group.

5. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modifications as well as failed reads and modifications attempts), you need to add three separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful modifications
   - Failed read attempts

Auditing Entry
Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

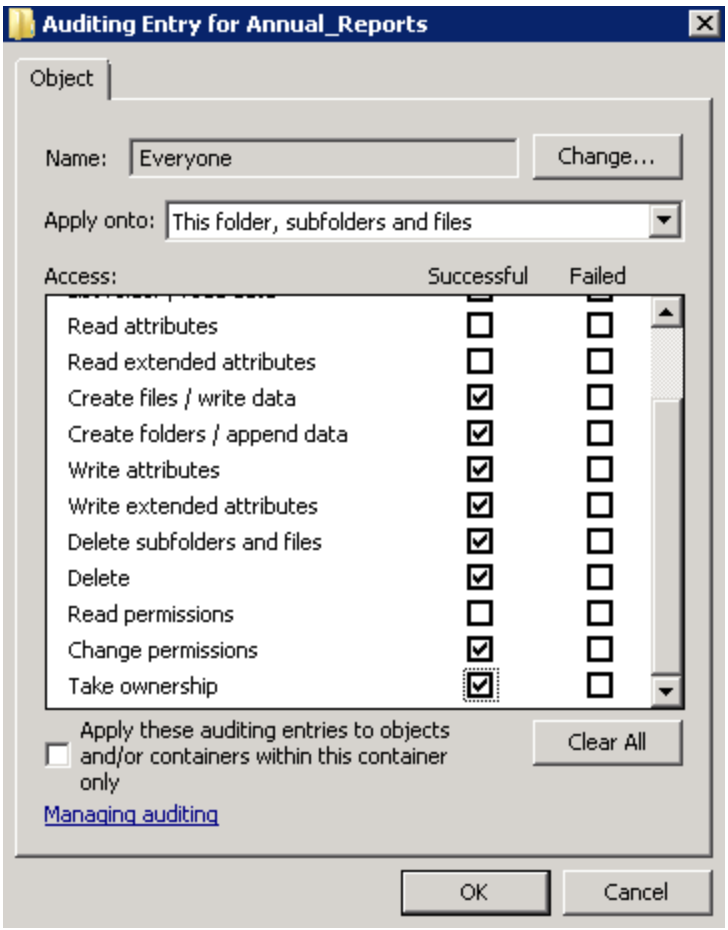


Auditing Entry

- Apply onto—Select *"Files only"*.
- Check *"Successful"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful modifications

The Auditing Entry below shows Advanced Permissions for auditing successful modifications only:



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Successful"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**

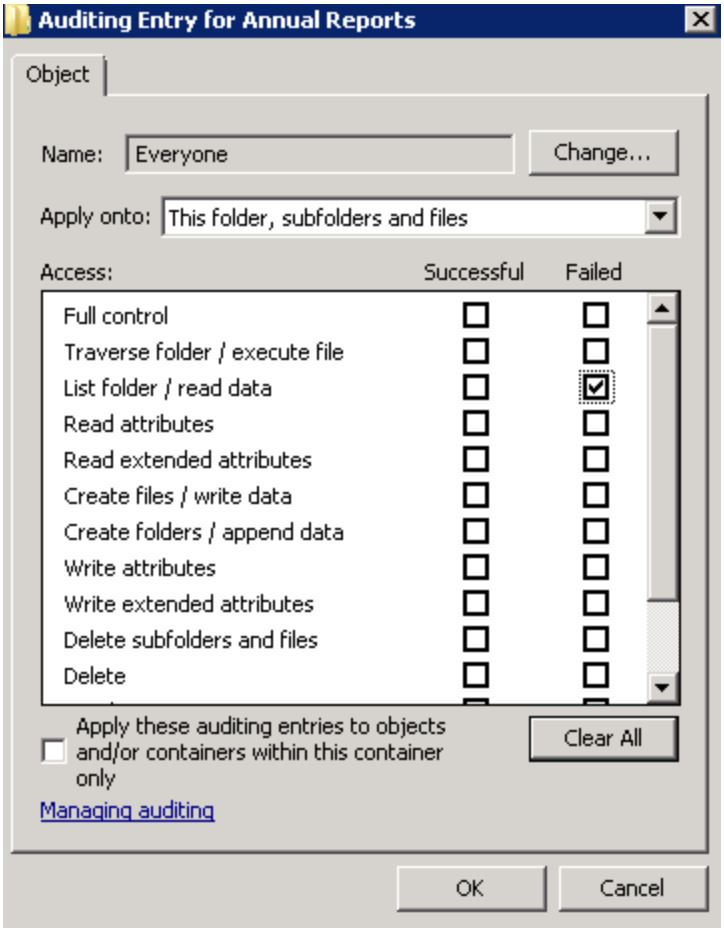
Auditing Entry

- **Delete subfolders and files**
- **Delete**
- **Change permissions**
- **Take ownership**

- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed read attempts

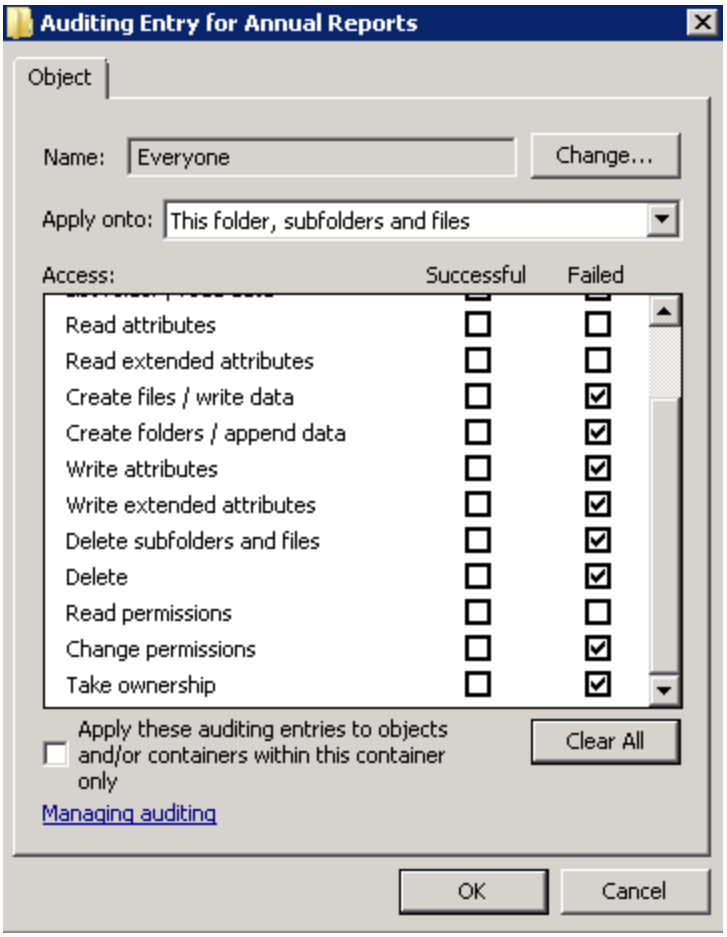
The Auditing Entry below shows Advanced Permissions for auditing failed read attempts only:



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Auditing Entry
Failed modification attempts

The Auditing Entry below shows Advanced Permissions for auditing failed modification attempts only:



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**

Auditing Entry

- **Take ownership**

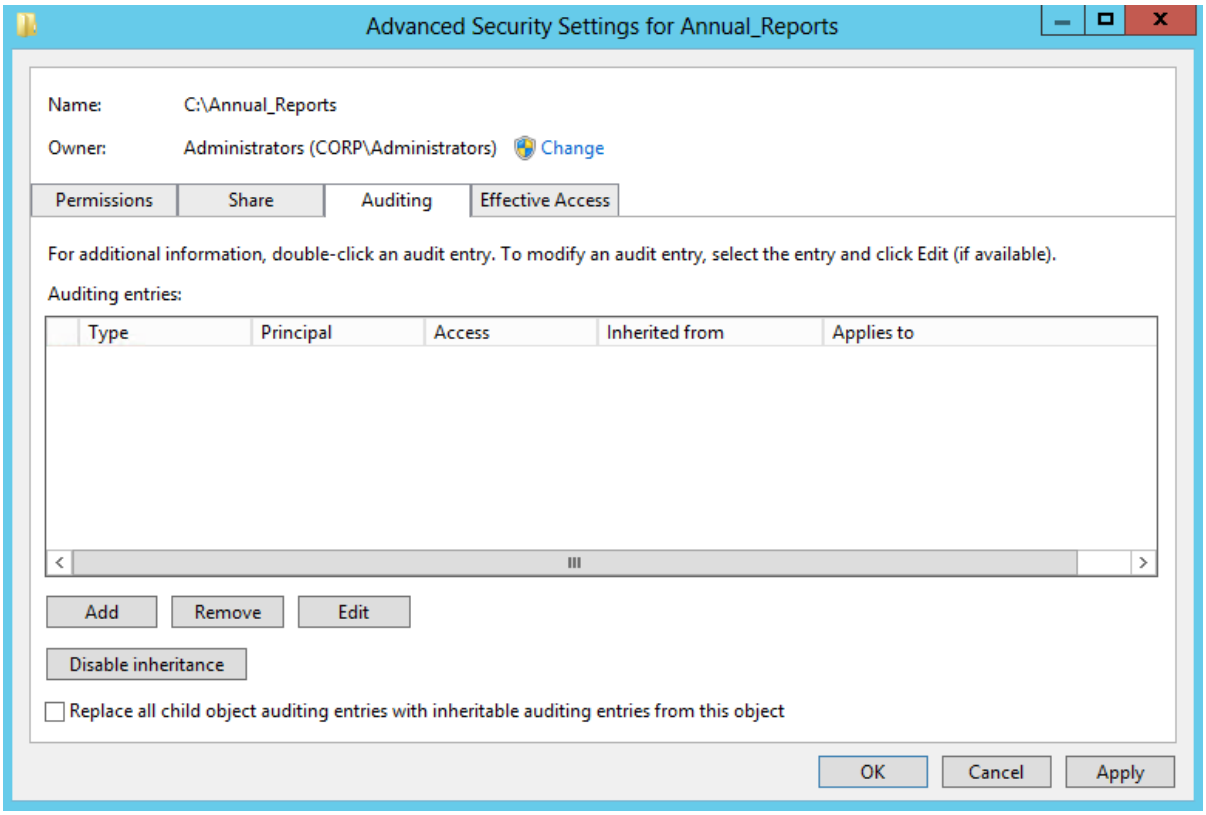
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

1. Navigate to the root shared folder, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

   NOTE: If there is no such tab, it means a wrong security style has been specified for the volume holding this file share. See Configure Audit Settings for CIFS File Shares for more information.

3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. Click **Add** to add a new principal. You can also select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.
5. In the **Auditing Entry for <Folder_Name>** dialog, click the **Select a principal link** and specify **Everyone**.

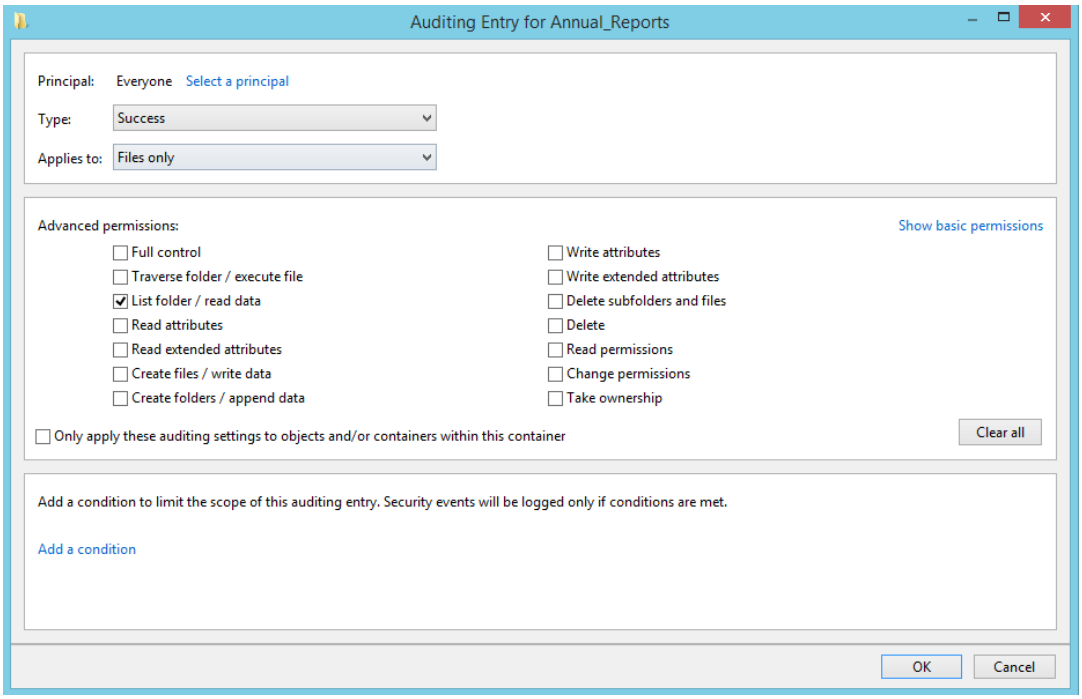
NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. In this case, the product will only monitor user accounts that belong to the selected group.

6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed reads and modifications attempts), you need to add three separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful modifications
   - Failed read attempts

Auditing Entry
Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

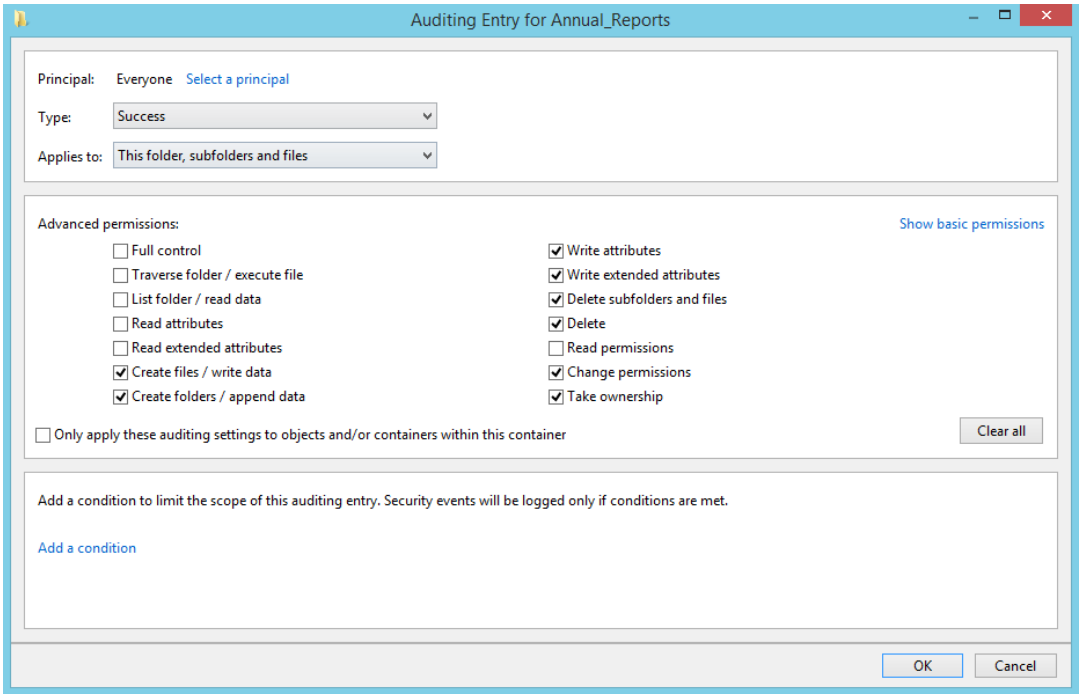


- Type—Set to *"Success"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Auditing Entry

Successful modifications

The Auditing Entry below shows Advanced Permissions for auditing successful modifications only:

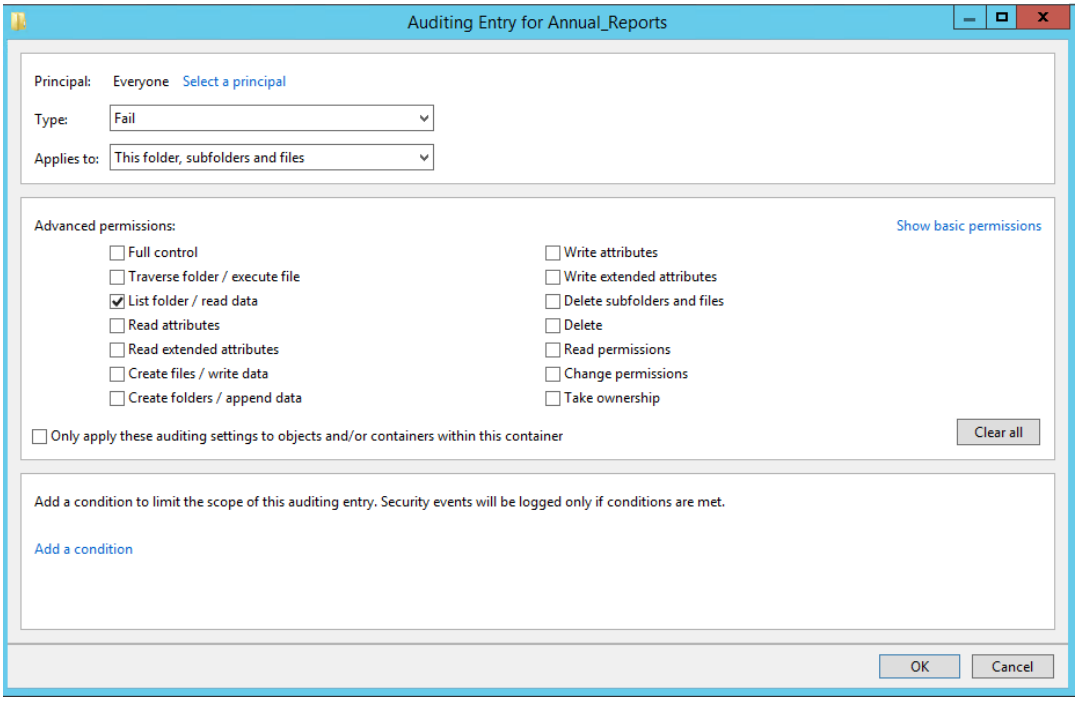


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Auditing Entry

Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts:

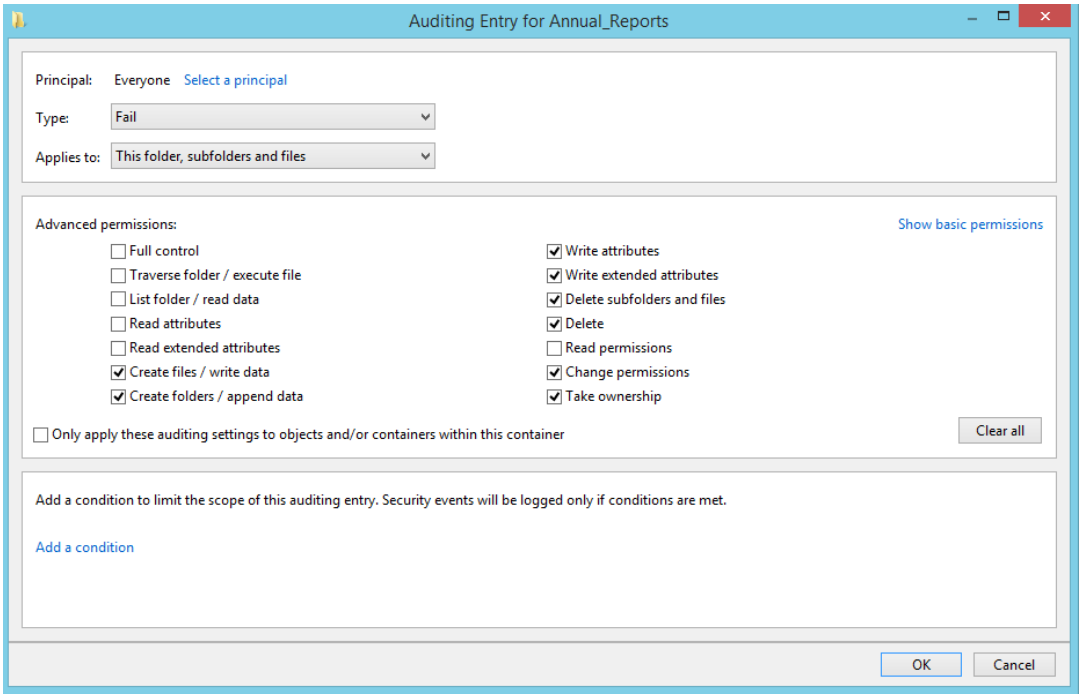


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed modification attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read and modification attempts:

Auditing Entry



- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change permissions**
  - **Take ownership**
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

4.8. Configure SharePoint Farm for Auditing

You can configure your SharePoint farm for auditing in one of the following ways:

- Automatically when creating a Managed Object. If you select to configure audit in the target SharePoint farm automatically, your current audit settings will be checked on each data collection and adjusted if necessary.

  Also, after collecting data from site collections, Netwrix Auditor will trim events older than 1 day.

- Manually. Perform the following procedures:
  - Configure Audit Log Trimming on your SharePoint farm.
  - Configure Events Auditing Settings on your SharePoint farm.
  - Enable SharePoint Administration Service on the computer where SharePoint Central Administration is installed and where you intend to deploy Netwrix Auditor for SharePoint Core Service.

4.8.1. Configure Audit Log Trimming

1. Log in as an administrator to the audited SharePoint site collection.
2. At the top level of your site collection, navigate to **Settings** → **Site Settings**.
3. Select **Site collection audit settings** under **Site Collection Administration**.
4. In the **Audit Log Trimming** section, do the following:
   - Set **Automatically trim the audit log for this site** to *"Yes"*.
   - In **Specify the number of days of audit log data to retain** set retention to 7 days.

     NOTE: You may keep the existing audit log retention provided that it is set to 7 days or less.

4.8.2. Configure Events Auditing Settings

1. Log in as an administrator to the audited SharePoint site collection.
2. At the top level of your site collection, navigate to **Settings** → **Site Settings**.
3. Select **Site collection audit settings** under **Site Collection Administration**.
4. In the **List, Libraries, and Sites** section, select **Editing users and permissions**

   NOTE: Enable **Opening or downloading documents, viewing items in lists, or viewing item properties** for read access auditing.

4.8.3. Enable SharePoint Administration Service

This service is must be started to ensure the Netwrix Auditor for SharePoint Core Service successful installation. Perform the procedure below, prior to the Core Service installation. See Install Netwrix Auditor for SharePoint Core Service for more information.

1. On the computer where SharePoint Central Administration is installed and where you intend to deploy Netwrix Auditor for SharePoint Core Service, open the **Services Management Console**. Navigate to **Start** → **Administrative Tools** → **Services**.
2. Locate the **SharePoint Administration** service (SPAdminV4), right-click it and select **Properties**.
3. In the **General** tab, set **Startup type** to *"Automatic"* and click **Apply**.
4. Click **Start** to start the service.

4.9. Configure Windows Server for Auditing

You can configure Windows Servers for auditing in one of the following ways:

- Automatically when creating a Managed Object

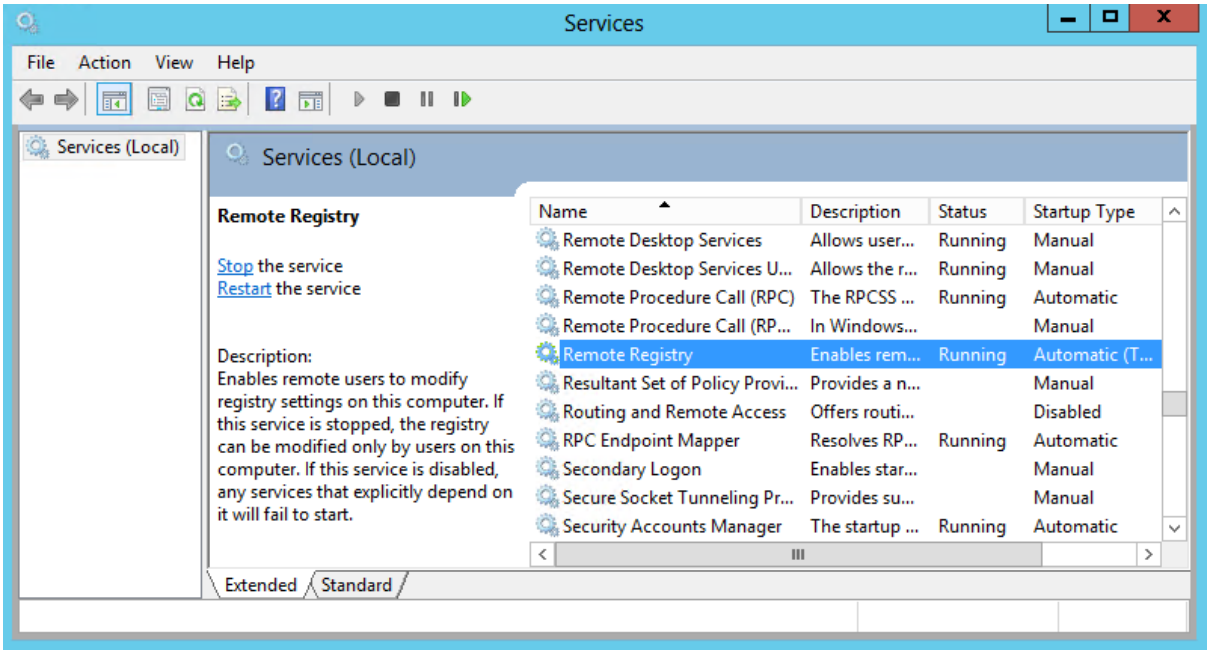
  If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

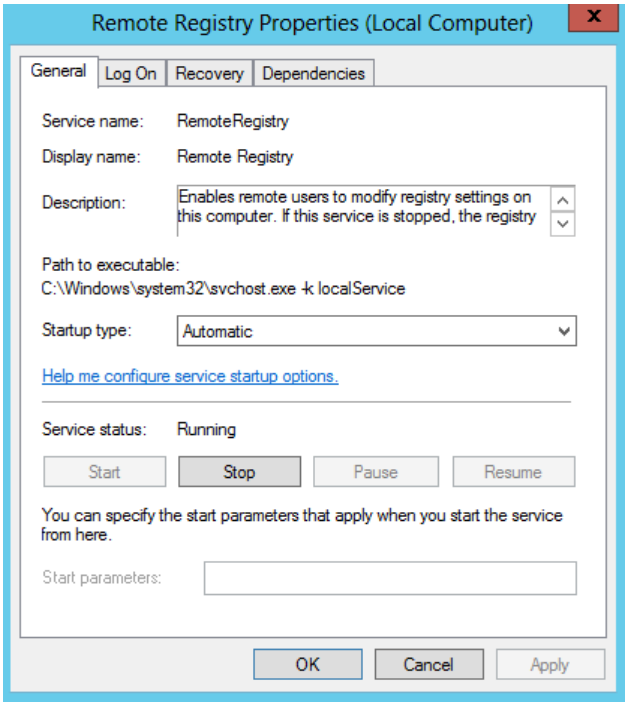
- Manually. Perform the following procedures:
  - Enable Remote Registry and Windows Management Instrumentation Services
  - Configure Windows Registry Audit Settings
  - Configure Local Audit Policies or Configure Advanced Audit Policies
  - Configure Event Log Size and Retention Settings
  - Configure Windows Firewall Inbound Connection Rules

4.9.1. Enable Remote Registry and Windows Management Instrumentation Services

1. Navigate to **Start** → **Administrative Tools** → **Services**.



2. In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.
5. Locate the **Windows Management Instrumentation** service and repeat these steps.

4.9.2. Configure Windows Registry Audit Settings

Windows Registry audit permissions must be configured so that the "Who" and "When" values are reported correctly for each change. Configure these settings on each Windows server you want to audit.

The following audit permissions must be set to *"Successful"* for the `HKEY_LOCAL_MACHINE\SOFTWARE`, `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys:

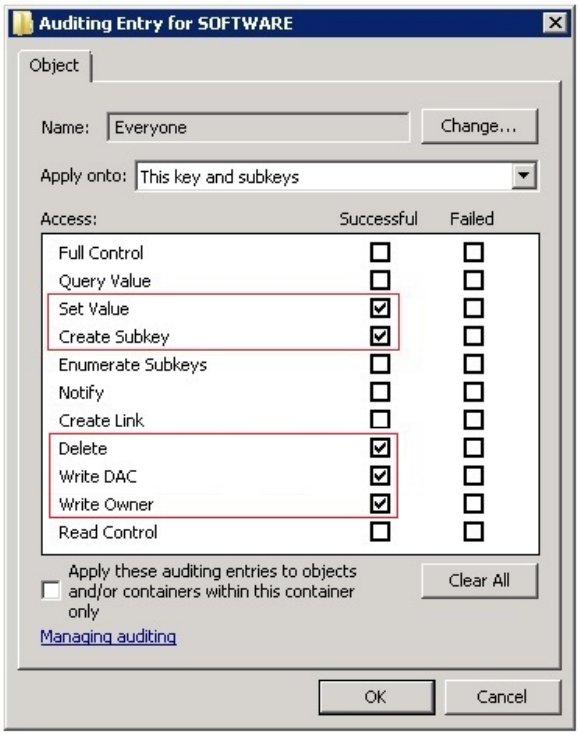
- Set Value
- Create Subkey
- Delete
- Write DAC
- Write Owner

Perform one of the following procedures depending on the OS version:

- To configure Windows registry audit settings on pre-Windows Server 2012 versions
- To configure Windows registry audit settings on Windows Server 2012 and above

To configure Windows registry audit settings on pre-Windows Server 2012 versions

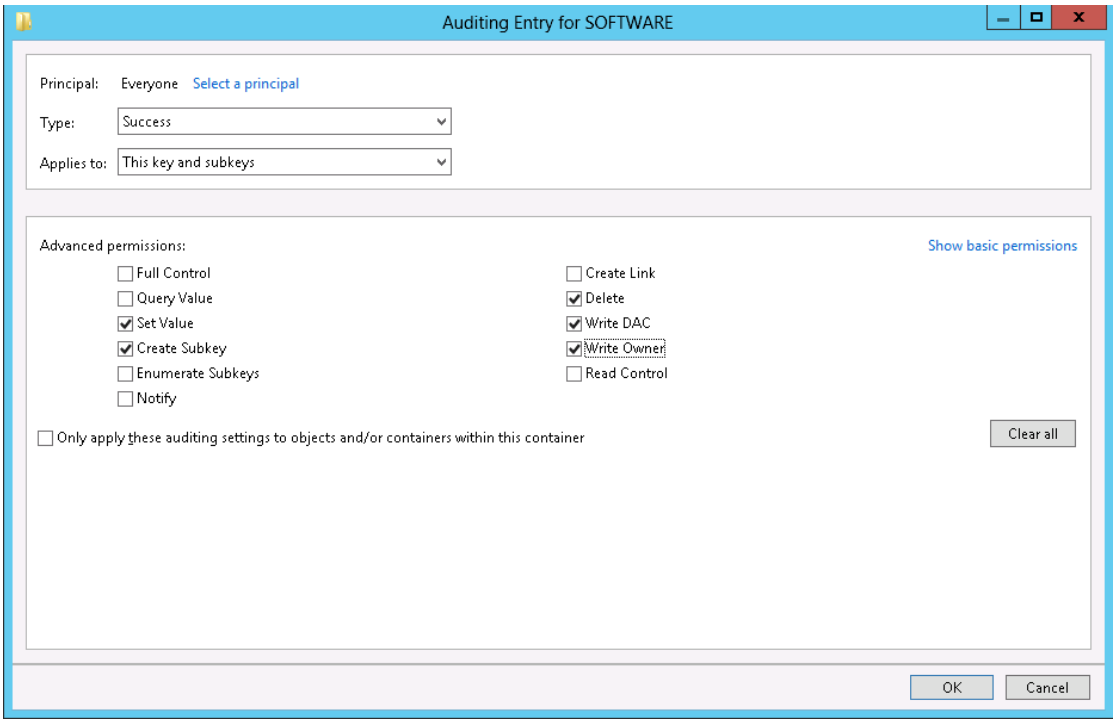
1. On your target server, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click **Advanced**.
4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.
5. Select the **Everyone** group.
6. In the **Auditing Entry for SOFTWARE** dialog, select *"Successful"* for the following access types:
    - **Set Value**
    - **Create Subkey**
    - **Delete**
    - **Write DAC**
    - **Write Owner**



7. Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys.

To configure Windows registry audit settings on Windows Server 2012 and above

1. On your target server, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click **Advanced**.
4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.
5. Click **Select a principal link** and specify the **Everyone** group in the **Enter the object name to select** field.
6. Set **Type** to *"Success"* and **Applies to** to *"This key and subkeys"*.
7. Click **Show advanced permissions** and select the following access types:
   - **Set Value**
   - **Create Subkey**
   - **Delete**
   - **Write DAC**
   - **Write Owner**



8. Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys.

4.9.3. Configure Local Audit Policies

Local audit policies must be configured on the target servers to get the "Who" and "When" values for the changes to the following monitored system components:

- Services
- Hardware and system drivers
- Windows registry
- Scheduled tasks
- Local users and groups
- General computer settings

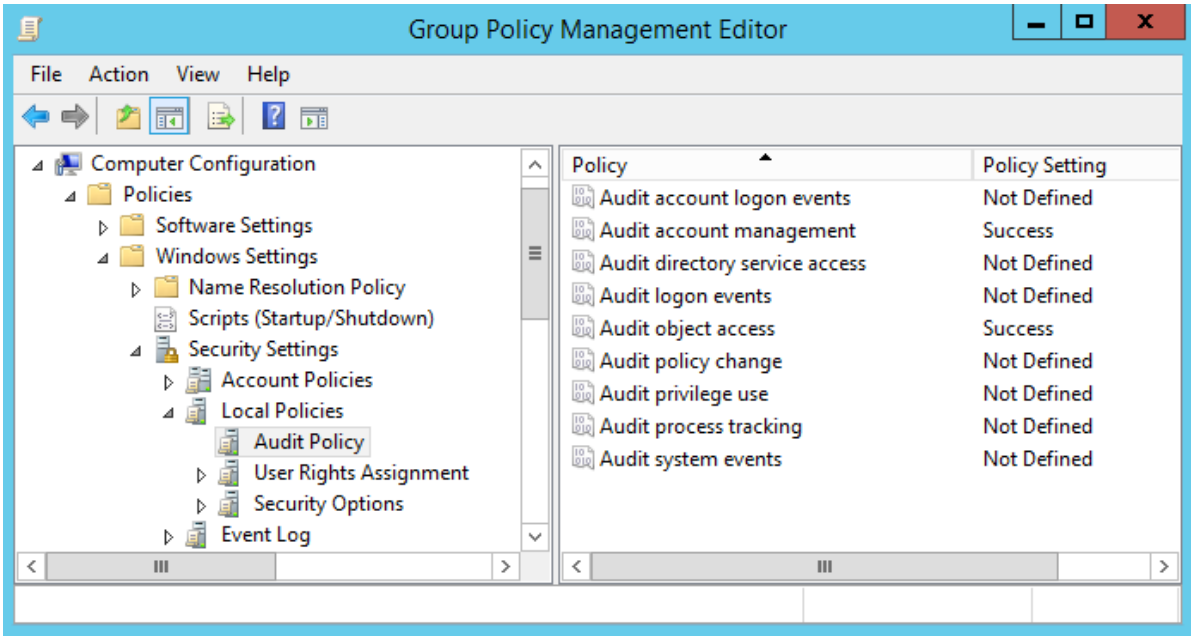
You can also configure advanced audit policies for same purpose. See Configure Advanced Audit Policies for more information.

NOTE: There are several methods to configure local audit policies, and this guide covers just one of them. Consider the possible impact on your environment and select the method that best suits your purposes. Note that if you follow the procedures below, audit settings will be applied to the whole domain.

To configure local audit policies

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains**, right-click **<domain_name>** and select **Create a GPO in this domain and Link it here**.
3. Enter the name for the new GPO.
4. Right-click the newly created GPO and select **Edit**.
5. 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** → **Audit Policy.**
6. Configure the following audit policies.

Policy Name	Audit Events
Audit account management	*"Success"*
Audit object access	*"Success"*



7. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

4.9.4. Configure Advanced Audit Policies

Advanced audit policies can be configured instead of local policies. Any of them are required if you want to get the "Who" and "When" values for the changes to the following monitored system components:

- Services
- Hardware and system drivers
- Windows registry
- Scheduled tasks
- Local users and groups
- General computer settings

Perform the following procedures:

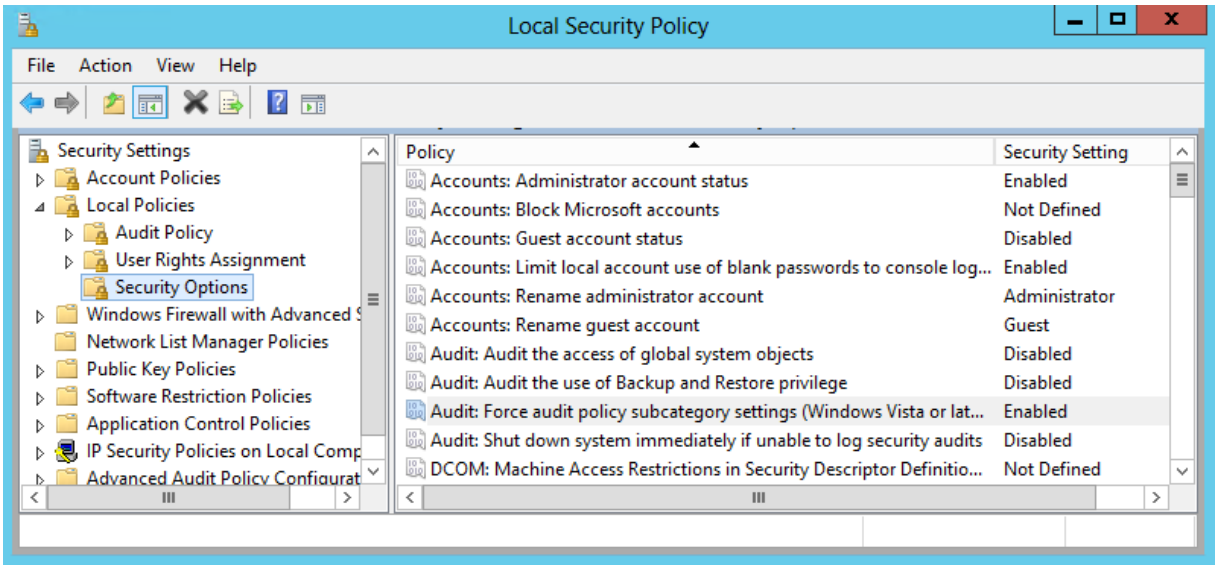
- To configure security options
- To configure advanced audit policy on Windows Server 2008 / Windows Vista
- To configure advanced audit policies on Windows Server 2008 R2 / Windows Vista and above

To configure security options

NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** option.

To do it, perform the following steps:

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **All Programs** → **Administrative Tools** → **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **Security Options** and locate the **Audit: Force audit policy subcategory settings (Windows Vista or later)** policy.



3. Double-click the policy and enable it.

To configure advanced audit policy on Windows Server 2008 / Windows Vista

In Windows Server 2008 / Windows Vista, audit policies are not integrated with the Group Policies and can only be deployed using logon scripts generated with the native Windows **auditpol.exe** command line tool. Therefore, these settings are not permanent and will be lost after server reboot.

NOTE: The procedure below explains how to configure Advanced audit policy for a single server. If you audit multiple servers, you may want to create logon scripts and distribute them to all target machines via Group Policy. Refer to Microsoft Knowledge Base article: How to use Group Policy to configure detailed security auditing settings for more information.

1. On an audited server, navigate to **Start** → **Run** and type *"cmd"*.
2. Disable the **Object Access** and **Account Management** categories by executing the following command in the command line interface:

   ```
   auditpol /set /category:"Object Access" /success:disable /failure:disable
   ```

   ```
   auditpol /set /category:"Account Management" /success:disable
   /failure:disable
   ```

3. Enable the following audit subcategories:
   - **Audit Security Group Management**
   - **Audit User Account Management**
   - **Audit Handle Manipulation**
   - **Audit Other Object Access Events**
   - **Audit Registry**
4. Execute the following commands in the command line interface:

   ```
   auditpol /set /subcategory:"Audit Security Group Management"
   /success:enable /failure:disable
   ```

   ```
   auditpol /set /subcategory:"Audit User Account Management" /success:enable
   /failure:disable
   ```

   ```
   auditpol /set /subcategory:"Handle Manipulation" /success:enable
   /failure:disable
   ```

   ```
   auditpol /set /subcategory:"Audit Other Object Access Events"
   /success:enable /failure:disable
   ```

   ```
   auditpol /set /subcategory:"Audit Registry" /success:enable
   /failure:disable
   ```

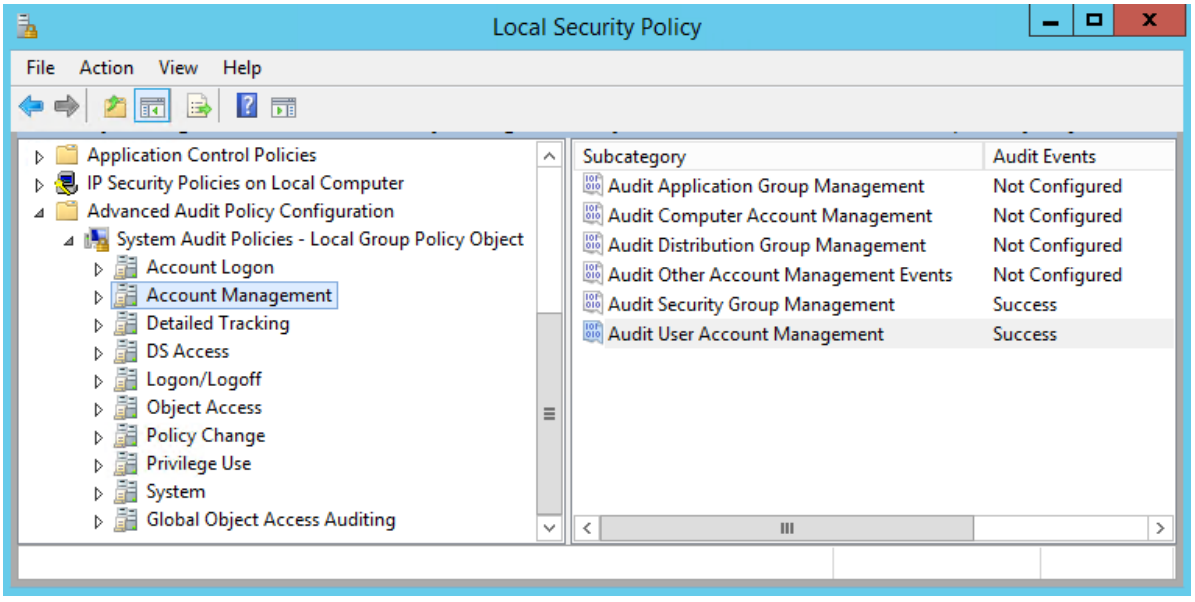
   NOTE: It is recommended to disable all other subcategories unless you need them for other purposes. You can check your current effective settings by executing the following commands: `auditpol /get /category:"Object Access"` and `auditpol /get /category:"Account Management"`.

To configure advanced audit policies on Windows Server 2008 R2 / Windows Vista and above

In Windows Server 2008 R2 and Windows 7 and above, Advanced audit policies are integrated with Group Policies, so they can be applied via Group Policy Object or Local Security Policies. The procedure below describes how to apply Advanced policies via Local Security Policy console.

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Administrative Tools** → **Local Security Policy**.
2. In the left pane, navigate to **Security Settings** → **Advanced Audit Policy Configuration** → **System Audit Policies**.
3. Configure the following audit policies.

Policy Subnode	Policy Name	Audit Events
Account Management	• **Audit Security Group Management** • **Audit User Account Management**	*"Success"*
Object Access	• **Audit Handle Manipulation** • **Audit Other Object Access Events** • **Audit Registry**	*"Success"*

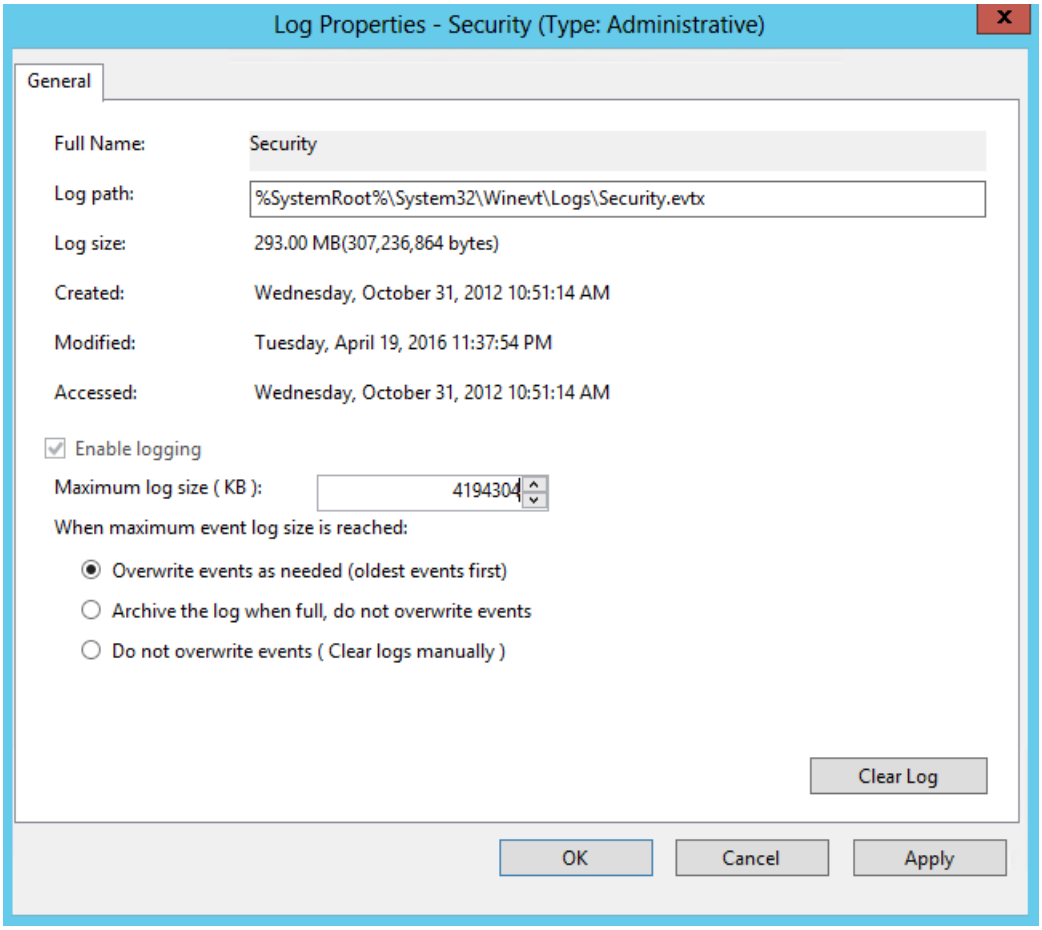


4.9.5. Configure Event Log Size and Retention Settings

To prevent data loss, you need to specify the maximum size for the Application, Security, System and Microsoft-Windows-TaskScheduler/Operational event logs. The procedure below provides you with just one of a number of possible ways to specify the event log settings. If you have multiple target computers, you need to perform this procedure on each of them.

To configure the event log size and retention method

1. On a target server, navigate to **Start** → **Programs** → **Administrative Tools** → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Security** and select **Properties**.



3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field, specify the size—4GB.
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

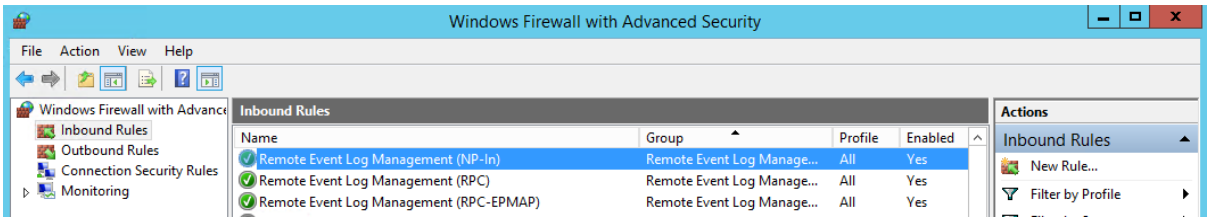
NOTE: Make sure the **Maximum security log size** group policy does not overwrite your log settings. To check this, start the **Group Policy Management** console, proceed to the GPO that affects your server, and navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log**.

6. Repeat these steps for the **Application** and **System** event logs under **Windows Logs**, and for **Microsoft-Windows-TaskScheduler/Operational** event log under **Applications and Services Logs** → **Microsoft** → **Windows** → **TaskScheduler** → **Operational**.

4.9.6. Configure Windows Firewall Inbound Connection Rules

NOTE: Also, you can configure Windows Firewall settings through Group Policy settings. To do this, edit the GPO affecting your firewall settings. Navigate to **Computer Configuration** → **Administrative Templates** → **Network** → **Network Connections** → **Windows Firewall**, select **Domain Profile** or **Standard Profile**. Then, enable the **Allow inbound remote administration exception**.

1. On each audited server, navigate to **Start** → **Control Panel** and select **Windows Firewall**.
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.



4. Enable the following inbound connection rules:
   - **Remote Event Log Management (NP-In)**
   - **Remote Event Log Management (RPC)**
   - **Remote Event Log Management (RPC-EPMAP)**
   - **Windows Management Instrumentation (ASync-In)**
   - **Windows Management Instrumentation (DCOM-In)**
   - **Windows Management Instrumentation (WMI-In)**
   - **Network Discovery (NB-Name-In)**
   - **File and Printer Sharing (NB-Name-In)**
   - **Remote Service Management (NP-In)**
   - **Remote Service Management (RPC)**
   - **Remote Service Management (RPC-EPMAP)**

4.10. Configure Infrastructure for Auditing Event Log

Do one of the following depending on the OS:

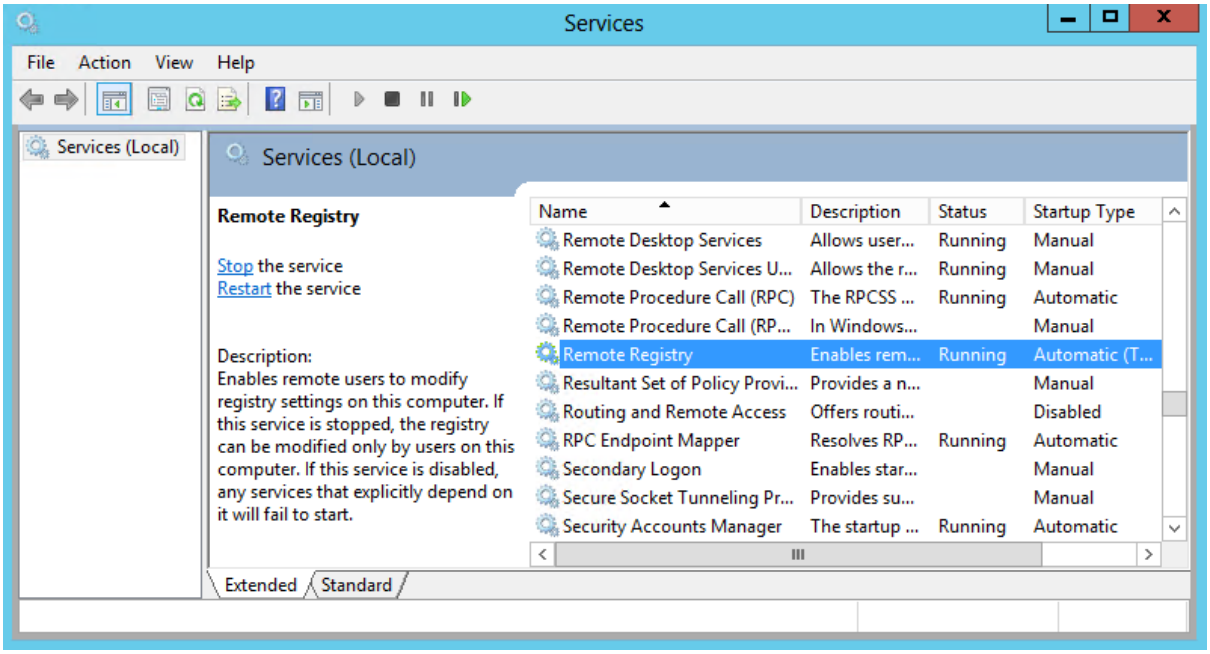
- Configure Event Log Auditing on Windows Computers
- Configure Event Log Auditing on Syslog-Based Platforms

4.10.1. Configure Event Log Auditing on Windows Computers

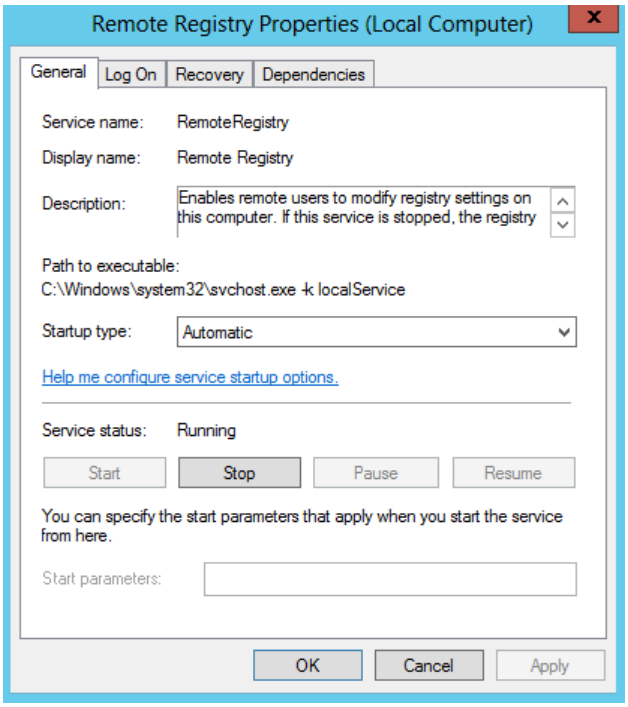
The **Remote Registry** service must be enabled on the target computers.

To enable the Remote Registry service

1. Navigate to **Start** → **Administrative Tools** → **Services**.



2. In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.

4.10.2. Configure Event Log Auditing on Syslog-Based Platforms

To be able to process Syslog events, you must configure the Syslog daemon to redirect these events to the computer where Netwrix Auditor is installed. Also, local UDP 514 port must be opened for inbound connections; it is done automatically during the product installation.

The procedure below explains how to configure redirection of **Auth log**, as predefined Syslog-based platforms in Netwrix Auditor have default rules to process this log only. You can create your own rules and configure syslog platform settings as described in the procedure below. See Netwrix Auditor Administrator's Guide for more information.

To configure a Syslog daemon to redirect events for Red Hat Enterprise Linux 5

1. Open the **/etc/syslog.conf** file.
2. Add the following line: `authpriv.* @FQDN/Netbios name` or `authpriv.* @ComputerIP`.

   NOTE: `FQDN/Netbios name` and `ComputerIP` must be the name and IP address of the computer where Netwrix Auditor is installed.
3. Navigate to the **/etc/sysconfig/syslog** file.

4. Change the **SYSLOGD_OPTIONS** value to *SYSLOGD_OPTIONS="-r –m 0"*.
5. Launch the **RHEL** console and execute the following command: `service syslog restart`.

To configure a Syslog daemon to redirect events for Ubuntu 11

1. Navigate to the **/etc/rsyslog.d/50-default.conf** file.
2. Add the following line: `authpriv.* @FQDN/Netbios name` or `authpriv.* @ComputerIP`

   NOTE: `FQDN/Netbios name` and `ComputerIP` must be the name and IP address of the computer where Netwrix Auditor is installed.
3. Launch the **UBUNTU** console and execute the following command: `service rsyslog restart`.

4.11. Configure Domain for Auditing Group Policy

You can configure your domain for auditing Group Policy in one of the following ways:

- Automatically when creating a Managed Object

  If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.
- Automatically through the **Active Directory Audit Configuration** wizard integrated in Netwrix Auditor Administrator Console

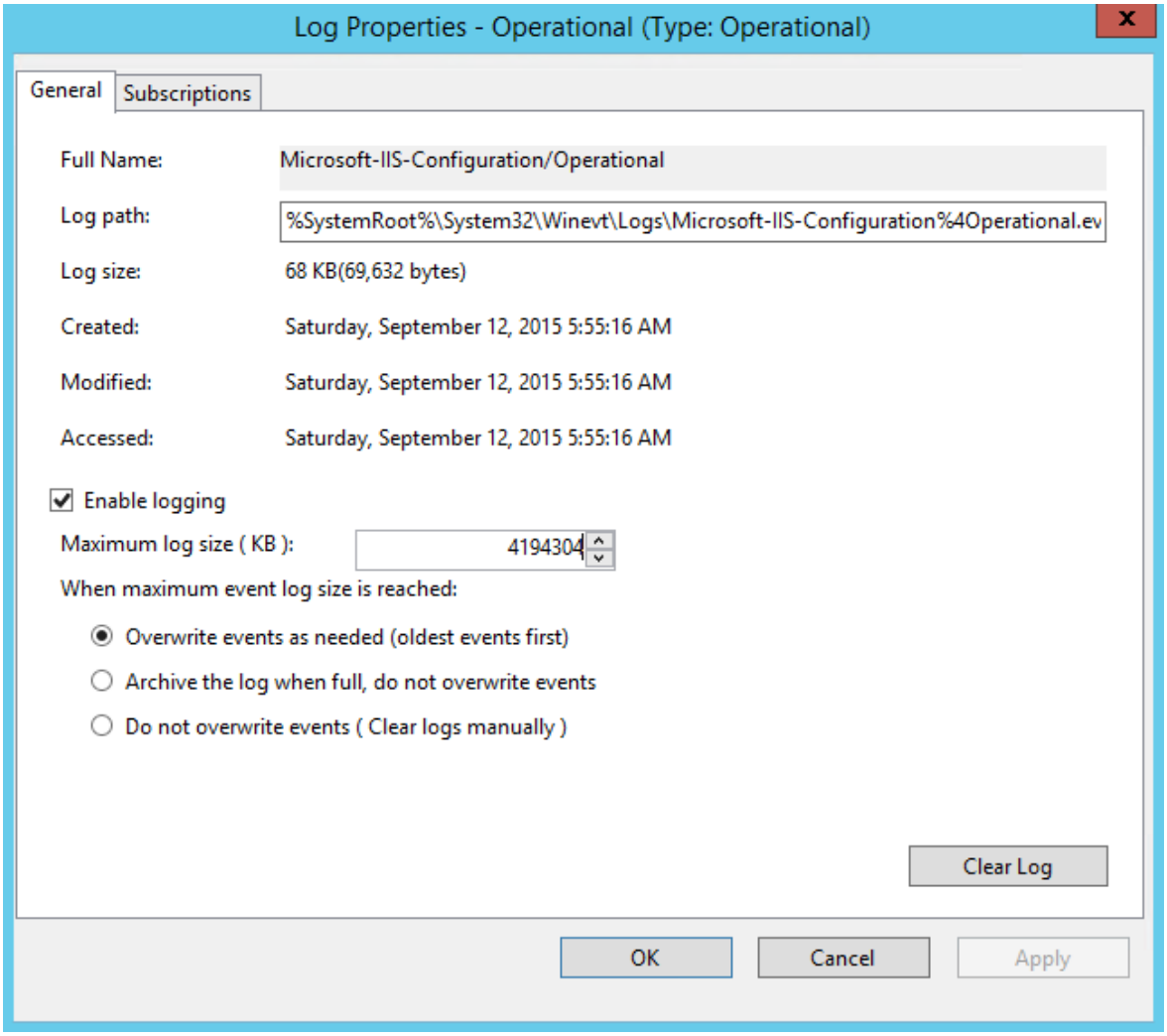
  With this wizard you can configure audit settings for Active Directory, Exchange and Group Policy. On each step, the wizard checks your audit settings and provides a report on their current values. If any of your current settings conflict with the configuration required for the product to function properly, these conflicts will be listed. In this case, you can choose whether you want to adjust your audit settings automatically and override your current settings, or if you want to configure them manually. For detailed instructions, refer to Netwrix Auditor Administrator's Guide.
- Manually. You need to adjust the same audit settings as those required for auditing Active Directory. See Configure Domain for Auditing Active Directory for more information.

4.12. Configure Infrastructure for Auditing IIS

NOTE: To be able to process Internet Information Services (IIS) events, you must enable the **Remote Registry** service on the target computers. See Configure Infrastructure for Auditing Event Log for more information.

To configure the Operational log size and retention method

1. On the computer where IIS is installed, navigate to **Start** → **Programs** → **Administrative Tools** → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Applications and Services Logs** → **Microsoft** → **Windows** and expand the **IIS-Configuration** node.
3. Right-click the **Operational** log and select **Properties**.



4. Make sure **Enable logging** is enabled.
5. Set **Maximum log size** to 4 GB.
6. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

4.13. Configure Infrastructure for Auditing Logon Activity

You can configure your IT infrastructure for auditing Logon Activity in one of the following ways:

- Automatically when creating a Managed Object

  If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

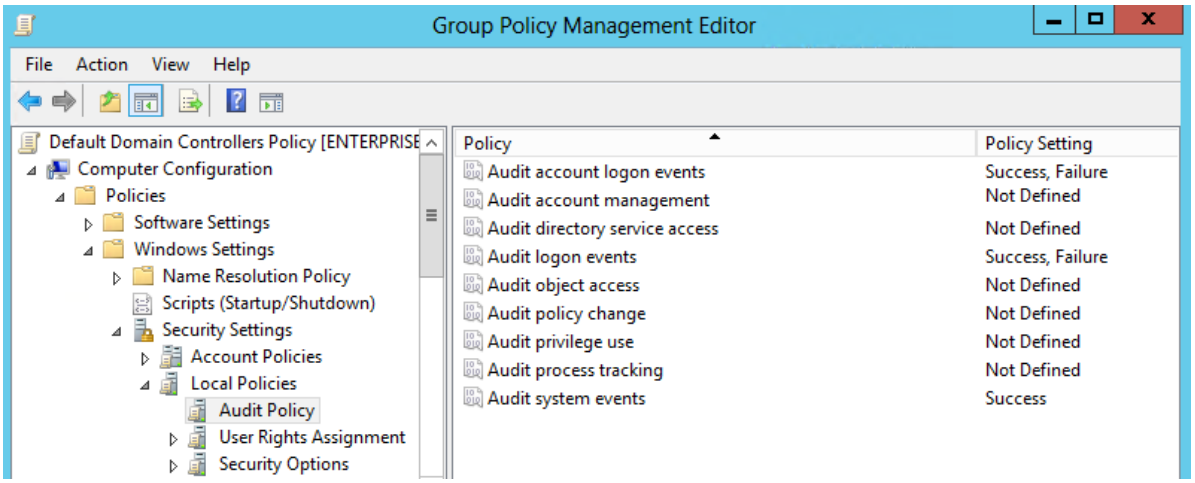
- Manually. To configure your domain manually for auditing Logon Activity, perform the following procedures:
  - Configure Basic Domain Audit Policies or Configure Advanced Audit Policies
  - Configure Security Event Log Size and Retention Settings
  - Configure Windows Firewall Inbound Connection Rules

4.13.1. Configure Basic Domain Audit Policies

Basic local audit policies allow tracking changes to user accounts and groups and identifying originating workstations. You can configure advanced audit policies for the same purpose too. See Configure Advanced Audit Policies for more information.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers 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** → **Audit Policy.**
4. Configure the following audit policies.

Policy	Audit Events
Audit Logon Events	*"Success"* and *"Failure"*
Audit Account Logon Events	*"Success"* and *"Failure"*
Audit system events	*"Success"*



5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

4.13.2. Configure Advanced Audit Policies

You can configure advanced audit policies instead of basic domain policies to collect Logon Activity changes with more granularity.

Perform the following procedures:

- To configure security options
- To configure advanced audit policies

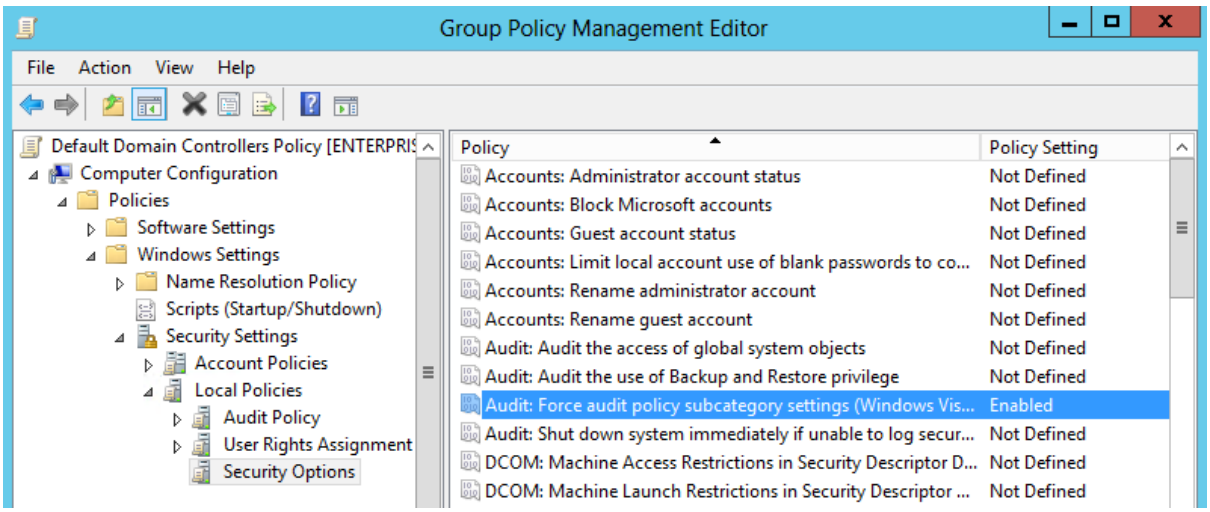
To configure security options

NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** option.

To do it, perform the following steps:

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers 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** → **Security Options**.
4. Locate the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override**

audit policy category settings and make sure that policy setting is set to *"Enabled"*.

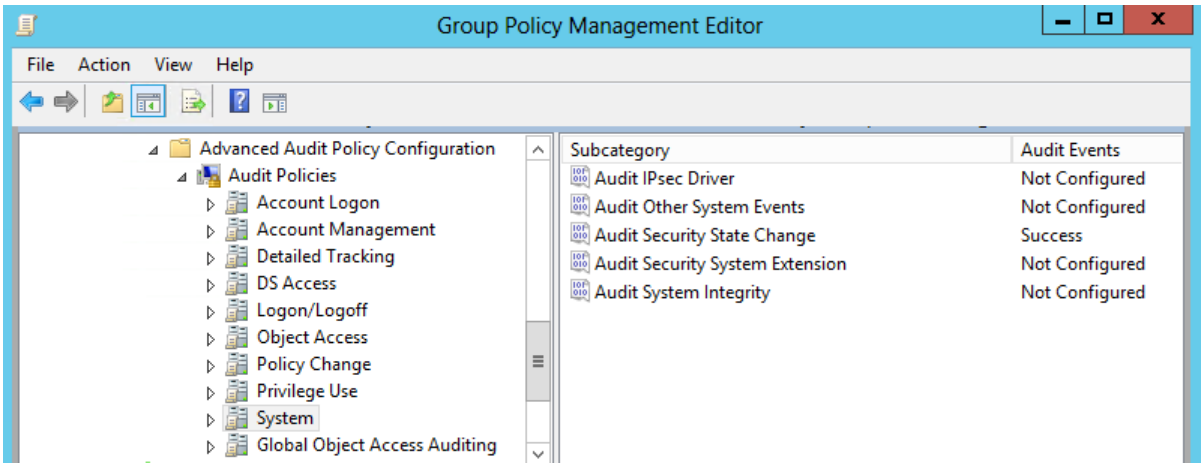


5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

To configure advanced audit policies

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers 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** → **Advanced Audit Policy Configuration** → **Audit Policies** .
4. Configure the following audit policies.

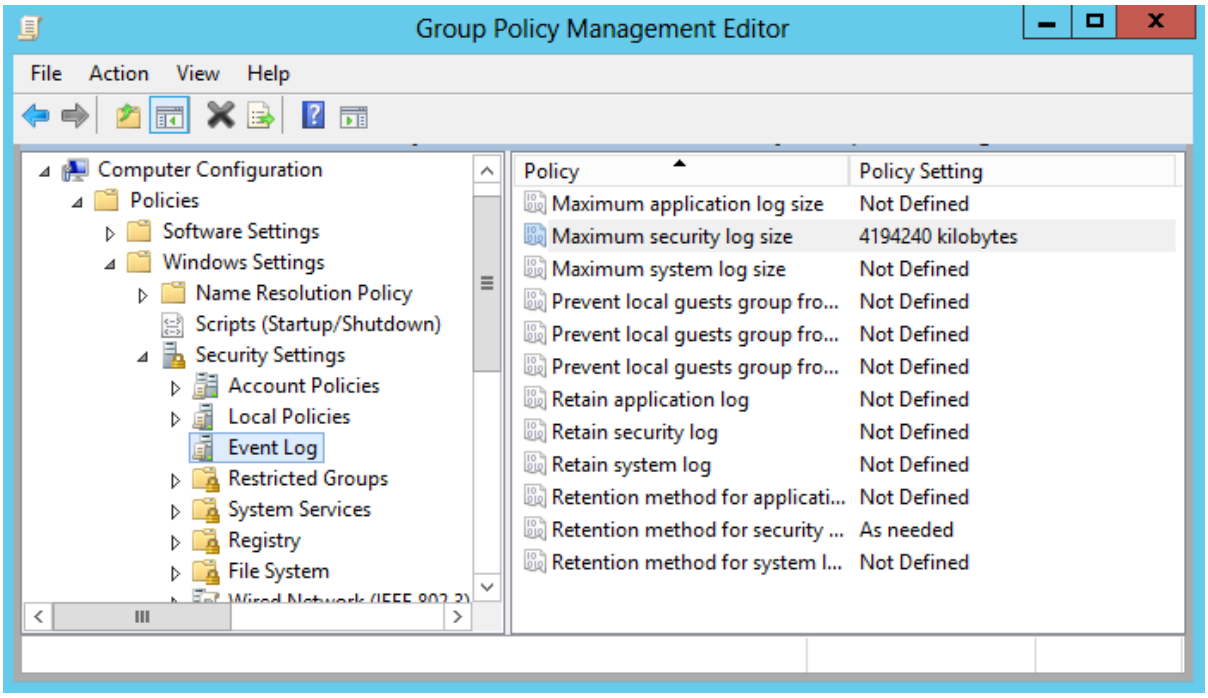
Policy Subnode	Policy Name	Audit Events
Account Logon	• **Audit Kerberos Service Ticket Operations** • **Audit Kerberos Authentication Service** • **Audit Credential Validation**	*"Success"* and *"Failure"*
Logon/Logoff	• **Audit Logoff** • **Audit Other Logon/Logoff Events**	*"Success"*
	• **Audit Logon**	"*Success*" and *"Failure"*
System	• **Audit Security State Change**	*"Success"*



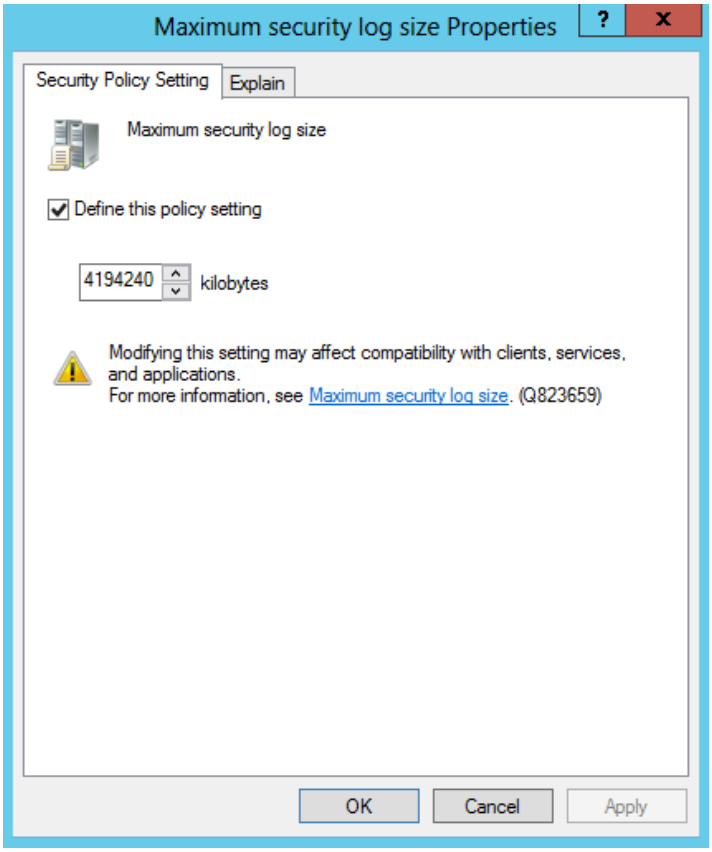
5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

4.13.3. Configure Security Event Log Size and Retention Settings

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. Navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log** and double-click the **Maximum security log size** policy.

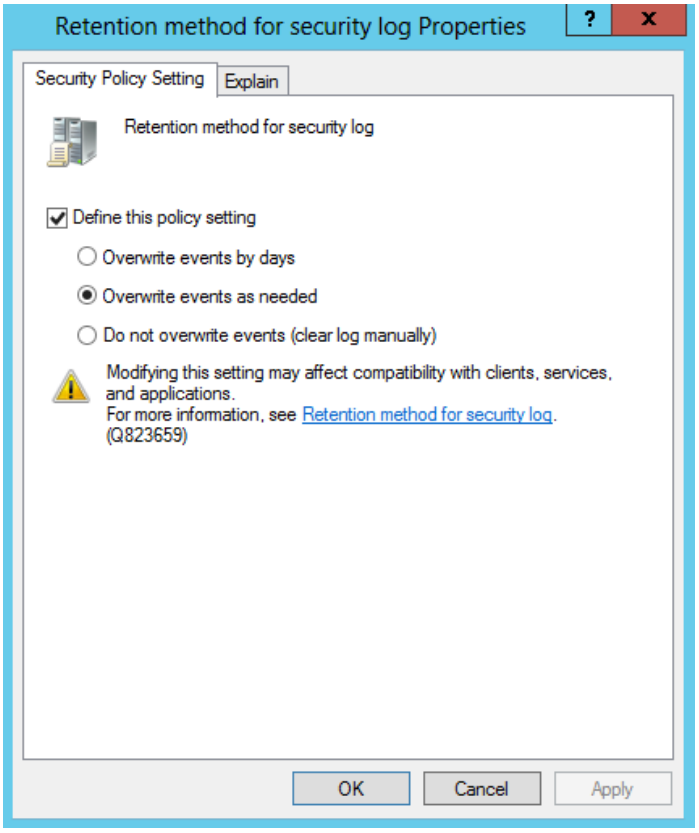


4. In the **Maximum security log size Properties** dialog, select **Define this policy setting** and set maximum security log size to *"4194240"* kilobytes (4GB).



5. Select the **Retention method for security log** policy. In the **Retention method for security log**

Properties dialog, check **Define this policy** and select **Overwrite events as needed**.

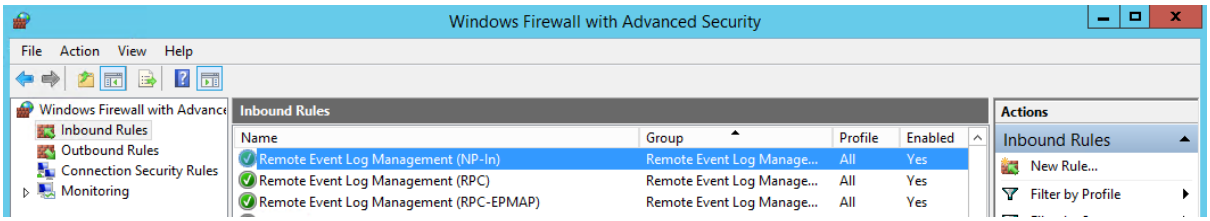


6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

4.13.4. Configure Windows Firewall Inbound Connection Rules

If you do not use the **Network traffic compression** option for data collection, configure Windows Firewall inbound rules.

1. On every domain controller, navigate to **Start** → **Control Panel** and select **Windows Firewall**.
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.



4. Enable the following inbound connection rules:
   - **Remote Event Log Management (NP-In)**
   - **Remote Event Log Management (RPC)**
   - **Remote Event Log Management (RPC-EPMAP)**

4.14. Configure Computers for Auditing User Activity

Perform the following procedures to configure computers for auditing user activity:

- Configure Data Collection Settings
- Configure Video Recordings Playback Settings

NOTE: Before configuring computers, make sure that the User Activity Core Service is installed on the audited computers. See Install Netwrix Auditor User Activity Core Service for more information.

4.14.1. Configure Data Collection Settings

To successfully track user activity, make sure that the following settings are configured on the audited computers and on the computer where Netwrix Auditor Administrator Console is installed:

- The **Windows Management Instrumentation** and the **Remote Registry** services are running and their **Startup Type** is set to *"Automatic"*. See To check the status and startup type of Windows services for more information.
- The **File and Printer Sharing** and the **Windows Management Instrumentation** features are allowed to communicate through Windows Firewall. See To allow Windows features to communicate through Firewall for more information.
- Local TCP Port 9004 is opened for inbound connections on the computer where Netwrix Auditor is installed. This is done automatically on the product installation.
- Local TCP Port 9003 is opened for inbound connections on the audited computers. See To open Local TCP Port 9003 for inbound connections for more information.
- Remote TCP Port 9004 is opened for outbound connections on the audited computers. See To open Remote TCP Port 9004 for outbound connections for more information.

To check the status and startup type of Windows services

1. Navigate to **Start** → **Administrative Tools** → **Services**.
2. In the **Services** snap-in, locate the **Remote Registry** service and make sure that its status is *"Started"* (on pre-Windows Server 2012 versions) and *"Running"* (on Windows Server 2012 and above). If it is not, right-click the service and select **Start** from the pop-up menu.

3. Check that the **Startup Type** is set to *"Automatic"*. If it is not, double-click the service. In the **Remote Registry Properties** dialog, in the **General** tab, select *"Automatic"* from the drop-down list.
4. Perform the steps above for the **Windows Management Instrumentation** service.

To allow Windows features to communicate through Firewall

1. Navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Allow a program or feature through Windows Firewall** on the left.
3. In the **Allow an app or feature through Windows Firewall** page that opens, locate the **File and Printer Sharing** feature and make sure that the corresponding checkbox is selected under **Domain**.
4. Repeat step 3 for the **Windows Management Instrumentation (WMI)** feature.

To open Local TCP Port 9003 for inbound connections

1. On a target computer navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
4. Click **New Rule**. In the **New Inbound Rule** wizard, complete the steps as described below.

Option	Setting
Rule Type	**Program**
Program	Specify the path to the Core Service. By default, *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Core Service\UAVRAgent.exe*.
Action	**Allow the connection**
Profile	Applies to **Domain**
Name	Rule name, for example **UA Core Service inbound rule**.

5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:
   - Set **Protocol** type to *"TCP"*.
   - Set **Local port** to *"Specific Ports"* and specify to *"9003"*.

To open Remote TCP Port 9004 for outbound connections

1. On a target computer, navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
4. Click **New Rule**. In the **New Inbound Rule** wizard, complete the steps as described below:

Option	Setting
Rule Type	**Program**
Program	Specify the path to the Core Service. By default, *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Core Service\UAVRAgent.exe*.
Action	**Allow the connection**
Profile	Applies to **Domain**
Name	Rule name, for example **UA Core Service outbound rule**.

5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:
   - Set **Protocol** type to *"TCP"*.
   - Set **Remote port** to *"Specific Ports"* and specify to *"9004"*.

4.14.2. Configure Video Recordings Playback Settings

Video recordings of users' activity can be watched both in Netwrix Auditor Administrator Console and the Netwrix Auditor client. Recordings are also available as links in web-based reports and email-based Activity Summaries.

To be able to watch video files captured by Netwrix Auditor, the following settings must be configured:

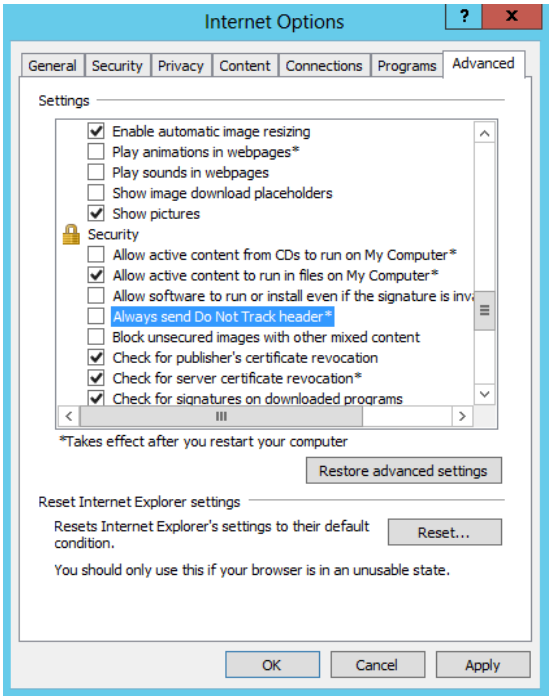
- Microsoft Internet Explorer 7.0 and above must be installed and ActiveX must be enabled.
- Internet Explorer security settings must be configured properly. See To configure Internet Explorer security settings for more information.
- JavaScript must be enabled. See To enable JavaScript for more information.
- Internet Explorer Enhanced Security Configuration (IE ESC) must be disabled. See To disable Internet Explorer Enhanced Security Configuration (IE ESC) for more information.
- The user must belong to the **Netwrix Auditor Client Users** group that has access to the **Netwrix_**

UAVR$ shared folder where video files are stored. Both the group and the folder are created automatically by Netwrix Auditor. See To add an account to Netwrix Auditor users for more information.

- A dedicated codec must be installed. This codec is installed automatically on the computer where Netwrix Auditor is deployed, and on the monitored computers. To install it on a different computer, download it from http:/www.Netwrix.com/download/ScreenPressorNetwrix.zip.
- The **Ink and Handwriting Services**, **Media Foundation**, and **Desktop Experience** Windows features must be installed on the computer where Netwrix Auditor Administrator Console is deployed. These features allow enabling Windows Media Player and share video recordings via DLNA. See To enable Windows features for more information.

To configure Internet Explorer security settings

1. In **Internet Explorer**, navigate to **Tools** → **Internet Options**.
2. Switch to the **Security** tab and select **Local Intranet**. Click **Custom Level**.
3. In the **Security Settings – Local Intranet Zone** dialog, scroll down to **Downloads**, and make sure **File download** is set to *"Enable"*.
4. In the **Internet Options** dialog switch to the **Advanced** tab.
5. Scroll down to **Security** and make sure **Allow active content to run in files on My Computer** is selected.



To enable JavaScript

1. In **Internet Explorer**, navigate to **Tools** → **Internet Options**.
2. Switch to the **Security** tab and select **Internet**. Click **Custom Level**.
3. In the **Security Settings – Internet Zone** dialog, scroll down to **Scripting** and make sure **Active scripting** is set to *"Enable"*.

To disable Internet Explorer Enhanced Security Configuration (IE ESC)

1. Navigate to **Start** → **Administrative Tools** → **Server Manager**.
2. In the **Security Information** section, click the **Configure IE ESC** link on the right and turn it off.

To enable Windows features

Depending on your Windows Server version, do one of the following:

- If Netwrix Auditor Administrator Console is installed on Windows Server 2008 R2:
  1. Navigate to **Start** → **Server Manager**.
  2. Navigate to **Server Manager <your_computer_name>** → **Features** and click **Add features**.
  3. In the **Add Features Wizard**, select the following Windows features:
     - **Ink and Handwriting Services**
     - **Desktop Experience**

     Follow the installation prompts.
  4. Restart your computer to complete features installation.
- If Netwrix Auditor Administrator Console is installed on Windows Server 2012 and above:
  1. Navigate to **Start** → **Server Manager**.
  2. In the **Server Manager** window, click **Add roles and features**.
  3. On the **Select Features** step, select the following Windows features:
     - **Ink and Handwriting Services**
     - **Media Foundation**
     - **User Interface and Infrastructure** → **Desktop Experience**.

     Follow the installation prompts.

     NOTE: If you have Windows corruption errors when installing **Windows Media Foundation**, run the **Deployment Image Servicing and Management (DISM)** tool from the command prompt with administrative rights. For detailed information, refer to the

Microsoft article: Fix Windows corruption errors by using the DISM or System Update Readiness tool.

4. Restart your computer to complete features installation.

5. Configure Netwrix Auditor Roles

Role-based system within Netwrix Auditor ensures that only relevant users have access to sensitive audit data and ability to change configuration and settings that affect data collection and auditing scope. The following roles are distinguished within Netwrix Auditor:

Role	Description
Netwrix Auditor administrator	A user account who can run Netwrix Auditor Administrator Console, configure Managed Objects, update SMTP and Audit Database settings. Administrator also has access to audit data via the Netwrix Auditor client. See Configure Netwrix Auditor Administrator Rights and Permissions for more information.
Netwrix Auditor user	A user who can run the Netwrix Auditor client, perform searches on audit data and generate reports. See Configure Netwrix Auditor User Rights and Permissions for more information.
Data Processing Account	An account used by Netwrix Auditor to collect audit data from the target systems.
Audit Database service account	An account used by Netwrix Auditor to write collected audit data to the Audit Database. See Configure Audit Database Service Account for more information.
SSRS service account	An account used by Netwrix Auditor to upload data to the Report Server. See Configure SSRS Service Account for more information.

5.1. Configure Netwrix Auditor Administrator Rights and Permissions

A user who installed Netwrix Auditor automatically is assigned Netwrix Auditor administrator permissions and has full access to both Netwrix Auditor Administrator Console and the Netwrix Auditor client functionality. This role should be assigned to a very limited number of employees—typically, only the owner of the Netwrix Auditor host in your environment.

If you want other users to be able to access Netwrix Auditor Administrator Console, they must be members of the local **Netwrix Auditor Administrators** and **Administrators** groups.

To add an account to Netwrix Auditor administrators

1. On the computer where Netwrix Auditor Administrator Console is installed, start the **Local Users and Computers** snap-in.
2. Navigate to the **Groups** node and locate the **Netwrix Auditor Administrators** group.
3. In the **Netwrix Auditor Administrators Properties** dialog, click **Add**.
4. Specify users you want to be included in this group.
5. Locate the **Administrators** group and add users there.

5.2. Configure Netwrix Auditor User Rights and Permissions

Users who want to access audit data, run AuditIntelligence searches and generate reports in the Netwrix Auditor client must be:

- Members of the local **Netwrix Auditor Client Users** group on the computer where Netwrix Auditor Server resides. See To add an account to Netwrix Auditor users for more information.
- Granted the **Browser** role on the Report Server/specific reports on the Report Server. See To assign the Browser role to a user for more information.
- Granted the **Read** permission on file shares where report subscriptions will be saved. See To assign Read permission on a shared folder where report subscriptions will be stored for more information.

  NOTE: Report subscriptions are saved to file shares\Netwrix Auditor host under the Default Data Processing Account, but users who are going to access them must be granted read access to these shares. It is recommended to create a dedicated folder and grant access to the entire **Netwrix Auditor Client Users** group.

It is recommended to grant read access only to those employees who deal with data collected across all audited systems, such as IT managers, security officers and internal auditors. Granting read permissions to a significant number of employees may lead to uncontrollable audit data distribution.

To add an account to Netwrix Auditor users

1. On the computer where Netwrix Auditor Administrator Console is installed, start the **Local Users and Computers** snap-in.
2. Navigate to the **Groups** node and locate the **Netwrix Auditor Client Users** group.
3. In the **Netwrix Auditor Client Users Properties** dialog, click **Add**.
4. Specify users you want to be included in this group.

To assign the Browser role to a user

1. Open the **Report Manager** URL in your web browser.
2. Navigate to one of the following locations:

To grant access to...	Navigate to...
All reports	On the **Home** page, navigate to **Folder Settings** and click **New Role Assignment** (the path can slightly vary depending on your SQL Server version).
Reports on a certain audited system	Navigate to the report folder you want to grant access to select **Folder Settings**, select the **Security** tab and click **Edit Item Security** and then **New Role Assignment**.
Specific reports	Navigate to the folder where this report is hosted, expand a context menu and select **Security**. Click **Edit Item Security** and then **New Role Assignment**.

3. Specify an account in the following format: *domain\user*. The account must belong to the same domain where Netwrix Auditor is installed, or to a trusted domain.
4. Select **Browser**.

To assign Read permission on a shared folder where report subscriptions will be stored

NOTE: The procedure below applies to Windows Server 2012 R2 and may vary slightly depending on your OS.

1. Navigate to a folder where report subscriptions will be stored, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Sharing** tab and click **Advanced Sharing**.
3. In the **Advanced Sharing** dialog, click **Permissions**.
4. In the **Permissions for <Share_Name>** dialog, add accounts one for one or specify the **Netwrix Auditor Client Users** group, then check the **Allow** flag next to **Read**.

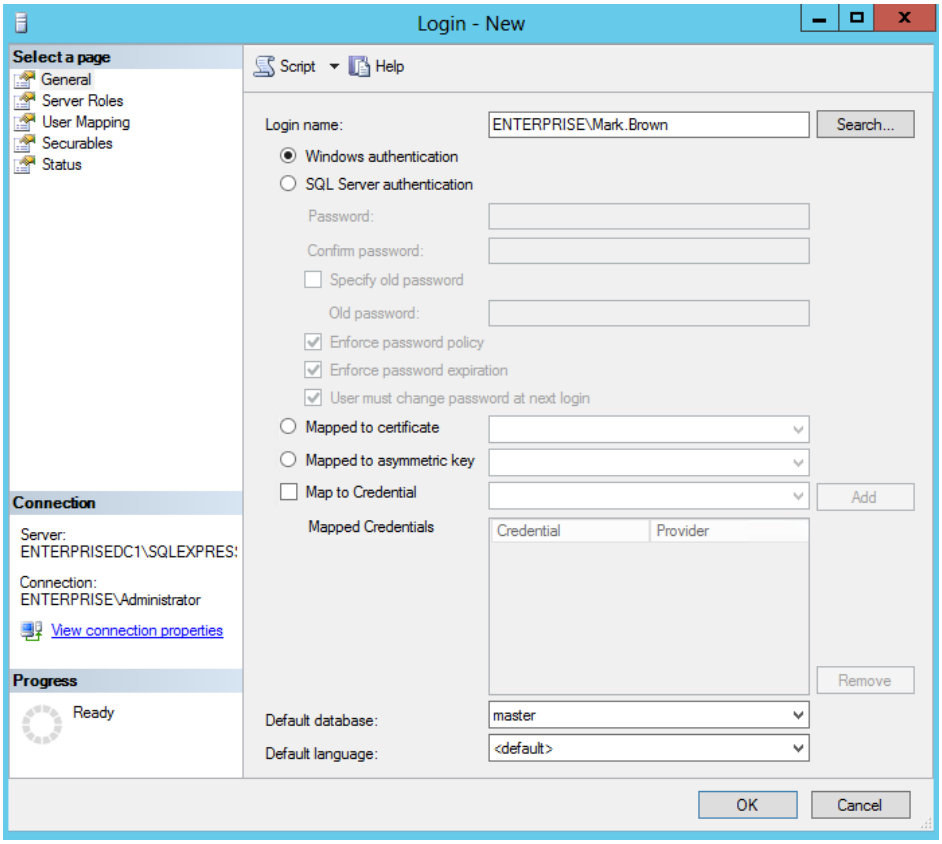
5.3. Configure Audit Database Service Account

The account used to write the collected audit data to the Audit Database must be granted **Database owner (db_owner)** role and the **dbcreator** server role on specified SQL Server instance.

To assign the dbcreator and db_owner roles

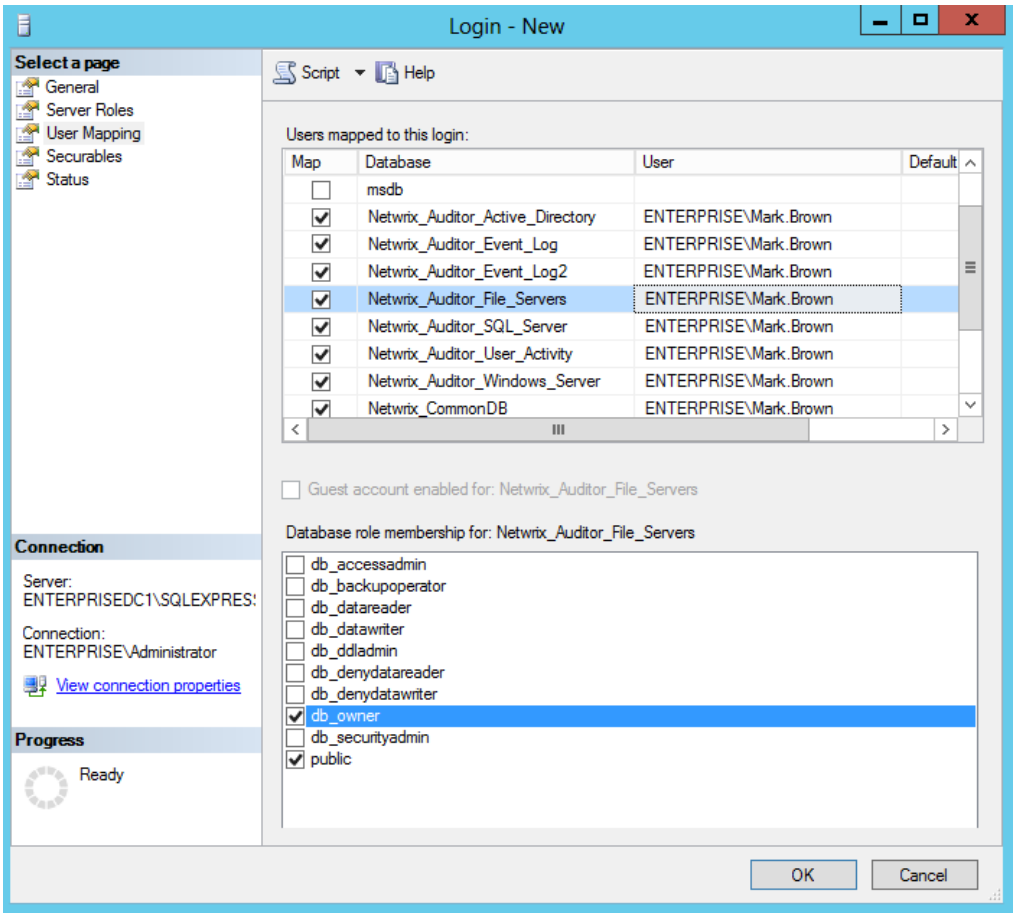
1. On the computer where audited SQL Server instance is installed, navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.

2. Connect to the server.
3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the pop-up menu.



4. Click **Search** next to **Login Name** and specify the user that you want to assign the **db_owner** role to.
5. Select **Server roles** on the left and assign the **dbcreator** role to the new login.
6. Select the **User Mapping** tab. Select all databases used by Netwrix Auditor to store audit data in the upper pane and check **db_owner** in the lower pane.

NOTE: If the account that you want to assign the **db_owner** role to has been already added to **SQL Server Logins**, expand the **Security** → **Logins** node, right-click the account, select **Properties** from the pop-up menu, and edit its roles.



5.4. Configure SSRS Service Account

An account used to upload data to the Report Server must be granted the **Content Manager** role on the SSRS Home folder.

To assign the Content Manager role

1. Navigate to your **Report Manager** URL
2. On the **Home** page, navigate to **Folder Settings** and click **New Role Assignment** (the path can slightly vary depending on your SQL Server version).
3. Specify an account in the following format: *domain\user*. The account must belong to the same domain where Netwrix Auditor is installed, or to a trusted domain.
4. Select **Content Manager**.

5.5. Configure Data Processing Account Rights and Permissions

The Data Processing Account is specified on the Managed Object creation and is used to collect audit data from the target systems.

In most cases, this account must be a member of the **Domain Admins** group, provided that the workstation with Netwrix Auditor installed and the audited system belong to the same domain.

If the computer where Netwrix Auditor is installed and the audited system belong to different workgroups or domains, the audited system must have accounts with the same name and password as the account under which Netwrix Auditor runs. All these accounts must belong to the **local Administrators** groups.

To ensure successful data collection the Data Processing Account must comply with the following requirements depending on the audited system.

Audited system	Rights and permissions
Active Directory	• A member of the **Domain Admins** group / the **Manage auditing and security log** policy must be defined for this account • The **Log on as a batch job** policy must be defined for this account—is applied automatically • A member of the **local Administrators** group on the computer where the product is installed • The **Read** rights to the Active Directory **Deleted Objects** container • If event logs autobackup is enabled: permissions to the following registry key on each domain controller in the target domain: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* AND a member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators** • If event logs autobackup is enabled: the **Share Read** and **Write** permissions and the **Security Full control** permissions for the logs backup folder • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.

Audited system	Rights and permissions
Exchange	• A member of the **Domain Admins** group / The **Manage auditing and security log** policy defined for this account • The **Log on as a batch job** policy defined for this account—is applied automatically • A member of the **local Administrators** group on the computer where the product is installed • The account must belong to the **Organization Management** or **Records Management** group / the **Audit Logs management** role must be assigned to this account (only required if the audited AD domain has an Exchange organization running Exchange 2010 or 2013). • The **Read** rights on the Active Directory **Deleted Objects** container • If event logs autobackup is enabled: permissions to the following registry key on each DC in the target domain: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* AND the member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators** • If event logs autobackup is enabled: the**Share Read** and **Write** permissions and **Security Full control** permissions for the logs backup folder • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
Exchange Online	***On the computer where Netwrix Auditor Administrator Console is installed:*** • A member of the **local Administrators** group • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to

Audited system	Rights and permissions

	file servers under the Default Data Processing Account.
	
	On the target server:
	• To connect to Exchange Online, your personal Microsoft account must be assigned the following Exchange admin roles:
	  • **Audit logs**
	  • **Mail Recipients**
	  • **View-Only Configuration**

Windows File Servers	• A member of the **local Administrators** group If the computer where the product is installed and the audited servers belong to different domains, the target computers must have accounts with the same name and password as the Data Processing Account. All these accounts must be assigned the **local Administrators** permissions. • The **Log on as a batch job** policy must be defined for this account • The **Manage auditing and security log** policy must be defined for this account on a file server • The **Read** share permission on the audited shared folders • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
EMC Isilon	*On the computer where Netwrix Auditor Administrator Console is installed:* • A member of the **local Administrators** group • The **Log on as a batch job** policy defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to

Audited system	Rights and permissions
	file servers under the Default Data Processing Account. *On the target server:* **NOTE:** This is only required if you are going to configure EMC Isilon for auditing manually. • A member of the **BUILTIN\Administrators** group • The **Read** permissions on to the audited shared folders • The **Read** permissions on to the folder where audit events are logged (*/ifs/.ifsvar/audit/*) • To connect to **EMC Isilon**, an account must be assigned a custom role (e.g., netwrix_audit) that has the following privileges: Platform API (ISI_PRIV_LOGIN_PAPI) readonly Auth (ISI_PRIV_AUTH) readonly Audit (ISI_PRIV_AUDIT) readonly Backup (ISI_PRIV_IFS_BACKUP) readonly **NOTE:** An account used to connect to a cluster put into compliance mode must comply with some specific requirements.
EMC Celerra/ VNX/VNXe	*On the computer where Netwrix Auditor Administrator Console is installed:* • A member of the **local Administrators** group • The **Log on as a batch job** policy defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account. *On the target server:* • The **Read** share permissions on to the audited shared folders • A member of **local Administrators** group

Audited system	Rights and permissions

NetApp Filer	***On the computer where Netwrix Auditor Administrator Console is installed:***
	• A member of the **local Administrators** group
	• The **Log on as a batch job** policy must be defined for this account
	• The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*)
	• The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved
	NOTE: Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
	On the target server:
	• The **Read** share permission on the audited shared folders
	• To connect to **NetApp Data ONTAP 7** or **Data ONTAP 8 in 7-mode**, an account must have the following capabilities:
	  • login-http-admin
	  • api-vfiler-list-info
	  • api-volume-get-root-name
	  • api-system-cli
	  • api-options-get
	  • cli-cifs
	• To connect to **NetApp Cluctered Data ONTAP 8**, an account must be assigned a custom role (e.g., fsa_ role) on SVM that has the following capabilities with access query levels:
	  • version readonly
	  • volume readonly
	  • vserver audit readonly
	  • vserver audit rotate-log all
	  • vserver cifs share readonly
	NOTE: You can also assign the builtin **vsadmin** role.
	If you want to authenticate with AD user account, you must enable it to

Audited system	Rights and permissions
	access SVM through ONTAPI. The credentials are case sensitive.
SharePoint	***Required for Netwrix Auditor to function properly:*** • A member of the **local Administrators** group • A member of the **Domain Users** group • The **Log on as a service** policy must be defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account. ***Required for the automatic installation of Netwrix Auditor for SharePoint Core Service:*** • A member of the **local Administrators** group on SharePoint server, where the Core Service will be deployed • The **SharePoint_Shell_Access** role on the SharePoint SQL Server configuration database
SQL Server	• A member of the **local Administrators** group • The **System Administrator** role on the target SQL Server If the computer where the product is installed and the audited SQL Server belong to different domains, the audited servers must have accounts with the same name and password as the Data Processing Account. This account must be granted the **System Administrator** role on the audited SQL Server and be a member of the **local Administrators** group on the computer where the product is installed. • The **Log on as a batch job** policy defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to

Audited system	Rights and permissions
	file servers under the Default Data Processing Account.
VMware	• A member of the **local Administrators** group • At least **Read-only** role on the audited hosts • The **Log on as a batch job** policy defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
Windows Server (including DNS)	• A member of the **local Administrators** group If the computer where the product is installed and the audited servers belong to different domains, the target computers must have accounts with the same name and password as the Data Processing Account. All these accounts must be assigned the **local Administrators** permissions. • The **Log on as a batch job** policy defined for this account • The **Manage auditing and security log** policy must be defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
Event Log (including Cisco, IIS)	• A member of the **local Administrators** group • The **Log on as a batch job** policy must be defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved

Audited system	Rights and permissions
	NOTE: Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
Group Policy	• A member of the **Domain Admins** group / **Manage auditing and security log** policy defined for this account • The **Log on as a batch job** policy defined for this account—is applied automatically • The **Read** rights on the Active Directory **Deleted Objects** container • If event logs autobackup is enabled: permissions to the following registry key on each domain controller in the target domain: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* AND a member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators** • If event logs autobackup is enabled: the **Share Read** and **Write** permissions and the **Security Full control** permissions for the logs backup folder • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
Inactive Users in Active Directory	• A member of the **Domain Admins** group • The **Log on as a batch job** policy must be defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*)
Logon Activity	• A member of the **local Administrators** group • If network traffic compression disabled: the **Manage auditing and security log** policy must be defined for this account • If network traffic compression enabled: the account must belong to the **Domain Admins** group • The account must belong to one of the following domain groups: **Backup**

Audited system	Rights and permissions
	Operators or **Server Operators** (only if the account is not a member of the **Domain Admins** group). • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.
Password Expiration in Active Directory	• A member of the **local Administrators** group • A member of the **Domain Users** group • The **Log on as a batch job** policy must be defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*)
User Activity	• A member of the **local Administrators** group • The **Write** permission for the product logs • The **Log on as a batch job** policy defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*) • The **Change** share permission and the **Create files / Write data** folder permission on file shares where report subscriptions will be saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Default Data Processing Account.

Follow the procedures below to configure some basic Data Processing Account rights and permissions:

- Configure Manage Auditing and Security Log Policy
- Define Log On As a Batch Job Policy
- Define Log On As a Service Policy
- Assign System Administrator Role
- Grant Permissions for AD Deleted Objects Container
- Assign Permissions To Registry Key
- Add Account to Organization Management Group

- Assign Audit Logs Role To Account
- Assign SharePoint_Shell_Access Role
- Assign Change and Create files/Write Data Permissions to Upload Subscriptions to File Server
- Create Role on NetApp Clustered Data ONTAP 8 and Enable AD User Access
- Assign Audit Logs, Mail Recipients and View-Only Configuration Admin Roles to Account
- Configure Role on Your EMC Isilon Cluster

5.5.1. Configure Manage Auditing and Security Log Policy

NOTE: Perform this procedure only if the Data Processing Account does not belong to the **Domain Admins** group.

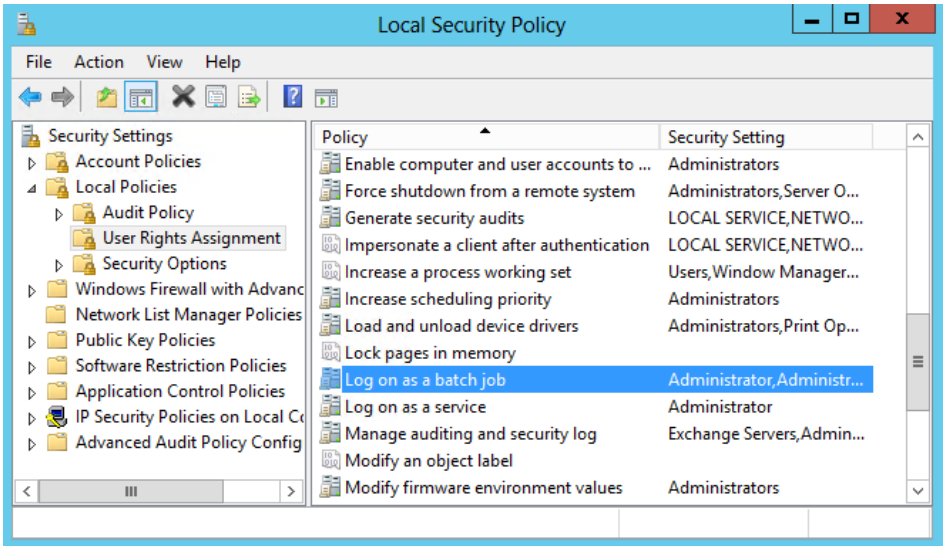
1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers 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.**
4. On the right, double-click the **User Rights Assignment** policy.
5. Locate the **Manage auditing and security log** policy and double-click it.
6. In the **Manage auditing and security log Properties** dialog, click **Add User or Group**, specify the user that you want to define this policy for.
7. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

5.5.2. Define Log On As a Batch Job Policy

On Managed Object creation, the **Log on as a batch job** policy is automatically defined for the Data Processing Account as a local security policy. However, if you have the **Deny log on as a batch job** policy defined locally or on the domain level, the local **Log on as a batch job** policy will be reset. In this case, redefine the **Deny log on as a batch job** policy through the **Local Security Policy** console on your computer or on the domain level through the **Group Policy Management** console.

1. On the computer where Netwrix Auditor is installed, open the **Local Security Policy** snap-in: navigate to **Start** → **All Programs** → **Administrative Tools** and select **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **User Rights Assignment** and locate the **Log on**

as a batch job policy.



3. Double-click the **Log on as a batch job** policy, and click **Add User or Group**. Specify the account that you want to define this policy for.

5.5.3. Define Log On As a Service Policy

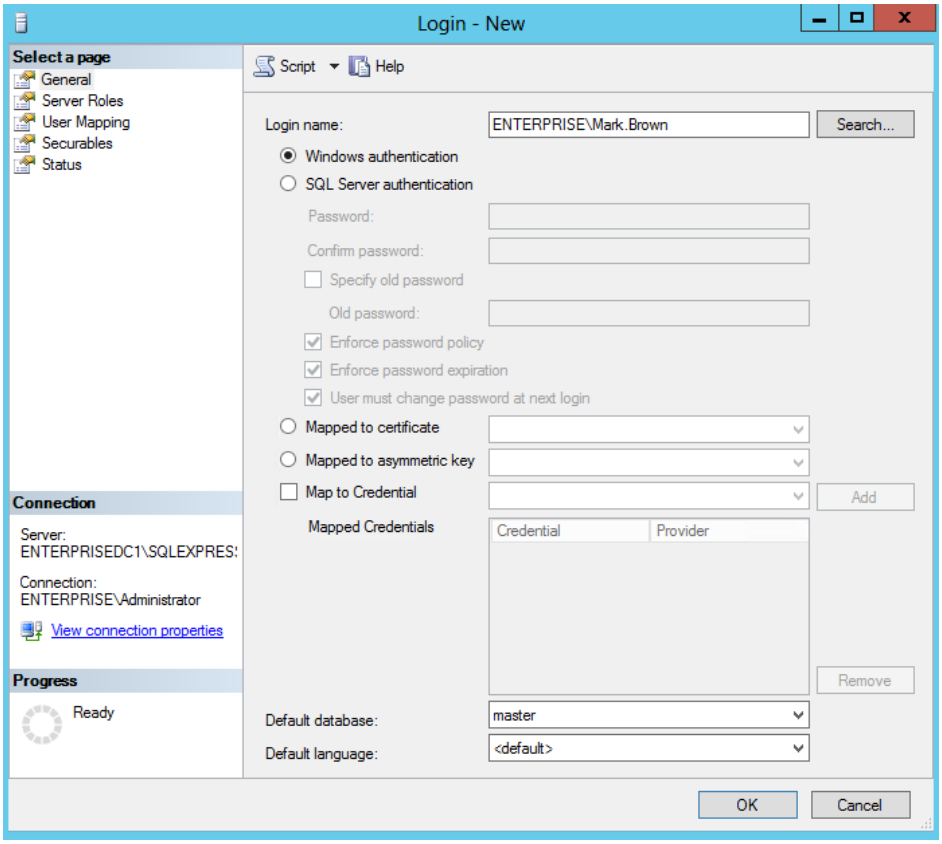
On the SharePoint Managed Object creation, the **Log on as a service** policy is automatically defined for the Data Processing Account as a local security policy. However, if you have the **Deny log on as a service** policy defined locally or on the domain level, the local **Log on as a service** policy will be reset. In this case, redefine the **Deny log on as a service** policy through the **Local Security Policy** console on your computer or on the domain level through the **Group Policy Management** console.

1. On the computer where Netwrix Auditor is installed, open the **Local Security Policy** snap-in: navigate to **Start** → **All Programs** → **Administrative Tools** and select **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **User Rights Assignment** and locate the **Log on as a service** policy.
3. Double-click the **Log on as a service** policy, and click **Add User or Group**. Specify the account that you want to define this policy for.

5.5.4. Assign System Administrator Role

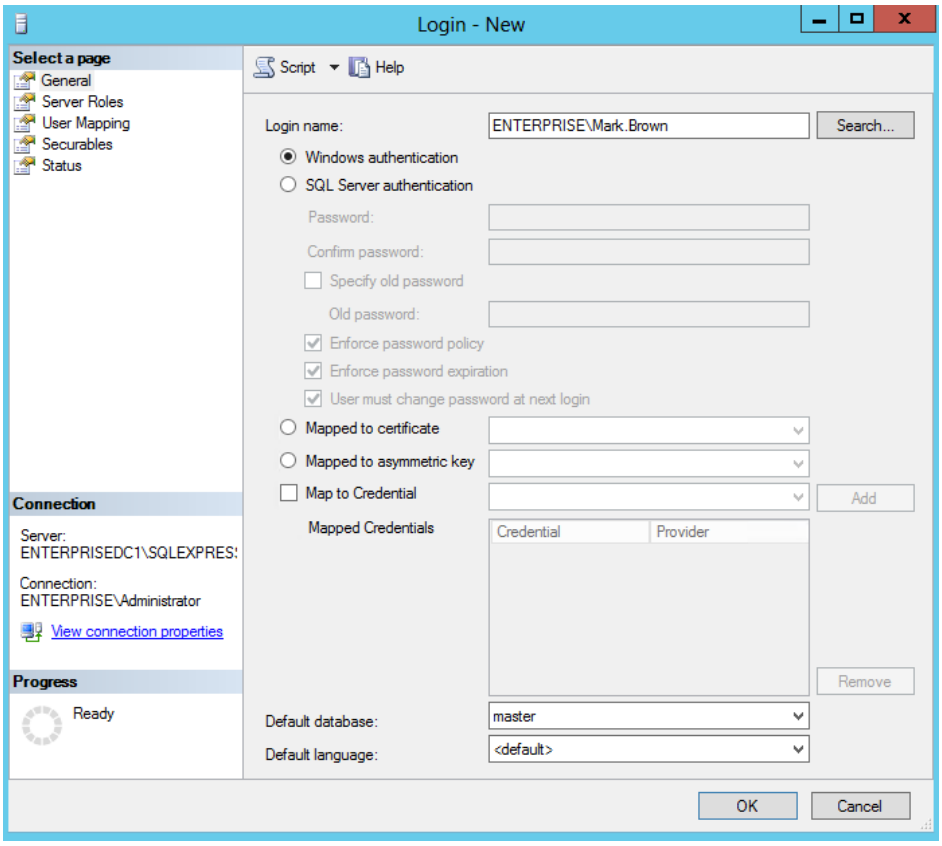
1. On the computer where audited SQL Server instance is installed, navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.
2. Connect to the server.
3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from

the pop-up menu.



4. Click **Search** next to **Login Name** and specify the user that you want to assign the **sysadmin** role to.
5. Specify the **Server roles** tab and assign the **sysadmin** role to the new login.

1. On the computer where audited SQL Server instance is installed, navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.
2. Connect to the server.
3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the pop-up menu.



4. Click **Search** next to **Login Name** and specify the user that you want to assign the **sysadmin** role to.
5. Specify the **Server roles** tab and assign the **sysadmin** role to the new login.

5.5.5. Grant Permissions for AD Deleted Objects Container

NOTE: Perform this procedure only if the Data Processing Account does not belong to the **Domain Admins** group.

1. Log on to any domain controller in the target domain with a user account that is a member of the **Domain Admins** group.
2. Navigate to **Start** → **Run** and type *"cmd"*.
3. Input the following command: `dsacls <deleted_object_dn> /takeownership`

   where `deleted_object_dn` is the distinguished name of the deleted directory object.

   For example: `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /takeownership`
4. To grant permission to view objects in the **Deleted Objects** container to a user or a group, type the following command: `dsacls <deleted_object_dn> /G <user_or_group>:<Permissions>`

where `deleted_object_dn` is the distinguished name of the deleted directory object and `user_or_group` is the user or group for whom the permission applies, and `Permissions` is the permission to grant.

For example, `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /G Corp\jsmith:LCRP`

In this example, the user CORP\jsmith has been granted **List Contents** and **Read Property** permissions for the **Deleted Objects** container in the **corp.local** domain. These permissions let this user view the contents of the **Deleted Objects** container, but do not let this user make any changes to objects in this container. These permissions are equivalent to the default permissions that are granted to the **Domain Admins** group.

1. Log on to any domain controller in the target domain with a user account that is a member of the **Domain Admins** group.
2. Navigate to **Start** → **Run** and type *"cmd"*.
3. Input the following command: `dsacls <deleted_object_dn> /takeownership`

   where `deleted_object_dn` is the distinguished name of the deleted directory object.

   For example: `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /takeownership`
4. To grant permission to view objects in the **Deleted Objects** container to a user or a group, type the following command: `dsacls <deleted_object_dn> /G <user_or_group>:<Permissions>`

   where `deleted_object_dn` is the distinguished name of the deleted directory object and `user_or_group` is the user or group for whom the permission applies, and `Permissions` is the permission to grant.

   For example, `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /G Corp\jsmith:LCRP`

   In this example, the user CORP\jsmith has been granted **List Contents** and **Read Property** permissions for the **Deleted Objects** container in the **corp.local** domain. These permissions let this user view the contents of the **Deleted Objects** container, but do not let this user make any changes to objects in this container. These permissions are equivalent to the default permissions that are granted to the **Domain Admins** group.

5.5.6. Assign Permissions To Registry Key

NOTE: Perform this procedure only if the Data Processing Account does not belong to the **Domain Admins** group. This procedure must be performed on each domain controller in the audited domain. If your domain contains multiple domain controllers, you may prefer a different method, for example assigning permissions through Group Policy.

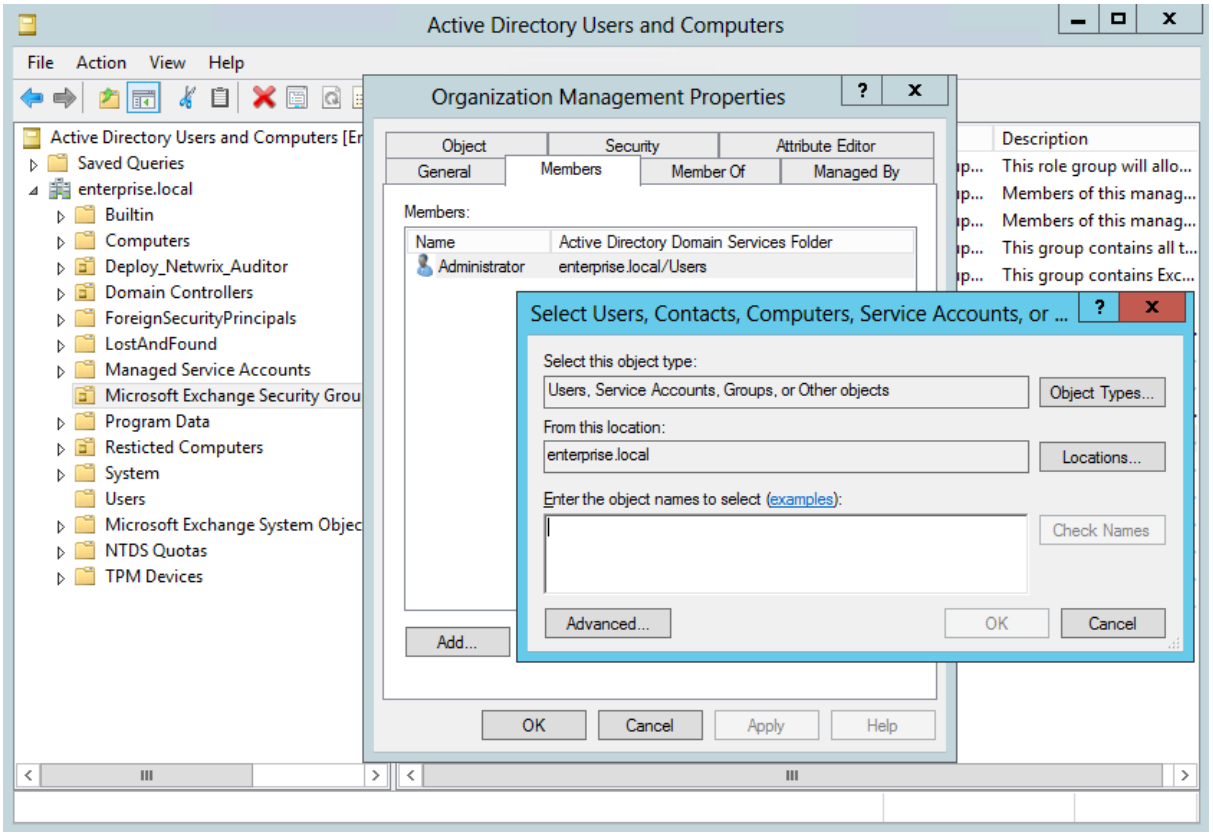
1. On your target server, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
2. In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security*. Right-click the **Security** node and select **Permissions** from the pop-up

menu.

3. Click **Add** and enter the name of the user that you want to grant permissions to.
4. Check **Allow** next to the **Read** permission.

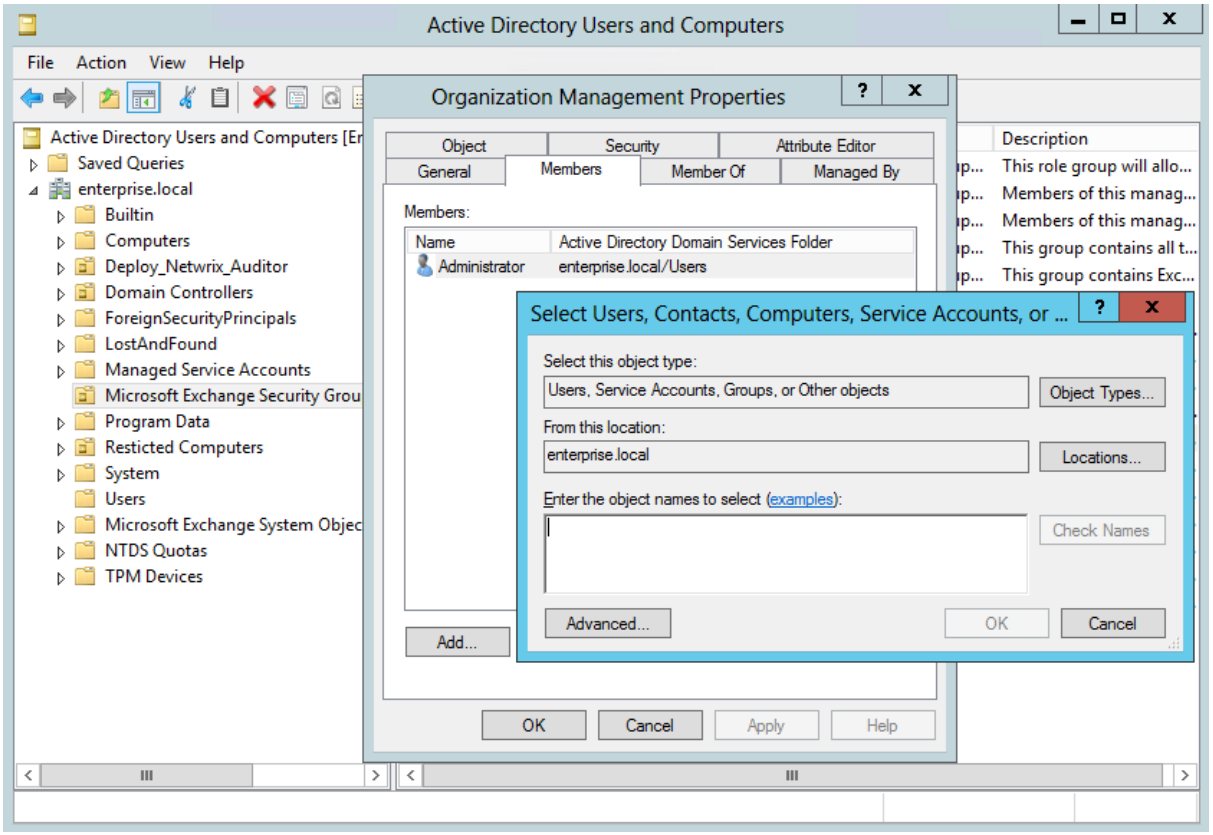
5.5.7. Add Account to Organization Management Group

1. Navigate to **Start** → **Active Directory Users and Computers** on any domain controller in the root domain of the forest where Microsoft Exchange 2010 or 2013 is installed.
2. In the left pane, navigate to **<domain_name>** → **Microsoft Exchange Security Groups**.
3. On the right, locate the **Organization Management** group and double-click it.
4. In the **Organization Management Properties** dialog that opens, select the **Members** tab and click **Add**.



NOTE: If for some reason you do not want this account to belong to the **Organization Management** group, you can add it to the **Records Management** group in the same way. The **Records Management** group is less powerful, and accounts belonging to it have fewer rights and permissions.

1. Navigate to **Start** → **Active Directory Users and Computers** on any domain controller in the root domain of the forest where Microsoft Exchange 2010 or 2013 is installed.
2. In the left pane, navigate to **<domain_name>** → **Microsoft Exchange Security Groups**.
3. On the right, locate the **Organization Management** group and double-click it.
4. In the **Organization Management Properties** dialog that opens, select the **Members** tab and click **Add**.



NOTE: If for some reason you do not want this account to belong to the **Organization Management** group, you can add it to the **Records Management** group in the same way. The **Records Management** group is less powerful, and accounts belonging to it have fewer rights and permissions.

5.5.8. Assign Audit Logs Role To Account

NOTE: Perform this procedure only if you do not want to add the Data Processing Account to the **Organization Management** or the **Records Management** group.

1. On the computer where Microsoft Exchange 2010 or 2013 is installed, open the **Exchange Management Shell** under an account that belongs to the **Organization Management** group.
2. Use the following syntax to assign the **Audit Log** role to a user:

```
New-ManagementRoleAssignment -Name <assignment name> -User <UserName> -Role
<role name>
```

For example:

```
New-ManagementRoleAssignment -Name "AuditLogsNetwrixRole" -User Corp\jsmith
-Role "Audit Logs"
```

In this example, the user CORP\jsmith has been assigned the **Audit Logs** role.

5.5.9. Assign SharePoint_Shell_Access Role

The account that runs Netwrix Auditor for SharePoint Core Service installation must be granted the **SharePoint_Shell_Access** role on SharePoint SQL Server configuration database. If you select to deploy the Netwrix Auditor for SharePoint Core Service automatically on the **Create New Managed Object** wizard completion, the installation will be performed under the Data Processing Account.

1. In your SharePoint server, click **Start** → **Microsoft SharePoint Products <version> SharePoint Management Shell**.
2. Execute the following command:

   ```
   Add-SPShellAdmin –UserName <domain\user>
   ```

5.5.10. Assign Change and Create files/Write Data Permissions to Upload Subscriptions to File Server

NOTE: The procedure below applies to Windows Server 2012 R2 and may vary slightly depending on your OS.

1. Navigate to a folder where report subscriptions will be stored, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Sharing** tab and click **Advanced Sharing**.
3. In the **Advanced Sharing** dialog, click **Permissions**.
4. In the **Permissions for <Share_Name>** dialog, select a principal or add a new, then check the **Allow** flag next to **Change**.
5. Apply settings and return to the **<Share_Name> Properties** dialog.
6. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
7. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Permissions** tab, select a principal and click **Edit**, or click **Add** to add a new one.
8. Apply the following settings to your Permission Entry.

- Specify a Netwrix Auditor user as principal.
- Set **Type** to *"Allow"*.
- Set **Applies to** to *"This folder, subfolders and files"*.
- Check **Create files / write data** in the **Advanced permissions** section.

1. Navigate to a folder where report subscriptions will be stored, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Sharing** tab and click **Advanced Sharing**.
3. In the **Advanced Sharing** dialog, click **Permissions**.
4. In the **Permissions for <Share_Name>** dialog, select a principal or add a new, then check the **Allow** flag next to **Change**.
5. Apply settings and return to the **<Share_Name> Properties** dialog.
6. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
7. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Permissions** tab, select a principal and click **Edit**, or click **Add** to add a new one.
8. Apply the following settings to your Permission Entry.
   - Specify a Netwrix Auditor user as principal.
   - Set **Type** to *"Allow"*.
   - Set **Applies to** to *"This folder, subfolders and files"*.
   - Check **Create files / write data** in the **Advanced permissions** section.

NOTE: Report subscriptions are saved to file shares\Netwrix Auditor host under the Default Data Processing Account, but users who are going to access them must be granted read access to these shares. It is recommended to create a dedicated folder and grant access to the entire **Netwrix Auditor Client Users** group.

5.5.11. Create Role on NetApp Clustered Data ONTAP 8 and Enable AD User Access

NOTE: You must be a cluster administrator to run the commands below.

1. Create a new role (e.g., fsa_role) on your SVM (e.g., vs1). For example:

   ```
   security login role create -role fsa_role -cmddirname version -access
   readonly -vserver vs1
   ```

2. Add the following capabilities to the role:
   - version readonly

- volume readonly
- vserver audit readonly
- vserver audit rotate-log all
- vserver cifs share readonly

The capabilities must be assigned one by one. For example:

```
security login role modify -role fsa_role -cmddirname version -access
readonly -vserver vs1

security login role modify -role fsa_role -cmddirname volume -access
readonly -vserver vs1

security login role modify -role fsa_role -cmddirname "vserver audit"

-access readonly -vserver vs1

security login role modify -role fsa_role -cmddirname "vserver audit
rotate-log" -access all vs1

security login role modify -role fsa_role -cmddirname "vserver cifs share"
-access readonly -vserver vs1
```

Review currently applied capabilities. For example:

```
security login role show -vserver vs1 -role fsa_role
```

3. Create a login for your Data Processing Account—an account that authenticates and collects data from NetApp. If you want to use an AD account as Data Processing Account, enable it to access SVM through ONTAPI. For example:

```
security login create -vserver vs1 -username Enterprise\Administrator

-application ontapi -authmethod domain -role fsa_role
```

where `Enterprise\Administrator` is your Data Processing Account name.

5.5.12. Assign Audit Logs, Mail Recipients and View-Only Configuration Admin Roles to Account

1. Sign in to Office 365 using your Microsoft account.
2. On the **Office 365 Home** page, click **Admin** tile and select **Admin** → **Exchange** on the left.
3. In the **Exchange admin center**, navigate to **Permissions** → **admin roles**.
4. Create a new role group. Assign the following settings to the newly created role group:

Option	Description
Name	Specify a name for the new role group (e.g., audit_logs).
Description	Enter a role group description (optionally).
Write scope	Select a write scope.
Roles	Assign the following roles: • **Audit Logs** • **Mail Recipients** • **View-Only Configuration**
Members	Add your account.

NOTE: If you already configured specific role scopes for role groups (for example, multiple management role scopes or exclusive scopes) using Shell, you cannot assign new roles to these role groups via Exchange admin center. For detailed instructions on how to configure roles using Shell, read the following Microsoft article: Manage role groups.

5.5.13. Configure Role on Your EMC Isilon Cluster

An EMC Isilon cluster can operate in one of the following modes:

- **Standard or Normal mode**
- **Smartlock Enterprise mode**
- **Smartlock Compliance mode**

For your convenience, Netwrix provides a special shell script for configuring an audited EMC Isilon cluster and granting necessary privileges to the account that is used to collect audit data. Depending on your cluster operation mode, review the following sections:

- To configure EMC Isilon cluster in Normal and Enterprise mode via shell script
- To configure EMC Isilon cluster in Compliance mode via shell script

If, for some reasons, you want to configure Data Processing Account for EMC Isilon manually, you need to perform all steps for manual audit configuration, otherwise the product will not function properly. See the following sections for more information:

- To configure EMC Isilon cluster in Normal and Enterprise mode manually
- To configure EMC Isilon cluster in Compliance mode manually

6. Upgrade and Migration

This chapter provides step-by-step instructions on how to upgrade your current version of Netwrix Auditor to the newest version available.

NOTE: Read the chapter below only if you have already installed previous versions of Netwrix Auditor in your IT infrastructure. Otherwise, refer to Install Netwrix Auditor for basic installation instructions.

Netwrix recommends to upgrade from older versions of Netwrix Auditor to 8.0 in order to take advantage of new features. Also, for your convenience, Netwrix may produce maintenance releases within the same product version. Such service releases contain a collection of updates, fixes and enhancements, delivered in the form of a single installable package. They may also implement new features.

Refer to the table below to find a relevant upgrade scenario:

Upgrade scenario
7.0 or 7.1 → NEW  Applicable to Netwrix Auditor 7.0, 7.1, and 8.0 (upgrade within the same version). No special upgrade procedures are required—simply install Netwrix Auditor8.0. During installation your Netwrix Auditor configuration and data will be preserved. • Upgrade From Netwrix Auditor 7.0 or 7.1
6.5 ↓ 7.0 or 7.1 → NEW 

Upgrade scenario

Applicable to Netwrix Auditor 7.0 or 7.1 previously upgraded from 6.5 or below.

NOTE: Upgrade from Netwrix Auditor 6.5 and below to 7.0 is a mandatory procedure, otherwise the product will not work. For detailed instructions on how to migrate to Netwrix Auditor 7.0, see Netwrix Auditor Installation and Configuration Guide 7.0 → **Upgrade from Previous Versions**.

Since you have already performed migration while upgrading to 7.0, refer to a simple upgrade procedure (upgrade through installation). Also, it is necessary to transfer your old audit data (6.5 and below) to the Long-Term Archive-compatible format using the **Netwrix AuditArchive Migration Tool**.

- Upgrade From Netwrix Auditor 7.0 or 7.1
- Migrate Legacy Data From Old Audit Archive

6.1. Upgrade From Netwrix Auditor 7.0 or 7.1

You can upgrade Netwrix Auditor 7.0 or 7.1 to 8.0 simply by running the installation package. Netwrix Auditor automatically upgrades to the latest version while preserving its configuration.

To upgrade Netwrix Auditor

1. Download Netwrix Auditor installation package.
2. Close Netwrix Auditor Administrator Console and Netwrix Auditor client.
3. Run the installation package on the computer, where Netwrix Auditor Administrator Console resides. Refer to Install the Product for detailed instructions on how to install Netwrix Auditor.
4. Once installation completes, upgrade your Audit Database. To do this, launch Netwrix Auditor Administrator Console, navigate to **AuditArchive** → **Audit Database** and then click **Upgrade**.

To upgrade Non-Owner Mailbox Access Auditing tool for Exchange

The procedure below explains how to upgrade Non-Owner Mailbox Access Auditing tool for Exchange if you run Netwrix Auditor 7.0.97 and below previously upgraded from 6.5 version.

1. Start **Task Manager** and make sure that the **NOMBA.exe** process is not running.
2. Navigate to **Start** → **Control Panel** → **Programs and Features** and remove the **Netwrix Non-owner Mailbox Access Reporter for Exchange**.
3. Run the installation package to perform an upgrade.
4. Launch **Non-Owner Mailbox Access Auditing** tool:

- In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Exchange Server** and click **Track Access** next to **Non-owner Mailbox Access Auditing** in the right pane.

OR

- Navigate to *%Netwrix Auditor installation folder%\Non-owner Mailbox Access Reporter for Exchange* and double-click the **NOMBA.exe**

5. Enter your license details when asked or you can do it later in **Netwrix Auditor Administrator Console** under the **License** node.
6. In the dialog that opens, click **Apply**.

As Non-Owner Mailbox Access Auditing tool upgrades data collection will continue with the latest changes, Change Summaries will come on the old schedule.

To complete migration for File Servers

NOTE: Perform the procedure below only if you uploaded historical state-in-time snapshots to the Audit Database. Otherwise, the "Object Permissions by Object" and "Account Permissions" reports will show no data for past states.

1. Launch Netwrix Auditor Administrator Console and navigate to **your_Managed_Object_name** → **File Servers** → **Audit Database Settings** → **State-in-Time Reports**.
2. Reload snapshots (move them from the right column to the left and back).

6.2. Migrate Legacy Data From Old Audit Archive

In 7.0, Netwrix Auditor introduced a new format for storing audit data—Long-Term Archive. For your convenience, Netwrix provides the AuditArchive Migration tool that allows you to import data from the old file-based Audit Archive (available in Netwrix Auditor 6.5 or below) to the new file-based Long-Term Archive.

NOTE: Before you begin, install Netwrix Auditor 8.0 and upgrade your configuration with **Migration Tool**.

To migrate audit data

1. In the Netwrix Auditor Administrator Console, navigate to **AuditArchive** → **Long-Term Archive** and select the **Migrate** link.
2. In the **Audit Archive Migration Tool** window, browse for your Netwrix Auditor 6.5 AuditArchive (the default path is *C:\ProgramData\NetWrix\Management Console\Data*).
3. Click **Migrate** to start the migration process. **AuditArchive Migration Tool** automatically moves your audit data to the new location.

NOTE: Depending on the amount of your Netwrix Auditor 6.5 audit data, migration may take a while to complete. You can minimize the **AuditArchive Migration Tool** screen and keep working with Netwrix Auditor.

Once migration completes, you will see a message with migration status— successful or with warnings/errors.

7. Uninstall Netwrix Auditor

7.1. Uninstall Netwrix Auditor Compression and Core Services

NOTE: Perform the procedures below if you used Compression Services and Core Services for data collection (i.e., the **Network traffic compression** option was enabled).

Some Netwrix Auditor Compression services are stopped but not removed during Netwrix Auditor uninstallation. You need to delete them manually prior to Netwrix Auditor uninstallation.

Perform the following procedures to uninstall the Netwrix Auditor Compression services:

- To delete Netwrix Auditor for Active Directory Compression Service
- To delete Netwrix Auditor for File Servers Compression Service
- To delete Netwrix Auditor for SharePoint Core Service
- To delete Netwrix Auditor for Windows Server Compression Service
- To delete Netwrix Auditor Mailbox Access Core Service
- To delete Netwrix Auditor User Activity Core Service

To delete Netwrix Auditor for Active Directory Compression Service

1. On the computer where Netwrix Auditor Administrator Console is installed, navigate to **Start** → **Run** and type *"cmd"*.
2. Execute the following command:

   ```
   Netwrix_ Auditor_ installation_ folder\Active Directory Auditing\adcr.exe
   /removecompressionservice domain=<domain name>
   ```

   where `<domain name>` is the name of the monitored domain in the FQDN format.

   NOTE: if any argument contains spaces, use double quotes.

   Example:

   ```
   "C:\Program Files\Netwrix\Active Directory Auditing\adcr.exe"
   /removecompressionservice domain=domain.local
   ```

3. To delete Compression Services from a specific domain controller, execute the following command:

   ```
   Netwrix_ Auditor_ installation_ folder\Active Directory Auditing\adcr.exe
   /removecompressionservice dc=<domain controller name>
   ```

   NOTE: if any argument contains spaces, use double quotes.

To delete Netwrix Auditor for File Servers Compression Service

NOTE: Perform this procedure only if you enable the **Network traffic compression** option for data collection.

1. On the target servers, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **Netwrix Auditor for File Servers Compression Service** and click **Uninstall**.

To delete Netwrix Auditor for SharePoint Core Service

NOTE: During the Netwrix Auditor for SharePoint Core Service installation / uninstallation your SharePoint sites may be unavailable.

1. In the audited SharePoint farm, navigate to the computer where Central Administration is installed and where the Netwrix Auditor for SharePoint Core Service resides.
2. Navigate to **Start** → **Control Panel** → **Programs and Features**.
3. Select **Netwrix Auditor for SharePoint Core Service** and click **Uninstall**.

   NOTE: Once you click **Uninstall** you cannot cancel the uninstallation. The Netwrix Auditor for SharePoint Core Service will be uninstalled even if you click **Cancel**.

To delete Netwrix Auditor for Windows Server Compression Service

NOTE: Perform this procedure only if you enabled the Compression Service for data collection.

1. On the target servers, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **Netwrix Auditor for Windows Server Compression Service** and click **Uninstall**.

To delete Netwrix Auditor Mailbox Access Core Service

1. On every computer where a monitored Exchange is installed, navigate to **Start** → **Run** and type *"cmd"*.
2. Execute the following command:

   ```
   sc delete "Netwrix Auditor Mailbox Access Core Service"
   ```

3. Remove the following folder: *%SYSTEMROOT%\Netwrix Auditor\Netwrix Auditor Mailbox Access Core Service*.

   NOTE: If any argument contains spaces, use double quotes.

To delete Netwrix Auditor User Activity Core Service

- Remove the Core Service via Netwrix Auditor Administrator Console:
  1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** in the left pane.
  2. In the right pane select the **Items** tab.
  3. Select a computer in the list and click **Remove**. The Netwrix Auditor User Activity Core Service will be deleted from the selected computer. Perform this action with other computers.
  4. In the left pane navigate to **Managed Objects** → **your_Managed_Object_name** → **User Activity** → **Monitored Computers.** Make sure that the computers you have removed from auditing are no longer present in the list.
  5. In case some computers are still present in the list, select them one by one and click **Retry Uninstallation**. If this does not help, remove the Core Services manually from the target computers through **Programs and Features**.
- Remove the Netwrix Auditor User Activity Core Service manually on each audited computer:
  1. Navigate to **Start** → **Control Panel** → **Programs and Features**.
  2. Select **Netwrix Auditor User Activity Core Service** and click **Uninstall**.

7.2. Uninstall Netwrix Auditor

NOTE: If you enabled network traffic compression for data collection, make sure to disable it before uninstalling the product. Some network compression services must be removed manually. Uninstall Netwrix Auditor Compression and Core Services

To uninstall Netwrix Auditor

1. On the computer where Netwrix Auditor is installed, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **Netwrix Auditor** and click **Uninstall**.

8. Appendix

This section contains instructions on how to install the third-party components that are not included in the Netwrix Auditor installation package, but are required for the product to function properly.

Refer to the following sections for step-by-step instructions on how to:

- Install Group Policy Management Console
- Install ADSI Edit
- Install Microsoft SQL Server
- Configure Ports for Inbound Connections

8.1. Install Group Policy Management Console

Group Policy Management Console is an administrative tool for managing Group Policy across the enterprise. If you want to audit Group Policy, Group Policy Management Console must be installed on the computer where Netwrix Auditor is deployed.

To install GPMC on Windows Server 2008 R2

1. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane, click **Add Features** and select **Group Policy Management**.
3. Click **Install** to enable it.

To install GPMC on Windows Server 2012 and above

1. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane, select **Group Policy Management**.
3. Click **Next** to proceed to confirmation page.
4. Click **Install** to enable it.

To install GPMC on Windows 7

1. Download and install **Remote Server Administration Tools** that include Group Policy Management Console.

2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Feature Administration Tools** and select **Group Policy Management Tools**.
4. Click **Install**.

To install GPMC on Windows 8

1. Download and install **Remote Server Administrator Tools** that include Group Policy Management Console.
2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Feature Administration Tools** and select **Group Policy Management Tools**.

To install GPMC on Windows 8.1

1. Download and install **Remote Server Administrator Tools** that include Group Policy Management Console.
2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Feature Administration Tools** and select **Group Policy Management Tools**.

8.2. Install ADSI Edit

The ADSI Edit utility is used to view and manage objects and attributes in an Active Directory forest. ADSI Edit is required to manually configure audit settings in the target domain. It must be installed on any domain controller in the domain you want to start auditing.

To install ADSI Edit on Windows Server 2008 and Windows Server 2008 R2

1. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane, click **Add Features**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools** .
4. Click **Next** to proceed to the confirmation page.
5. Click **Install** to enable it.

To install ADSI Edit on Windows Server 2012 and above

1. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **Next** to proceed to the confirmation page.
5. Click **Install** to enable it.

To install ADSI Edit on Windows 7

1. Download and install Remote Server Administration Tools that include ADSI Edit.
2. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **OK**.

To install ADSI Edit on Windows 8 and above

1. Download and install Remote Server Administration Tools.
2. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **OK**.

To install GPMC on Windows 8.1

1. Download and install **Remote Server Administrator Tools** that include Group Policy Management Console.
2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **OK**.

8.3. Install Microsoft SQL Server

This section provides instructions on how to:

- Install Microsoft SQL Server 2014 Express
- Verify Reporting Services Installation

8.3.1. Install Microsoft SQL Server 2014 Express

This section only provides instructions on how to install SQL Server 2014 Express with Advanced Services and configure the Reporting Services required for Netwrix Auditor to function properly. For full installation and configuration instructions, refer to Microsoft documentation.

1. Download SQL Server 2014.
2. Run the installation package and follow the instructions of the wizard until you get to the **Feature Selection** page. On this page, ensure that the **Reporting Services** option is selected under **Instance Features**.
3. Proceed with the wizard until you get to the **Server Configuration** page. On this page, ensure that the **SQL Server Reporting Services** will run under the **Network Service account**, and its startup type is set to *"Automatic"*.
4. Follow the instructions of the wizard to complete the installation.

8.3.2. Verify Reporting Services Installation

As a rule, Netwrix Auditor can use Reporting Services installed with the default settings. However, to ensure that Reporting Services is properly configured, it is recommended to perform the following procedure:

NOTE: You must be logged in as a member of the **local Administrators** group on the computer where SQL Server 2014 Express is installed.

1. Depending on SQL Server version installed, navigate to **Start** → **All Apps** → **SQL Server Reporting Services Configuration Manager**.
2. In the **Reporting Services Configuration Connection** dialog, make sure that your local report server instance (for example, *"SQLExpress"*) is selected and click **Connect**.
3. In the **Reporting Services Configuration Manager** left pane, select **Web Service URL**. Make sure that **Virtual Directory** is set to *"ReportServer_<YourSqlServerInstanceName>"* (e.g., *ReportServer_SQLEXPRESS* for *SQLEXPRESS* instance) and **TCP Port** is set to *"80"*.
4. In the **Reporting Services Configuration Manager** left pane, select **Database**. Make sure that the **SQL Server Name** and **Database Name** fields contain correct values. If the fields contain incorrect

values, click **Change Database** and complete the **Report Server Database Configuration** wizard.

5. In the **Reporting Services Configuration Manager** left pane, select **Report Manager URL**. Make sure **Virtual Directory** is set correctly, and that the URL is valid.

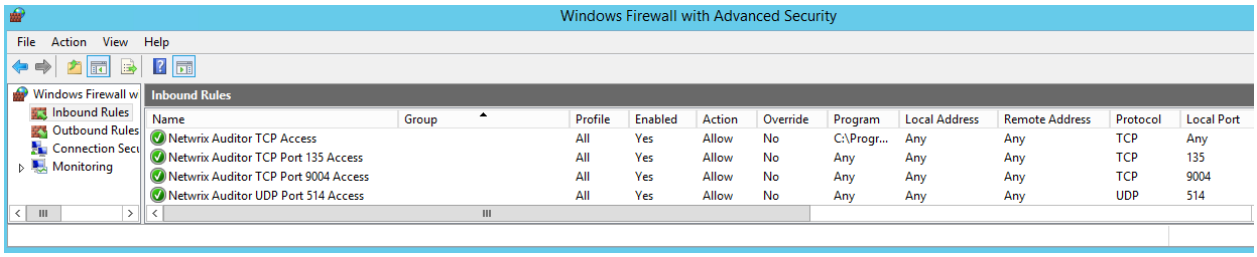
8.4. Configure Ports for Inbound Connections

The following local ports must be opened for inbound connections on the computer where Netwrix Auditor Administrator Console is installed:

- TCP 135
- TCP 9004
- UDP 514

NOTE: You do not need to open any additional ports on computers where Netwrix Auditor clients are installed.

If you are running Windows Firewall on the computer where Netwrix Auditor Administrator Console is going to be installed, these ports will be opened automatically for inbound connections after Netwrix Auditor installation. If you use a third-party firewall, you must create rules for inbound connections manually.



NOTE: Before installing Netwrix Auditor, make sure that the **Windows Firewall** service is started.

To configure rules manually

1. Start the **Windows Firewall** service.
2. Navigate to **Start** → **Control Panel** and select **Windows Firewall**.
3. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
4. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
5. Click **New Rule**. In the **New Inbound Rule** wizard, complete the following steps:
   - On the **Rule Type** step, select **Port**.
   - On the **Protocol and Ports** step, select **TCP**. In the **Specific local ports** field specify *"135"*.

- On the **Action** step, select the **Allow the connection** action.
- On the **Profile** step, make sure that the rule applies to all profiles (**Domain**, **Private**, **Public**).
- On the **Name** step, specify the rule's name, for example **Netwrix Auditor TCP port 135 Access**.

6. Repeat these steps and create inbound rules for the **UDP 514** and **TCP 9004** ports.

Index

E

G

I

L

M