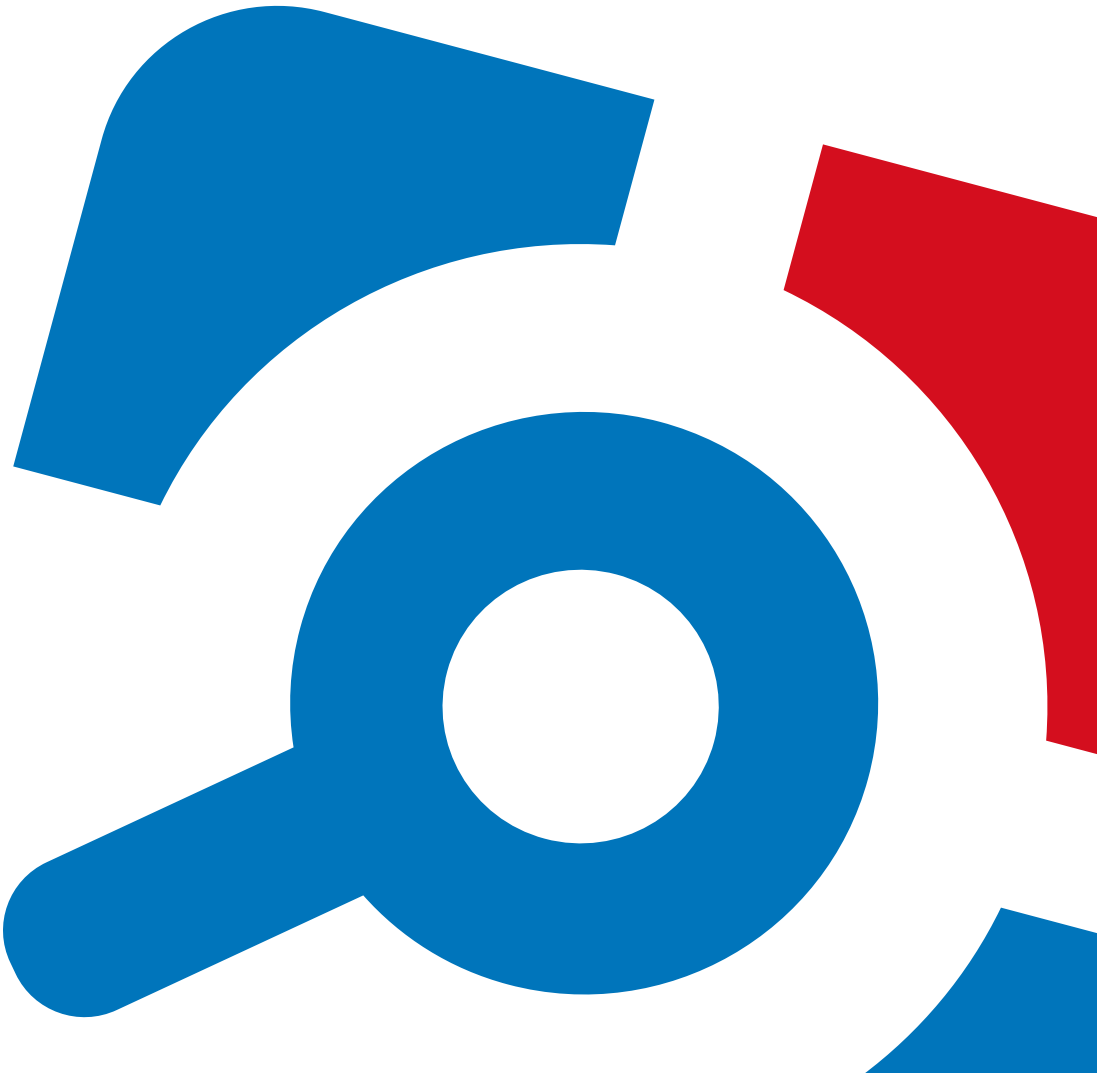
netwrix

Netwrix Auditor

Installation and Configuration Guide

Version: 9.0
7/3/2017



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 system 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 a visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments to protect sensitive data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware, and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

Major benefits:

- Detect insider threats—on premises and in the cloud
- Pass compliance audits with less effort and expense
- Increase productivity of IT security and operations teams

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

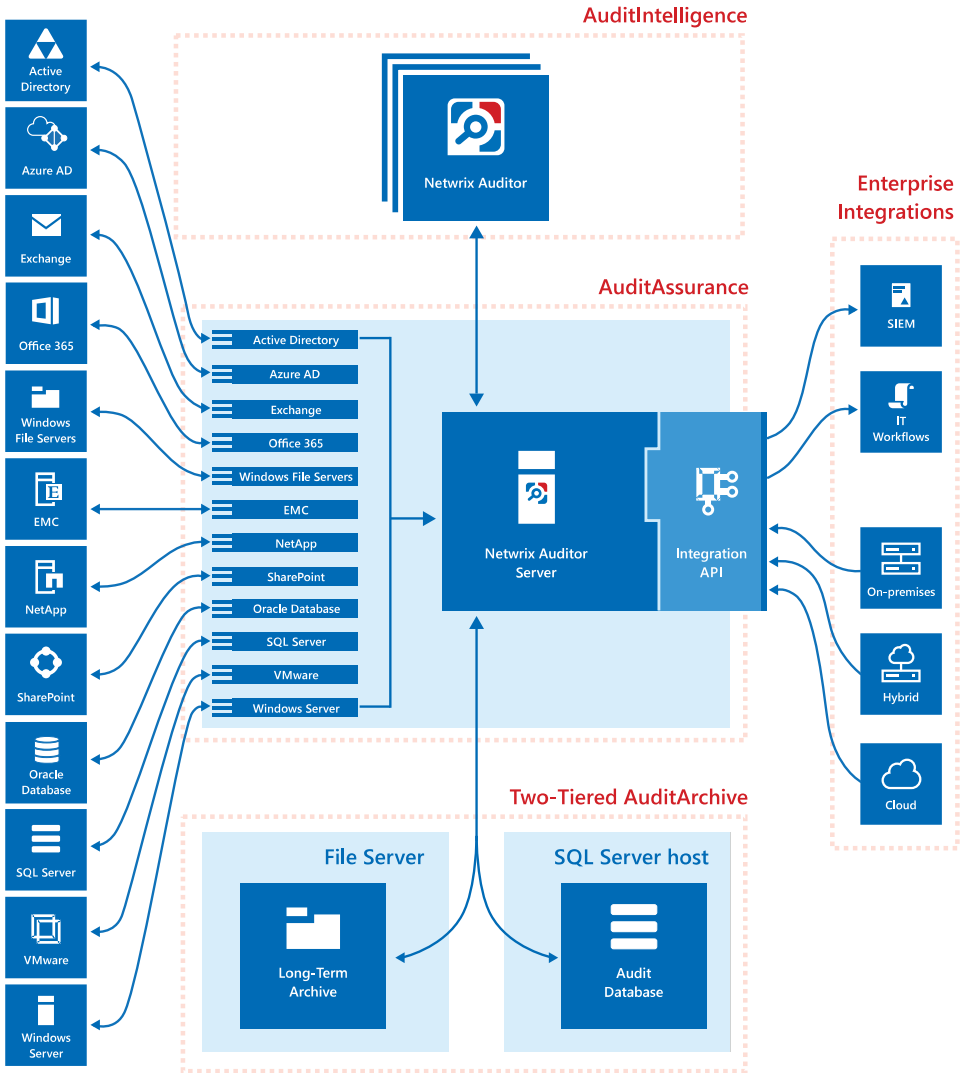
Application	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain 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 address specific tasks—detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a stand-alone Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.

Application	Features
Netwrix Auditor for Azure AD	Netwrix Auditor for Azure AD detects and reports on all changes made to Azure AD configuration and permissions, including Azure AD objects, user accounts, passwords, group membership, and more. The products also reports on successful and failed logon attempts.
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 and SharePoint Online. For Exchange Online, the product provides auditing of configuration and permissions changes. 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. For SharePoint Online, the product reports on read access and changes made to SharePoint Online sites, including modifications of content, security settings, and sharing permissions. In addition to SharePoint Online, OneDrive for Business changes are reported too.
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 VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
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 Oracle Database	Netwrix Auditor for Oracle Database detects and reports on all changes made to your Oracle Database instance configuration, privileges and security settings, including database objects and directories, user accounts, audit policies, sensitive data, and triggers.

Application	Features
	The product also reports on 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, database content, and logon activity.
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. With a stand-alone Event Log Manager tool, Netwrix Auditor collects Windows event logs 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.

1.2. How It Works

The image below provides overview of Netwrix Auditor architecture and gives a brief description of product components and incorporated technologies.



The **AuditIntelligence** technology, or simply **Intelligence**, is a brand new way of dealing with audit data, investigating incidents and enabling complete visibility across the entire IT infrastructure. **Intelligence** provides easy access to data and configuration for IT managers, business analysts and other relevant employees via a straightforward and user-friendly interface, **Netwrix Auditor client**. You can install as many **Netwrix Auditor** clients as needed on workstations in your network, so that your authorized team members can benefit from using audit data collected by a single **Netwrix Auditor Server** to investigate issues and keep track of changes.

AuditAssurance is a technology that consolidates data from multiple independent sources (event logs, configuration snapshots, change history records, etc.). This allows detecting *who* changed *what*, *where* and *when* each change was made, and *who* has access to *what* even if one or several sources of information do not contain all of the required data, for example because it was deleted, overwritten, and so on.

AuditAssurance is provided by **Netwrix Auditor Server** and **Integration API**. **Netwrix Auditor Server** is a core part of **Netwrix Auditor** that collects, transfers and processes data. It contains several internal

components responsible for gathering data from data sources. **Integration API** is a RESTful API that leverages data with custom on-premises or cloud systems even if they are not supported as data sources yet. API enables integration with third-party SIEM solutions by importing and exporting data to and from Netwrix Auditor.

Netwrix Auditor Server and **Integration API** interact with the **Two-Tiered AuditArchive** that is a scalable repository used for storing audit data collected by Netwrix Auditor and imported from other data sources and IT systems using **Integration API**. The **Two-Tiered AuditArchive** includes:

- The file-based **Long-Term Archive**
- The SQL-based short-term **Audit Database**

By default, data is written to both the Audit Database and the Long-Term Archive that is designed to store data in a compressed format for a longer period of time . With two-tiered AuditArchive you can store your data as long as required in the Long-Term Archive (by default, 120 months), but keep your operational storage fast and clean and use it for browsing recent data (by default, 180 days). At the same time, Netwrix Auditor allows you to extract data from the Long-Term Archive and import it to the Audit Database if you want to investigate past issues.

2. Netwrix Auditor 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:

- Supported Data Sources
- Requirements to Install Netwrix Auditor
- Supported Microsoft SQL Server Versions

2.1. Supported Data Sources

The table below lists systems that can be monitored with Netwrix Auditor:

Data source	Supported Versions
Active Directory (including Group Policy and Logon Activity; stand-alone Inactive User Tracker, Password Expiration Notifier, and Netwrix Auditor Object Restore for Active Directory)	Domain Controller OS versions: • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016
Azure AD	Azure Active Directory version provided within Microsoft Office 365
Exchange	• Microsoft Exchange Server 2007 • Microsoft Exchange Server 2010 SP1 and above • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2016 RTM, Exchange Server 2016 Cumulative Update 1– 5
Exchange Online	Exchange Online version provided within Microsoft Office 365
Windows File Servers	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows

Data source	Supported Versions
	7, Windows 8.1, and Windows 10 • Windows Server OS: Windows Server 2008 SP2 (32 and 64-bit)/2008 R2, Windows Server 2012/2012 R2, and Windows Server 2016
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, 8.0.0.0 , 8.1.0.0 (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 configuration only) • NetApp ONTAP 9.0, 9.1(CIFS configuration only)
Oracle Database	• Oracle Database 11g • Oracle Database 12c
SharePoint	• Microsoft SharePoint Foundation 2010 and SharePoint Server 2010 • Microsoft SharePoint Foundation 2013 and SharePoint Server 2013 • Microsoft SharePoint Server 2016
SharePoint Online	SharePoint Online version provided within Microsoft Office 365
SQL Server	• Microsoft SQL Server 2008 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016
VMware	• VMware vSphere (ESX) 4.0 – 6.5 • VMware vSphere Hypervisor (ESXi) 4.0 – 6.5 • VMware vCenter Server 4.0 – 6.5

Data source	Supported Versions
Windows Server	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8.1, and Windows 10 • Windows Server OS: Windows Server 2008 SP2 (32 and 64-bit)/2008 R2, Windows Server 2012/2012 R2, and Windows Server 2016
Cisco	Cisco ASA (Adaptive Security Appliance) and IOS (Internetwork Operating System)—see Netwrix Add-on Store for more information
DHCP	Windows Server OS: Windows Server 2008 R2, Windows Server 2012/2012 R2, and Windows Server 2016
DNS	Windows Server OS: Windows Server 2008 SP2 (32 and 64-bit)/2008 R2, Windows Server 2012/2012 R2, and Windows Server 2016
Event Log	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8.1, and Windows 10 • Windows Server OS: Windows Server 2008 SP2 (32 and 64-bit)/2008 R2, Windows Server 2012/2012 R2, and Windows Server 2016
IIS	IIS 7.0 and above
OneDrive for Business	OneDrive for Business version provided within Microsoft Office 365
User Activity	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8.1, and Windows 10 • Windows Server OS: Windows Server 2008 SP2 (32 and 64-bit)/2008 R2, Windows Server 2012/2012 R2, and Windows Server 2016

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:

2.2.1.1. Full Installation

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 64 bit, 2 GHz or any similar	Intel Core 2 Duo 2x or 4x 64 bit, 3 GHz or any similar, preferably a virtual machine
RAM	2 GB	8 GB Required size highly depends on the number of changes per day and may be up to 32 GB (approximately 3 million changes per day).
Disk space	• Netwrix Auditor Server— At least 5 GB must be allocated for internal components and short-term storage. To ensure audit trail continuity, the product caches some data locally prior to storing it to the AuditArchive. In large busy environments the cache may grow up to 100 GB. • Long-Term Archive and Audit Database—Up to 1 TB. The Long-Term Archive and the Audit Database are scalable repositories that can be stored locally or on another server. Actual required space depends on the daily amount of activity in the environment and the amount of data accumulated in the Audit Database and the Long-Term Archive, and their location and retention settings. 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 the minimum level. When the free disk space is less than 3 GB all Netwrix services will be stopped. Use these numbers only for initial estimations and be sure to correct them based on your data collection and monitoring workflow.	
Screen resolution	1280 x 1024	1920 x 1080 and higher

2.2.1.2. Client Installation

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2 GHz or any similar	Intel Core 2 Duo 2x or 4x 64 bit, 3 GHz or any similar, preferably a virtual machine
RAM	2 GB	8 GB
Disk space	200 MB	
Screen resolution	1280 x 1024	1920 x 1080 and higher

2.2.2. Software Requirements

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

Component	Full installation (both Netwrix Auditor Server and Netwrix Auditor client)	Client installation (only Netwrix Auditor client)
Operating system	• Windows Desktop OS (64- bit): Windows 7 SP1, Windows 8.1, and Windows 10 • Windows Server OS: Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2, and Windows Server 2016 **NOTE:** If you want to deploy Netwrix Auditor in a workgroup, install the product on Windows 8.1, Windows 10, Windows Server 2012/2012 R2, or Windows Server 2016.	• Windows Desktop OS (32 and 64-bit): Windows 7 SP1, Windows 8.1, and Windows 10 • Windows Server OS: Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2, and Windows Server 2016
.NET Framework	• 3.5 SP1, 4.0, 4.5, or 4.6 depending on your OS	—
Installer	• Windows Installer 3.1 and above	• Windows Installer 3.1 and above

2.2.2.1. Additional Components

In order to monitor some data sources, you may be required to install additional software components.

Data source	Components
• File Servers (DFS and cluster) • Windows Server (with enabled network traffic compression) • User Activity	***In the audited environment:*** • .NET Framework 3.5 SP1, 4.0, 4.5, or 4.6 depending on the target server
• SharePoint	***In the audited environment:*** • .NET Framework 3.5 SP1 on the computer that hosts SharePoint Central Administration in the audited SharePoint farm—required for Netwrix Auditor for SharePoint Core Service.
• Azure AD • SharePoint Online	In rare cases, these components may be required for data source monitoring. Netwrix Auditor will display a data collection error with details. ***On the computer where Netwrix Auditor Server is installed:*** • .NET Framework 4.5 or 4.6 • Microsoft Online Services Sign-In Assistant • Windows Azure Active Directory Module for Windows PowerShell
• Oracle Database	***On the computer where Netwrix Auditor Server is installed:*** • Microsoft Visual C++ 2010 Redistributable Package—can be installed automatically during the monitoring plan creation. • Oracle Data Provider for .NET and Oracle Instant Client Netwrix recommends downloading the package 64-bit Oracle Data Access Components 12c Release 4 (12.1.0.2.4) for Windows x64 (ODAC121024_x64.zip). Run the setup and select the **Data Provider for .NET** checkbox. Oracle Instant Client will be installed as well. Also, make sure the **Configure ODP.NET and/or Oracle Providers for ASP.Net at machine-wide level** checkbox is selected on the **ODP.NET (Oracle Data Provider)** step.
• Group Policy	***On the computer where Netwrix Auditor Server is installed:*** Group Policy Management Console. Download Remote Server Administration Tools that include GPMC for: • Windows 7

Data source	Components
	• Windows 8.1 • Windows 10 For Windows Server 2008/ 2008 R2/2012/2012 R2/2016, Group Policy Management is turned on as a Windows feature.

2.2.3. Deployment Options

Netwrix Auditor allows distributed deployment: the main product instance with Netwrix Auditor Server and remote Netwrix Auditor clients can be installed on multiple machines. The Audit Database and the Long-Term Archive can be located on the same computer with Netwrix Auditor Server or hosted separately provided that Netwrix Auditor Server can access them. See How It Works for more information on the product components and their interaction.

NOTE: Both Audit Database and Long-Term Archive are configured after Netwrix Auditor installation.

Netwrix Auditor should be installed on a workstation— installation on a domain controller is not supported. Review the following deployment options and mind the possible restrictions:

If Netwrix Auditor Server and the audit system reside...	Mind the following restrictions...
In the same domain	No restrictions
In trusted domains	No restrictions
In non-trusted domains	• The computer where Netwrix Auditor Server is installed must be able to access the target system (server, share, database instance, SharePoint farm, DC, etc.) by its DNS or NetBIOS name. • For monitoring Active Directory, File Servers, SharePoint, Group Policy, Inactive Users, Logon Activity, and Password Expiration, the domain where your target system resides as well as all domain controllers must be accessible by DNS or NetBIOS names—use the nslookup command-line tool to look up domain names. • For monitoring User Activity, each monitored computer (the computer where Netwrix Auditor User Activity Core Service resides) must be able to access the Netwrix Auditor Server host by its DNS or NetBIOS name.
In workgroups	• The computer where Netwrix Auditor Server is installed must be able to access the target system (server, share, database instance, SharePoint

If Netwrix Auditor Server and the audit system reside...	Mind the following restrictions...
	farm, DC, etc.) by its DNS or NetBIOS name. • For monitoring Active Directory, File Servers, SharePoint, Group Policy, Inactive Users, Logon Activity, and Password Expiration, the domain where your target system resides as well as all domain controllers must be accessible by DNS or NetBIOS names—use the nslookup command-line tool to look up domain names. • For monitoring User Activity, each monitored computer (the computer where Netwrix Auditor User Activity Core Service resides) must be able to access the Netwrix Auditor Server host by its DNS or NetBIOS name. • Netwrix Auditor Server, the Audit Database (both SQL Server and SSRS), and the Long-Term Archive must reside on the same computer. • The computer hosting Netwrix Auditor Server cannot run Windows 7 or Windows Server 2008 R2.

The remote Netwrix Auditor client can be installed on any workstation provided that a user who runs the product is granted all necessary permissions. See Configure Netwrix Auditor Service Accounts 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 state-in-time configuration.

If you want to generate reports and run searches in Netwrix Auditor, SQL Server must be deployed on the same computer where Netwrix Auditor Server 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.

Version	Edition
SQL Server 2008 R2	• Express Edition with Advanced Services • Standard or Enterprise 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
SQL Server 2016	• 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 downloads SQL Server 2014 Express Edition with Advanced Services and guides you through configuration procedure.

For your convenience, Netwrix provides instructions on the manual installation of 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.

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

NOTE: For instructions on upgrade procedures, refer to Upgrade to the Latest Version.

To install Netwrix Auditor

1. Download Netwrix Auditor 9.0 on Netwrix website.

   NOTE: Before installing Netwrix Auditor, make sure that the **Windows Firewall** service is started. If you use a third-party firewall, see Protocols and Ports Required for Netwrix Auditor Server. 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 the main component called Netwrix Auditor Server 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 a client console on a remote machine to provide access to configuration and audit data.
5. On the **Destination Folder** step, specify the installation folder.
6. Click **Install**.

After a successful installation, Netwrix Auditor shortcut will be added to the **Start** menu/screen and the product will start.

Netwrix looks beyond the traditional on-premises installation and provides Netwrix Auditor for cloud and virtual environments. For example, you can deploy Netwrix Auditor on a pre-configured Microsoft Azure virtual machine or install it as a virtual appliance on your VMware vSphere or Hyper-V virtualization server. For more information on additional deployment options, visit Virtual Appliance page.

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 when setting up auditing in Netwrix Auditor 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.

- .Net Framework 3.5 SP1 is 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. On the computer where Netwrix Auditor Server resides,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 when setting up auditing in Netwrix Auditor. If, for some reason, installation has failed, you must install the Core Service manually on each audited computer.

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

1. On the computer where Netwrix Auditor Server resides, 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 configuration and 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

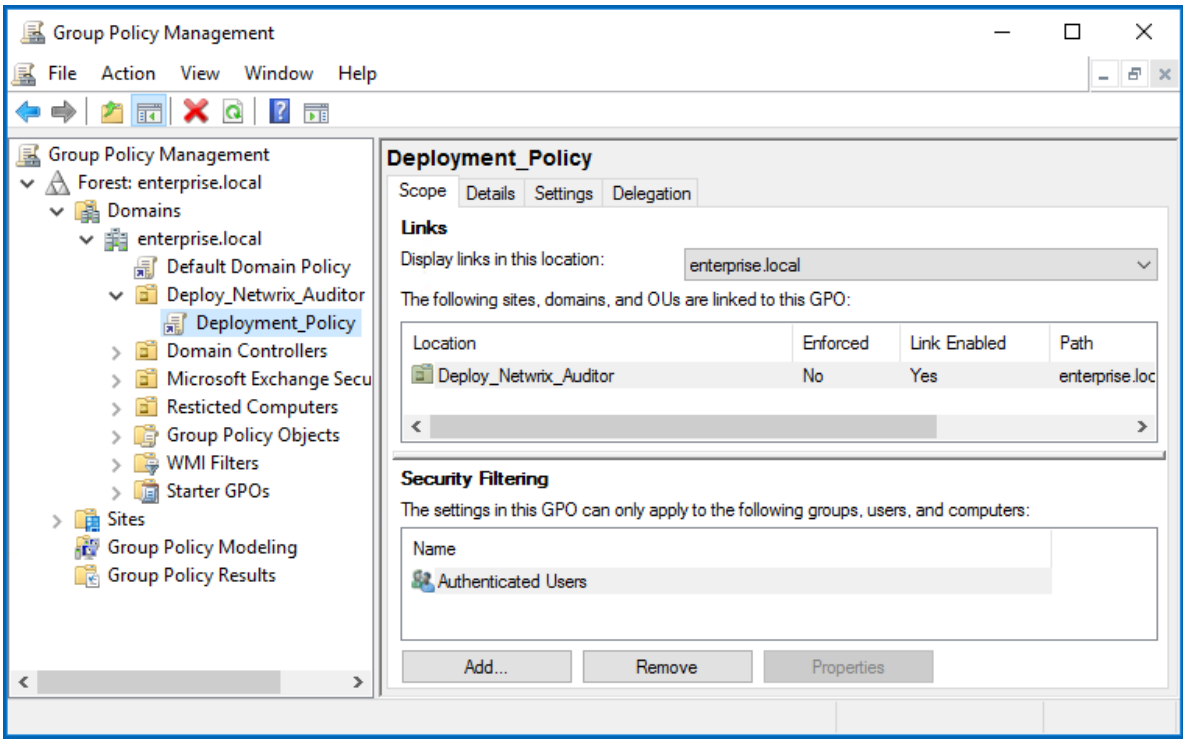
1. Create a shared folder that will be used for distributing the installation package.

   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.

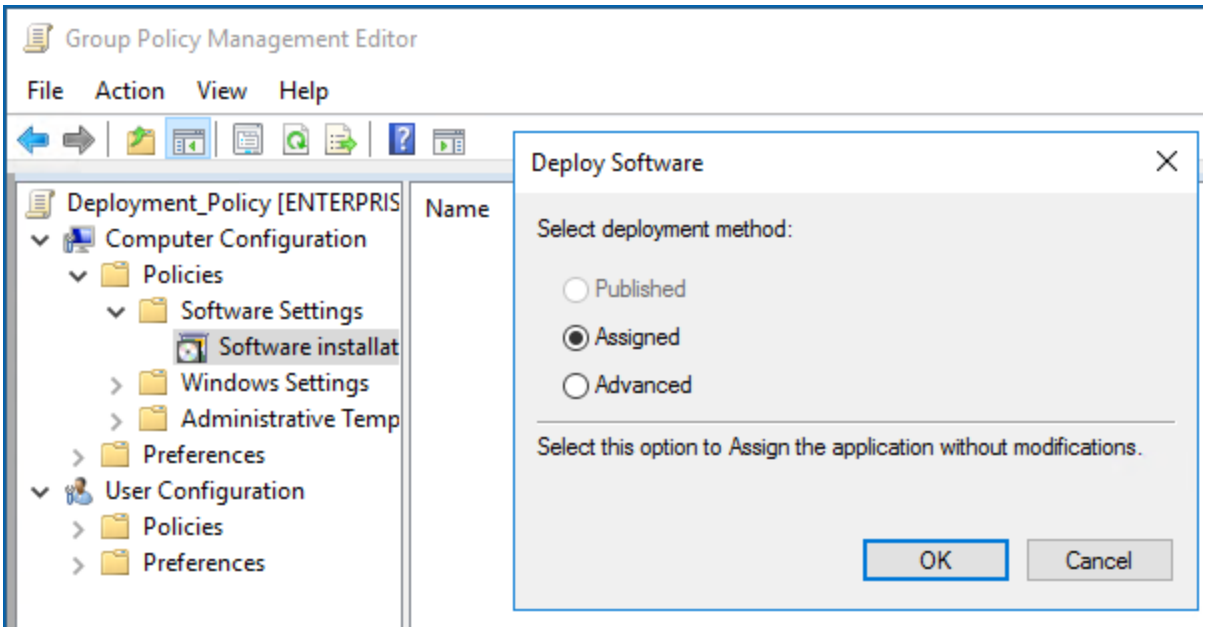
3.3.3. Create a Group Policy to Deploy Netwrix Auditor

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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**.

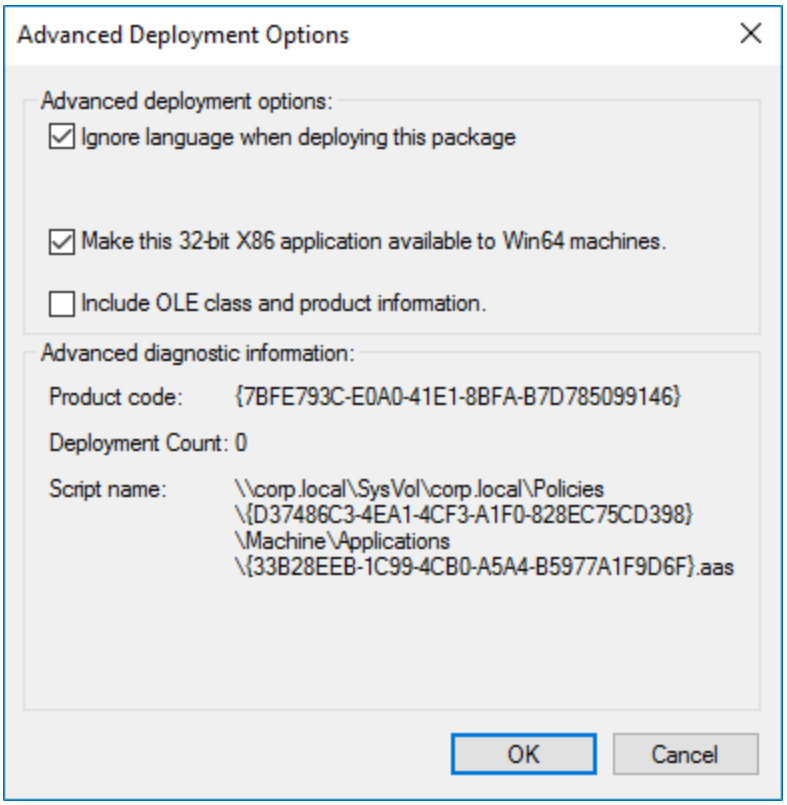


3. Right-click the newly created GPO and select **Edit** from the pop-up menu.
4. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Software Settings** → **Software installation.**
5. In the right page, right-click 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. Upgrade to the Latest Version

This chapter provides step-by-step instructions on how to upgrade your current version of Netwrix Auditor to the newest version available. Netwrix recommends that you upgrade from older versions of Netwrix Auditor to 9.0 in order to take advantage of new features.

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.

In addition to major releases, 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
8.5 → NEW  Applicable to Netwrix Auditor 8.5 and 9.0 (upgrade within the same version). No special upgrade procedure required—simply install Netwrix Auditor 9.0. During installation your Netwrix Auditor configuration and data will be preserved. Make sure to review upgrade notices before performing upgrade. See Upgrade from 8.5 for more information.
8.0 → 8.5 → NEW 

Upgrade scenario
Applicable to Netwrix Auditor 8.0. You must upgrade sequentially: first to 8.5 and then to 9.0. During upgrade your Netwrix Auditor configuration and data will be preserved. Make sure to review upgrade notices before performing upgrade.

4.1. Upgrade from 8.5

You can upgrade Netwrix Auditor 8.5 to 9.0 by running the installation package. Netwrix Auditor automatically upgrades to the latest version while preserving its configuration.

4.1.1. Before You Start

1. Make sure you followed basic precaution measures. See Upgrade to the Latest Version for more information.
2. Wait for all running data collections to complete and close Netwrix Auditor Administrator Console and Netwrix Auditor client.
3. While not obligatory, it might be helpful to review your Netwrix Auditor 8.5 configuration and read the following topics before running the upgrade: Review Major Changes and Review Additional Upgrade Notes

4.1.2. Perform Upgrade

Run the installation package on the computer, where Netwrix Auditor Server resides. Refer to Install the Product for detailed instructions on how to install Netwrix Auditor. The product will disable scheduled tasks, it may ask you to stop processes if necessary, and then Netwrix Auditor will migrate data and configuration.

4.1.3. Review Major Changes

In 9.0, Netwrix replaced MMC-based Netwrix Auditor Administrator Console with a new Netwrix Auditor client—a single interface that provides access to both auditing configuration and intelligence data. The elaborate role-based access system integrated in the product ensures that even with a single interface only relevant employees have access to the options and data they need.

Netwrix introduced a new concept of organizing your auditing and change tracking routines—a monitoring plan. A monitoring plan is different from a Managed Object since it is not limited to a single type (e.g., a domain or computer collection). The plan can include several data sources (known as audited systems in 8.5 and below) that share common settings, such as notification delivery settings and database settings. Each data source within a plan can be configured to monitor multiple items (e.g., several domains or

SharePoint farms). During the upgrade, Netwrix Auditor will replace old Managed Objects with new monitoring plans. To learn more about monitoring plans, refer to Netwrix Auditor Administration Guide.

In 8.5, you could specify a database for each audited system within a Managed Object. Unlike Managed Objects, each monitoring plan is associated with its own database for storing audit data, i.e., data collected across all data sources is written to a single database. This is helpful if you want to delegate control of data collected by this plan. The database settings will be updated as follows:

- If a Managed Object was configured to audit a single audited system, Netwrix Auditor 9.0 will preserve settings and will continue to write data to specified database after the upgrade.

  For example, if you had a Managed Object configured to audit Active Directory changes and write data to the default database (Netwrix_Auditor_Active_Directory), Netwrix Auditor 9.0 will create a new monitoring plan and will continue data to the Netwrix_Auditor_Active_Directory database.

- If a Managed Object was configured to monitor several audited systems (e.g., File Servers, Windows Server, and SQL Server in a single Computer Collection), Netwrix Auditor 9.0 will create a new monitoring plan with these data sources and will write newly collected data to one of the databases that were in use previously. In most cases, Netwrix Auditor 9.0 picks an Active Directory or File Servers database as a primary database. Data contained in other databases will be still available for search and reporting.

Starting with 9.0, the Activity Summary delivery settings are managed on the monitoring plan level. During the upgrade, Netwrix Auditor retrieves the enabled recipients list for each audited system within a Managed Object and adds these emails to a new combined list. After the upgrade, navigate to your plan settings and review Activity Summary recipients in the **Edit settings** → **Notifications**. For example, if your Managed Object was configured to monitor SQL Server and Oracle Database, a recipients lists will be merged into a single list in a newly created plan. The addressees will receive both SQL Server and Oracle Database emails. Other notification options will be set as follows:

- Delivery frequency will be set to a minimum value detected across the notification settings specified in your Managed Object. For example, if you received File Servers notification every 12 hours and Windows Server notification every 24 hours, in 9.0 you will receive all notifications every 12 hours.
- If any Activity Summary was sent as a CSV attachment or compressed CSV attachment, this setting will be propagated to all activity summaries sent by this plan.

4.1.4. Review Additional Upgrade Notes

Review additional upgrade details:

- Most Netwrix Auditor functionality becomes service-based. Data collection scheduled tasks created by Netwrix Auditor 8.5 are disabled after upgrade. If you had a custom scheduled configured for your tasks, navigate to **Task Scheduler** and review the **Triggers** tab for each task. You will be able to apply the same settings on **Notifications** page for your plan in Netwrix Auditor. You can remove tasks manually after upgrade.

- Netwrix Auditor introduces new customizable and easy-to-configure alerts. Active Directory alerts that were present in Netwrix Auditor 8.5 are stored as text files in *%ProgramData%\Netwrix Auditor\AD Change Reporter\Rules\{domain}*. If you need any of this alerts, you have to recreate them manually in the product.
- Inactive user tracking, alerting on password expiration, restoring AD objects, and event log management procedures are handled in separate tools within Netwrix Auditor tool kit. You can find these tools under **Start** → **Netwrix Auditor**.
- Event Log Manager no longer allows collecting syslog events. If you want to monitor syslog, e.g., Cisco activity, download a special add-on from Netwrix Auditor Add-on Store. You might need to update parsing rules manually or order a customized add-on from Netwrix.
- The database that contains Event Log audit data cannot be upgraded to the latest version. To make Event Log data available for reporting, reload it from the Long-Term Archive. To do this, start Event Log Manager and click **Import Data**.
- Netwrix Auditor 9.0 starts file server monitoring with initial data collection. Some data collected between the upgrade and this data collection may be lost.
- After the upgrade, state-in-time snapshots become unavailable for reporting. To see your snapshots, reload them in Netwrix Auditor. To do it, navigate to your monitoring plan, drill-down to your data source settings, and then click **Manage** under the **Manage historical snapshots** section.
- The Audit Database retention period will be set to 180 days for all monitoring plans. Some data may be cleared by retention during the upgrade. If you need historical data, you can import it from the Long-Term Archive using **Investigations** in the product.
- Shortly after the upgrade, Netwrix Auditor can display incorrect monitoring statuses. With the next scheduled data collection, statuses will be updated and displayed normally.
- During upgrade process, you may receive temporary data collection errors which arise when uploading collected data to the Audit Database. This is expected activity, and the errors disapear once the Audit Database update completes.
- After the upgrade, Netwrix Auditor may lose a connection to Netwrix Auditor User Activity Core Services deployed on remote servers. Check status for each computer monitored with the User Activity data source. To do this, navigate to your plan page → **User Activity** data source → **Monitored Computers** tab and review statuses. If a computer status is **Not responding**, navigate to this computer and restart the Netwrix Auditor User Activity Core Service.
- In Netwrix Auditor 9.0, Netwrix has updated API schemas. The scripts and add-ons designed for Netwrix Auditor 8.0 – 8.5 might become inoperable in Netwrix Auditor 9.0. Make sure to review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. The add-ons distributed through the Add-on store will be updated shortly after the product release. Download the latest add-on version in the Add-on Store.

5. Configure IT Infrastructure for Auditing and Monitoring

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 Server 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. You can enable Netwrix Auditor to continually enforce the relevant audit policies or configure them manually.

Data source	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 Server is installed:
	• The retention period for the backup logs can be customized (by default, it is set to *"50"*).

Data source	Required configuration
	• The **Secondary Logon** service must be running and its **Startup type** parameter must be set to *"Automatic"*.
Azure AD	No configuration required

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, 2013 or 2016).
	• 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, FolderBind, SendAs, SendOnBehalf, Create

Data source	Required configuration
	On the computer where Netwrix Auditor Server is installed: • The retention period for the backup logs can be customized (by default, it is set to *"50"*). • The **Secondary Logon** service must be running and its **Startup type** parameter must be set to *"Automatic"*.

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 configured in the **Advanced Security** → **Auditing** settings for the audited shared folders: List Folder / Read Data (Files only) — *"Success"* and *"Fail"* List Folder / Read Data (This folder, subfolders and files) — *"Fail"* Create Files / Write Data* — *"Success"* and *"Fail"* Create Folders / Append Data* — *"Success"* and *"Fail"* Write Attributes* — *"Success"* and *"Fail"* Write Extended Attributes* — *"Success"* and *"Fail"* Delete Subfolders and Files* — *"Success"* and *"Fail"* Delete* — *"Success"* and *"Fail"* Change Permissions* — *"Success"* and *"Fail"* Take Ownership* — *"Success"* and *"Fail"* **NOTE:** Select *"Fail"* only if you want to track failure events, it is not required for success events monitoring. If you want to get only state-in-time snapshots of your system configuration, limit your settings to the permissions marked with * and set it to *"Success"* (Apply onto: This folder, subfolders and files).

Data source	Required configuration

- The following **Advanced audit policy** settings must be configured:
  - The **Audit: Force audit policy subcategory settings (Windows Vista or later)** security option must be enabled.
  - Depending on your OS version, configure the categories as follows:

Windows Server 2008 / Windows Vista

Object Access	
Audit File Share	*"Success"*
Audit File System	*"Success"* and *"Failure"*
Audit Handle Manipulation	*"Success"* and *"Failure"*
Logon/Logoff	
Logon	*"Success"*
Logoff	*"Success"*
Policy Change	
Audit Audit Policy Change	*"Success"*
System	
Security State Change	*"Success"*

Windows Server 2008 R2 / Windows 7 and above

Object Access	
Audit File Share	*"Success"*
Audit File System	*"Success"* and *"Failure"*
Audit Handle Manipulation	*"Success"* and *"Failure"*
Audit Detailed file share	*"Failure"*
Logon/Logoff	
Logon	*"Success"*
Logoff	*"Success"*
Policy Change	
Audit Audit Policy Change	*"Success"*
System	
Security State Change	*"Success"*

If you want to get only state-in-time snapshots of your system configuration, limit your audit settings to the following policies:

Object Access	
Audit File System	*"Success"*

Data source	Required configuration

Audit Handle Manipulation	*"Success"*
Audit File Share	*"Success"*
Policy Change	
Audit Audit Policy Change	*"Success"*

NOTE: Applies only to Windows server (not to Windows Failover Cluster or a file share).

- The following legacy policies can be configured instead of advanced:
  - **Audit object access** policy must set to *"Success"* and *"Failure"*.
  - **Audit logon events** policy must be set to *"Success"*.
  - **Audit system events** policy must be set to *"Success"*.
  - **Audit policy change** must be set to *"Success"*.
- 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)

NOTE: The rules marked with * are required only if you do not want to use network traffic compression for auditing.

On the computer where Netwrix Auditor Server is installed:

- If your file shares contain symbolic links and you want to collect state-in-time

Data source	Required configuration
	data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

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
	On the computer where Netwrix Auditor Server is installed:
	• If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

EMC 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

Data source	Required configuration
	• Write Extended Attributes • Delete Subfolders and Files • Delete • Change Permissions • Take Ownership ***On the computer where Netwrix Auditor Server is installed:*** • If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

NetApp	***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_ 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** and **ONTAP 9**:
	  • `External Web Services: true`.

Data source	Required configuration

	For security reasons, it is recommended to enable only SSL access.
	• Firewall policy for data interfaces must be configured to allow ONTAPI protocol connections.
	• Audit settings must be configured as follows:
	`Auditing State: true`
	`Log Destination Path: /audit`
	`Categories of Events to Audit: file-ops, cifs-logon-logoff`
	`Log Format: evtx`
	`Log File Size Limit: 300MB`
	• 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
	On the computer where Netwrix Auditor Server is installed:
	• If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

Oracle Database	***In the audited environment:*** For **Standard Auditing** (Oracle Database 11g): • One of the following audit trails must be configured to store audit events:

Data source	Required configuration
	• Database audit trail • XML audit trail • XML or database audit trail with the ability to keep full text of SQL-specific query in audit records • Auditing of the following parameters can be enabled: • Configuration changes made by any user or specific users • Successful data access and changes • Failed data access and changes For **Unified Auditing** (Oracle Database 12g): • The audit policy must be created and enabled • Auditing of the following parameters can be enabled: • Configuration changes • Successful and failed data access and changes • `Oracle Data Pump`, `Oracle Recovery Manager (RMAN)` and `Oracle SQL*Loader Direct Path Load` components For **Fine Grained Auditing** (Oracle Database Enterprise Edition): • A special audit policy associated with columns in application tables must be created and enabled
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).
SharePoint Online (including OneDrive for Business)	No configuration required

Data source	Required configuration
SQL Server	No configuration required
VMware	No configuration required

Windows Server (including DNS, DHCP and removable media)	***In the audited environment:***
	• The **Remote Registry** and the **Windows Management Instrumentation (WMI)** service must be started.
	• The following advanced audit policy settings must be configured:
	  • The **Audit: Force audit policy subcategory settings (Windows Vista or later)** security option must be enabled.
	  • For **Windows Server 2008 / Windows Vista**—The **Object Access**, **Account Management**, and **Policy Change** categories must be disabled while the **Security Group Management, User Account Management, Handle Manipulation, Other Object Access Events**, **Registry**, **File Share**, and **Audit Policy Change** subcategories must be enabled for *"Success"*.
	  • For **Windows Server 2008 R2 / Windows 7 and above**—**Audit Security Group Management, Audit User Account Management, Audit Handle Manipulation, Audit Other Object Access Events**, **Audit Registry**, **Audit File Share**, and **Audit Audit Policy Change** advanced audit policies must be set to *"Success"*.
	• The following legacy audit policies can be configured instead of advanced: **Audit object access**, **Audit policy change**, and **Audit account management** must be set to *"Success"*.
	• The **Application, Security, System, Microsoft- Windows-TaskScheduler/Operational**, and **Microsoft-Windows-DNS-Server/Audit** event log maximum size must be set to 4 GB. The retention method 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)

Data source	Required configuration
	• 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) • Performance Logs and Alerts (DCOM-In) • Performance Logs and Alerts (TCP-In) **NOTE:** If the audited servers are behind the Firewall, review the list of protocols and ports required for Netwrix Auditor and make sure that these ports are opened. See Protocols and Ports Required for Netwrix Auditor Server for more information. • For auditing DHCP, the **Microsoft-Windows-Dhcp-Server/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"*. • For auditing removable storage media, two **Event Trace Session** objects must be created.
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**

Data source	Required configuration
	• **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)** • **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 Server 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 VNX/VNXe for Auditing
- Configure NetApp Filer for Auditing
- Configure Oracle Database for Auditing
- Configure SharePoint Farm for Auditing
- Configure Windows Server for Auditing
- Configure Infrastructure for Auditing Windows Event Logs
- Configure Domain for Auditing Group Policy
- Configure Infrastructure for Auditing IIS
- Configure Infrastructure for Auditing Logon Activity
- Configure Computers for Auditing User Activity

5.1. 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 monitoring plan

  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.

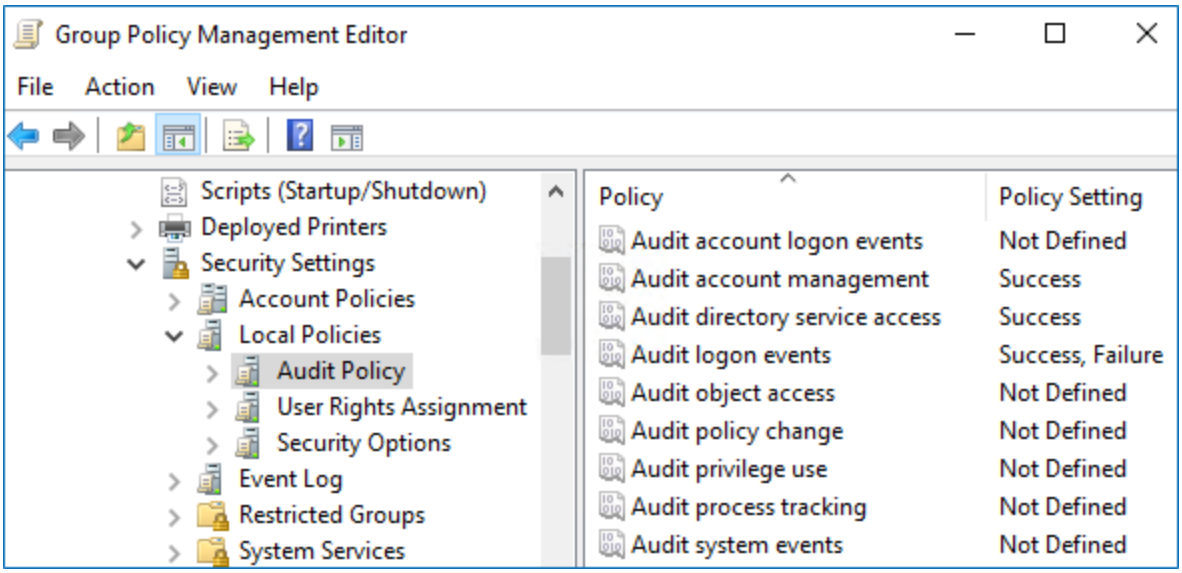
- Manually. To configure your domain for auditing manually, perform the following procedures:
  - Configure Basic Domain Audit Policies or Configure Advanced Audit Policies. Either local or advanced audit policies must be configured to track changes to accounts and groups, and to identify workstations where changes were made.
  - Configure Object-Level Auditing
  - Configure Security Event Log Size and Retention Settings
  - Adjust Active Directory Tombstone Lifetime
  - Enable Secondary Logon Service

5.1.1. 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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 Administration 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.

5.1.2. 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:

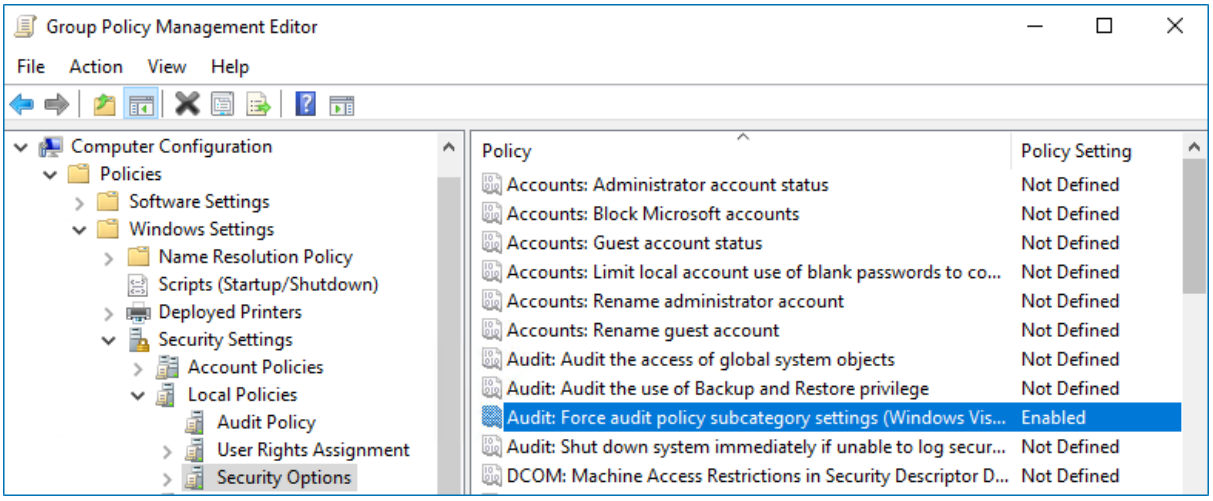
- To configure security options
- To configure advanced audit policies

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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"*.

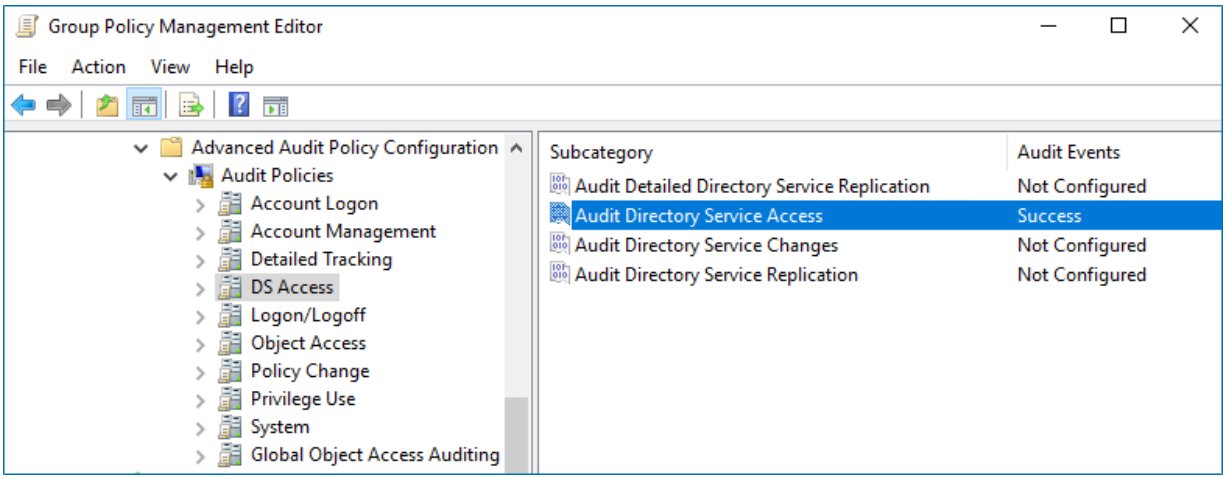


5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

To configure advanced audit policies

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

5.1.3. Configure Object-Level Auditing

Object-level auditing must be configured if you want to collect information on "Who" and "When". 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.

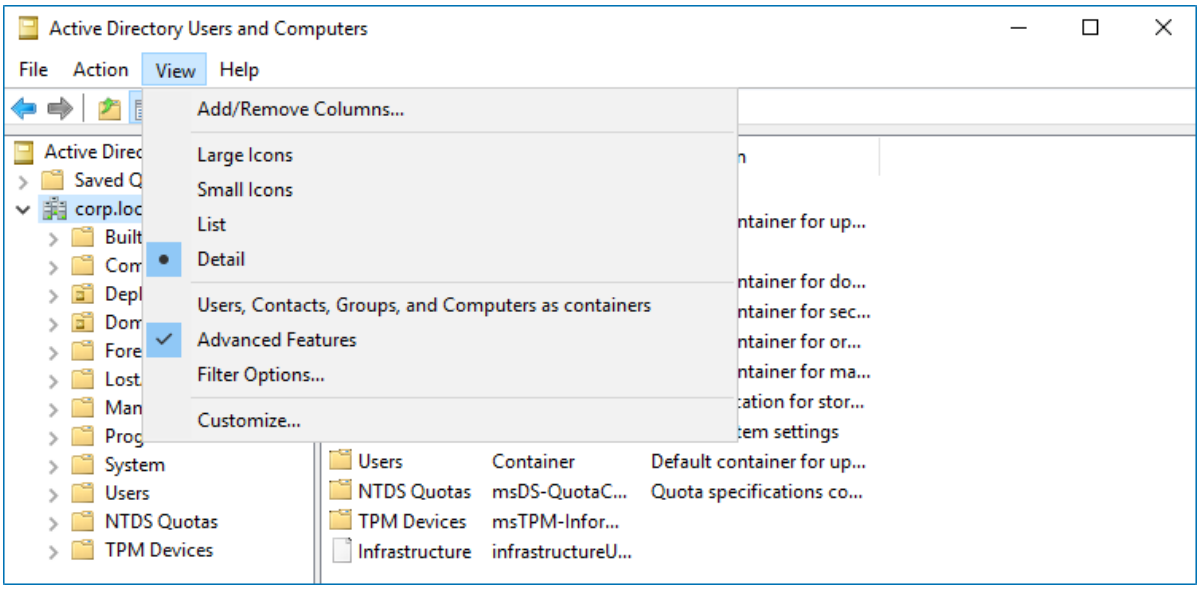
NOTE: Auditing of the Configuration partition is enabled by default. Refer to Netwrix Auditor Administration Guide for detailed instructions on how to enable auditing of changes to the Schema partition in the target AD domain.

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

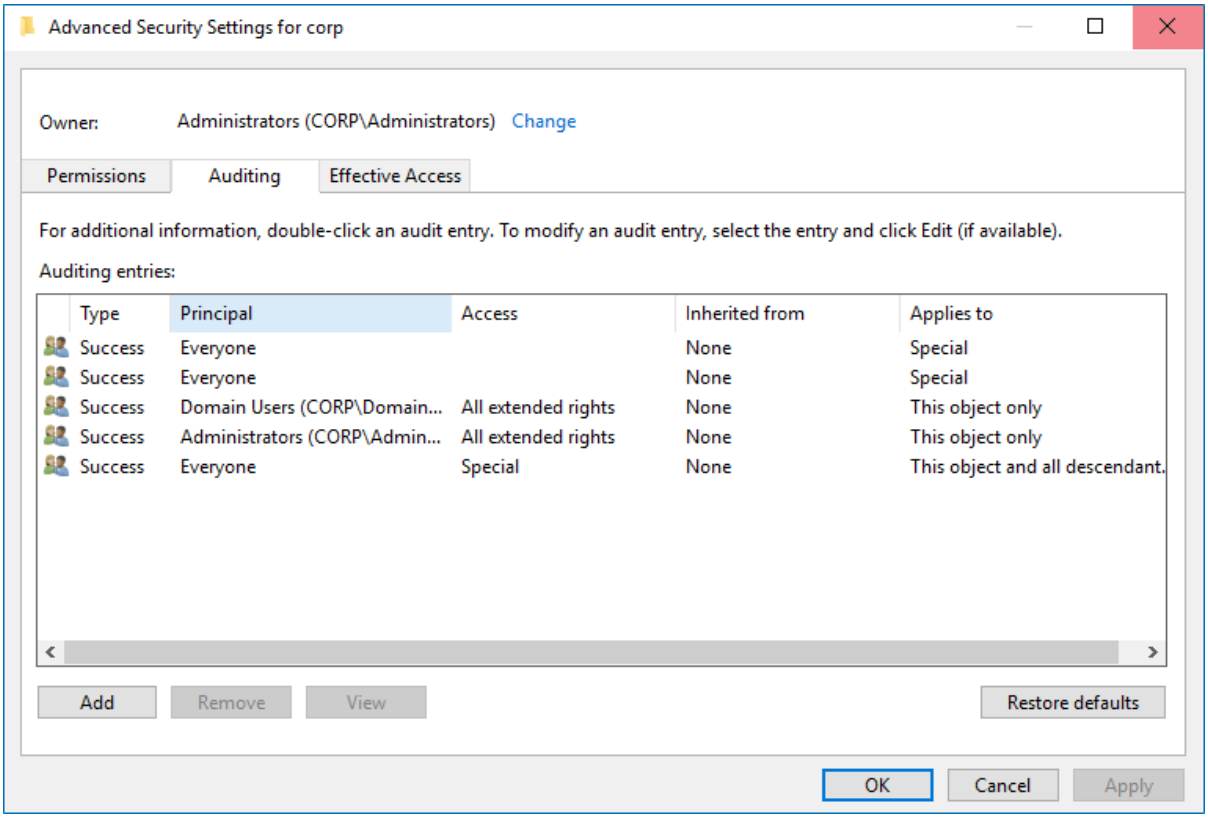
- To configure object-level auditing for the Domain partition
- To enable object-level auditing for the Configuration and Schema partitions

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

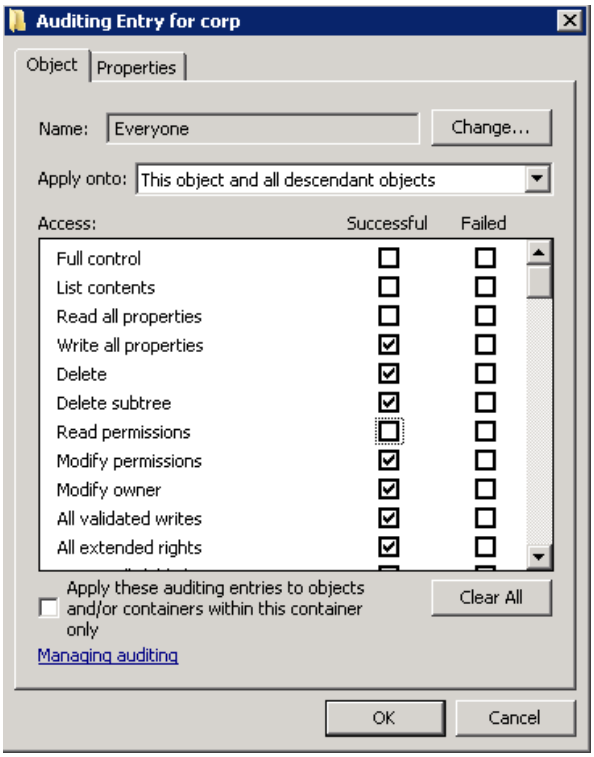


4. Do one of the following depending on the OS:

- 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

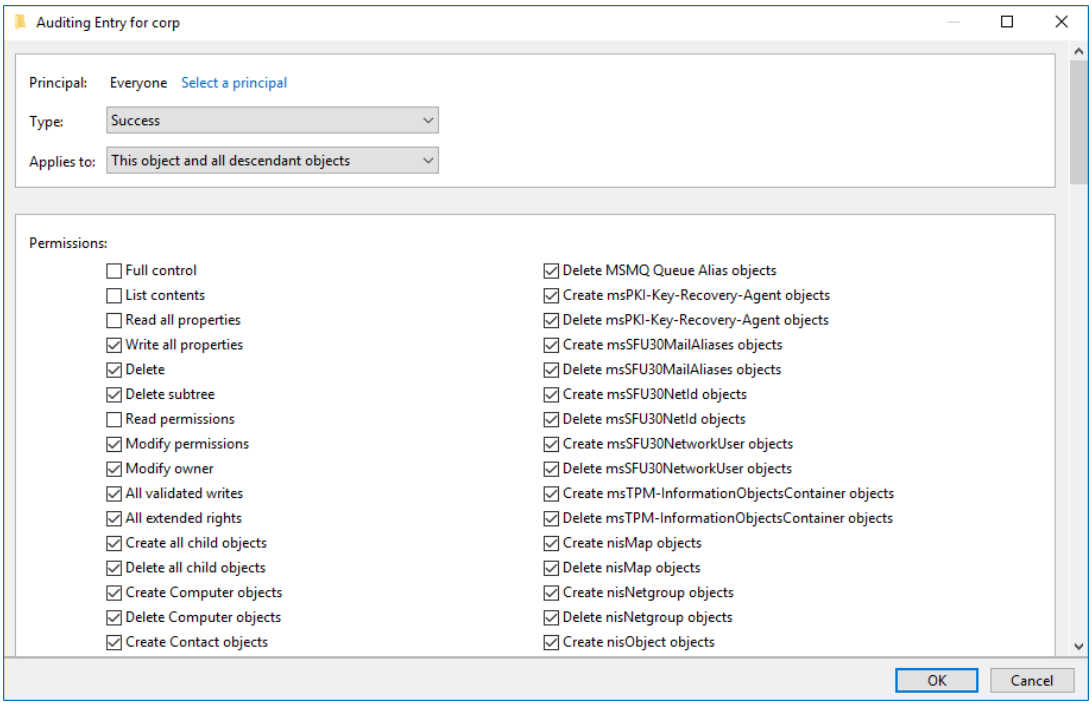
  a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

  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*.

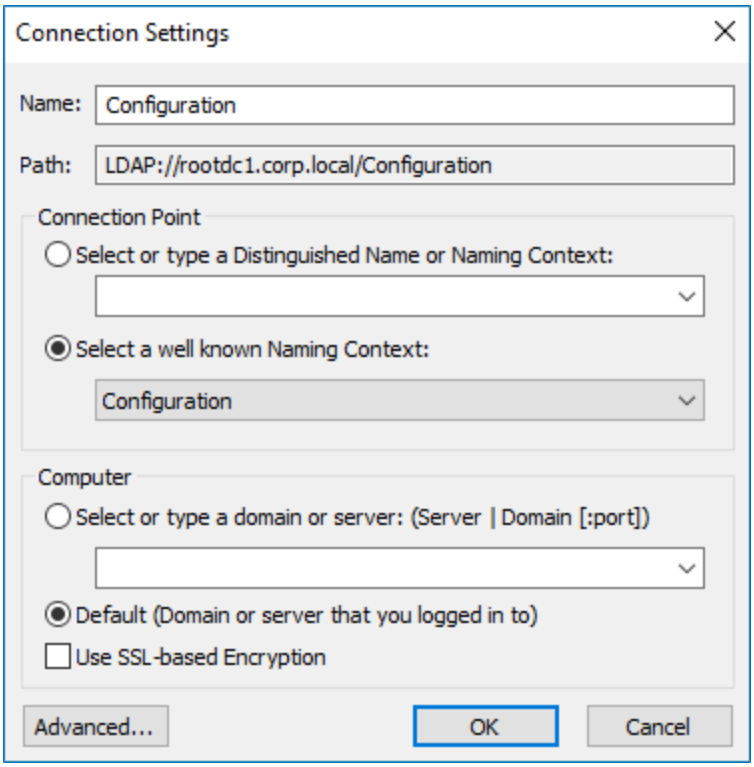
  e. Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.



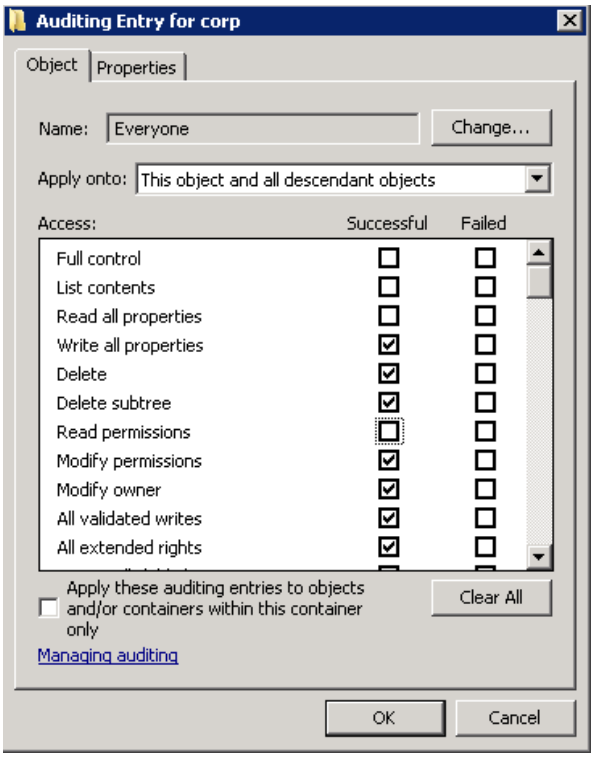
To enable object-level auditing for the Configuration and Schema partitions

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. On any domain controller in the target domain, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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

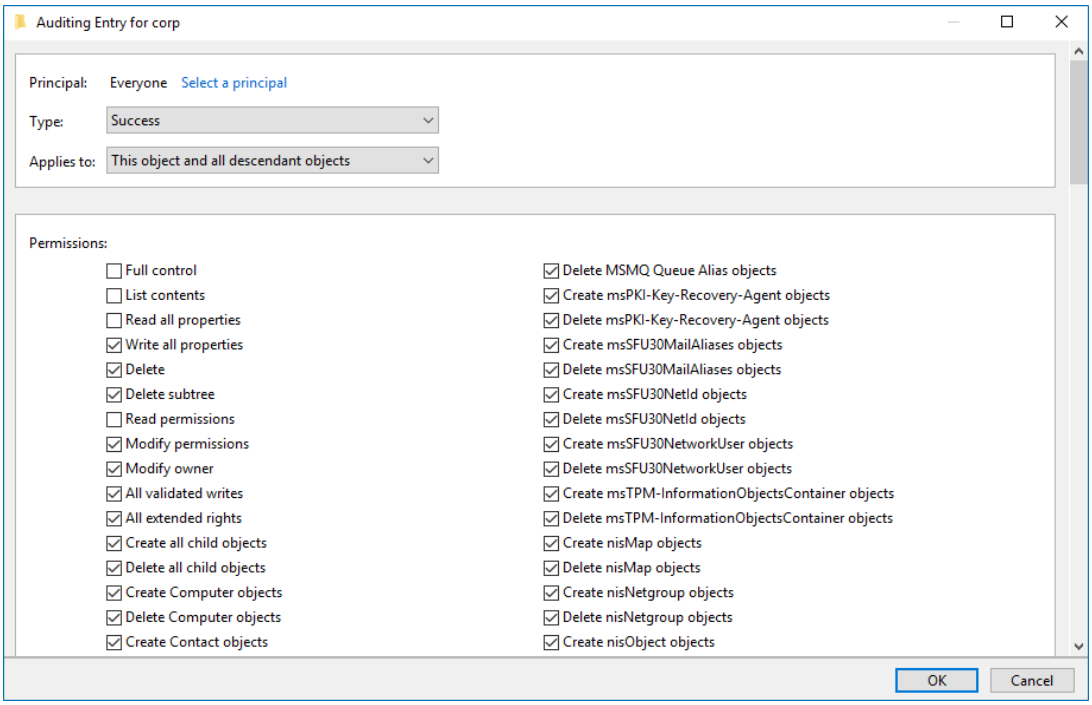
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

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.

5.1.4. 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, 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.

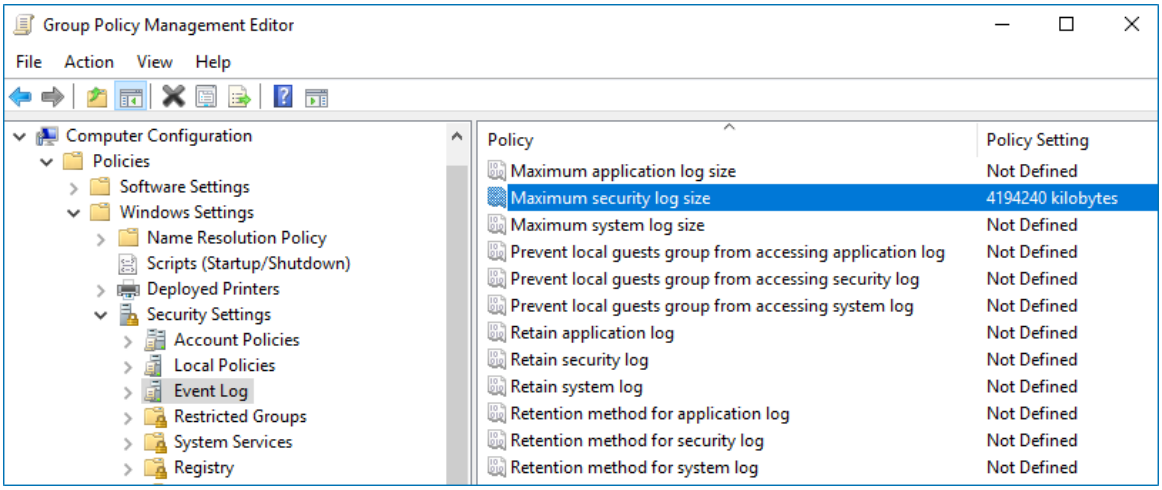
To adjust your **Security** event log size and retention settings, perform the following procedures:

- 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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 Server 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** to add the template.
5. Navigate to **Computer Configuration** → **Policies** → **Administrative Templates: Policy Definitions** → **Windows Component** → **Event Log Service** → **Security**. Do the following:

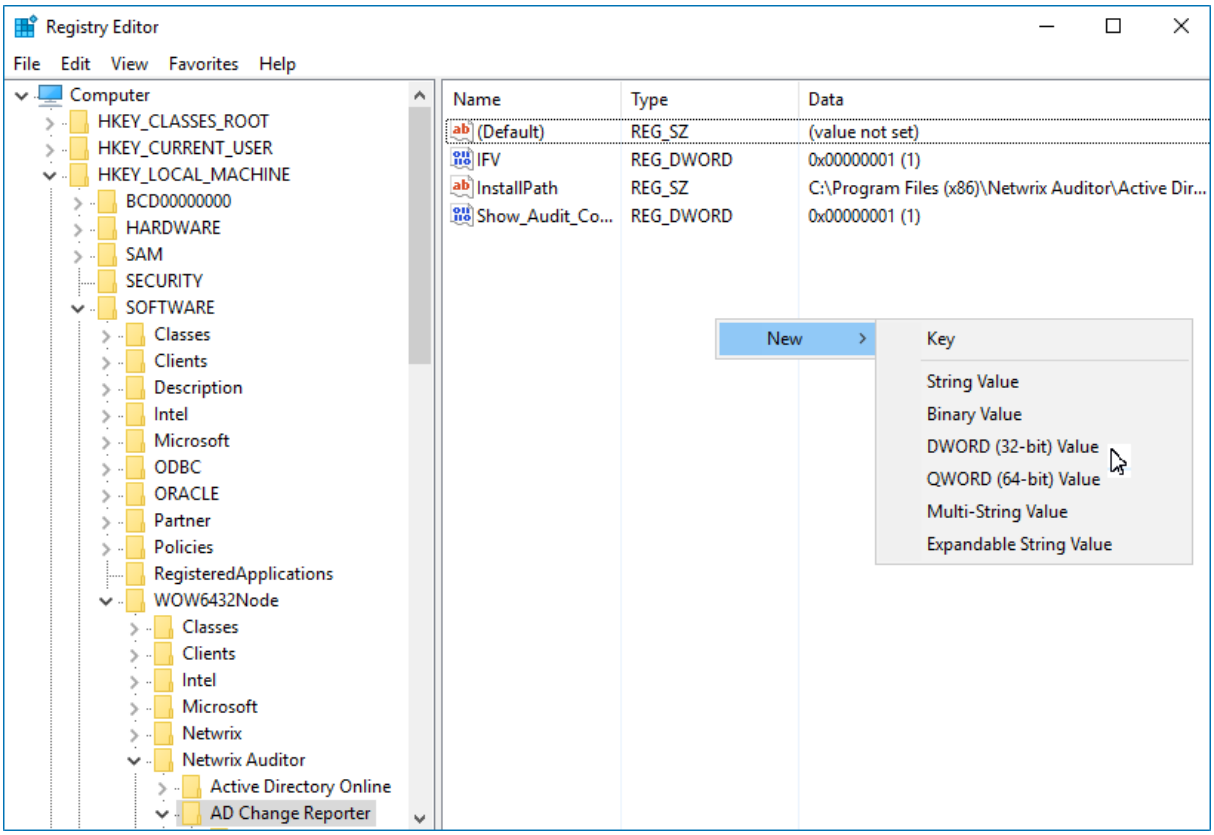
On...	Select...	Set to...
Windows Server 2008 / 2008 R2	• **Back up log automatically when full** • **Retain old events**	*"Enabled"*
Windows Server 2012 / 2012 R2 / 2016	• **Back up log automatically when full** • **Control Event Log behavior when the log file reaches its maximum size**	*"Enabled"*

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

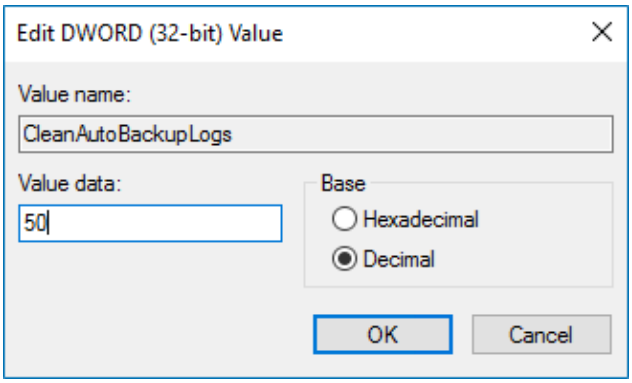
1. On the computer where Netwrix Auditor Server is installed, open **Registry Editor**: navigate to **Start**→ **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **AD Change Reporter**.
3. In the right-pane, right-click and select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

5.1.5. Adjust Active Directory Tombstone Lifetime

You can restore deleted Active Directory objects and their attributes using the Netwrix Auditor Object Restore for Active Directory tool shipped with Netwrix Auditor. The tool finds the information on deleted

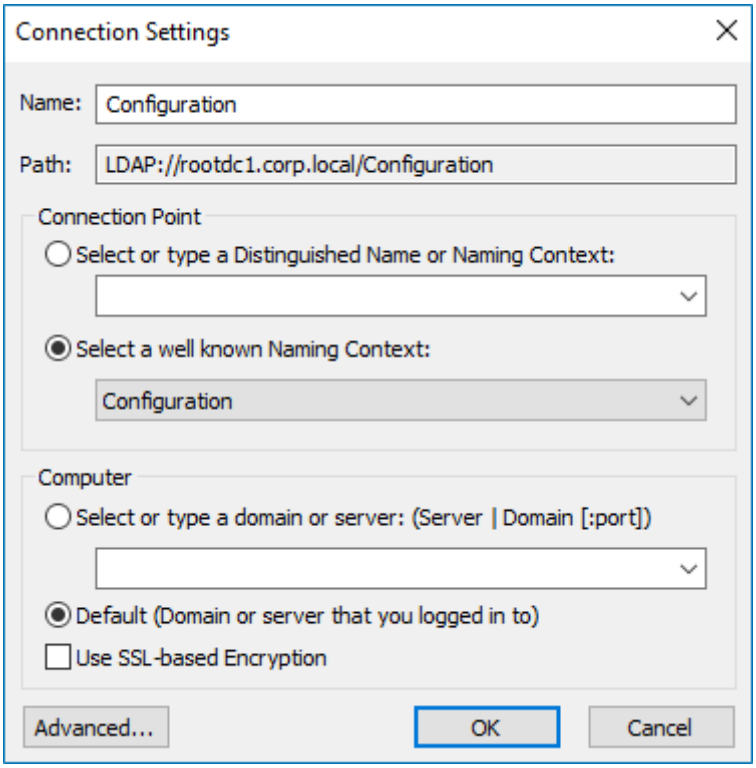
objects in the product snapshots (this data is stored in the Long-Term Archive, a local file-based storage of audit data) and AD tombstones.

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 setting 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

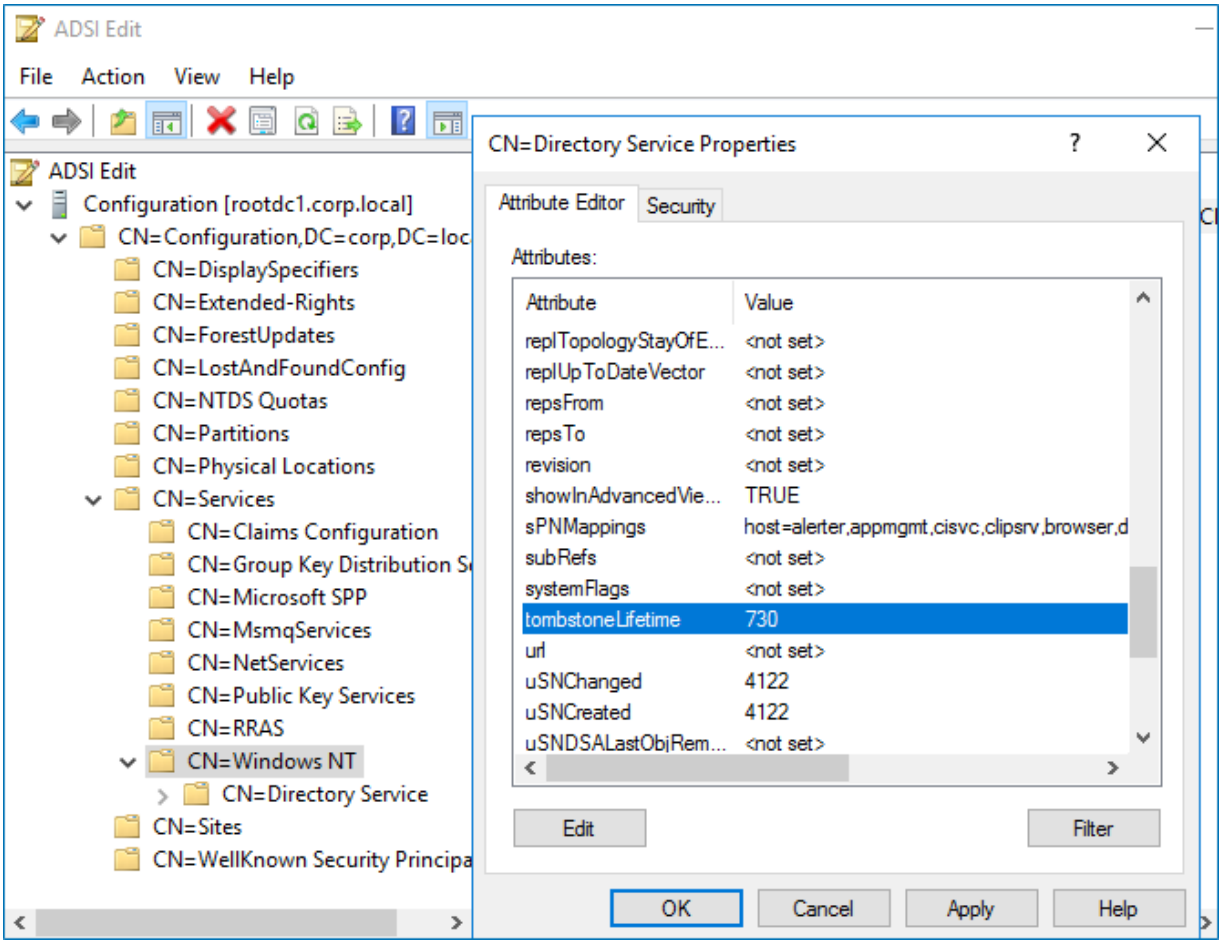
NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2008 and above, this component is installed together with the AD DS role, or it can be downloaded and installed along with Remote Server Administration Tools. Refer to Install ADSI Edit for detailed instructions on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

1. On any domain controller in the target domain, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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).

5.1.6. Enable Secondary Logon Service

1. On the computer where Netwrix Auditor Server resides, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Services**.
2. In the **Services** dialog, locate the **Secondary Logon** service, right-click it and select **Properties**.
3. In the **Secondary Logon Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.
4. In the **Services** dialog, ensure that **Secondary Logon** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.

5.2. Configure Infrastructure for Auditing Exchange

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

- Automatically when creating a monitoring plan

  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. 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, 2013, or 2016, 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.

5.2.1. Configure Exchange Administrator Audit Logging Settings

If the audited AD domain has an Exchange organization running Exchange 2010, 2013, or 2016, 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 and 2016

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

3. On the computer where Netwrix Auditor is installed, browse to the *%Netwrix Auditor Server 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. Make sure your policies allow script execution.

5.2.2. 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 and 2016

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 and 2016

Netwrix Auditor automatically configures auditing settings for Exchange 2013 and 2016. 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

Audit...	Steps...
	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` • `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.

5.3. Configure Infrastructure for Auditing Exchange Online

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

- Automatically when creating a monitoring plan. 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.

Audit...	Steps...
All mailboxes	1. On the local computer, navigate to **Start** → **Programs** → **Windows PowerShell**. 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 PowerShell**. 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`

Audit...	Steps...

- 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.

5.4. 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 object changes only. Tracking all 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. 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 monitoring plan

  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 Local Audit Policies or Configure Advanced Audit Policies
- Configure Event Log Size and Retention Settings
- Enable Remote Registry Service
- Configure Windows Firewall Inbound Connection Rules

NOTE: If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

5.4.1. 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:

Option		Description
Changes	Successful	Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion.
	Failed	Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it.
Read access	Successful	Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.

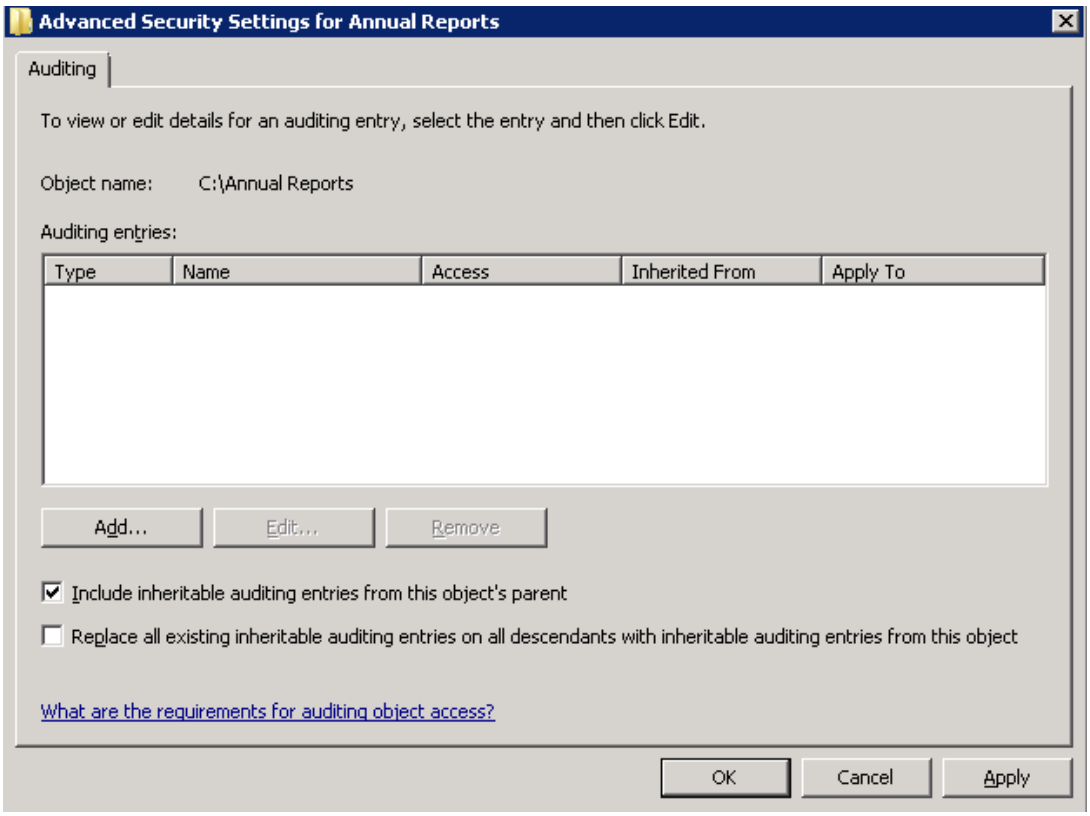
NOTE: Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, renaming, and copying. To track the copy action, enable successful read access and change auditing.

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 errors on incorrect audit configuration. This will not affect the reports or data searches

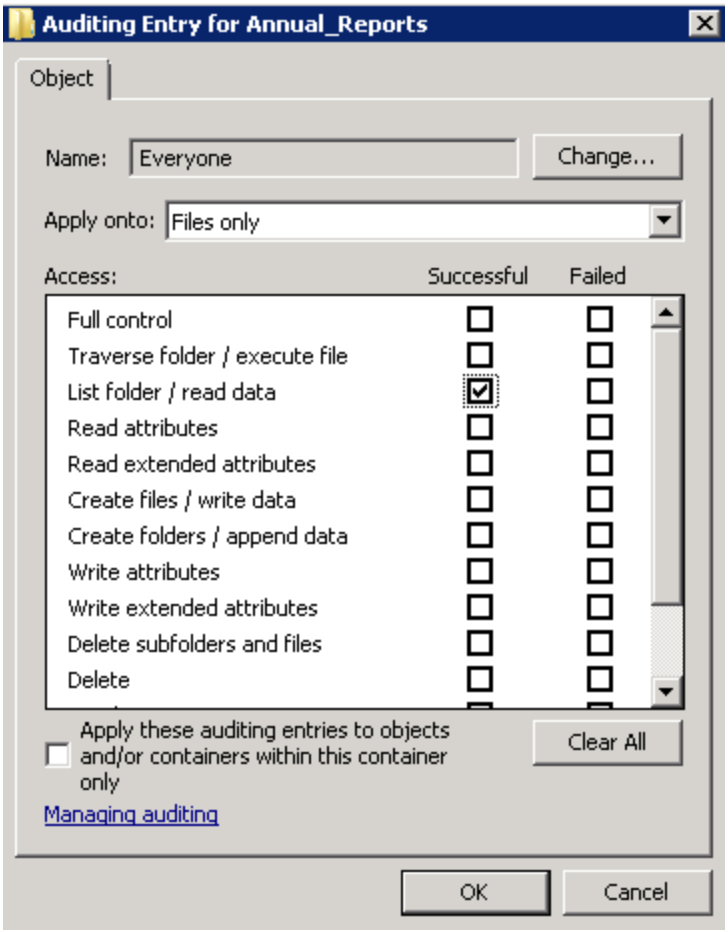
performed in the Netwrix Auditor client and the product will only audit user accounts that belong to the selected group.

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 and changes as well as failed read and change 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 changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry
Successful reads

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

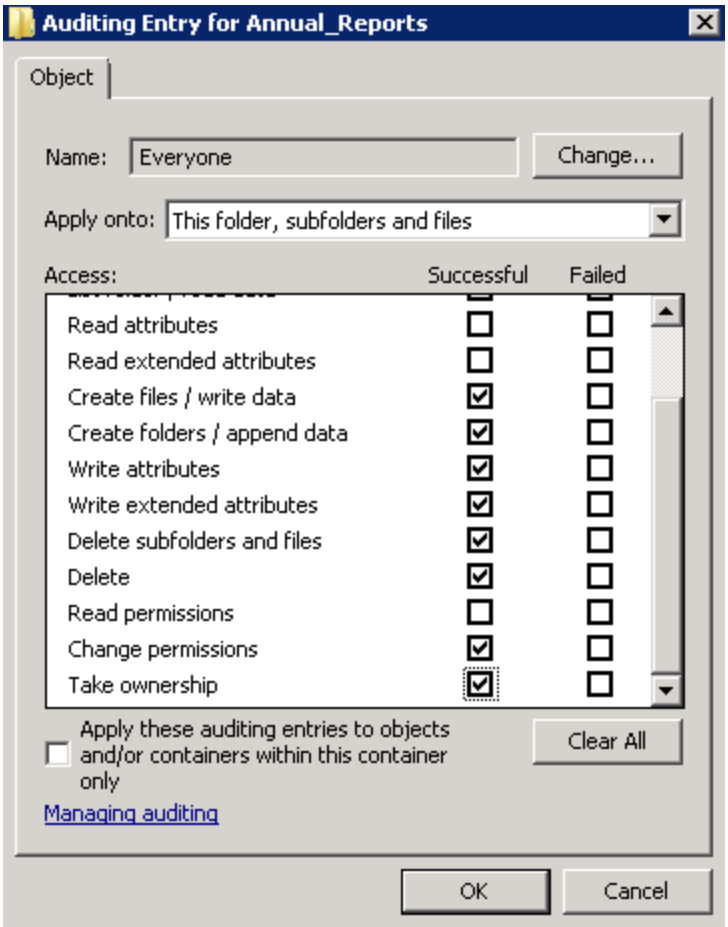


Auditing Entry

- Apply onto—Select *"Files only"*.
- Check *"Successful"* and *"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.

Successful changes

The Auditing Entry below shows Advanced Permissions for auditing successful changes 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**

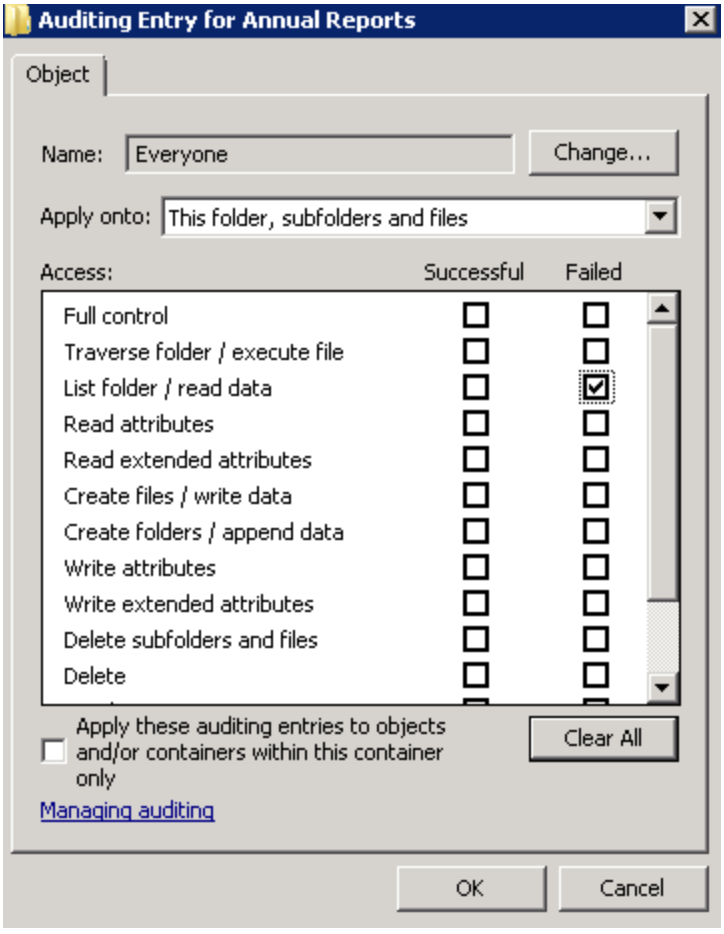
Auditing Entry

- **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.

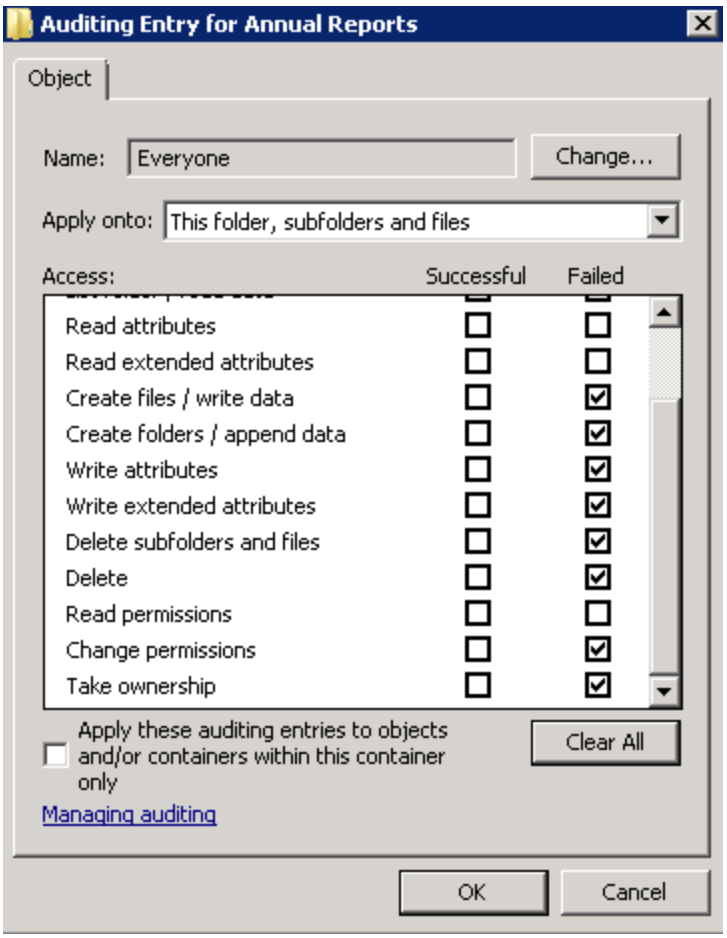
Failed read attempts

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**.

Auditing Entry
• Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.
Failed change attempts
The Auditing Entry below shows Advanced Permissions for auditing failed change 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**

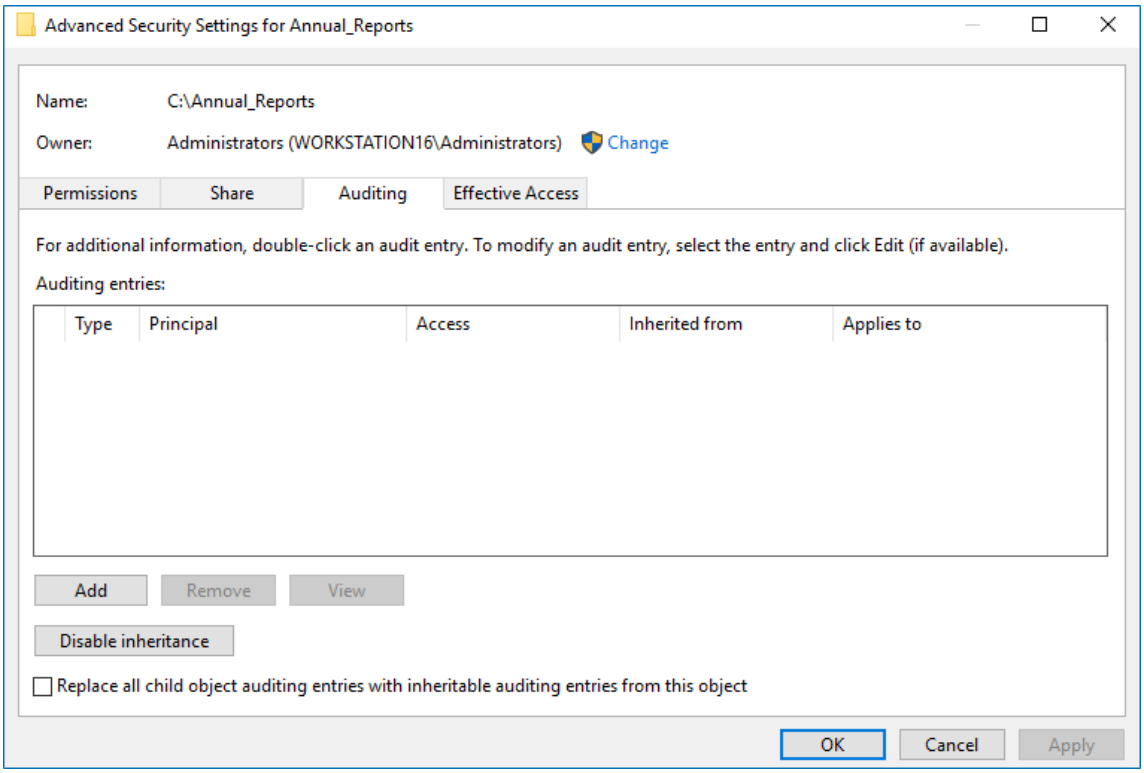
Auditing Entry

- **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.

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**.

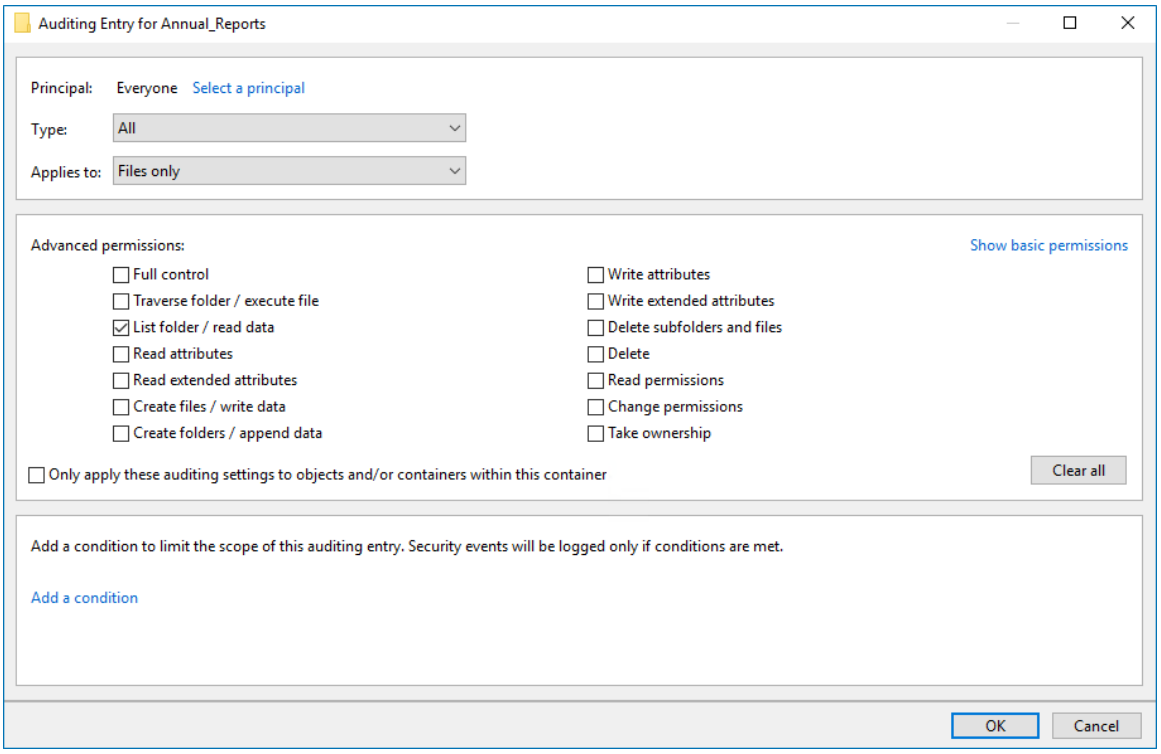
NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. The product will audit only user accounts that belong to the selected group.

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 changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry
Successful reads

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

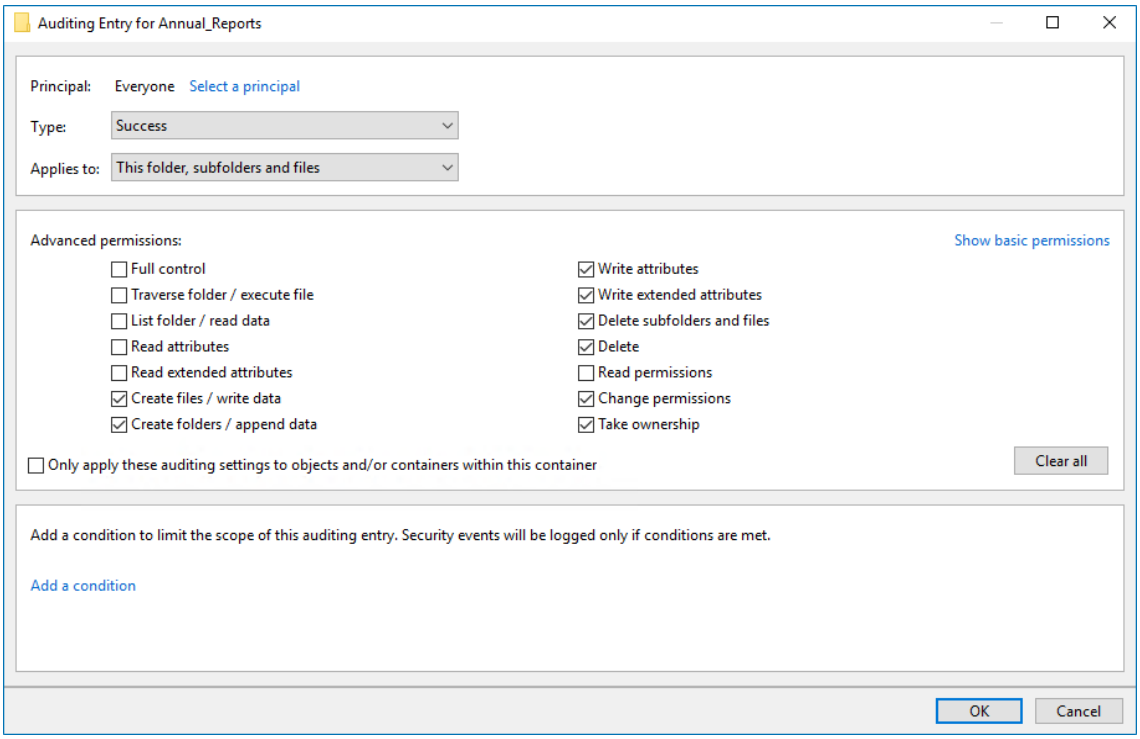


- Type—Set to *"All"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Auditing Entry

Successful changes

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

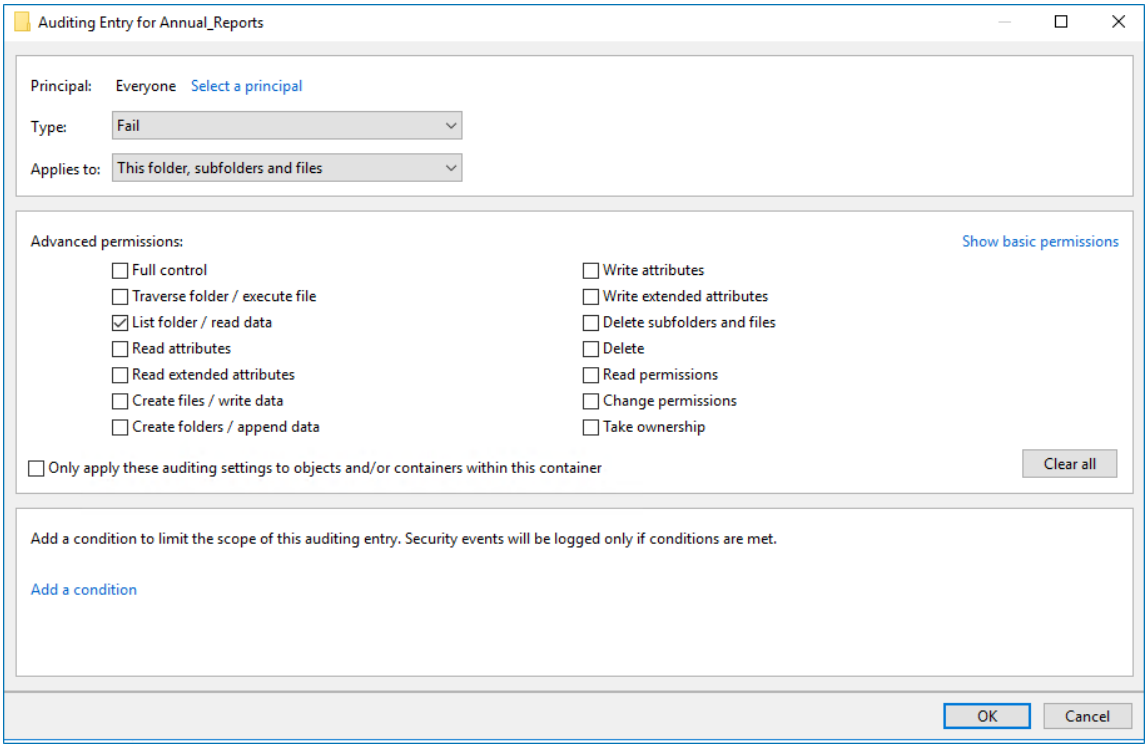


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change 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:

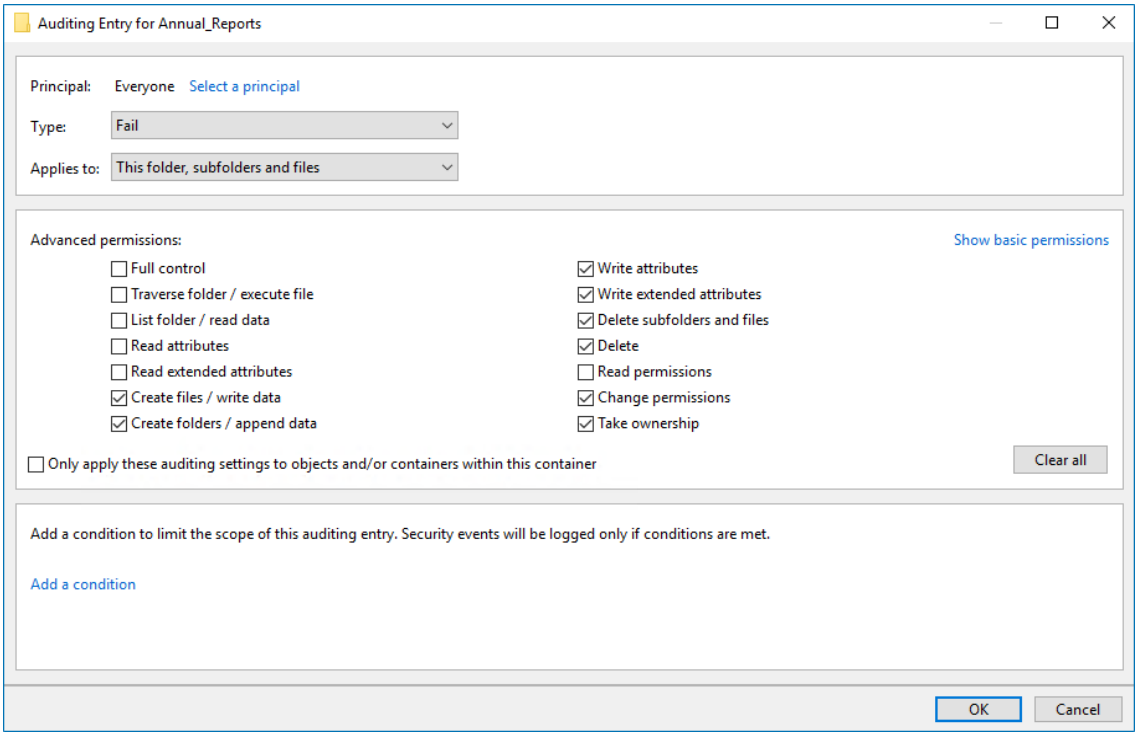


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed change attempts

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

Auditing Entry



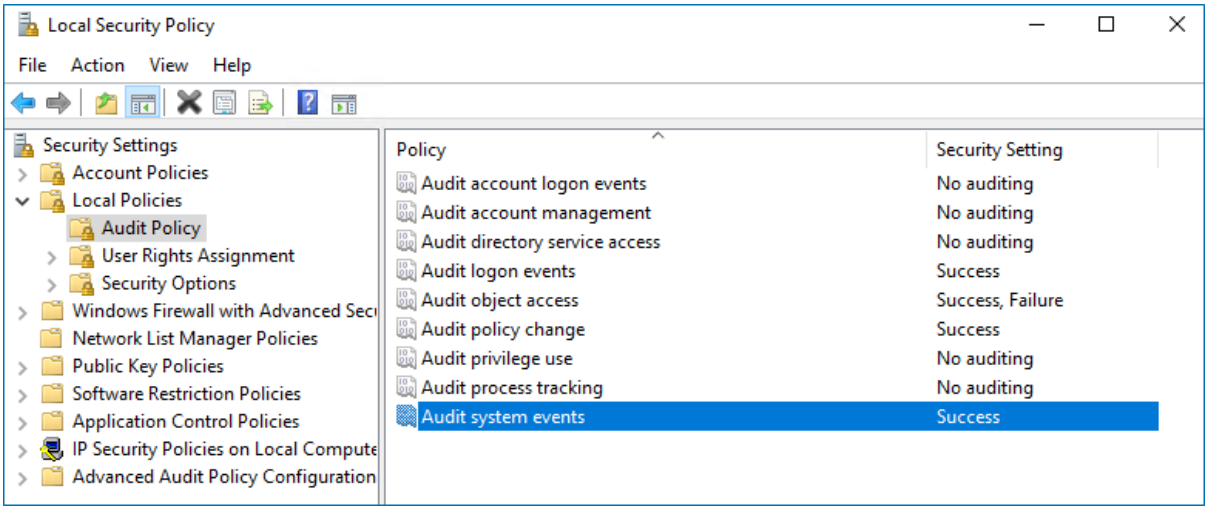
- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change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

5.4.2. Configure Local Audit Policies

You can choose whether to configure legacy policies as described below or to configure advanced policies. See Configure Advanced Audit Policies for more information.

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **Audit Policy**.

Policy Name	Audit Events
Audit object access	*"Success"* and *"Failure"*
Audit policy change	*"Success"*
Audit logon events	*"Success"*
Audit system events	*"Success"*



5.4.3. Configure Advanced Audit Policies

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 Local Audit Policies.

Perform the following procedures:

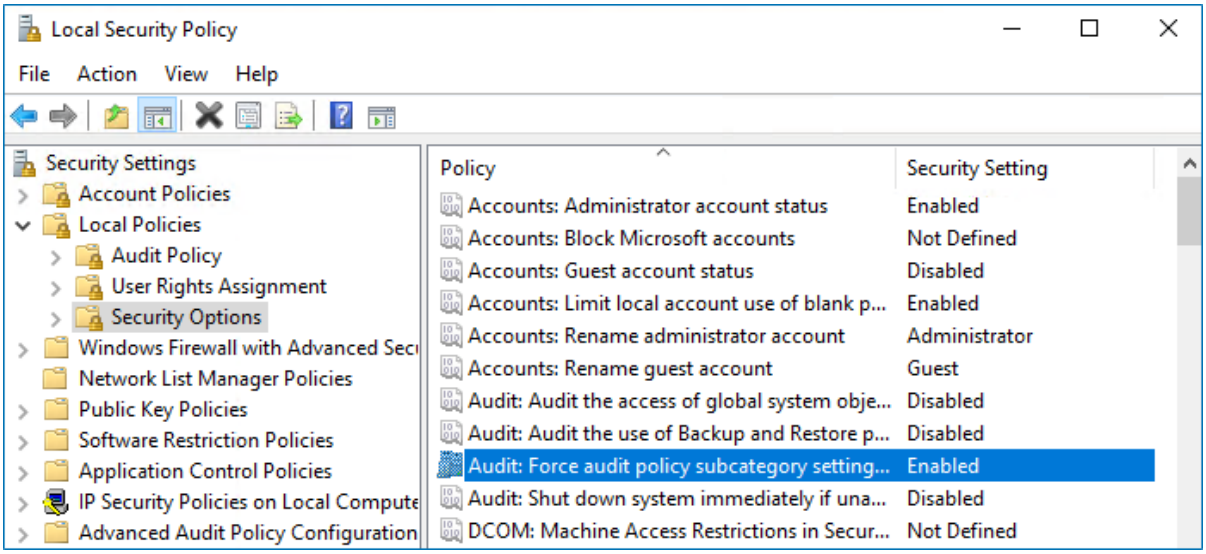
- To configure security options
- To configure advanced audit policy on Windows Server 2008 / Windows Vista
- To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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** and **Policy Change** categories by executing the following command in the

command line interface:

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

3. Enable the following audit subcategories:

Audit subcategory	Command
Handle Manipulation	`auditpol /set /subcategory:"Handle Manipulation" /success:enable /failure:enable`
File System	`auditpol /set /subcategory:"File System" /success:enable /failure:enable`
File Share	`auditpol /set /subcategory:"File Share" /success:enable /failure:disable`
Audit Policy Change	`auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:disable`
Security State Change	`auditpol /set /subcategory:"Security State Change" /success:enable`
Logon	`auditpol /set /subcategory:"Logon" /success:enable`
Logoff	`auditpol /set /subcategory:"Logoff" /success: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"` and `auditpol /get /category:"Policy Change"`.

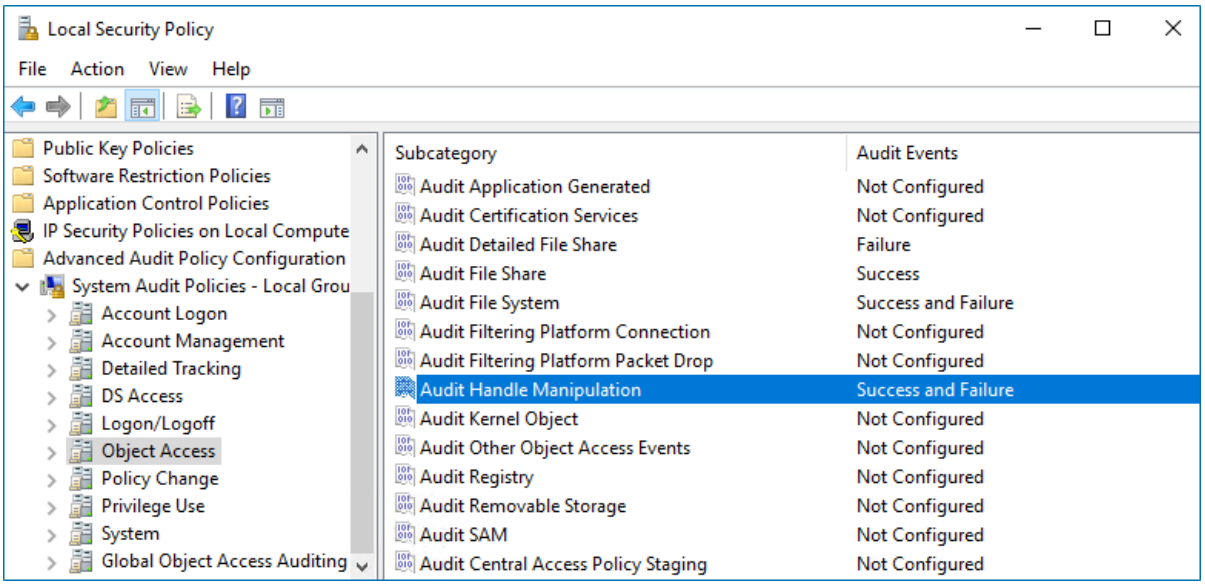
To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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
Object Access	• **Audit File System** • **Audit Handle Manipulation**	*"Success"* and/or *"Failure"* depending on the type of events you want to track.
	• **Audit Detailed File Share**	*"Failure"*
	• **Audit File Share**	*"Success"*
Policy Change	• **Audit Audit Policy Change**	*"Success"*
Logon/Logoff	• **Logon**	*"Success"*
	• **Logoff**	*"Success"*
System	• **Security State Change**	*"Success"*

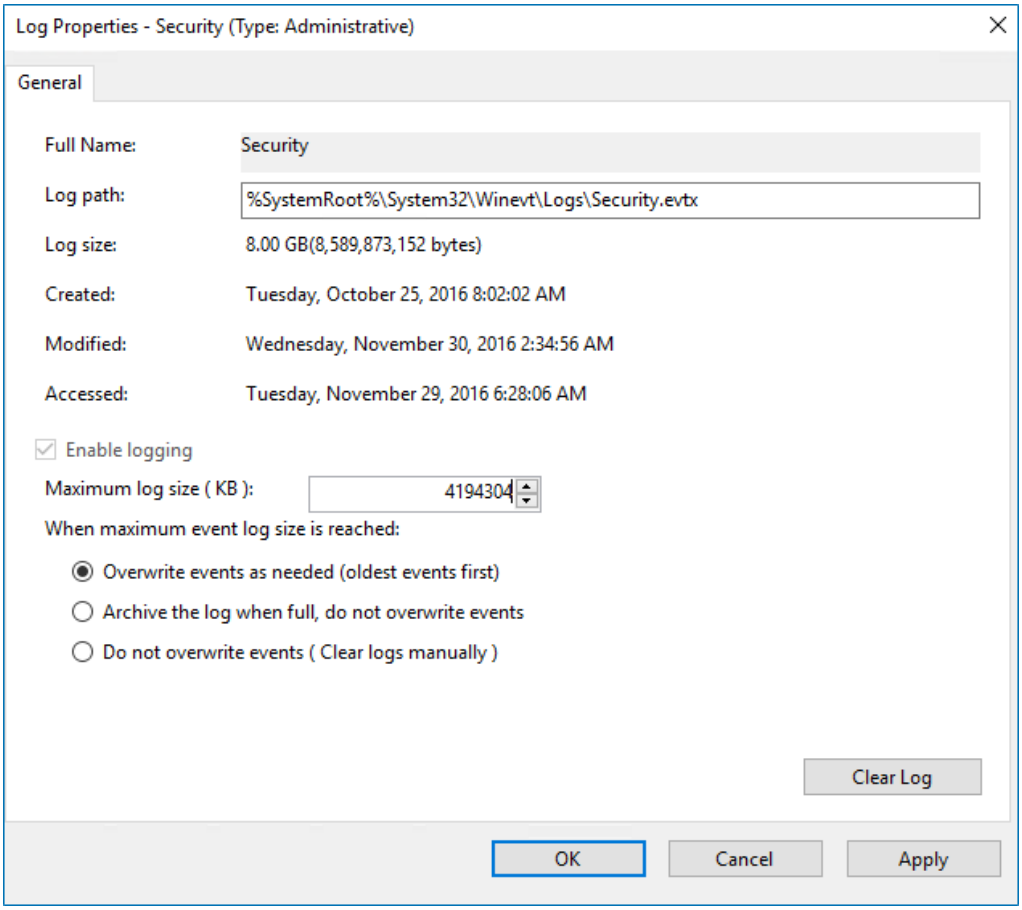


5.4.4. Configure Event Log Size and Retention Settings

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Security** and select **Properties**.



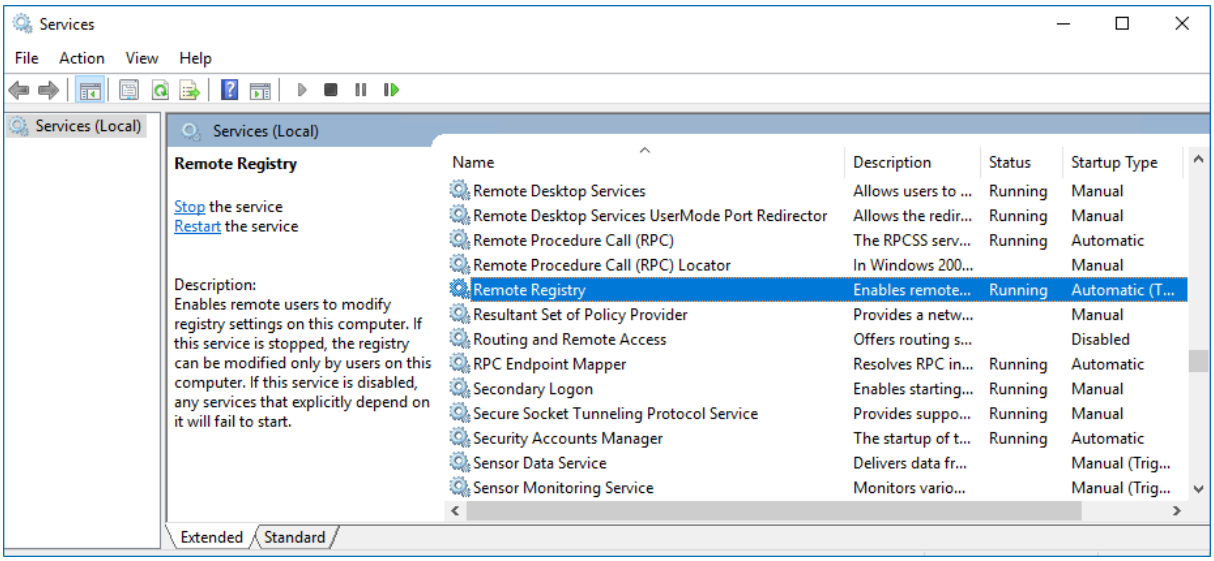
3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field, specify the size—4GB.
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

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**.

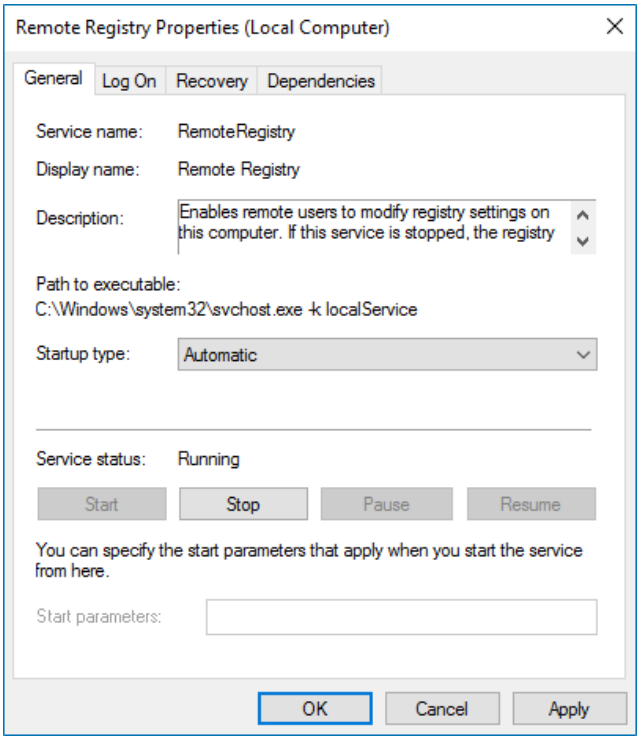
5.4.5. Enable Remote Registry Service

To enable the Remote Registry service

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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**.

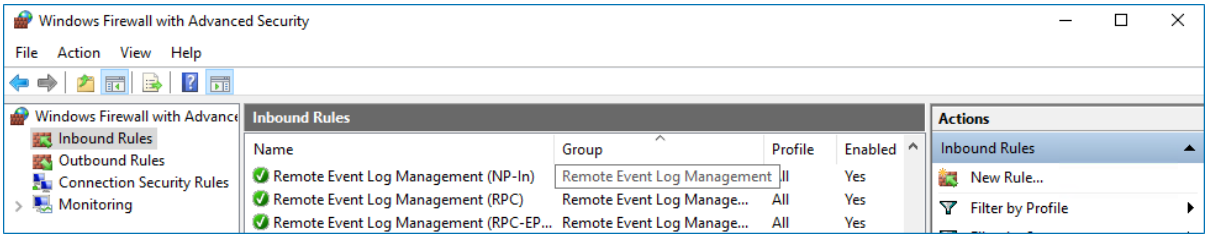


4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.

5.4.6. 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)**

5.4.7. Enable Symbolic Link Evaluations

By default, the **remote-to-local** and **remote-to-remote** symbolic link evaluations are unavailable when trying to follow them on the remote computers running Windows Vista and above. If you want to collect

state-in-time snapshots for file shares that contain these symbolic links, make sure that they are enabled on the computer that hosts Netwrix Auditor Server. Review the following for additional information:

- Refer to To enable symbolic link evaluations via command prompt for detailed instructions on how to enable symbolic links on a single computer.
- Refer to To enable symbolic link evaluations via Group Policy Management Console for detailed instructions on how to enable symbolic links for all computers in your domain.

To enable symbolic link evaluations via command prompt

1. On the computer where Netwrix Auditor Server resides, start the **Command Prompt** as administrator.
2. Review your symbolic links configuration:

   ```
   C:\>fsutil behavior query SymlinkEvaluation
   ```

   The default settings shall be as follows:

   ```
   Local to local symbolic links are enabled.
   Local to remote symbolic links are enabled.
   Remote to local symbolic links are disabled.
   Remote to remote symbolic links are disabled.
   ```

3. Enable the **remote-to-local** and **remote-to-remote** symbolic link evaluations:

   ```
   C:\>fsutil behavior set SymlinkEvaluation R2R:1 R2L:1
   ```

To enable symbolic link evaluations via Group Policy Management Console

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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**, navigate to **Computer Configuration** → **Policies** → **Administrative Templates: Policy definitions** → **System** → **Filesystem**.
4. In the **Filesystem** configuration, double click the **Selectively allow the evaluation of a symbolic link** setting.
5. In the dialog that opens, select **Enabled** and check all types of symbolic link evaluations under **Options**.
6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

5.5. Configure EMC VNX/VNXe for Auditing

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

- Automatically when creating a monitoring plan—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

NOTE: If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

5.5.1. 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 Server 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"*.

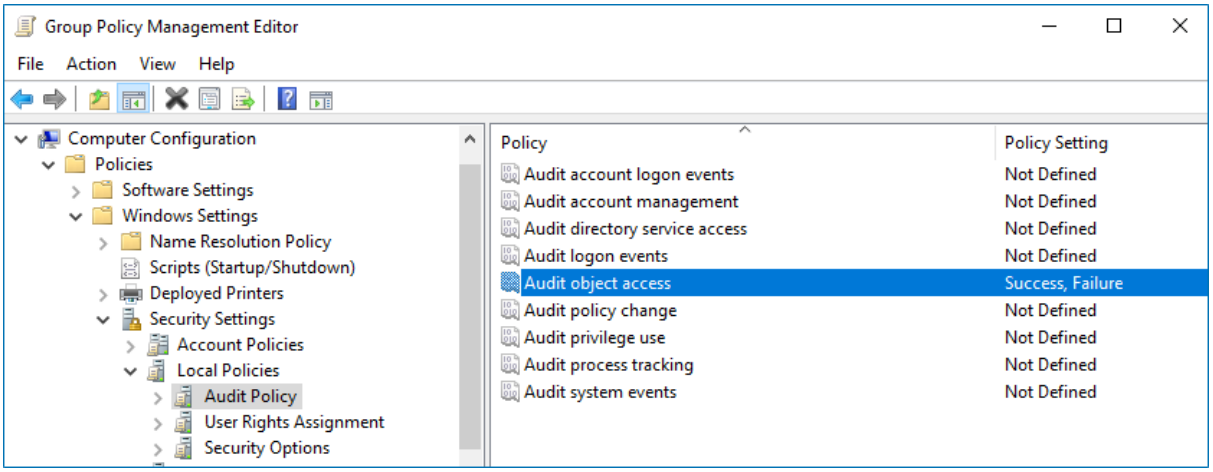
7. Set the **MaxSize** value to *"4 000 000 000 (decimal)"*.
8. Restart the corresponding Data Mover for the changes to take effect.

5.5.2. 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

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

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

Option		Description
Changes	Successful	Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion.
	Failed	Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it.
Read access	Successful	Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.

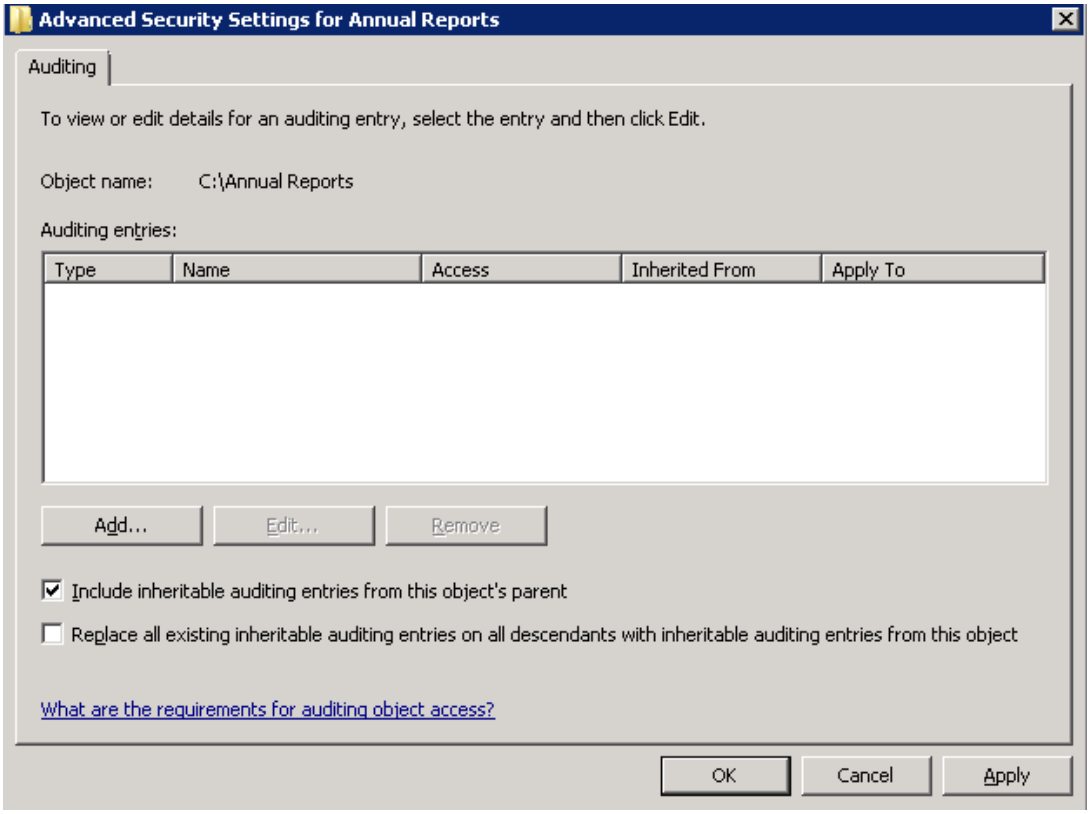
NOTE: Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, renaming, and copying. To track the copy action, enable successful read access and change auditing.

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**.

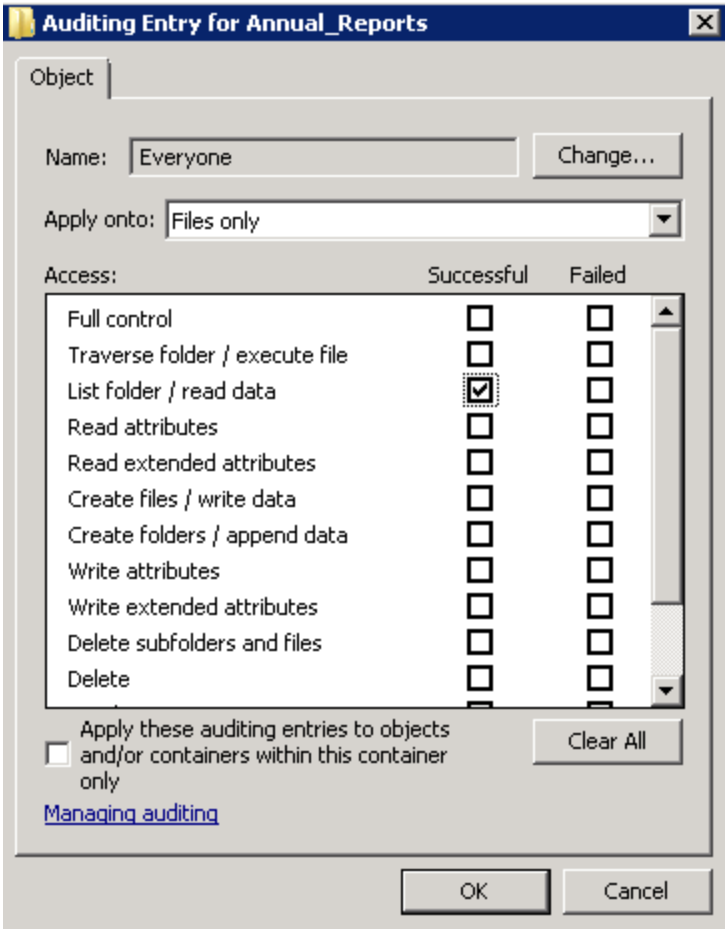
   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with errors on incorrect audit configuration. This will not affect the reports or data searches performed in the Netwrix Auditor client and the product will only audit user accounts that belong to the selected 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 and changes as well as failed read and change 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 changes
- Failed read attempts
- Failed change attempts

Auditing Entry
Successful reads

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

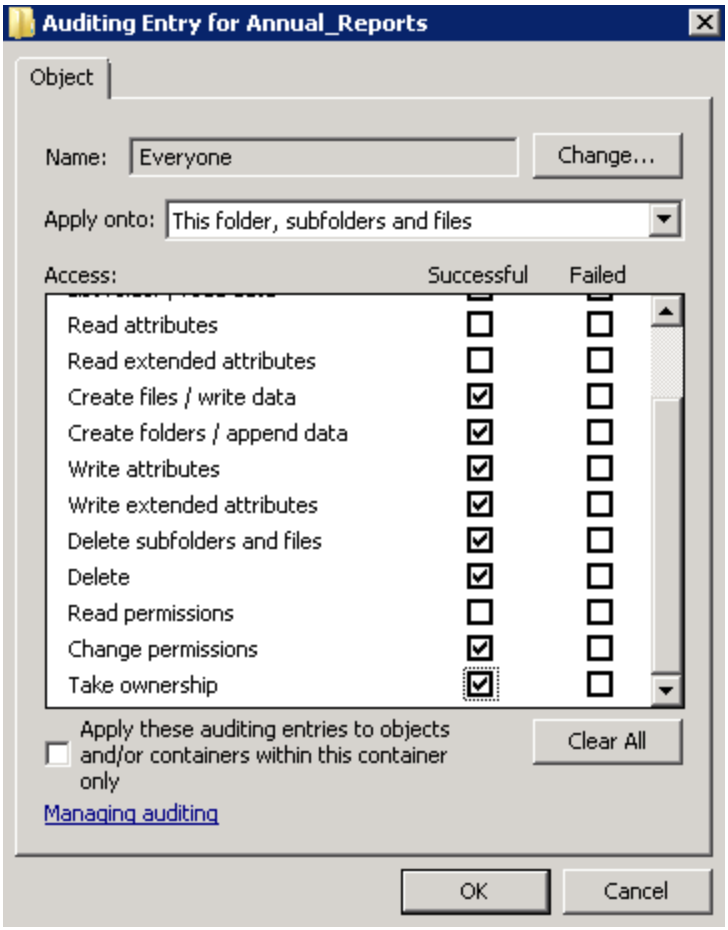


- Apply onto—Select *"Files only"*.
- Check *"Successful"* and *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful changes

Auditing Entry

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

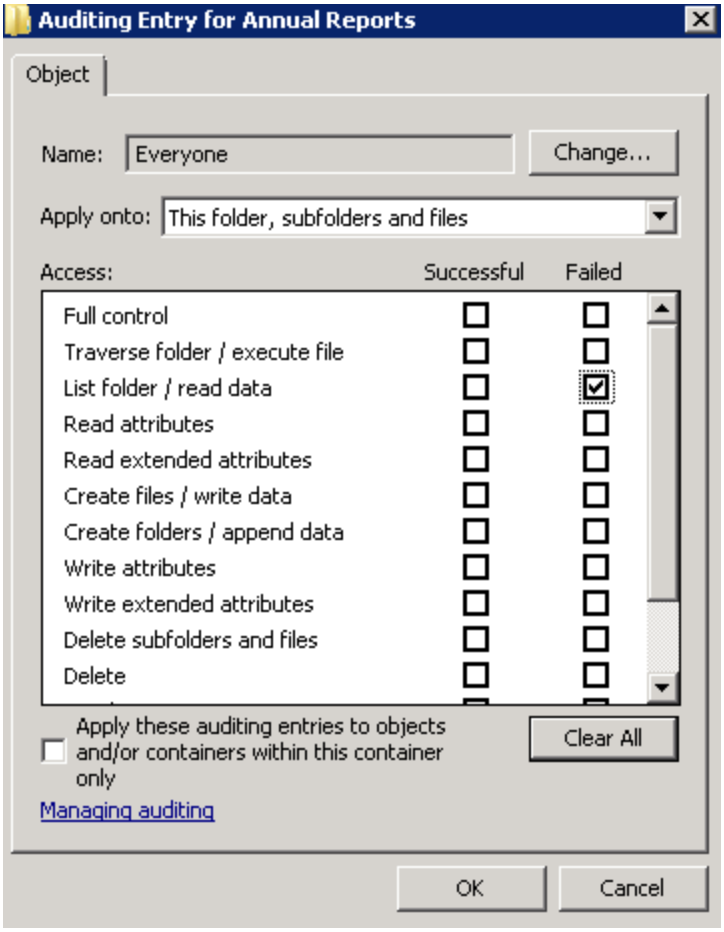


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Successful"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  -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

Auditing Entry
container only checkbox is cleared.

Failed read attempts

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

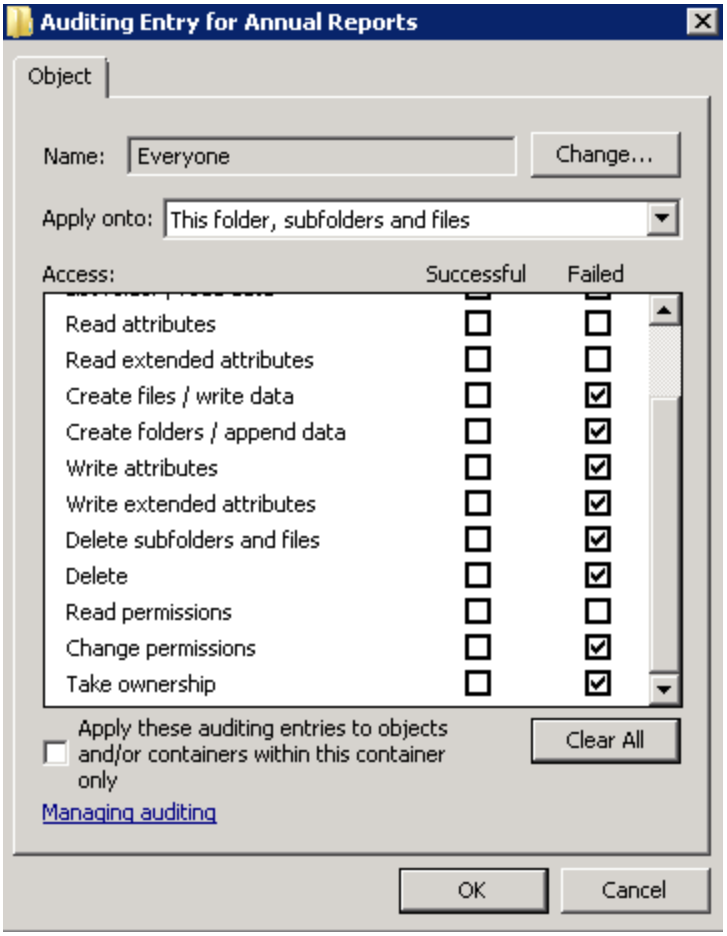


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed change attempts

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

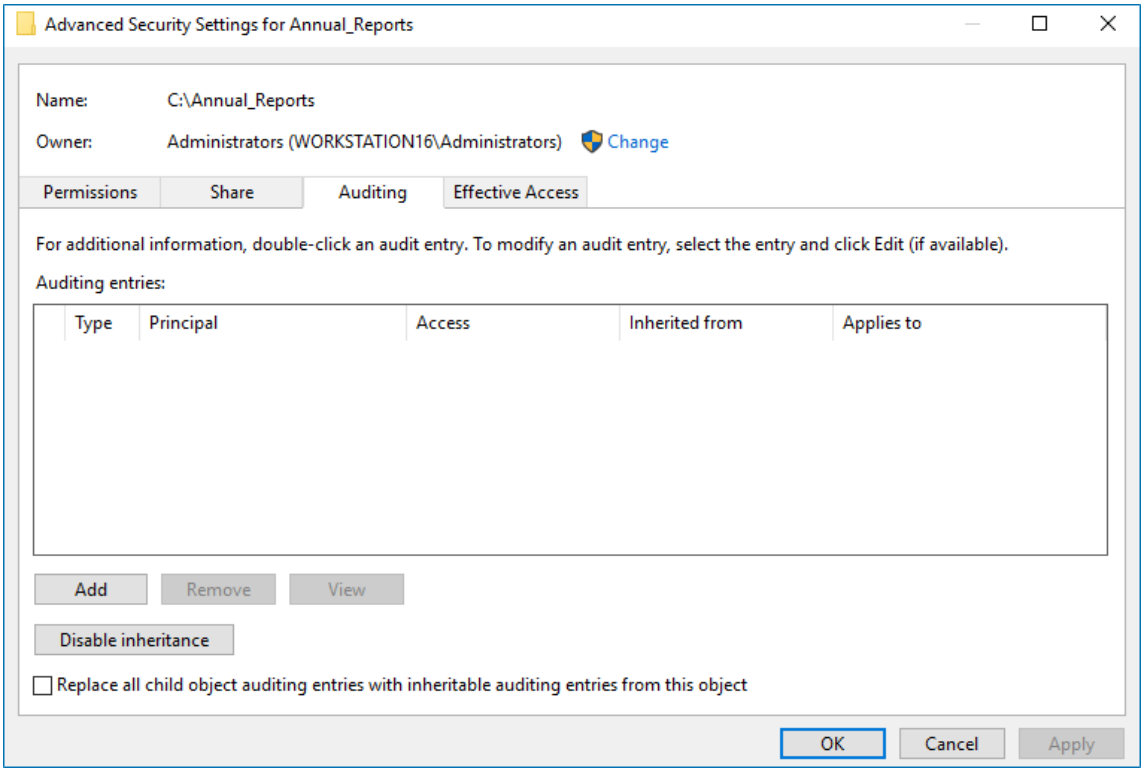
Auditing Entry



- 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.

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:

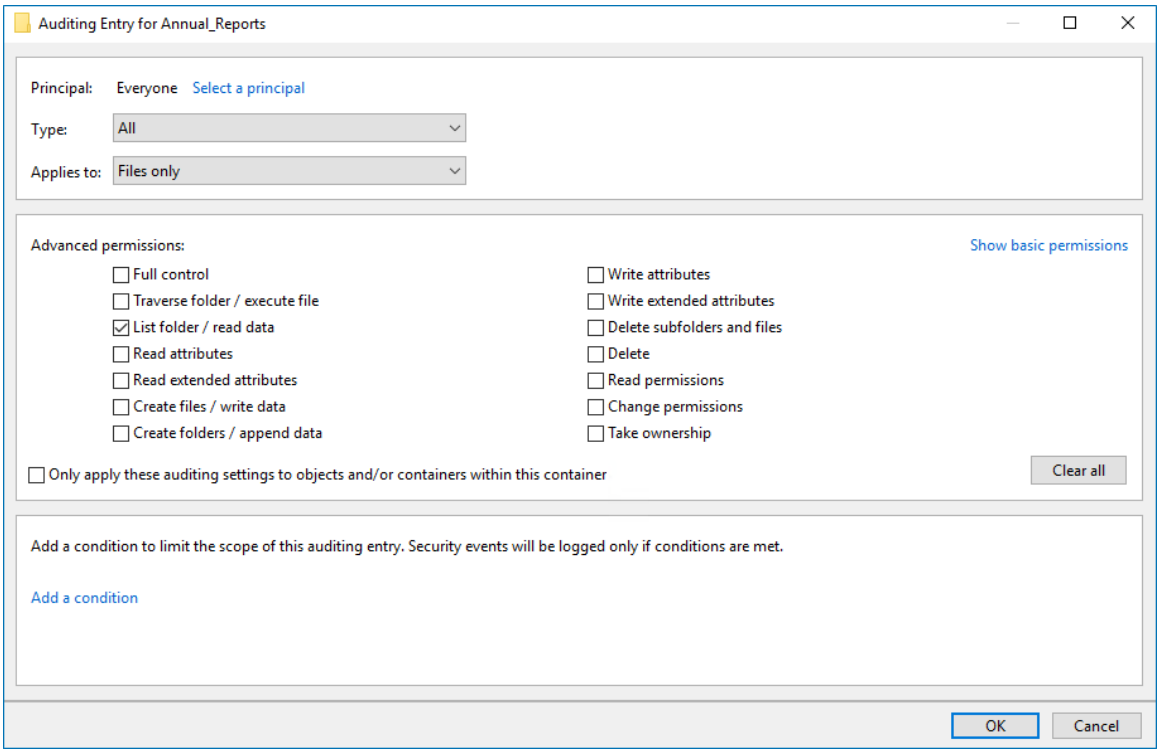
   - Successful reads
   - Successful changes

- Failed read attempts
- Failed change attempts

Auditing Entry

Successful reads

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

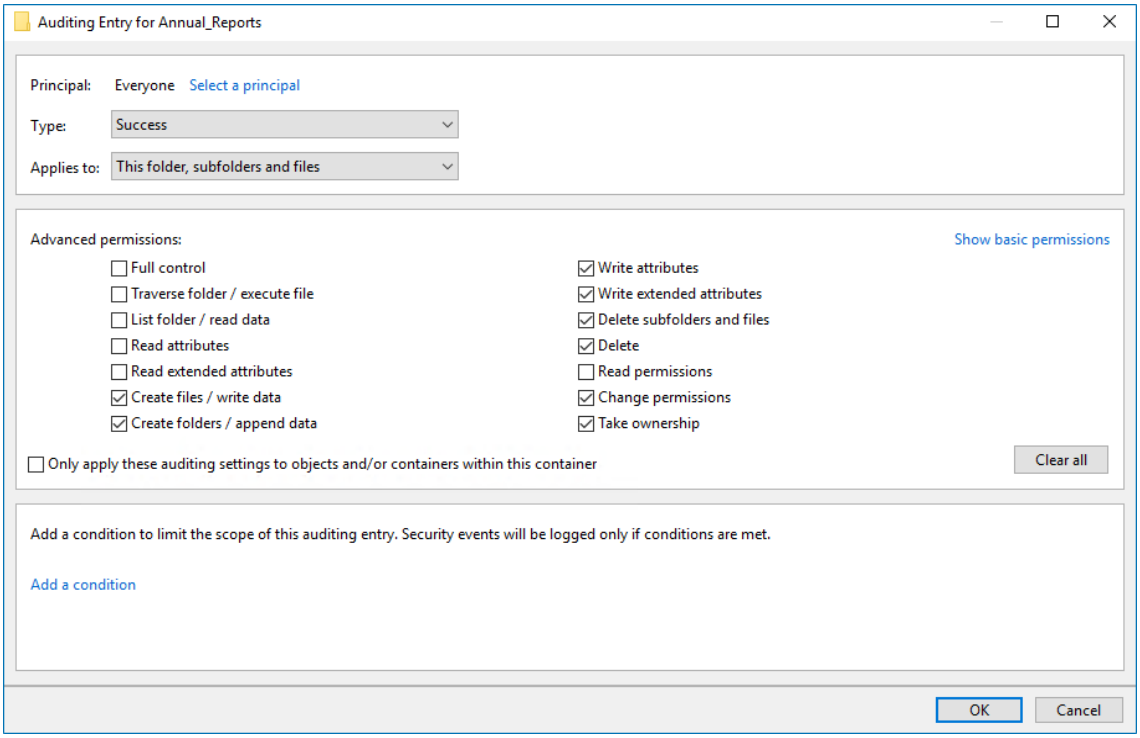


- Type—Set to *"All"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful changes

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

Auditing Entry

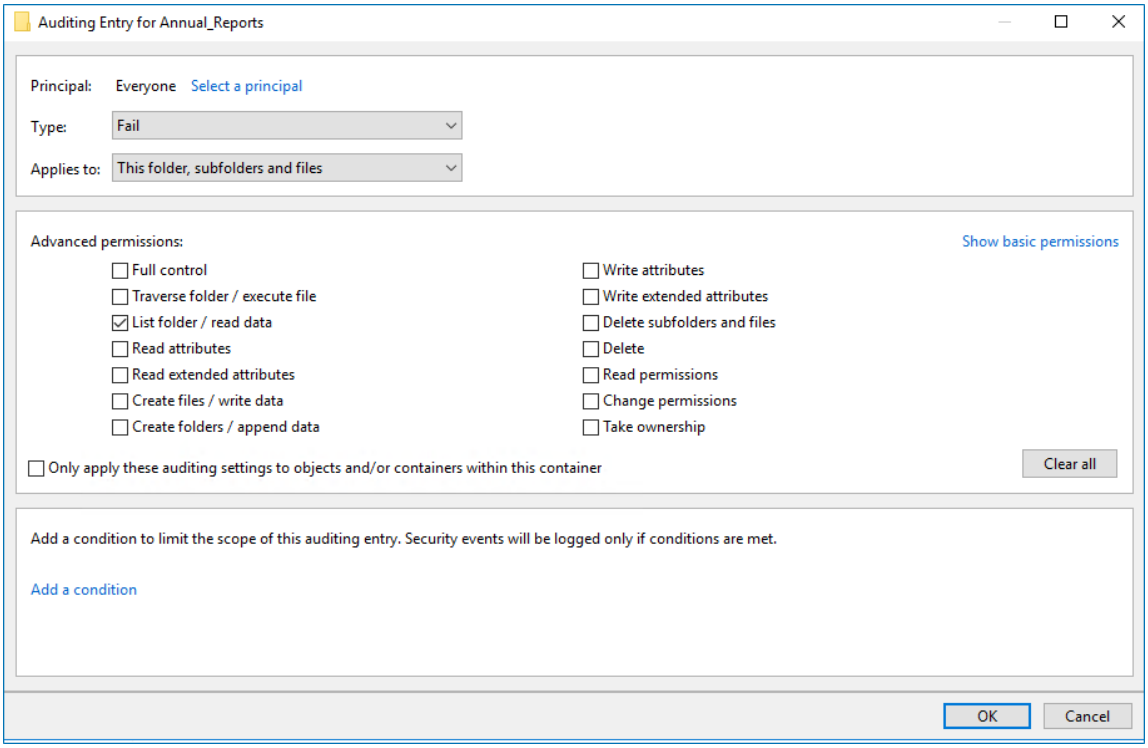


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change 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

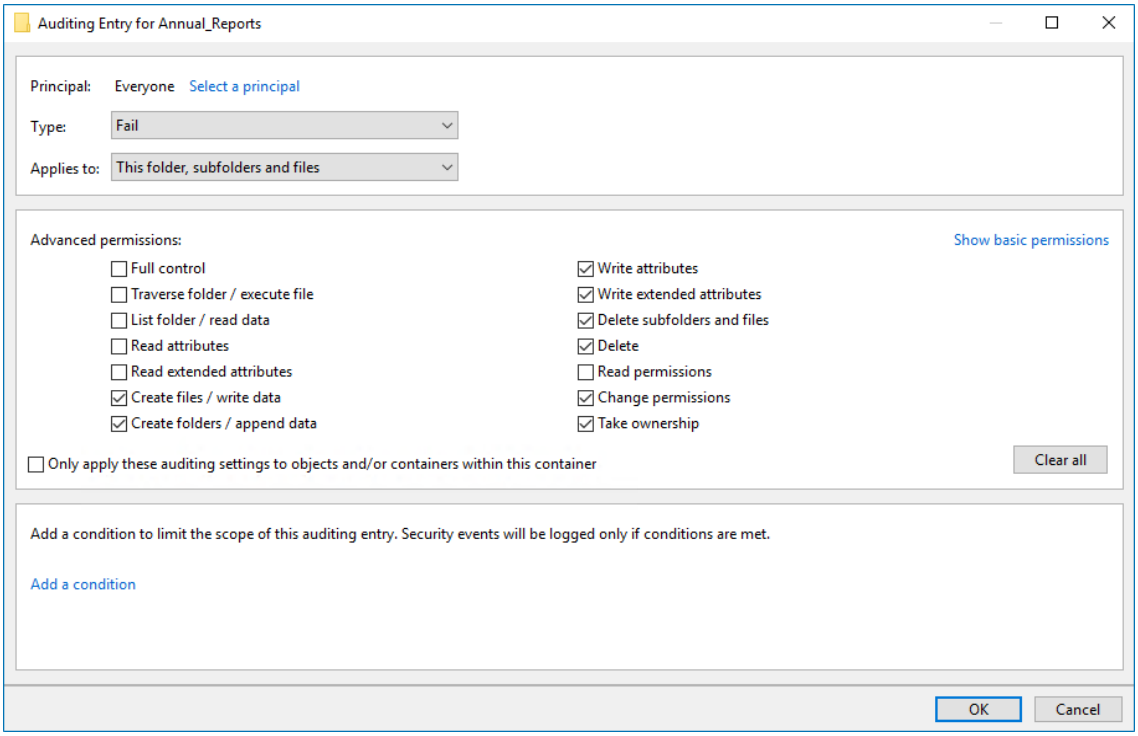


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change 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.

5.6. Configure EMC Isilon for Auditing

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

NOTE: If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

5.6.1. 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 Server 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 changes        1
   Failed change 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"*). Do one of the following, depending on your EMC Isilon version:

EMC Isilon 7.x	EMC Isilon 8.x
`isi audit settings modify --add-audited-zones=zone1 --protocol-auditing-enabled=true`	`Isi audit settings global 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.

EMC Isilon 7.x	EMC Isilon 8.x
Successful changes	
Audit Success: write, delete, set_security, rename	
`isi zone zones modify zone1 --audit- success=write,delete,set_security,rename`	`isi audit settings modify --zone= zone1 --audit-success= write,delete,set_security,rename`
Failed change attempts	
Audit Failure: create, write, delete, set_security, rename	

EMC Isilon 7.x	EMC Isilon 8.x
`isi zone zones modify zone1 --audit-failure=create,write,delete,set_security,rename`	`isi audit settings modify --zone= zone1 --audit-failure= create,write,delete,set_security,rename`
Successful reads Audit Success: read	
`isi zone zones modify zone1 --audit-success=read`	`isi audit settings modify --zone= zone1 --audit-success= read`
Failed read attempts Audit Failure: create, read	
`isi zone zones modify zone1 --audit-failure= create,read`	`isi audit settings modify --zone= 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"
```

5.6.2. 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 Server 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 changes        1
Failed change 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 collection account the *"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 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 collecting account the *"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 account name.

6. Configure protocol auditing for selected zone (for example, *"zone1"*). Do one of the following, depending on your EMC Isilon version:

EMC Isilon 7.x	EMC Isilon 8.x
`isi audit settings modify --add-audited-zones=zone1 --protocol-auditing-enabled=true`	`Isi audit settings global 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.

EMC Isilon 7.x	EMC Isilon 8.x
Successful changes Audit Success: write, delete, set_security, rename	
`isi zone zones modify zone1 --audit-success=write,delete,set_security,rename`	`isi audit settings modify --zone=zone1 --audit-success=write,delete,set_security,rename`
Failed change attempts Audit Failure: create, write, delete, set_security, rename	
`isi zone zones modify zone1 --audit-failure=create,write,delete,set_security,rename`	`isi audit settings modify --zone=zone1 --audit-failure=create,write,delete,set_security,rename`
Successful reads Audit Success: read	
`isi zone zones modify zone1 --audit-success=read`	`isi audit settings modify --zone=zone1 --audit-success= read`
Failed read attempts Audit Failure: create, read	
`isi zone zones modify zone1 --audit-failure= create,read`	`isi audit settings modify --zone=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"
```

5.7. Configure NetApp Filer for Auditing

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

- Automatically when creating a monitoring plan

  NOTE: For NetApp Data ONTAP 7 and 8 in 7-mode, configure audit automatically. For NetApp Clustered Data ONTAP 8 or ONTAP 9 only file share audit settings 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 and ONTAP 9 for Auditing
  - Configure Audit Settings for CIFS File Shares

NOTE: If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

5.7.1. 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

5.7.1.1. 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>
  ```

5.7.1.2. 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>
```

5.7.1.3. 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>
```

5.7.1.4. 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

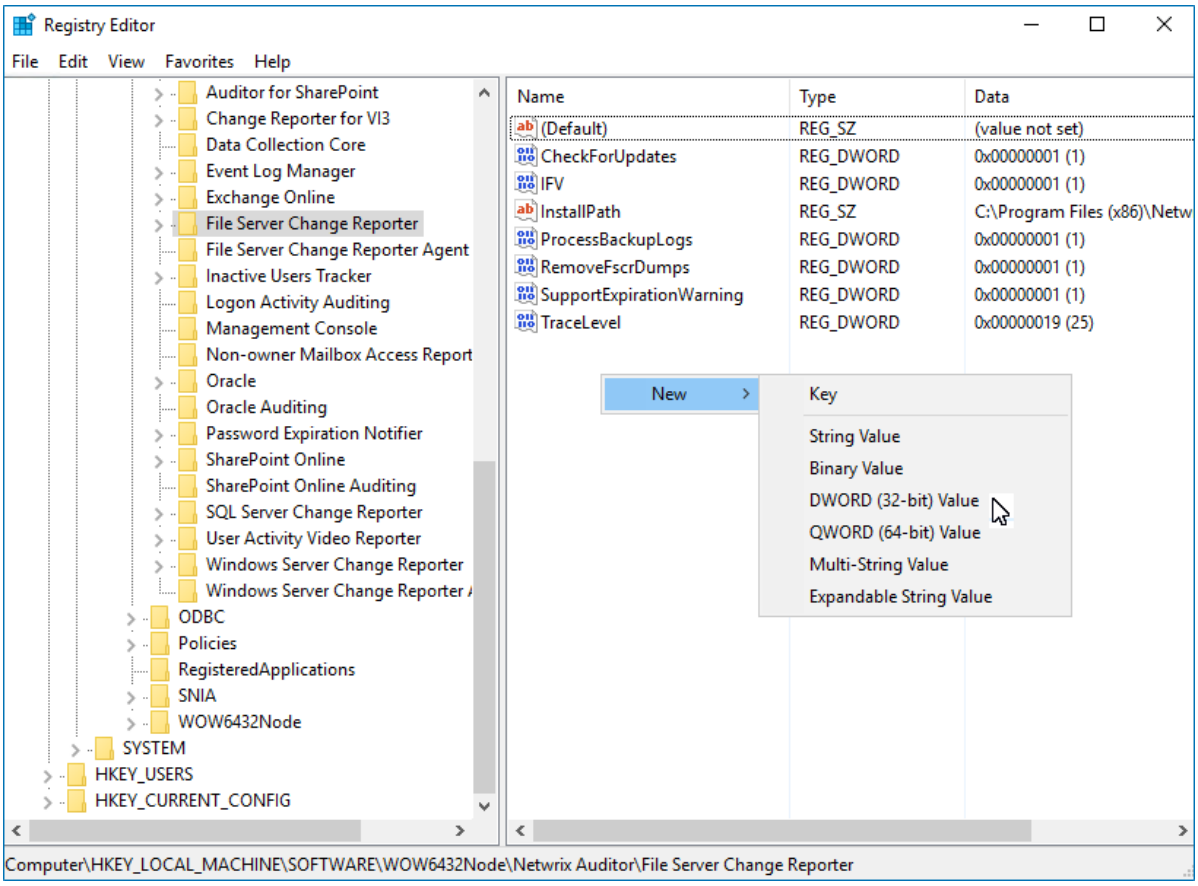
1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. In order to avoid overwriting of the security logs, set the following values:
   - `cifs.audit.logsize 300 000 000 (300 MB)`
   - `cifs.audit.autosave.onsize.enable 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

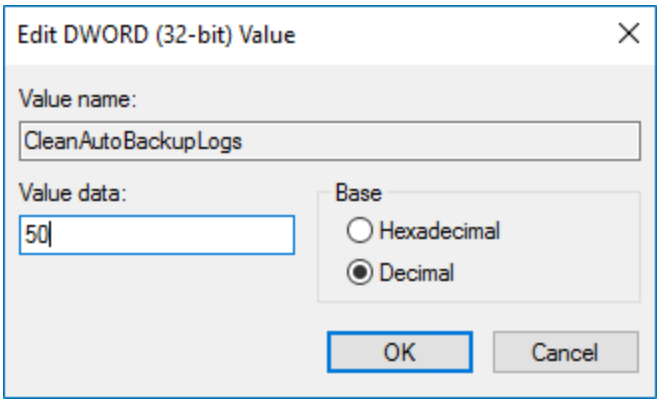
1. On the computer where Netwrix Auditor Server resides, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **File Server Change Reporter**.
3. In the right-pane, right-click and 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 with Netwrix Auditor.

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.

5.7.2. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Auditing

To configure Clustered Data ONTAP 8 and ONTAP 9 for auditing, perform the following procedures:

- Prerequisites
- Configure ONTAPI Web Access
- Configure Firewall Policy
- Configure Event Categories and Log

5.7.2.1. Prerequisites

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

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
ONTAP 9.0 and 9.1	• ONTAP 9 Documentation Center

Perform the steps below before proceeding with audit 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. For 8.3, 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 does not support auditing of Infinite Volumes.

5.7.2.2. 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). For example:

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

6. Make sure that the builtin **vsadmin** role or a custom role (e.g., fsa_role) assigned to your account specified for data collection 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.
```

5.7.2.3. Configure Firewall Policy

Configure firewall to make file shares and Clustered Data ONTAP HTTP/HTTPS ports accessible from the computer where Netwrix Auditor Server 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. Create firewall policy or edit existing policy to allow HTTP/HTTPS (note that modifying a policy you may overwrite some settings). For example:

To...	Execute...
NetApp Clustered Data ONTAP 8.2	
Create a policy	`cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
Modify existing policy	`cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy modify -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
NetApp Clustered Data ONTAP 8.3, ONTAP 9.0, and ONTAP 9.1	
Create a policy	`cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24` `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`
Modify existing policy	`cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24` `cluster1::> system services firewall policy modify -policy`

To...	Execute...
	`pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`

where `pol1` is your Firewall policy name and `192.168.1.0/24` is your subnet where Netwrix Auditor Server resides.

4. Apply the firewall policy to a LIF.

   ```
   cluster1::>network interface modify -vserver vs1 -lif vs1-cifs-lif1 -firewall-policy pol1
   ```

   To verify the policy was applied correctly, execute the following:

   ```
   cluster1::>network interface show -fields -firewall-policy
   ```

5.7.2.4. Configure Event Categories and Log

Perform the following procedures to configure audit:

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

To configure auditing state, event categories and log

Configure audit settings in the context of Cluster or Storage Virtual Machine. All examples in the procedure below apply to SVM, to execute commands in the context of Cluster, add `-vserver name`, where `name` is your server name.

1. Navigate to command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and switch to the context of SVM from the cluster. For example to switch to the SVM called `vs1`:

   ```
   cluster1::> vserver context -vserver vs1
   ```

   After a switch, you will be in the context of SVM:

   ```
   vs1::>
   ```

3. Create and enable audit. For more information on audit configuration, refer to NetApp documentation. For example:

To...	Execute...
Create audit	`vs1::> vserver audit create -destination <path to the volume>`

To...	Execute...
	In the example above, the `vserver audit create -destination /audit` command executed on the `vs1` SVM creates and enables audit on the volume `/audit`. **NOTE:** Netwrix Auditor accesses audit logs via file shares. Make sure the volume you specified is mounted on SVM and shared (e.g., `audit$` is a share name and its path is `/audit`).
Enable audit	`vs1::> vserver audit enable`

4. Review your audit settings. For example, on ONTAPI 8.3 the default audit is configured as follows:

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

                                 Auditing State: true
                            Log Destination Path: /audit
                  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
```

5. Check the following options:

Option	Setting
`Auditing State`	`true`
`Categories of Events to Audit`	`file-ops` **NOTE:** Only required if you use Clustered Data ONTAP 8.3, ONTAP 9.0, and ONTAP 9.1. You cannot select event categories if you use Clustered Data ONTAP 8.2.
`Log Format`	*"XML"* or *"EVTX"*

6. Modify the log file size limit—set to 300 MB. Execute:

```
vs1::> vserver audit modify -rotate-size 300MB
```

300MB is the recommended maximum log size proceeding from performance evaluations. Make sure there is enough disk space allocated for 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.

7. After configuration, double-check your settings.

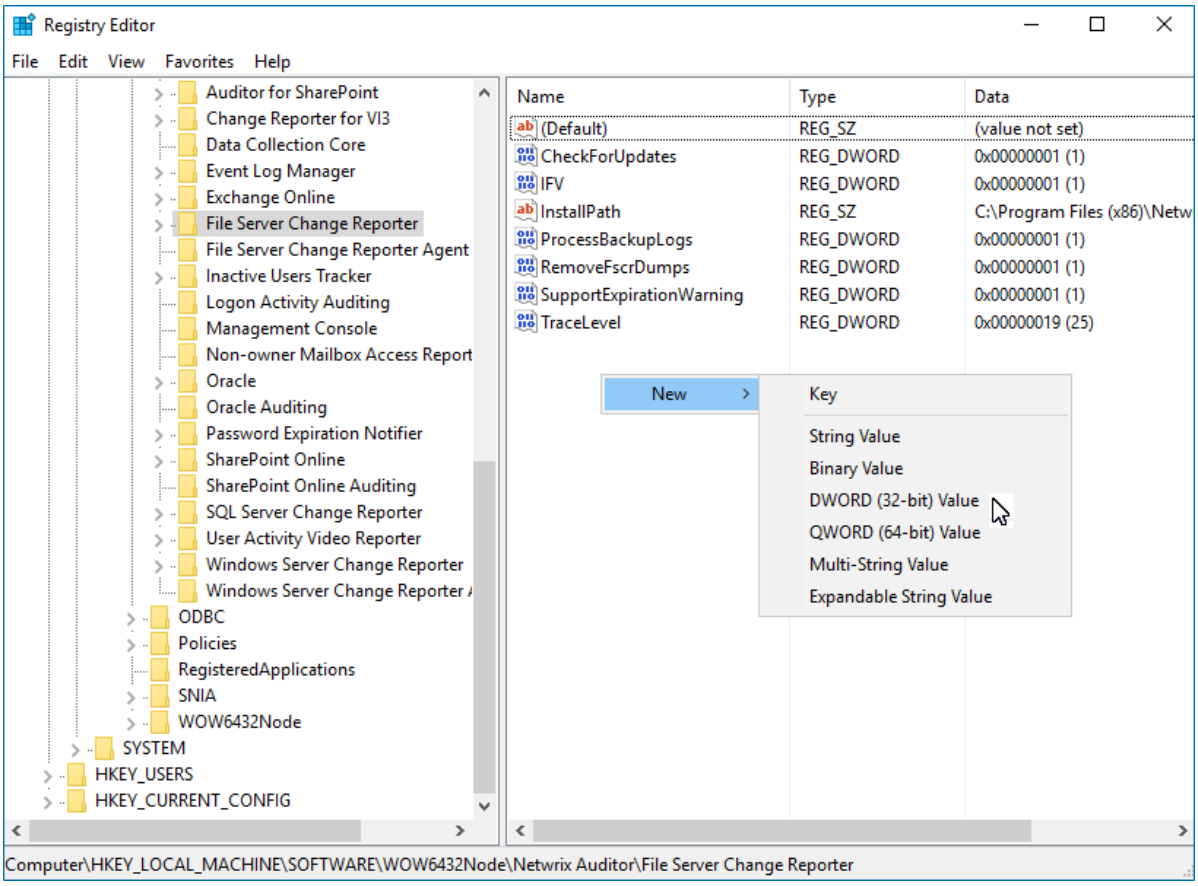
```
vs1::> vserver audit show -instance

                    Auditing State: true
              Log Destination Path: /audit
     Categories of Events to Audit: file-ops, cifs-logon-logoff
                        Log Format: evtx
                Log File Size Limit: 300MB
       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
```

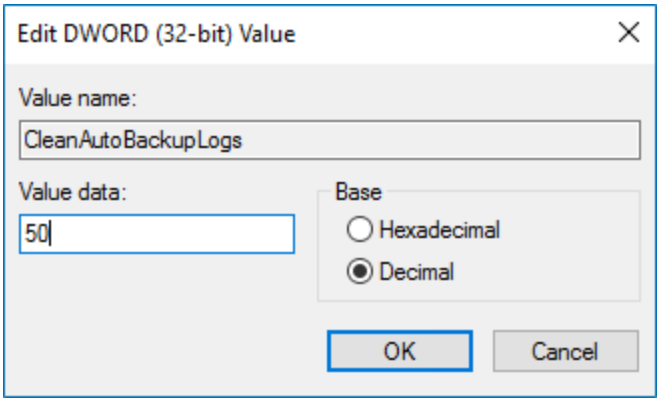
To configure logs retention period

1. On the computer where Netwrix Auditor Server resides, 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.

5.7.3. 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:

Option		Description
Changes	Successful	Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion.
	Failed	Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it.
Read access	Successful	Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.

NOTE: Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, renaming, and copying. To track the copy action, enable successful read access and change auditing.

Do one of the following depending on the OS:

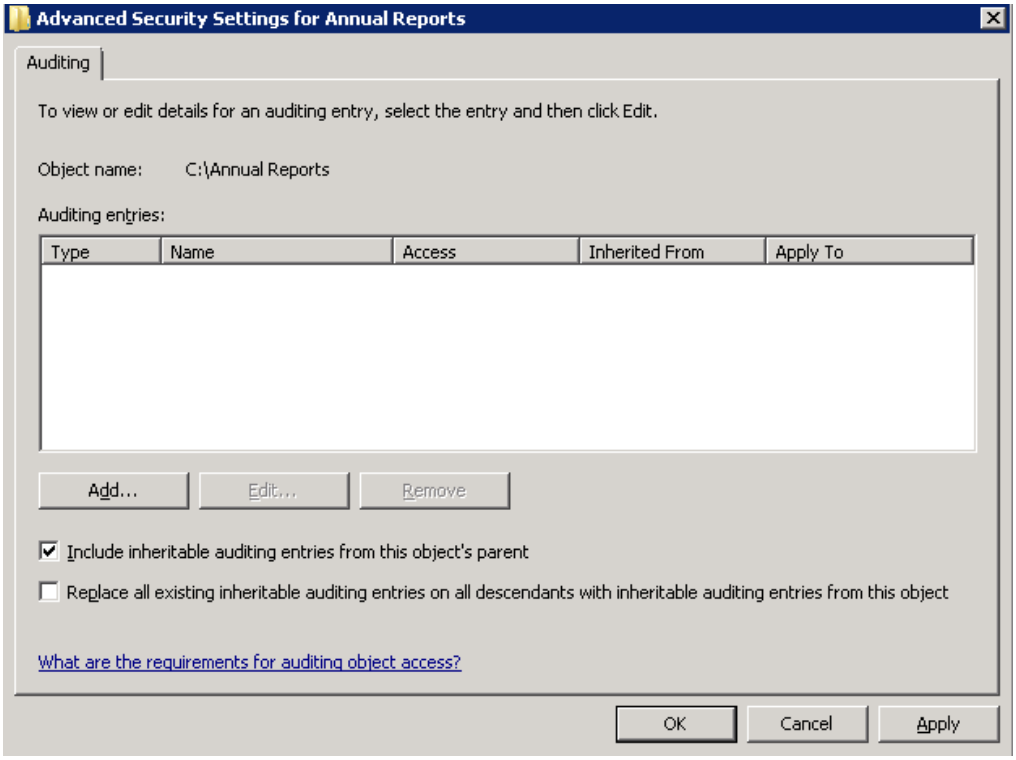
- To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions
- To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

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**.

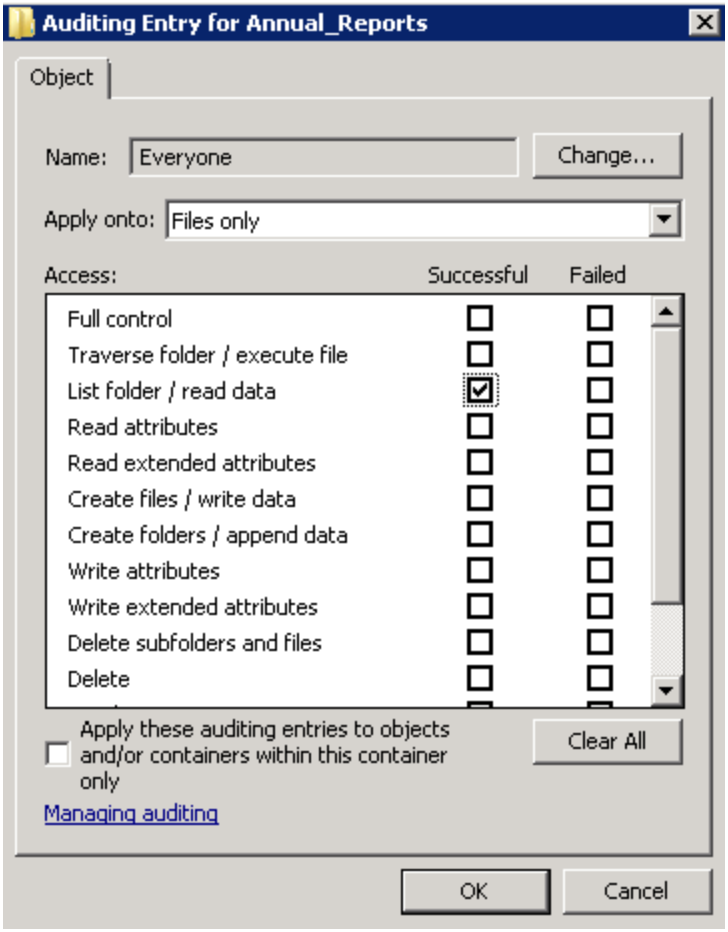
NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the Reports functionality and the product will only audit user accounts that belong to the selected group.

5. Apply settings to your Auditing Entries depending on actions that you want to audit. If you want to audit all actions (successful reads and changes as well as failed read and change 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 changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry
Successful reads

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

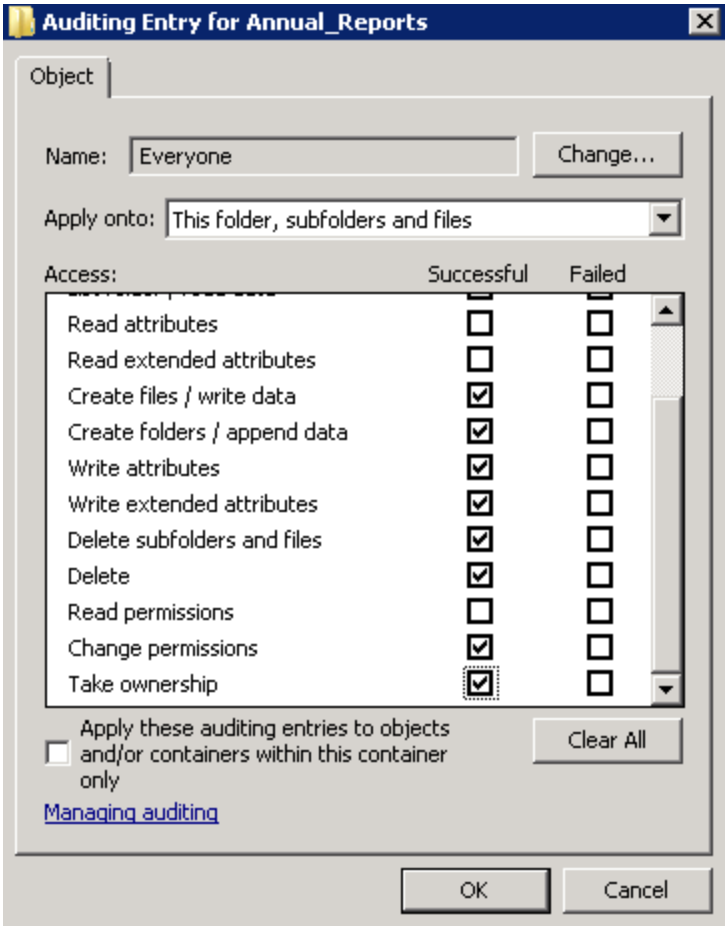


- Apply onto—Select *"Files only"*.
- Check *"Successful"* and *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful changes

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

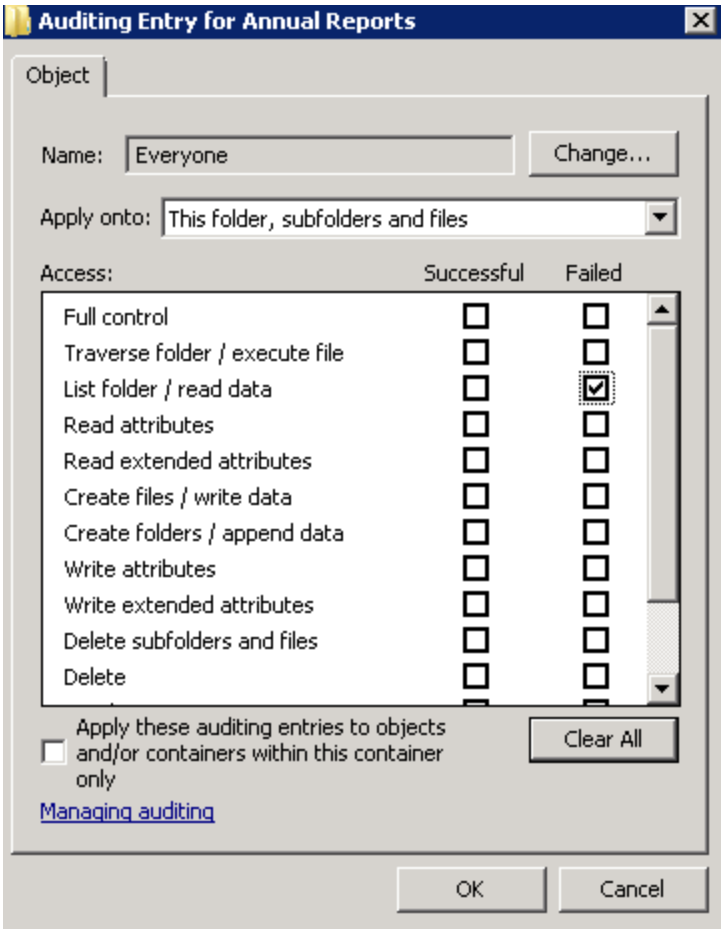
Auditing Entry



- 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:

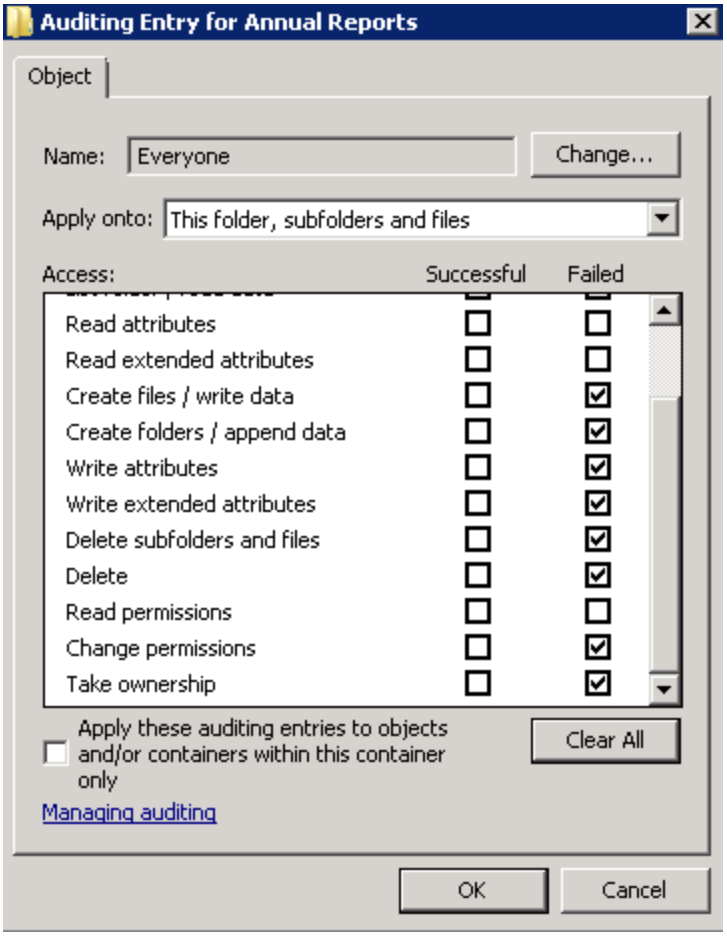


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed change attempts

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

Auditing Entry



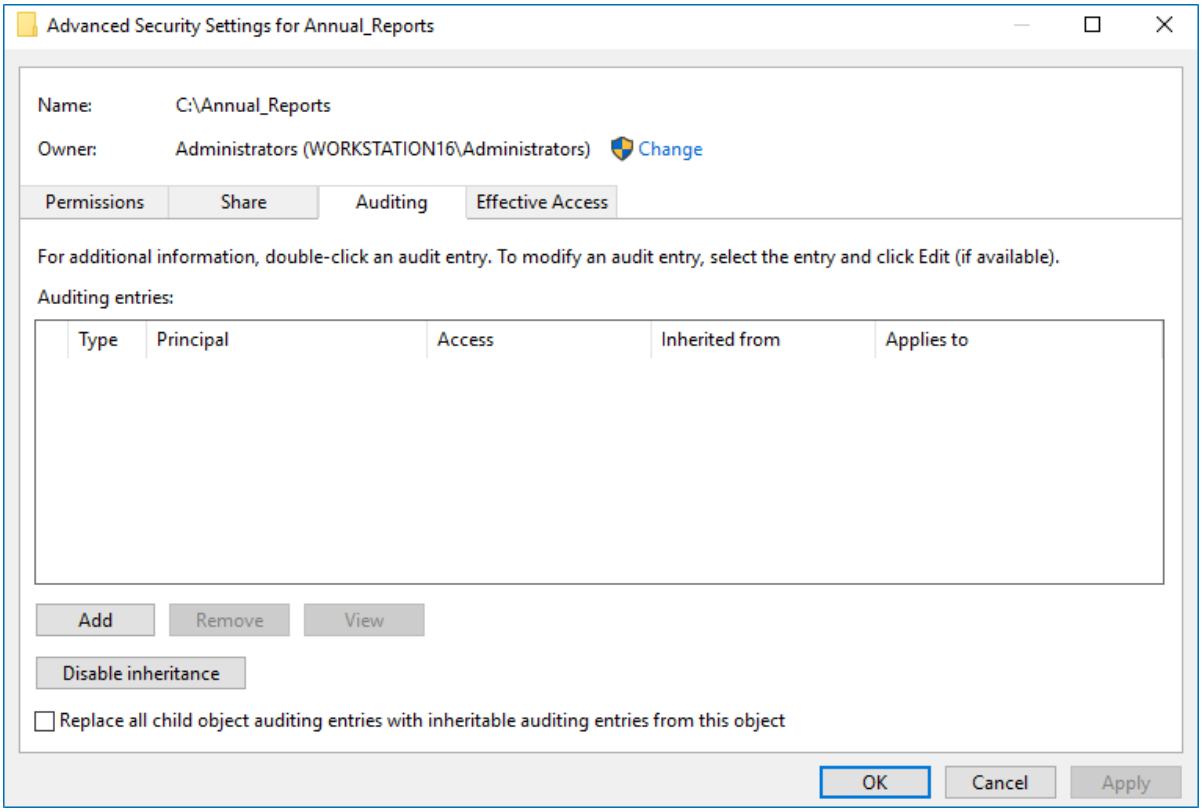
- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to the following permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change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

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 Qtree Security 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.

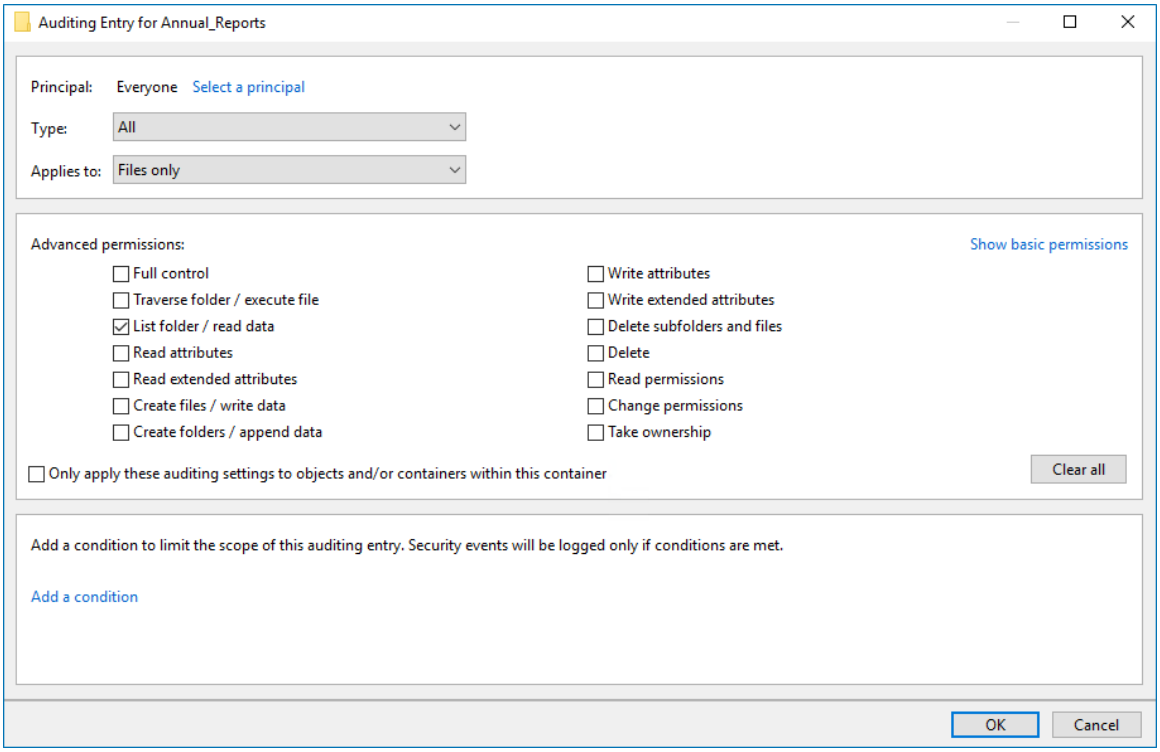
6. Apply settings to your Auditing Entries depending on actions that you want to audit. If you want to audit all actions (successful reads and changes as well as failed read and change attempts), you need

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 changes
- Failed read attempts
- Failed change attempts

Auditing Entry
Successful reads

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

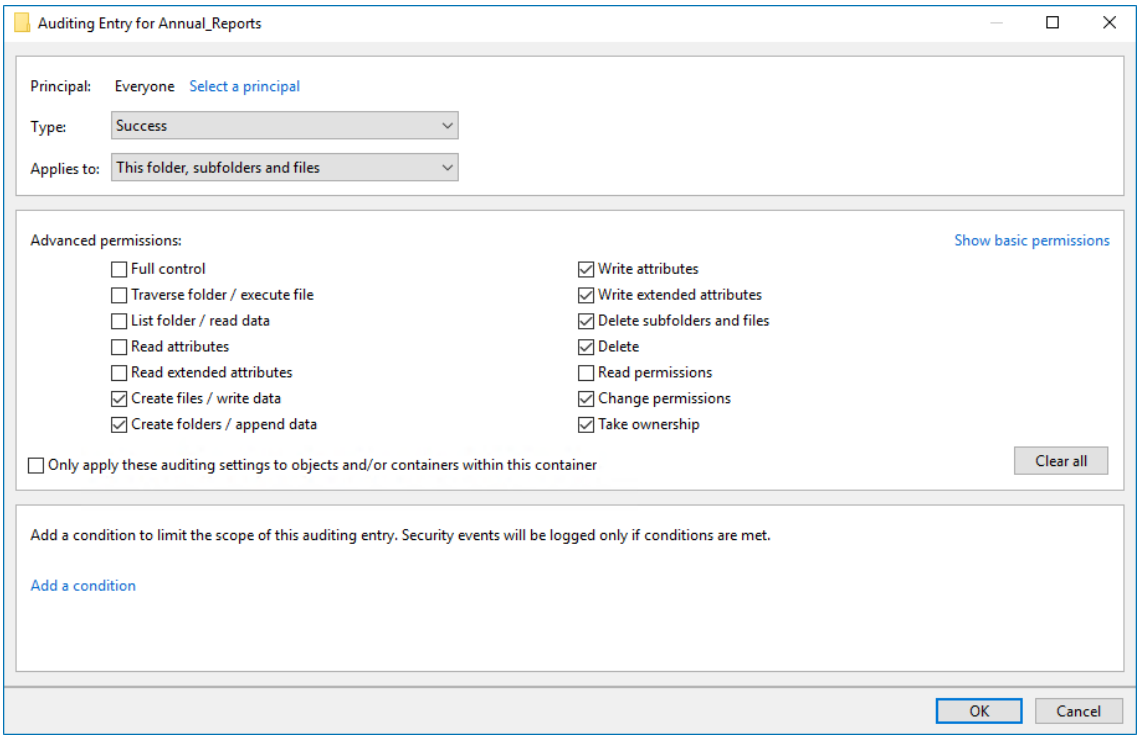


- Type—Set to *"All"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful changes

Auditing Entry

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

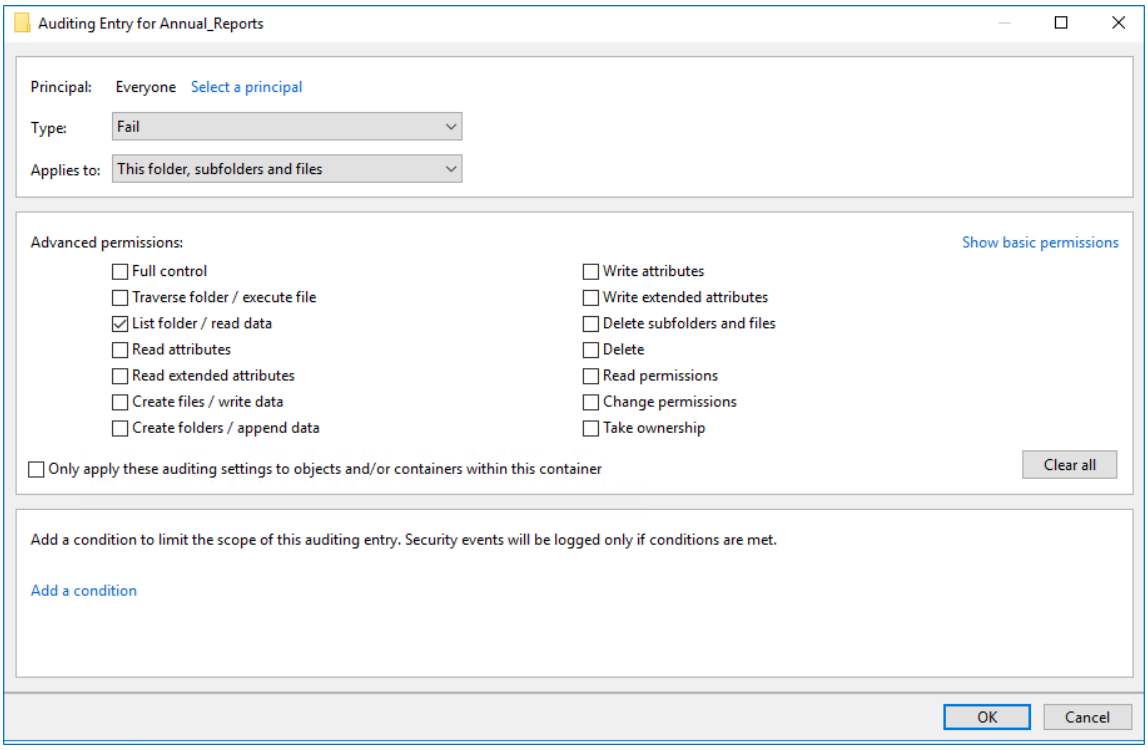


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Change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

Failed read attempts

Auditing Entry

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

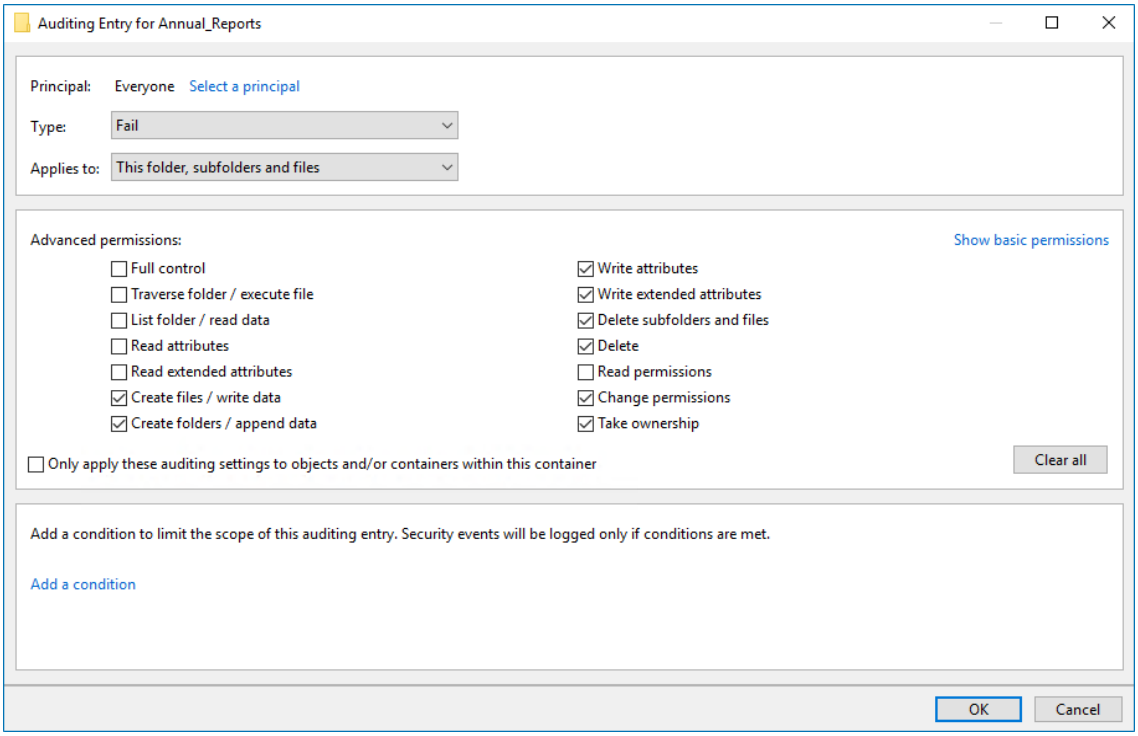


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change 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.

5.8. Configure Oracle Database for Auditing

Before you start auditing your Oracle Database with Netwrix Auditor, arrange your environment. Depending on your current database version and edition, Oracle provides different types of auditing:

- **Standard Auditing**—For Oracle Database 11g. In Standard Auditing, you use initialization parameters and the `AUDIT` and `NOAUDIT` SQL statements to audit SQL statements, privileges, schema objects, network and multitier activities. See Configure Oracle Database 11g for Auditing for more information.
- **Unified Auditing**—Recommended for Oracle Database 12c. Unified Auditing consolidates all auditing into a single repository and view. This provides a two-fold simplification: audit data can now be found in a single location and all audit data is in a single format. See Configure Oracle Database 12c for Auditing for more information.
- **Fine Grained Auditing**—Available for Oracle Database Enterprise Edition only. Allows auditing of actions associated with columns in application tables along with conditions necessary for an audit record to be generated. It helps focus on security-relevant columns and rows and ignore areas that are less important. See Configure Fine Grained Auditing for more information.

If you are unsure of your audit settings, refer to the following section:

- Verify Your Oracle Database Audit Settings

5.8.1. Configure Oracle Database 11g for Auditing

Perform the following steps to configure Standard Auditing on your Oracle Database:

- Select audit trail to store audit records. The following options are available in Oracle Database:

Audit trail	Description
Database audit trail	Set by default.
XML audit trail	Netwrix recommends to store audit records to XML audit trail. In this case, the product will report on actions performed by users with `SYSDBA` and `SYSOPER` privileges. Otherwise, these actions will not be audited.
OS files	Current version of Netwrix Auditor does not support this configuration.

- Enable auditing of selected Oracle Database parameters.

To select audit trail to store audit records

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

```
OracleUser as sysdba
```

Enter your password.

3. Select where to store audit records.

   Review the following for additional information:

To...	Execute the following command...
Store audit records to database audit trail. This is default configuration for Oracle Database. **NOTE:** If you want to store audit records to database audit trail, do not run this command.	`ALTER SYSTEM SET audit_trail=DB SCOPE=SPFILE;` **NOTE:** In this case, actions performed by user `SYS` and users connecting with `SYSDBA` and `SYSOPER` privileges will not be audited.

Store audit records to XML audit trail.	`ALTER SYSTEM SET audit_trail=XML SCOPE=SPFILE;`
	
	NOTE: If you want to enable auditing of actions performed by user `SYS` and users connecting with `SYSDBA` and `SYSOPER` privileges, execute the following command:
	
	`ALTER SYSTEM SET audit_sys_operations=TRUE SCOPE=SPFILE;`

Store audit records to XML or database audit trail and keep full text of SQL-specific query in audit records.
 	
NOTE: Only `ALTER` actions will be reported.
	For database audit trail:
	
	`ALTER SYSTEM SET audit_trail=DB, EXTENDED SCOPE=SPFILE;`
	
	For XML audit trail:
	
	`ALTER SYSTEM SET audit_trail=XML, EXTENDED SCOPE=SPFILE;`

4. Restart the database:

```
SHUTDOWN IMMEDIATE

STARTUP
```

NOTE: You do not need to restart the database if you changed auditing of objects. You only need to restart the database if you made a universal change, such as turning on or off all auditing. If you use Oracle Real Application Clusters (RAC), see the Starting and Stopping Instances and Oracle RAC Databases section in **Real Application Clusters Administration and Deployment Guide** for more information on restarting your instances.

To enable auditing of Oracle Database changes

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.
3. Enable auditing of selected parameters.

   Review the following for additional information:

To audit...	Execute the command...

Configuration changes	• For any user:
	`AUDIT ALTER SYSTEM,SYSTEM AUDIT,SESSION,TABLE,USER, VIEW,ROLE,PROCEDURE,TRIGGER,PROFILE,DIRECTORY, MATERIALIZED VIEW,SYSTEM GRANT,NOT EXISTS, ALTER TABLE,GRANT DIRECTORY,GRANT PROCEDURE, GRANT TABLE;`
	`AUDIT ALTER DATABASE, FLASHBACK ARCHIVE ADMINISTER;`
	NOTE: If you want to disable configuration auditing, use the following commands:
	`NOAUDIT ALTER SYSTEM,SYSTEM AUDIT,SESSION, TABLE,USER,VIEW,ROLE,PROCEDURE,TRIGGER,PROFILE, DIRECTORY,MATERIALIZED VIEW,SYSTEM GRANT, NOT EXISTS,ALTER TABLE,GRANT DIRECTORY, GRANT PROCEDURE,GRANT TABLE;`
	`NOAUDIT ALTER DATABASE, FLASHBACK ARCHIVE ADMINISTER;`
	• For specific user:
	`AUDIT SYSTEM GRANT, SESSION, TABLE, PROCEDURE BY <USER_NAME>;`
	NOTE: You can specify several users separated by commas.

Successful data access and changes	`AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME, FLASHBACK ON <TABLE_NAME> BY ACCESS WHENEVER SUCCESSFUL;`
Failed data access and changes	`AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME, FLASHBACK ON <TABLE_NAME> BY ACCESS WHENEVER NOT SUCCESSFUL;`

NOTE: After an audit parameter has been enabled or disabled, the product starts collecting data after succeeding logon session.

For additional information on `ALTER SYSTEM` and `AUDIT` parameters, see the following Oracle database administration documents:

- `AUDIT_TRAIL`
- `AUDIT`

Currently, Netwrix Auditor checks audit settings for Standard Auditing when configured to audit specified operations. If any of your current settings conflict with the audit configuration required for Netwrix Auditor, these conflicts will be listed in the **Netwrix Auditor System Health** event log.

5.8.2. Configure Oracle Database 12c for Auditing

The following auditing modes are available for Oracle Database 12c:

- **Mixed Mode**—Default auditing in a newly installed database. It enables both traditional and the new Unified audit facilities. Netwrix recommends not to use Mixed Mode auditing together with Netwrix Auditor. If you want to leave it as it is, make sure that your audit records are stored to the XML audit trail, otherwise Netwrix Auditor will not be able to collect changes made with `SYSDBA` or `SYSOPER` privilege.

  NOTE: The product does not log any errors on these events to the **Netwrix Auditor System Health** log.

- **Unified Auditing**—Recommended. See the following Oracle technical article for detailed instructions on how to enable Unified Auditing: Enabling Unified Auditing.

  Perform the following steps to configure Unified Auditing on your Oracle Database:

  - Create and enable an audit policy to audit specific parameters across your Oracle Database.

    NOTE: After an audit policy has been enabled or disabled, the product starts collecting data after succeeding logon session.

  - If needed, create and enable specific audit policies to audit successful data access and changes, user actions, component actions, etc.

To configure Oracle Database 12c Unified Auditing

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.

3. Create and enable audit policies. Review the following for additional information:

To audit...	Execute the command...
Configuration changes	• Create an audit policy (e.g., `nwx_actions_pol`) for any user: `CREATE AUDIT POLICY nwx_actions_pol ACTIONS CREATE TABLE,DROP TABLE,ALTER TABLE,GRANT,REVOKE, CREATE VIEW,DROP VIEW,CREATE PROCEDURE, ALTER PROCEDURE,RENAME,AUDIT,NOAUDIT, ALTER DATABASE,ALTER USER,ALTER SYSTEM, CREATE USER,CREATE ROLE,SET ROLE,DROP USER, DROP ROLE,CREATE TRIGGER,ALTER TRIGGER, DROP TRIGGER,CREATE PROFILE,DROP PROFILE, ALTER PROFILE,DROP PROCEDURE, CREATE MATERIALIZED VIEW,DROP MATERIALIZED VIEW, ALTER ROLE,TRUNCATE TABLE,CREATE FUNCTION, ALTER FUNCTION,DROP FUNCTION,CREATE PACKAGE, ALTER PACKAGE,DROP PACKAGE,CREATE PACKAGE BODY, ALTER PACKAGE BODY,DROP PACKAGE BODY,LOGON,LOGOFF, CREATE DIRECTORY,DROP DIRECTORY,CREATE JAVA, ALTER JAVA,DROP JAVA,PURGE TABLE, CREATE PLUGGABLE DATABASE,ALTER PLUGGABLE DATABASE, DROP PLUGGABLE DATABASE,CREATE AUDIT POLICY, ALTER AUDIT POLICY,DROP AUDIT POLICY, CREATE FLASHBACK ARCHIVE,ALTER FLASHBACK ARCHIVE, DROP FLASHBACK ARCHIVE;` • Enable the audit policy: `AUDIT POLICY nwx_actions_pol;` **NOTE:** To disable audit policy, use the following command: `NOAUDIT POLICY nwx_actions_pol;`

Data access and changes (successful and failed)	• Create the audit policy (e.g., `nwx_actions_obj_pol`):
	`CREATE AUDIT POLICY nwx_actions_obj_pol ACTIONS DELETE on hr.employees, INSERT on hr.employees, UPDATE on hr.employees, SELECT on hr.employees, FLASHBACK on hr.employees CONTAINER = CURRENT;`
	• Enable the audit policy (e.g., `nwx_actions_obj_pol`):
	`AUDIT POLICY nwx_actions_obj_pol;`

Component actions: `Oracle Data Pump`,	• Create the audit policies (e.g., `nwx_sqlloader_dp_pol`, etc.): **NOTE:** No special configuration required to audit RMAN events. `CREATE AUDIT POLICY nwx_datapump_exp_pol ACTIONS`

To audit...	Execute the command...
Oracle Recovery Manager, and Oracle SQL*Loader Direct Path Load	COMPONENT=DATAPUMP EXPORT; CREATE AUDIT POLICY nwx_datapump_imp_pol ACTIONS COMPONENT=DATAPUMP IMPORT; CREATE AUDIT POLICY nwx_sqlloader_dp_pol ACTIONS COMPONENT=DIRECT_LOAD LOAD; • Enable these policies: AUDIT POLICY nwx_datapump_exp_pol; AUDIT POLICY nwx_datapump_imp_pol; AUDIT POLICY nwx_sqlloader_dp_pol;

4. If necessary, enable more granular audit policies. Review the following for additional information:

To...	Execute the command...
Apply audit policy to selected users	AUDIT POLICY nwx_actions_pol BY SYS, SYSTEM, <user_name>;
Exclude user actions from being audited (e.g., exclude failed Operator actions)	AUDIT POLICY nwx_actions_pol EXCEPT Operator WHENEVER NOT SUCCESSFUL;
Audit successful actions of selected user (e.g., Operator)	AUDIT POLICY nwx_actions_pol BY Operator WHENEVER SUCCESSFUL;

For additional information on CREATE AUDIT POLICY and AUDIT POLICY parameters, see the following Oracle Database administration documents:

- CREATE AUDIT POLICY
- AUDIT POLICY

Currently, Netwrix Auditor checks audit settings for Unified Auditing when accomptability is enabled for ACTIONS. If any of your current settings conflict with the audit configuration required for Netwrix Auditor, these conflicts will be listed in the **Netwrix Auditor System Health** event log.

5.8.3. Configure Fine Grained Auditing

When configuring Fine Grained Auditing, you need to create an audit policy with required parameters set. The procedure below contains instructions on how to create, disable and delete such audit policies.

NOTE: Fine Grained audit policies can be configured for Oracle Database Enterprise Edition only. Keep in mind that if you have Fine Grained policies configured, you will receive a permanent error in the

Netwrix Auditor System Health log because Netwrix Auditor cannot detect it. Use Unified and Standard audit policies to keep track of data changes.

To configure Fine Grained Auditing

Below is an example of Fine Grained audit policy that enables auditing of audit statements (`INSERT`, `UPDATE`, `DELETE`, and `SELECT`) on table `hr.emp` to audit any query that accesses the `salary` column of the employee records that belong to `sales` department. Review the following for additional information:

To...	Execute the following command...
To create audit policy	`EXEC DBMS_FGA.ADD_POLICY(object_schema => 'hr', object_name => 'emp', policy_name => 'chk_hr_emp', audit_condition => 'dept = ''SALES'' ', audit_column => 'salary' statement_types => 'INSERT,UPDATE,DELETE,SELECT');`
To disable audit policy	`EXEC DBMS_FGA.DISABLE_POLICY(object_schema => 'hr', object_name =>'emp', policy_name => 'chk_hr_emp');`
To delete audit policy	`EXEC DBMS_FGA.DROP_POLICY(object_schema => 'hr', object_name =>'emp', policy_name => 'chk_hr_emp');`

NOTE: Refer to Oracle documentation for additional information on Fine Grained Auditing.

5.8.4. Verify Your Oracle Database Audit Settings

You can verify your Oracle Database audit settings manually. Do one of the following, depending on your Oracle Database version and edition.

Oracle Database version/edition	Command

Oracle Database 11g (Standard Auditing)	`SELECT audit_option, success, failure FROM dba_stmt_audit_opts;`
	
	NOTE: To review your initialization parameters, execute the following command:
	`SHOW PARAMETERS audit%r;`

Oracle Database 12c (Unified Auditing)	`select USER_NAME, ENABLED_OPT, SUCCESS, FAILURE from AUDIT_UNIFIED_ENABLED_POLICIES;`
Oracle Database	`SELECT POLICY_NAME, ENABLED from DBA_AUDIT_POLICIES;`

Oracle Database version/edition	Command
Enterprise Edition (Fine Grained Auditing)	

NOTE: If you want to clean your audit settings periodically, refer to the following Oracle Help Center article for more information: Database PL/SQL Packages and Types Reference.

5.9. Configure SharePoint Farm for Auditing

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

- Automatically when creating a monitoring plan. 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.

5.9.1. Configure Audit Log Trimming

1. Log in as an administrator to the audited SharePoint site collection.
2. Depending on SharePoint you are running, do one of the following:
   - SharePoint 2010—In the upper-left of your site collection, select **Site Actions** → **Site Settings**.
   - SharePoint 2013 and 2016—In the upper-right of your site collection, select **Settings (gear)** → **Site Settings**.
3. Under the **Site Collection Administration** section, select **Site collection audit settings**.
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.

5.9.2. Configure Events Auditing Settings

1. Log in as an administrator to the audited SharePoint site collection.
2. Depending on SharePoint you are running, do one of the following:
   - SharePoint 2010—In the upper-left of your site collection, select **Site Actions** → **Site Settings**.
   - SharePoint 2013 and 2016—In the upper-right of your site collection, select **Settings (gear)** → **Site Settings**.
3. Under the **Site Collection Administration** section, select **Site collection audit settings**.
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.

5.9.3. 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

5.10. Configure Windows Server for Auditing

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

- Automatically when creating a monitoring plan

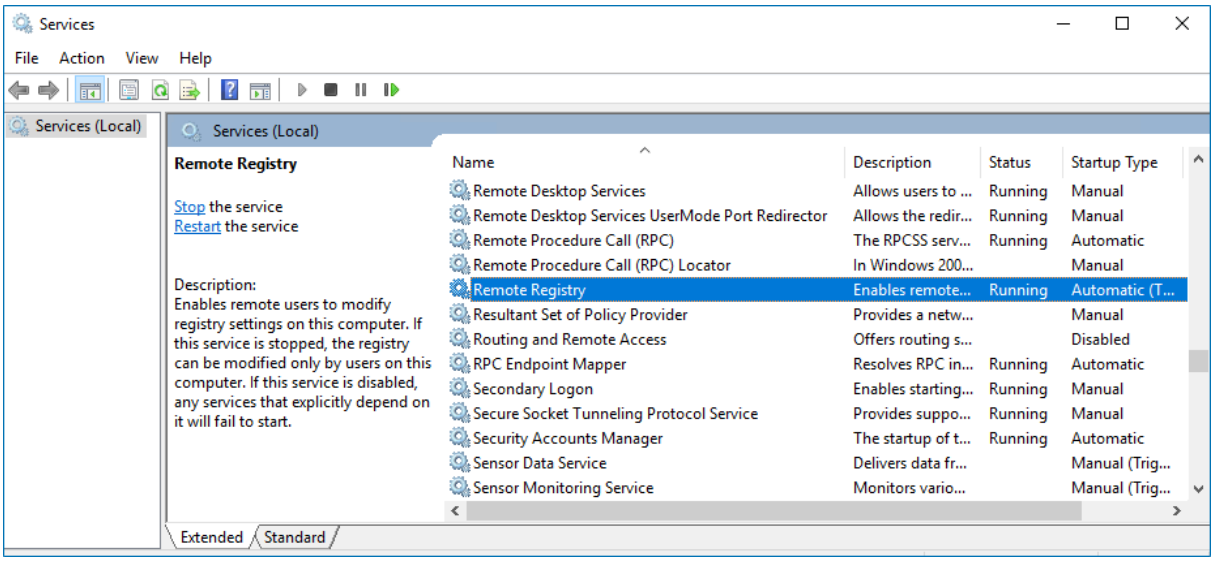
  If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  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.

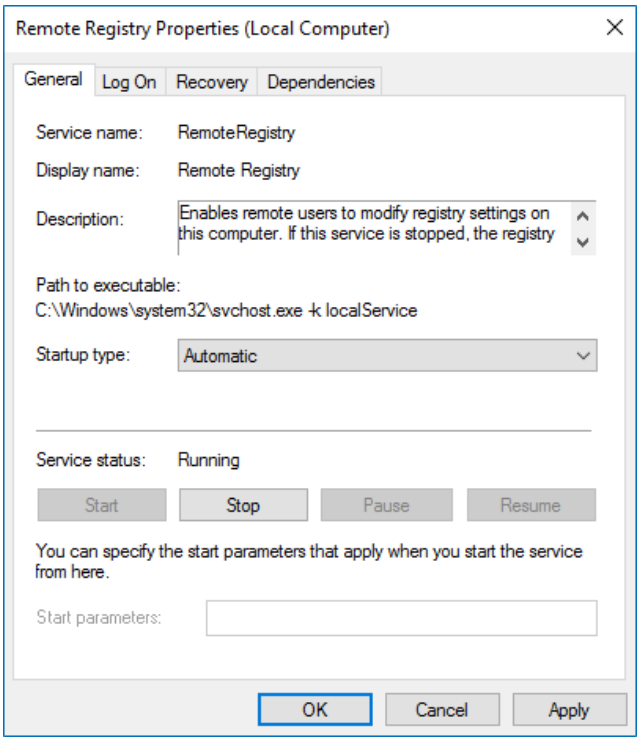
- Manually. Perform the following procedures:
  - Enable Remote Registry and Windows Management Instrumentation Services
  - Configure Windows Registry Audit Settings
  - Configure Local Audit Policies or Configure Advanced Audit Policies
  - Configure Event Log Size and Retention Settings
  - Configure Windows Firewall Inbound Connection Rules
  - Configure DHCP-Server Operational Log
  - Configure Auditing of Removable Storage Media

5.10.1. Enable Remote Registry and Windows Management Instrumentation Services

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

5.10.2. 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. Netwrix recommends using automatic audit configuration for more granular auditing. If you want to configure Windows Registry manually, follow the instructions below.

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

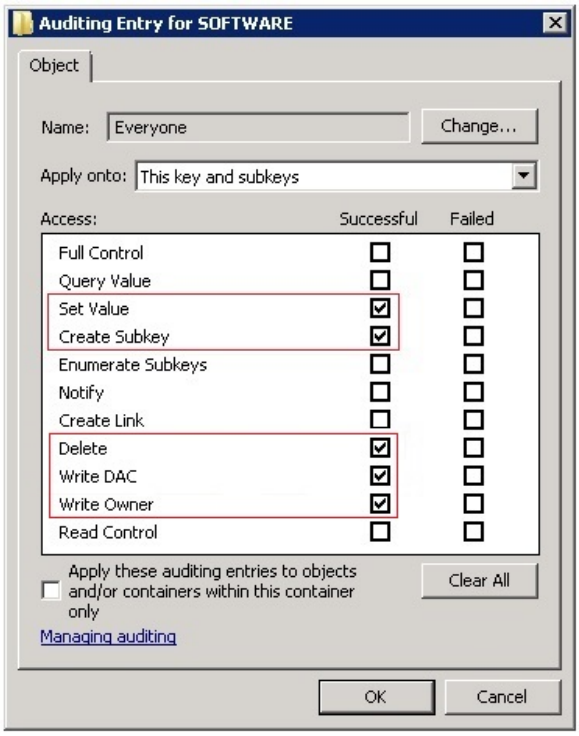
- Set Value
- Create Subkey
- Delete
- Write DAC
- Write Owner

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**



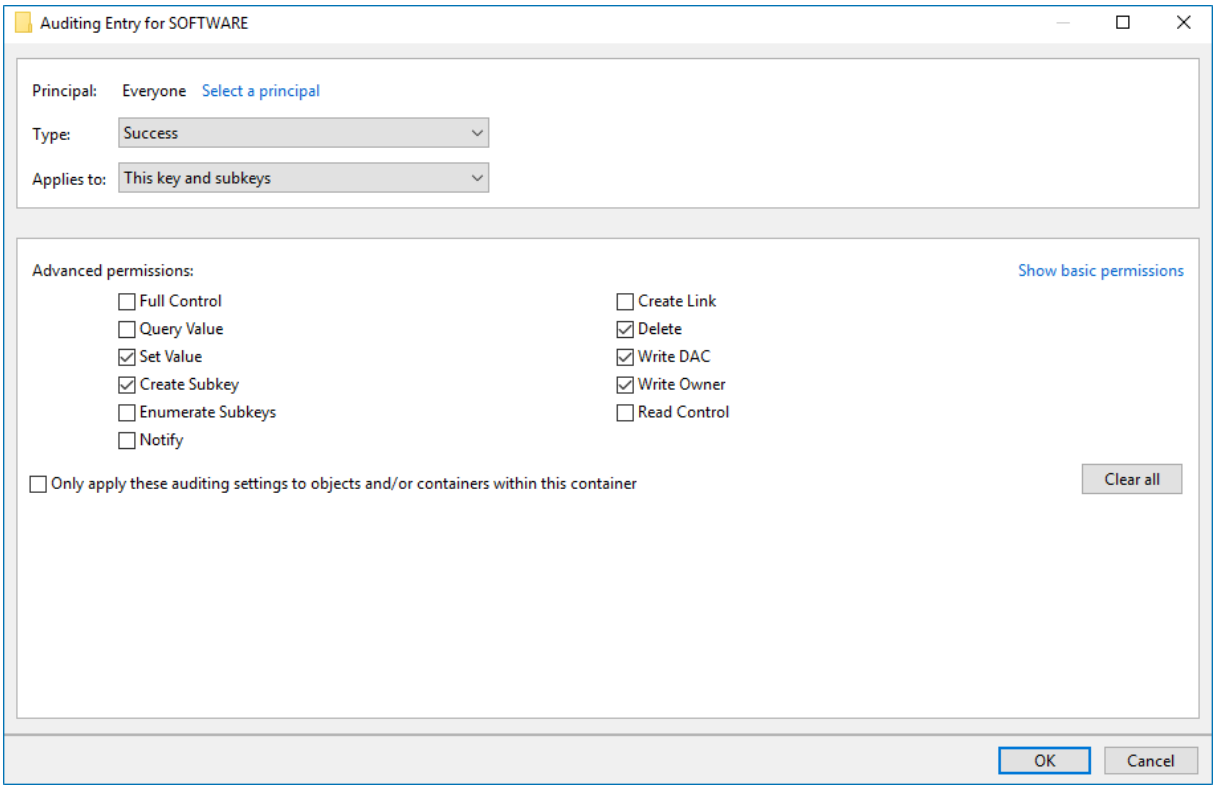
7. Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys.

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.

5.10.3. 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:

- Audit policies
- File shares
- Hardware and system drivers
- General computer settings
- Local users and groups
- Services
- Scheduled tasks
- Windows registry
- Removable media

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

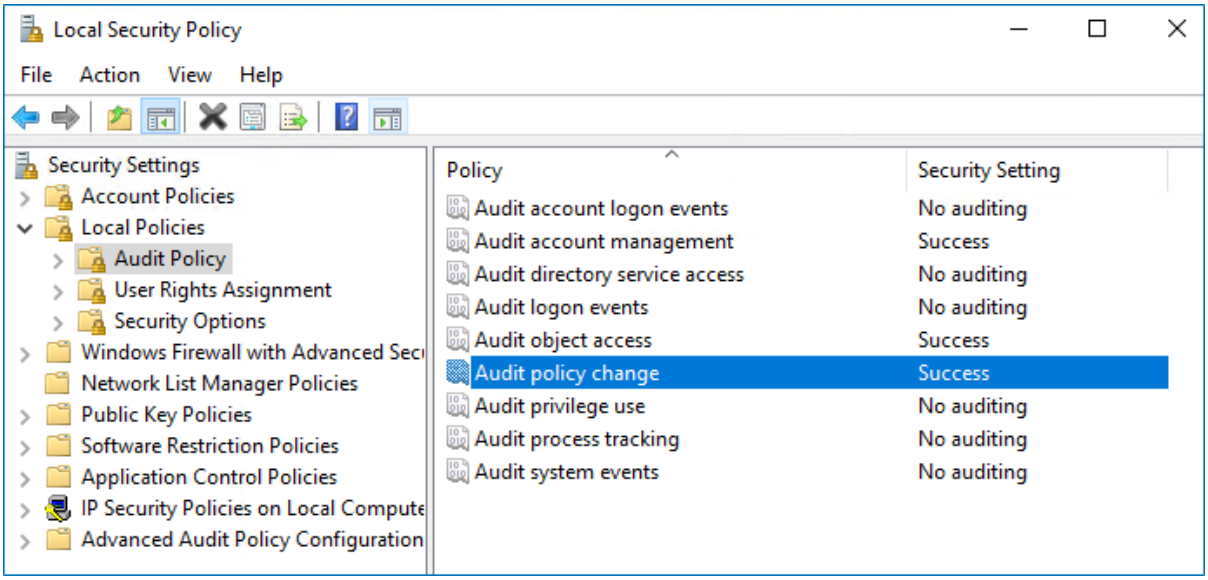
While there are several methods to configure local audit policies, this guide covers just one of them: how to configure policies locally with the **Local Security Policy** snap-in. To apply settings to the whole domain, use the Group Policy but consider the possible impact on your environment.

To configure local audit policies

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Local Security Policy**.

2. Navigate to **Security Settings** → **Local Policies** → **Audit Policy**.

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



5.10.4. 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:

- Audit policies
- File shares
- Hardware and system drivers
- General computer settings
- Local users and groups
- Services
- Scheduled tasks
- Windows registry
- Removable storage media

Perform the following procedures:

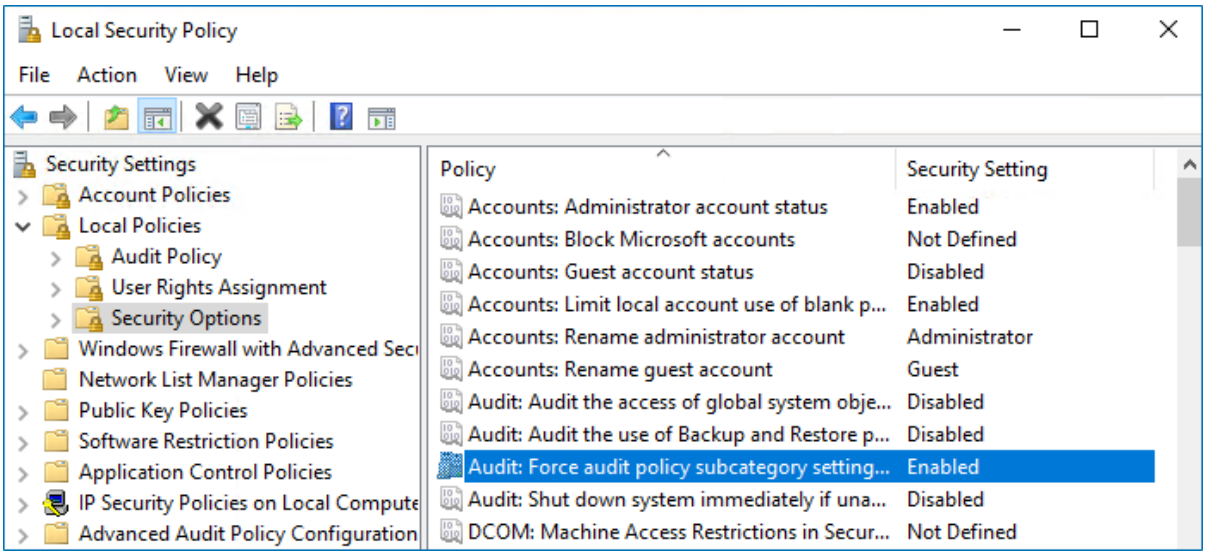
- To configure security options
- To configure advanced audit policy on Windows Server 2008 / Windows Vista
- To configure advanced audit policies on Windows Server 2008 R2 / Windows 7 and above

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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**, **Account Management**, and **Policy Change** 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
auditpol /set /category:"Policy Change" /success:disable /failure:disable
```

3. Enable the following audit subcategories:

Audit subcategory	Command
Security Group Management	`auditpol /set /subcategory:"Security Group Management" /success:enable /failure:disable`
User Account Management	`auditpol /set /subcategory:"User Account Management" /success:enable /failure:disable`
Handle Manipulation	`auditpol /set /subcategory:"Handle Manipulation" /success:enable /failure:disable`
Other Object Access Events	`auditpol /set /subcategory:"Other Object Access Events" /success:enable /failure:disable`
Registry	`auditpol /set /subcategory:"Registry" /success:enable /failure:disable`
File Share	`auditpol /set /subcategory:"File Share" /success:enable /failure:disable`
Audit Policy Change	`auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:disable`

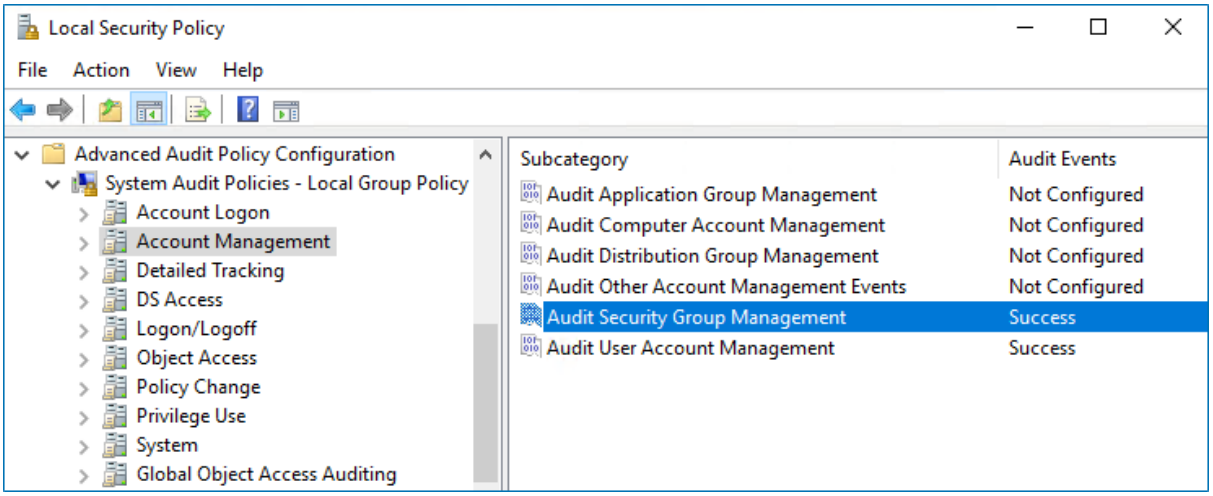
NOTE: It is recommended to disable all other subcategories unless you need them for other purposes. You can check your current effective settings by executing the following commands: `auditpol /get /category:"Object Access"`, `auditpol /get /category:"Policy Change"`, and `auditpol /get /category:"Account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

To configure advanced audit policies 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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** • **Audit File Share**	*"Success"*
Policy Change	• **Audit Audit Policy Change**	*"Success"*

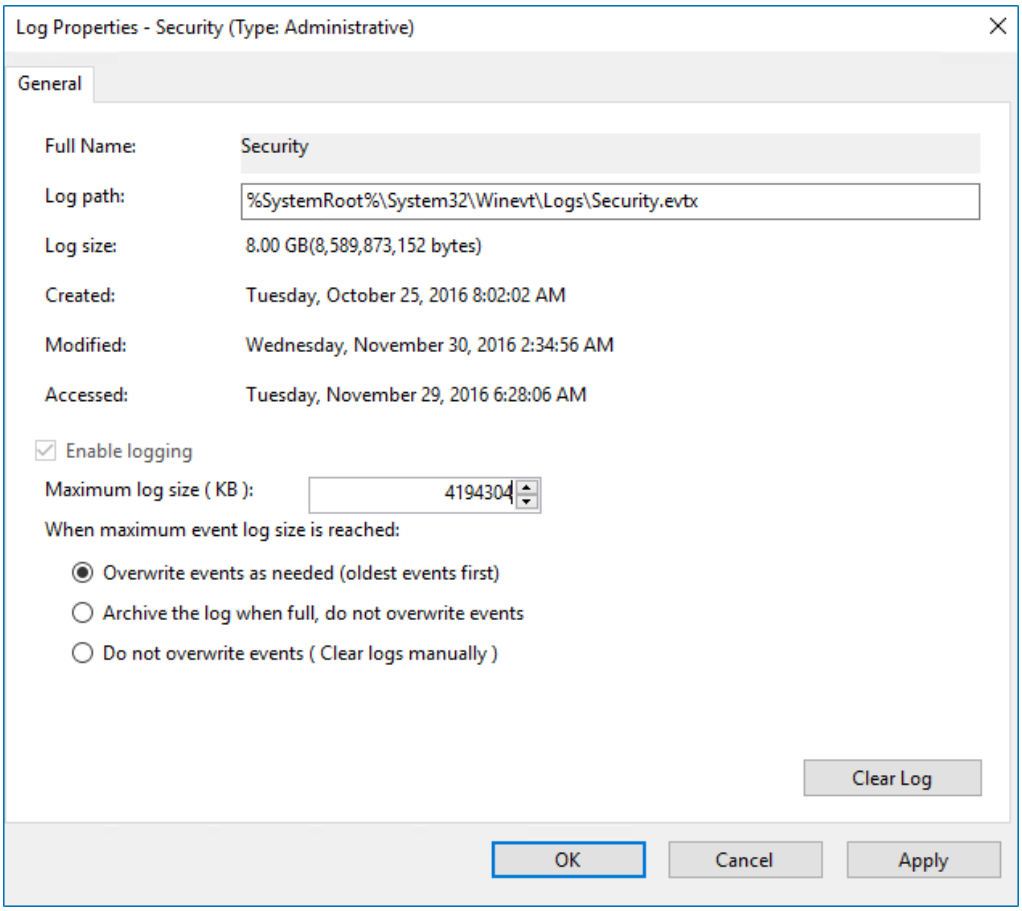


5.10.5. Configure Event Log Size and Retention Settings

To prevent data loss, you need to specify the maximum size for the following event logs: Application, Security, System, Microsoft- Windows- TaskScheduler/Operational, and Microsoft- Windows- DNS-Server/Audit (only for DCs running Windows Server 2012 R2 and above). 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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 following event logs:
   - **Windows Logs** → **Application**
   - **Windows Logs** → **System**

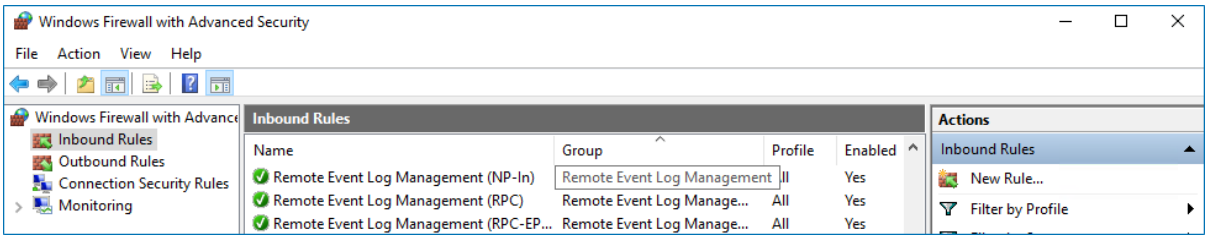
- **Applications and Services Logs** → **Microsoft** → **Windows** → **TaskScheduler** → **Operational** → **Microsoft-Windows-TaskScheduler/Operational**
- **Applications and Services Logs** → **Microsoft** → **Windows** → **DNS-Server** → **Audit**

  NOTE: The log is available on Windows Server 2012 R2 and above and is not enabled by default. See Microsoft documentation for more information on how to enable this log.

5.10.6. 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)**

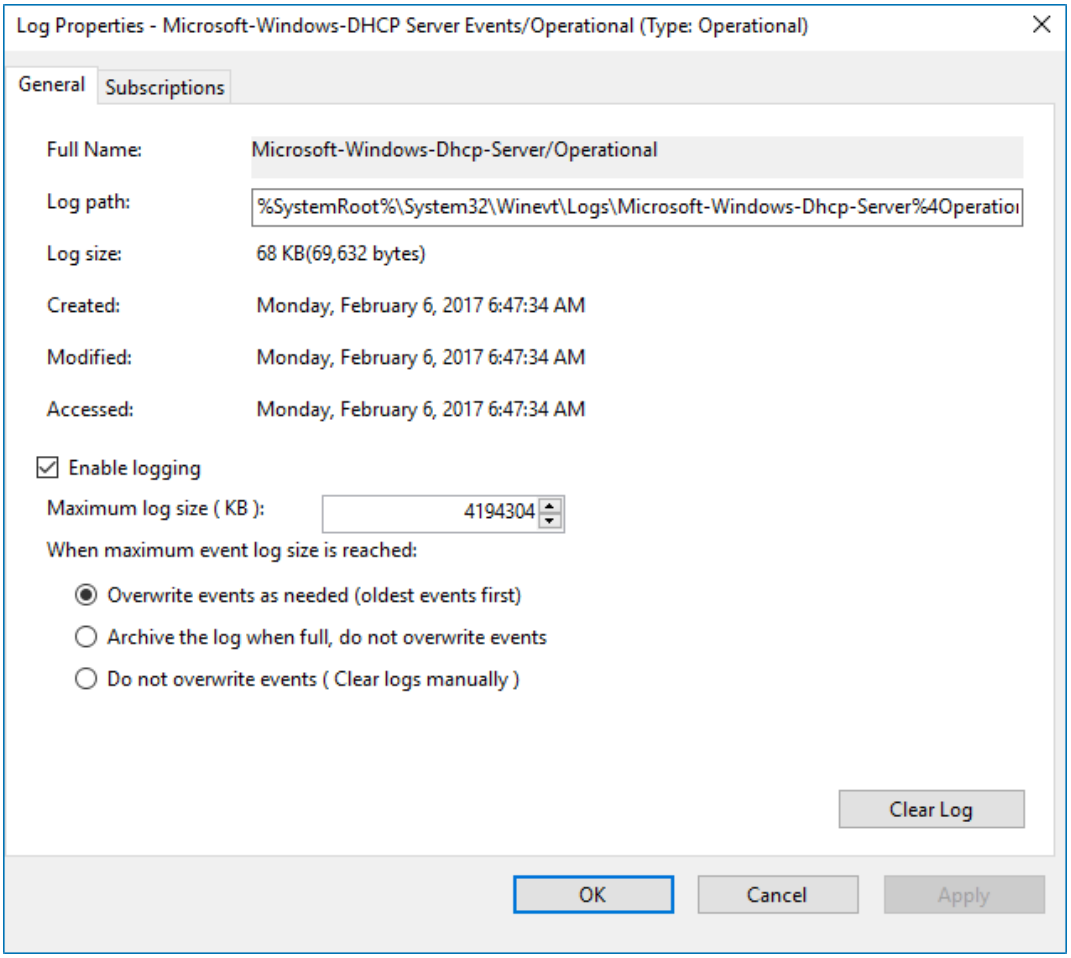
- **Remote Service Management (RPC-EPMAP)**
- **Performance Logs and Alerts (DCOM-In)**
- **Performance Logs and Alerts (Tcp-In)**

5.10.7. Configure DHCP-Server Operational Log

Configure these settings only if you want to monitor DHCP changes.

NOTE: The **DHCP** role is required to view and enable the **DHCP-Operational log**.

1. On the computer where DHCP server role is installed, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Applications and Services Logs** → **Microsoft** → **Windows** and expand the **DHCP-Server** 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)**.

5.10.8. Configure Auditing of Removable Storage Media

You can configure IT infrastructure for auditing removable storage media both locally and remotely.

Review the following for additional information:

- To configure removable storage media auditing on the local server
- To configure removable storage media auditing remotely
- To review Event Trace Session objects' configuration

To configure removable storage media auditing on the local server

1. On the target server, create the following catalog: *"%ALLUSERSPROFILE%\Netwrix Auditor\Windows Server Audit\ETS\"* to store event logs. Refer to To review Event Trace Session objects' configuration for detailed instructions on how to modify the root directory.

   NOTE: If you do not want to use the Netwrix Auditor for Windows Server Compression Service for data collection, make sure that this path is readable via any shared resource.

   After environment variable substitution, the path shall be as follows:

   C:\ProgramData\Netwrix Auditor\Windows Server Audit\ETS

   NOTE: If your environment variable accesses another directory, update the path.
2. Run the **Command Prompt** as Administrator.
3. Execute the commands below.
   - To create the Event Trace Session object:

     ```
     logman import -n "Session\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>"
     ```
   - To start the Event Trace Session object automatically every time the server starts:

     ```
     logman import -n "AutoSession\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>"
     ```

     where:

     - `NetwrixAuditorForWindowsServer`—Fixed name the product uses to identify the Event Trace Session object. The name cannot be changed.

- `<path to the EventTraceSessionTemplate.xml file>`—Path to the **Event Trace Session template** file that comes with Netwrix Auditor. The default path is *"C:\Program Files (x86)\Netwrix Auditor\Windows Server Auditing\EventTraceSessionTemplate.xml"*.

To configure removable storage media auditing remotely

1. On the target server, create the following catalog: *"%ALLUSERSPROFILE%\Netwrix Auditor\Windows Server Audit\ETS\"* to write data to. Refer to To review Event Trace Session objects' configuration for detailed instructions on how to modify the root directory.

   NOTE: If you do not want to use the Netwrix Auditor for Windows Server Compression Service for data collection, make sure that this path is readable via any shared resource.

   After environment variable substitution, the path shall be as follows:

   \\<*target_server_name*>\c$*ProgramData*\Netwrix Auditor\Windows Server Audit\ETS

   NOTE: If your environment variable accesses another directory, update the path.

2. Run the **Command Prompt** under the target server Administrator's account.
3. Execute the commands below.

   - To create the Event Trace Session object:

     ```
     logman import -n "Session\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>" -s <target server name>
     ```

   - To create the Event Trace Session object automatically every time the server starts:

     ```
     logman import -n "AutoSession\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>" -s <target server name>
     ```

     where:

     - `NetwrixAuditorForWindowsServer`—Fixed name the product uses to identify the Event Trace Session object. The name cannot be changed.
     - `<path to the EventTraceSessionTemplate.xml file>`—Path to the **Event Trace Session template** file that comes with Netwrix Auditor. The default path is *"C:\Program Files (x86)\Netwrix Auditor\Windows Server Auditing"*.
     - `<target server name>`—Name of the target server. Provide a server name by entering its FQDN, NETBIOS or IPv4 address.

To review Event Trace Session objects' configuration

NOTE: An Administrator can only modify the root directory and log file name. Other configurations are not supported by Netwrix Auditor.

1. On the target server, navigate to **Start** → **Administrative Tools** → **Performance Monitor**.
2. In the **Performance Monitor** snap-in, navigate to **Performance** → **Data Collectors Set** → **Event Trace Sessions**.
3. Stop the **NetwrixAuditorForWindowsServer** object.
4. Locate the **NetwrixAuditorForWindowsServer** object, right-click it and select **Properties**. Complete the following fields:

Option	Description
Directory → **Root Directory**	Path to the directory where event log is stored. If you want to change root directory, do the following: 1. Under the **Root directory** option, click **Browse** and select a new root directory. 2. Navigate to *C:\ProgramData\Netwrix Auditor\Windows Server Audit* and copy the **ETS** folder to a new location.
File → **Log file name**	Name of the event log where the events will be stored.

5. Start the **NetwrixAuditorForWindowsServer** object.
6. In the **Performance Monitor** snap-in, navigate to **Performance** → **Data Collectors Set** → **Startup Event Trace Sessions**.
7. Locate the **NetwrixAuditorForWindowsServer** object, right-click it and select **Properties**. Complete the following fields:

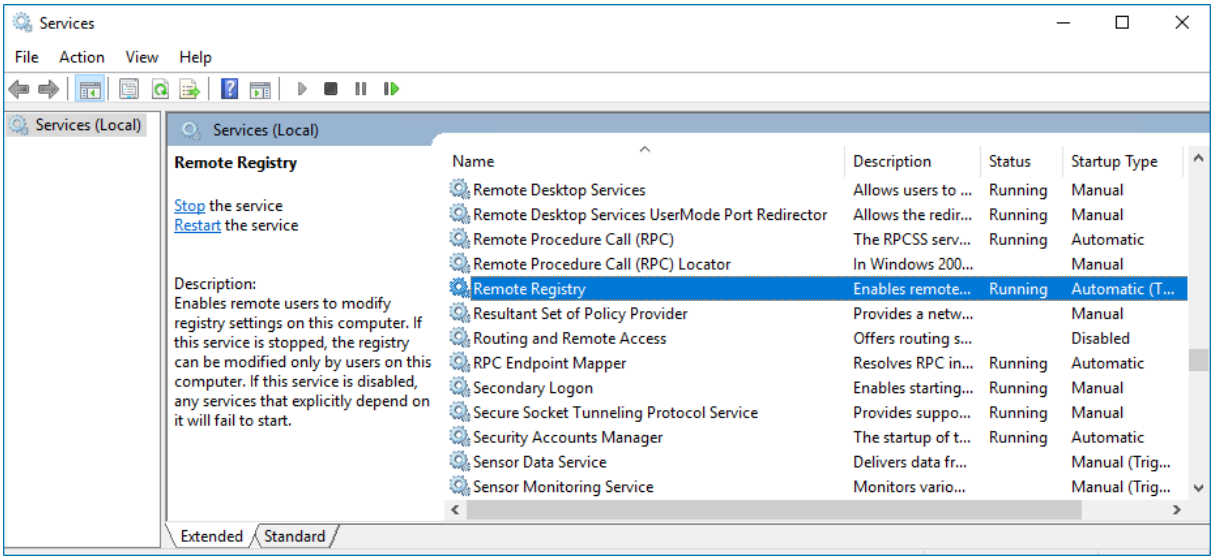
Option	Description
Directory → **Root Directory**	Path to the directory where event log is stored. Under the **Root directory** option, click **Browse** and select a new root directory.
File → **Log file name**	Name of the event log where the events will be stored.

5.11. Configure Infrastructure for Auditing Windows Event Logs

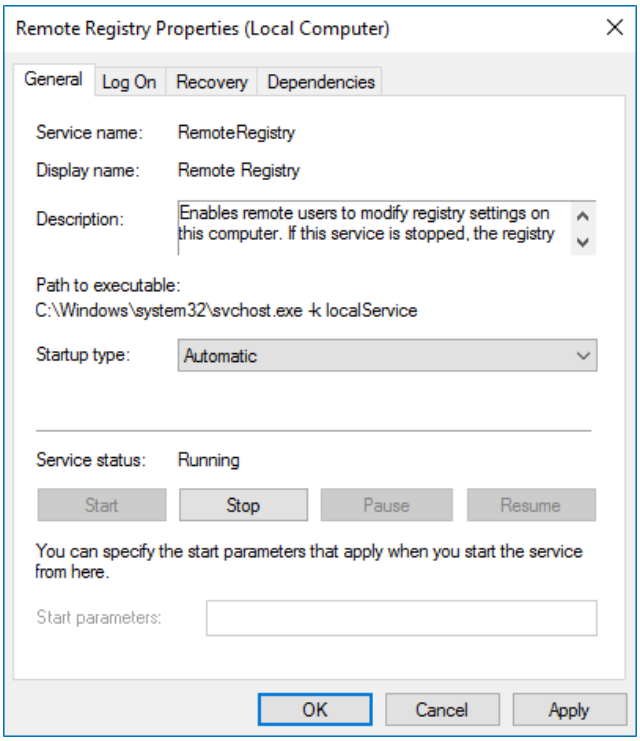
The **Remote Registry** service must be enabled on the target computers.

To enable the Remote Registry service

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

5.12. 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 monitoring plan

  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.

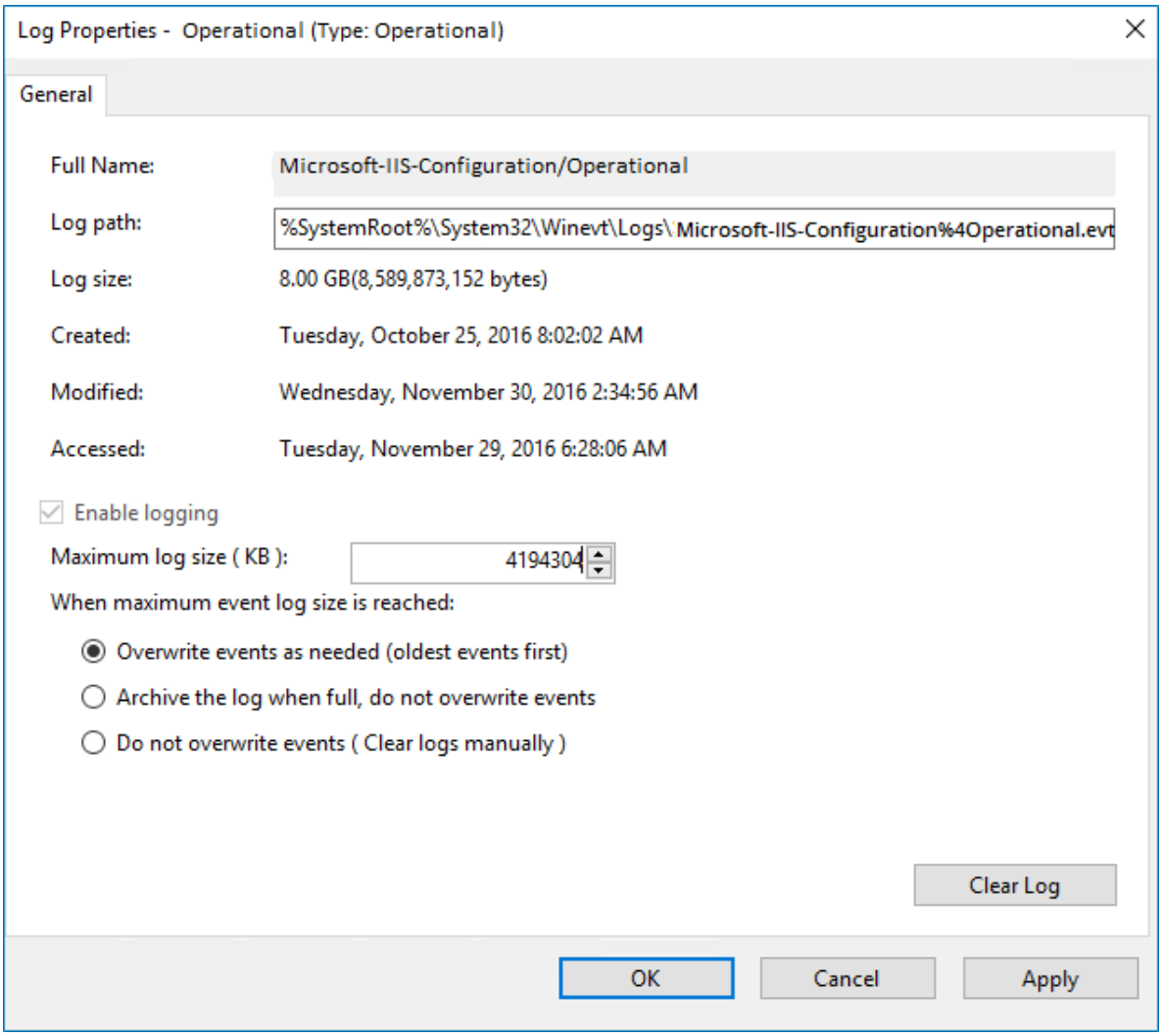
- Manually. You need to adjust the same audit settings as those required for auditing Active Directory. See Configure Domain for Auditing Active Directory for more information.

5.13. 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 Windows Event Logs for more information.

To configure the Operational log size and retention method

1. On the computer where IIS is installed, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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)**.

5.14. 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 monitoring plan

  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.

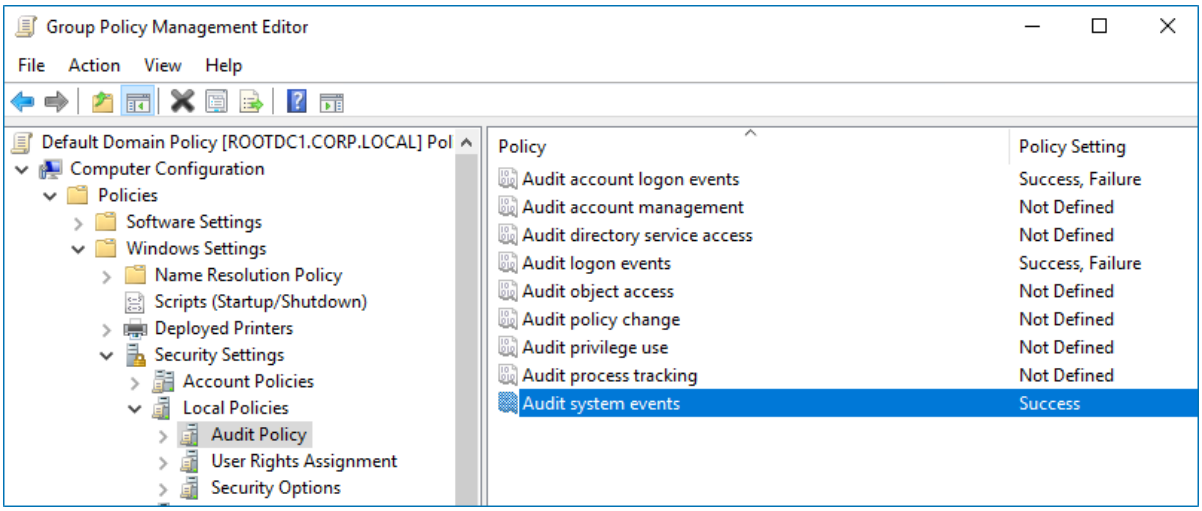
- Manually. To configure your domain manually for auditing Logon Activity, perform the following procedures:
  - Configure Basic Domain Audit Policies or Configure Advanced Audit Policies
  - Configure Security Event Log Size and Retention Settings
  - Configure Windows Firewall Inbound Connection Rules

5.14.1. 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

5.14.2. 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

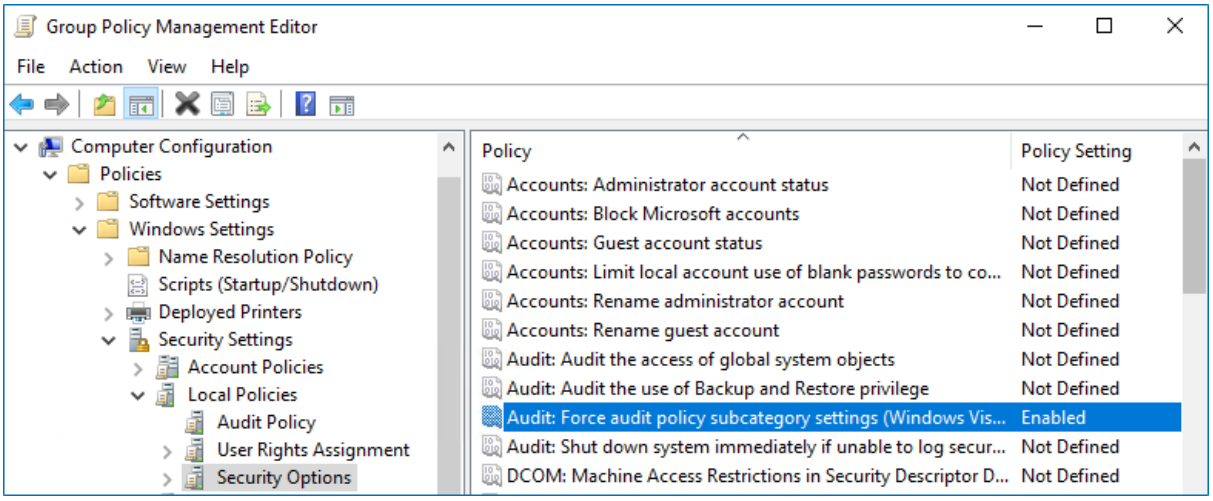
To configure security options

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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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"*.



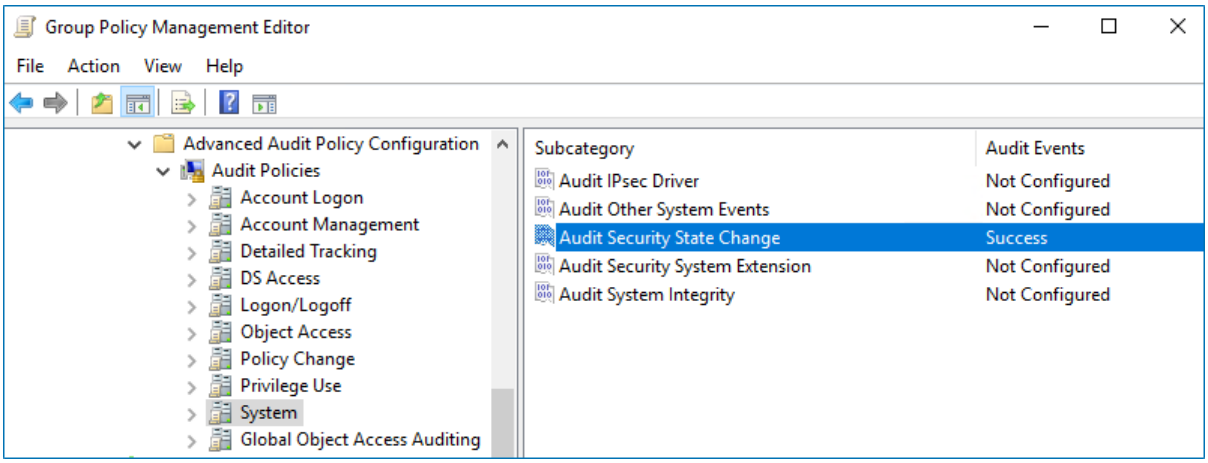
5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

To configure advanced audit policies

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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"*

Policy Subnode	Policy Name	Audit Events
	• **Audit Other Account Logon Events** **NOTE:** Required if at least one domain controller in the monitored domain runs Windows Server 2012 R2.	*"Success"* and *"Failure"*
Logon/Logoff	• **Audit Logoff** • **Audit Other Logon/Logoff Events**	*"Success"*
	• **Audit Logon**	*"Success"* and *"Failure"*
System	• **Audit Security State Change**	*"Success"*

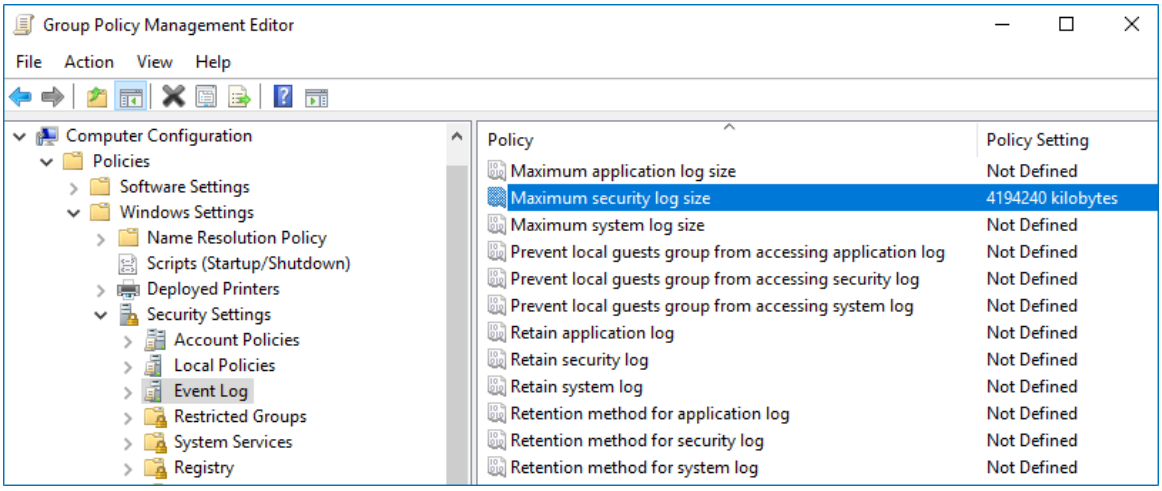


5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

5.14.3. 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

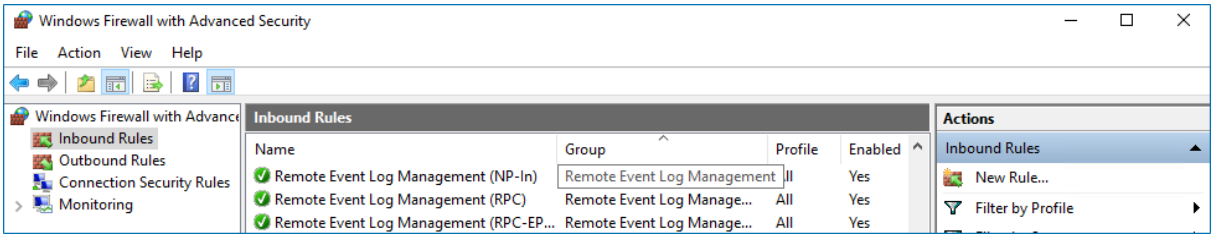


4. In the **Maximum security log size Properties** dialog, select **Define this policy setting** and set maximum security log size to *"4194240"* kilobytes (4GB).
5. Select the **Retention method for security log** policy. In the **Retention method for security log Properties** dialog, check **Define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

5.14.4. Configure Windows Firewall Inbound Connection Rules

For successful data collection, Netwrix Auditor may have to create inbound Firewall rules. If you do not enable the **Network traffic compression** option, the product will try creating these rules automatically and will notify you it fails to do so. In this case, you have to configure Windows Firewall inbound rules manually.

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)**

5.15. 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.

5.15.1. 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 Server 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 Server 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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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"*.

5.15.2. Configure Video Recordings Playback Settings

Video recordings of users' activity can be watched in any Netwrix Auditor client. Also, recordings are 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 have read permissions (resultant set) to the **Netwrix_UAVR$** shared folder where video files are stored. By default, all members of the **Netwrix Auditor Client Users** group can access

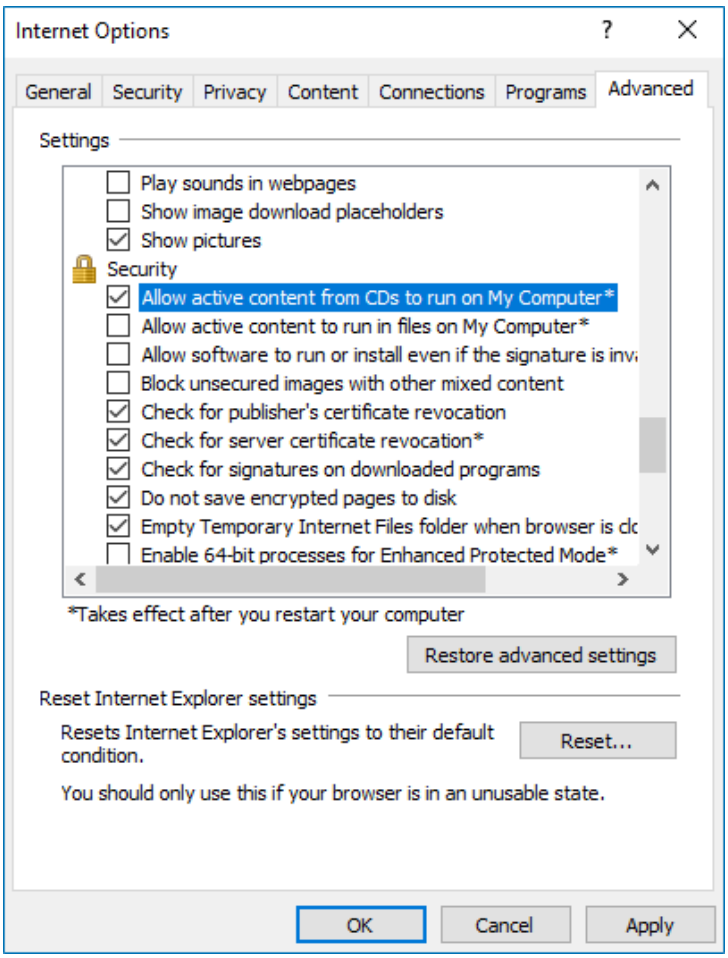
this shared folder. Both the group and the folder are created automatically by Netwrix Auditor. Make sure to grant sufficient permissions on folder or explicitly add user to the group (regardless his or her role delegated in the product). See To add an account to Netwrix Auditor Client Users group for 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 https:/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 Server is deployed. These features allow enabling Windows Media Player and sharing 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. Locate **Security** and check **Allow active content to run in files on My Computer***.



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** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Server Manager**.
2. In the **Security Information** section, click the **Configure IE ESC** link on the right and turn it off.

To add an account to Netwrix Auditor Client Users group

NOTE: All members of the **Netwrix Auditor Client Users** group are granted the **Global reviewer** role in Netwrix Auditor and have access to all collected data.

1. On the computer where Netwrix Auditor Server 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 enable Windows features

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

- If Netwrix Auditor Server 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 Server 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.

6. Configure Netwrix Auditor Service Accounts

To interact with external components (SQL Server-based Audit Database, Report Server, etc.), Netwrix Auditor uses the following service accounts:

Service account	Description
Account for data collection	An account used by Netwrix Auditor to collect audit data from the target systems. See Configure Data Collecting Account for more information.
Audit Database service account	An account used by Netwrix Auditor to write collected audit data to the Audit Database. See Configure Audit Database Account for more information.
SSRS service account	An account used by Netwrix Auditor to upload data to the Report Server. See Configure SSRS Account for more information.
Long-Term Archive service account	An account used to write data to the Long-Term Archive and upload report subscriptions to shared folders. The **LocalSystem** account is selected by default. See Configure Long-Term Archive Account for more information.

6.1. Configure Data Collecting Account

This service account is specified on the monitoring plan creation and is used to collect audit data from the data source items. To ensure successful data collection, Netwrix recommends creating a special service account in advance. The account must comply with the following requirements depending on the data source.

Data source	Rights and permissions
Active Directory	***On the computer where Netwrix Auditor Server is installed:*** • A member of the local **Administrators** group (only for auditing local or trusted domain)

Data source	Rights and permissions

	In the target domain:
	• A member of the **Domain Admins** group / The **Manage auditing and security log** policy defined for this account
	• The **Read** permissions 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*
	  • A member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators**
	  • The **Read/Write** share permission and **Full control** security permission on the logs backup folder

Azure AD	*In the Cloud:* • The account must be assigned the **Global Administrator** role in Azure AD (**Company Administrator** in Azure AD PowerShell terms)— only required when first configuring a monitoring plan for auditing Azure AD domain. Later, any regular account can be used to collect audit data. **NOTE:** Accounts with multi-factor authentication are not supported.

Exchange	*On the computer where Netwrix Auditor Server is installed:*
	• A member of the local **Administrators** group (only for auditing local or trusted domain)
	
	In the target domain:
	• A member of the **Domain Admins** group / The **Manage auditing and security log** policy defined for this account
	• The **Read** permissions 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*
	  • A member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators**

Data source	Rights and permissions
	• The **Read/Write** share permission and **Full control** security permission on the logs backup folder • 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, 2013, or 2016).
Exchange Online	***In the Cloud:*** • 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	***On the target server:*** • The **Manage auditing and security log** and **Backup files and directories** policies must be defined for this account on a file server • The **Read** share permission on the audited shared folders • A member of the local **Administrators** group • For auditing DFS file shares, the account must be a member of the **Server Operators** group in the domain where the file server belongs to
EMC Isilon	***On the target server:*** **NOTE:** This is only required if you are going to configure EMC Isilon for auditing manually. • A member of the local **Administrators** group • The **Read** permissions on the audited shared folders • The **Read** permissions on 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

Data source	Rights and permissions
	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 VNX/VNXe	*On the target server:* • The **Read** share permissions on to the audited shared folders • A member of the local **Administrators** group

NetApp	*On the target server:*
	• A member of the local **Administrators** group
	• The **Read** permissions (resultant set) on the audited shared folders
	• The **Read** permissions (resultant set) on the audit logs folder and its contents and **Delete** permissions (resultant set) on the contents of this folder
	• 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 Clustered Data ONTAP 8** or **ONTAP 9**, 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 readonly

Data source	Rights and permissions
	NOTE: You can also assign the builtin **vsadmin** role. If you want to authenticate with AD user account, you must enable it to access SVM through ONTAPI. The credentials are case sensitive.
Oracle Database	***On the target server:*** • The `CREATE SESSION` system privilege must be granted to an account used to connect to Oracle Database • Depending on your Oracle Database version, the `SELECT` privilege on the following objects must be granted to an account used to connect to Oracle Database: Oracle Database 11g • `aud$` • `gv_$xml_audit_trail` • `dba_stmt_audit_opts` • `v_$parameter` • `dba_obj_audit_opts` • `dba_audit_policies` • `dba_audit_mgmt_clean_events` • `gv_$instance` • `fga_log$` Oracle Database 12c In addition to the privileges above, add the `SELECT` privilege on the following objects: • `gv_$unified_audit_trail` • `all_unified_audit_actions` • `audit_unified_policies` • `audit_unified_enabled_policies` **NOTE:** If you are going to configure Fine Grained Auditing, grant privileges, depending on your Oracle Database version, and make sure that you use Oracle Database Enterprise Edition. Alternatively, you can grant the default administrator role to an account.
SharePoint	***On the target server:***

Data source	Rights and permissions
	• 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
SharePoint Online (including OneDrive for Business)	*In the Cloud:* • The account must be assigned the **Global Administrator** role in Azure AD domain (**Company Administrator** in Azure AD PowerShell terms)— only required when first configuring a monitoring plan. Later, any regular account can be used to collect audit data. **NOTE:** Accounts with multi-factor authentication are not supported.
SQL Server	*On the target server:* • The **System Administrator** role on the target SQL Server
VMware	*On the target server:* • At least **Read-only** role on the audited hosts
Windows Server (including DNS and DHCP)	*On the target server:* • The **Manage auditing and security log** policy must be defined for this account • A member of the local **Administrators** group
Event Log (including IIS)—collected with Event Log Manager	*On the target server:* • A member of the local **Administrators** group
Group Policy	*On the computer where Netwrix Auditor Server is installed:* • A member of the local **Administrators** group (only for auditing local or trusted domain) *In the target domain:* • A member of the **Domain Admins** group / The **Manage auditing and security log** policy defined for this account • The **Read** permissions on the Active Directory **Deleted Objects** container

Data source	Rights and permissions

	• 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*
	  • A member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators**
	  • The **Read/Write** share permission and **Full control** security permission on the logs backup folder

Inactive Users in Active Directory—collected with Inactive User Tracker	***In the target domain:*** • A member of the **Domain Admins** group
Logon Activity	***In the target domain:*** • 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 Operators** or **Server Operators** (only if the account is not a member of the **Domain Admins** group).
Password Expiration in Active Directory—collected with Password Expiration Notifier	***In the target domain:*** • A member of the **Domain Users** group
User Activity	***On the target server:*** • A member of the local **Administrators** group

Follow the procedures below to configure some basic rights and permissions required for data collection:

- Configure Manage Auditing and Security Log Policy
- 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 System Administrator Role
- Assign Audit Logs, Mail Recipients and View-Only Configuration Admin Roles to Office 365 Account
- Configure Back up Files and Directories Policy
- Configure Role on Your EMC Isilon Cluster
- Create Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enable AD User Access
- Grant Create Session and Select Privileges to Account
- Assign Global Administrator Role to Office 365 Account

6.1.1. Configure Manage Auditing and Security Log Policy

NOTE: Perform this procedure only if the account selected for data collection is not a member of the **Domain Admins** group.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **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.

6.1.2. Grant Permissions for AD Deleted Objects Container

NOTE: Perform this procedure only if the account selected for data collection is not a member of 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.

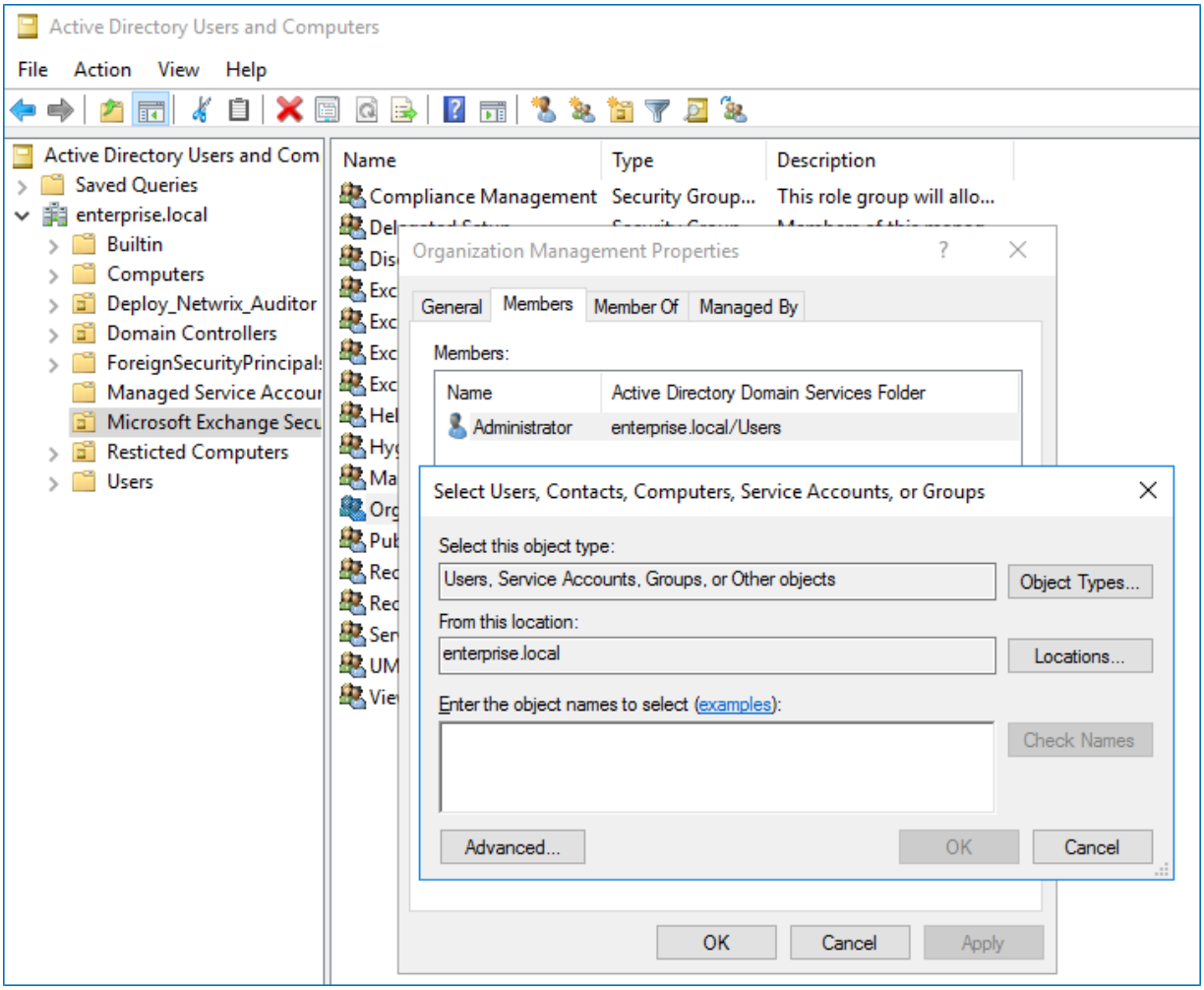
6.1.3. Assign Permissions To Registry Key

NOTE: Perform this procedure only if the account selected for data collection is not a member of 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*.
3. Right-click the **Security** node and select **Permissions** from the pop-up menu.
4. Click **Add** and enter the name of the user that you want to grant permissions to.
5. Check **Allow** next to the **Read** permission.

6.1.4. 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, 2013, or 2016 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.

6.1.5. Assign Audit Logs Role To Account

NOTE: Perform this procedure only if the account selected for data collection is not a member of the **Organization Management** or the **Records Management** group.

1. On the computer where Microsoft Exchange 2010, 2013 or 2016 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.

6.1.6. Assign Audit Logs, Mail Recipients and View-Only Configuration Admin Roles to Office 365 Account

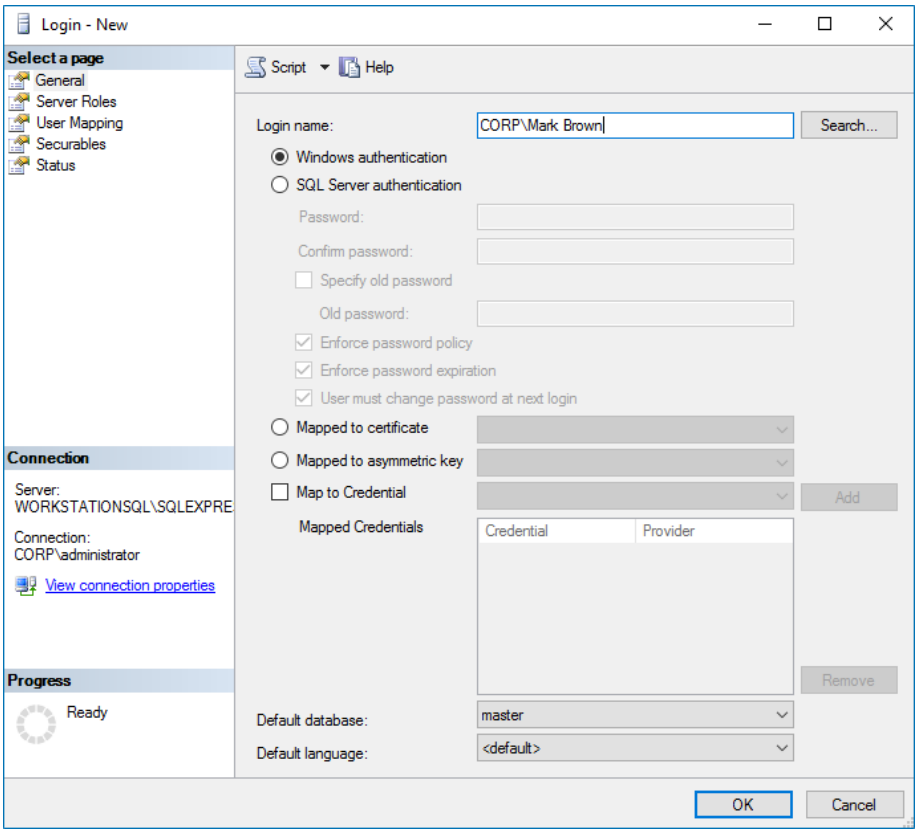
1. Sign in to Office 365 using your Microsoft account.
2. On the **Office 365 Home** page, click **Admin** tile and select **Admin** → **Exchange** on the left.
3. In the **Exchange admin center**, navigate to **Permissions** → **admin roles**.
4. Create a new role group. Assign the following settings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

6.1.7. 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.

6.1.8. 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 when configuring auditing in Netwrix Auditor, the installation will be performed under the account specified for data collection.

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

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

6.1.9. Configure Back up Files and Directories Policy

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **User Right Assignment.**
3. Locate the **Back up files and directories** policy and double-click it.
4. In the **Back up files and directories Properties** dialog, click **Add User or Group**, specify the user that you want to define this policy for.

6.1.10. Create Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 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 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" -
access readonly -vserver vs1
```

Review currently applied capabilities. For example:

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

3. Create a login for the account that is going to authenticate and collect data from NetApp. If you want to use an AD account for collecting data, 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 collecting account.

6.1.11. 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 grant all the necessary permissions to Isilon data collecting account 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

6.1.12. Grant Create Session and Select Privileges to Account

An account used to collect data on your Oracle Database must be granted the following privileges:

- `CREATE SESSION`. Allows an account to connect to a database.
- `SELECT`. Allows an account to retrieve data from one or more tables, views, etc.

Alternatively, you can grant the default administrator role to an account. This role has all privileges required for Netwrix Auditor to function properly:

```
GRANT DBA TO <> <account_name>;
```

The procedure below lists the step-by-step instructions on how to grant these privileges to an account.

To grant CREATE SESSION and SELECT privileges

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.
3. Grant the `CREATE SESSION` system privilege to an account. You can grant this privilege to an existing account or create a new one.

To...	Execute...
Create a new account	`CREATE USER <account_name> IDENTIFIED BY PASSWORD;`
Grant the privilege	`GRANT CREATE SESSION TO <account_name>;`

4. Depending on your Oracle Database version, grant the `SELECT` privilege on the objects below to an account. Review the following for additional information:

For...	Execute...
Oracle Database 11g	• `GRANT SELECT ON aud$ TO <account_name>;` • `GRANT SELECT ON gv_$xml_audit_trail TO <account_name>;` • `GRANT SELECT ON dba_stmt_audit_opts TO <account_name>;` • `GRANT SELECT ON gv_$instance TO <account_name>;` • `GRANT SELECT ON v_$parameter TO <account_name>;` • `GRANT SELECT ON dba_audit_mgmt_clean_events TO <account_name>;` • `GRANT SELECT ON dba_obj_audit_opts TO <account_name>;`

For...	Execute...
	• `GRANT SELECT ON dba_audit_policies TO <account_name>;` • `GRANT SELECT ON fga_log$ TO <account_name>;`
Oracle Database 12c	In addition to the privileges above, grant the `SELECT` privilege on the following objects: • `GRANT SELECT ON gv_$unified_audit_trail TO <account_name>;` • `GRANT SELECT ON all_unified_audit_actions TO <account_name>;` • `GRANT SELECT ON audit_unified_policies TO <account_name>;` • `GRANT SELECT ON audit_unified_enabled_policies TO <account_name>;`

NOTE: If you are going to configure Fine Grained Auditing, grant privileges, depending on your Oracle Database version, and make sure that you use Oracle Database Enterprise Edition.

6.1.13. Assign Global Administrator Role to Office 365 Account

1. Sign in to Office 365 using your Microsoft account.
2. On the **Office 365 Home** page, click **Admin** tile and select **Users** → **Active Users** on the left.
3. Select a user from the list and click **Edit User Roles** in the user preview section.
4. Select **Global administrator**.

NOTE: The Global administrator role is required when first creating Office 365 monitoring plan—a dedicated application is created in your Azure AD domain. Later, any regular account can be used to collect audit data.

Accounts with multi-factor authentication are not supported.

6.1.14. Configure Back up Files and Directories Policy

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **User Right Assignment.**
3. Locate the **Back up files and directories** policy and double-click it.

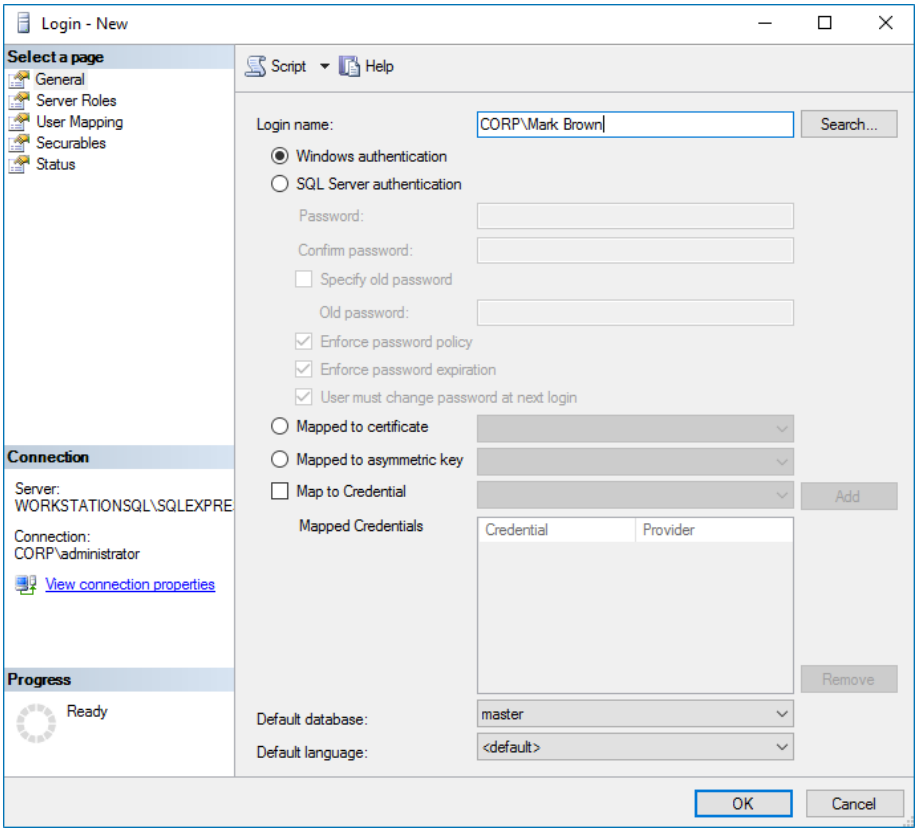
4. In the **Back up files and directories Properties** dialog, click **Add User or Group**, specify the user that you want to define this policy for.

6.2. Configure Audit Database 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 SQL Server instance with Audit Database resides, 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.

6.3. Configure SSRS 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**.

6.3.1. Grant Additional Permissions on Report Server

To be able to generate a report, any user assigned the **Global administrator**, **Global reviewer**, or **Reviewer** role must be granted the **Browser** role on the Report Server. Netwrix Auditor grants this role automatically when adding a user. If for some reason the product was unable to grant the role, do it manually.

To assign the Browser role to a user

1. Open the **Report Manager** URL in your web browser.
2. Depending on the user's delegated scope, select the entire **Home** folder or drill-down to specific data sources or event reports.
3. Navigate to **Manage Folder** (the path can slightly vary depending on your SQL Server version) and select **Add group or user**.
4. Specify an account in the following format: *domain\user*. The account must belong to the same domain where Netwrix Auditor Server is installed, or to a trusted domain.
5. Select **Browser**.

6.4. Configure Long-Term Archive Account

An account used to write data to the Long-Term Archive and upload report subscriptions to shared folders. By default, the **LocalSystem** account is used for the archive stored locally and the computer account is

used for archive stored on a file share.

If you want to store the Long-Term Archive on a file share, you can specify custom account in **Settings** → **Long-Term Archive** in Netwrix Auditor. The custom Long-Term Archive service account must be granted the following rights and permissions:

- The **List folder / read data**, **Read attributes**, **Read extended attributes**, **Create files / write data**, **Create folders / append data**, **Write attributes**, **Write extended attributes**, **Delete subfolders and files**, and **Read permissions** advanced permissions on the folder where the Long-Term Archive is stored
- The **Change** share permission and the **Create files / write data** folder permission on file shares where report subscriptions are saved

  NOTE: Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Long-Term Archive service account as well.

To assign permissions on the Long-Term Archive folder

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

1. Navigate to a folder where the Long-Term Archive will be stored, right-click it and select **Properties**.
2. In the **<Folder_name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security** dialog, select the **Permissions** tab and click **Add**.
4. In the **Permission Entry for <Folder_Name>** dialog, apply the following settings:
   - Specify an account as principal.
   - Set **Type** to *"Allow"*.
   - Set **Applies to** to *"This folder, subfolders and files"*.
   - Switch to the **Advanced permissions** section.
   - Check the following permissions:
     - **List folder / read data**
     - **Read attributes**
     - **Read extended attributes**
     - **Create files / write data**
     - **Create folders / append data**
     - **Write attributes**
     - **Write extended attributes**

- **Delete subfolders and files**
- **Read permissions**

To assign Change and Create Files/Write Data permissions to upload subscriptions to file shares

NOTE: The procedure below applies to Windows Server 2012 R2 and above 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.

   NOTE: The users who are going to access report subscriptions must be granted read access to these shares. Netwrix recommends you to create a dedicated folder and grant access to the entire **Netwrix Auditor Client Users** group or any other group assigned the **Global reviewer** role in Netwrix Auditor.

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 Server resides, 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 client on the computer where Netwrix Auditor Server resides:

1. Navigate to **All monitoring plans** and specify the plan.
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 **All monitoring plans** → **User Activity monitoring plan** → **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. See Uninstall Netwrix Auditor Compression and Core Services for more information.

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**.

NOTE: If you uninstall an instance on Netwrix Auditor that includes Server part (full installation), all remote client consoles will become inoperable.

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
- Protocols and Ports Required for Netwrix Auditor Server

8.1. Install Group Policy Management Console

Group Policy Management Console is an administrative tool for managing Group Policy across the company. If you want to audit Group Policy, Group Policy Management Console must be installed on the computer where Netwrix Auditor Server resides.

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, proceed to the **Features** tab in the left pane, and then 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 **Add Roles and Features Wizard** dialog that opens, proceed to the **Features** tab in the left pane, and then select **Group Policy Management**.
3. Click **Next** to proceed to confirmation page.
4. Click **Install** to enable it.

To install GPMC on Windows 7, Windows 8.1, and Windows 10

1. Depending on your OS, download and install **Remote Server Administrator Tools** that include Group Policy Management Console.
   - Windows 7
   - Windows 8.1
   - Windows 10
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, and then 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 **Add Roles and Features Wizard** dialog that opens, proceed to the **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.

8.3. Protocols and Ports Required for Netwrix Auditor Server

During installation, Netwrix Auditor automatically creates inbound Windows Firewall rules for the essential ports required for the product to function properly. If you use a third-party firewall, make sure these ports are open for outbound connections on the source and inbound connections on the target.

Port	Protocol	Source	Target	Purpose
135	TCP	Computer where Netwrix Auditor is installed	Netwrix Auditor Server	Netwrix Auditor remote client console
9004	TCP	Monitored computers	Netwrix Auditor Server	Core services responsible for user activity monitoring
9699	TCP	Script / query host	Netwrix Auditor Server	Netwrix Auditor Integration API
Dynamic: 1024 -65535	TCP	Netwrix Auditor Server Netwrix Auditor client console	Netwrix Auditor Server	Netwrix Auditor internal components interaction. Allow **C:\Program Files (x86)\Netwrix Auditor\Audit Core\NwCoreSvc.exe** to use the port.

For detailed information on ports and protocols used to collect data from the data sources, contact Netwrix technical support.

8.4. Install Microsoft SQL Server

This section provides instructions on how to:

- Install Microsoft SQL Server 2014 Express
- Verify Reporting Services Installation

8.4.1. 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.

8.4.2. 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, 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.

Index

V

W