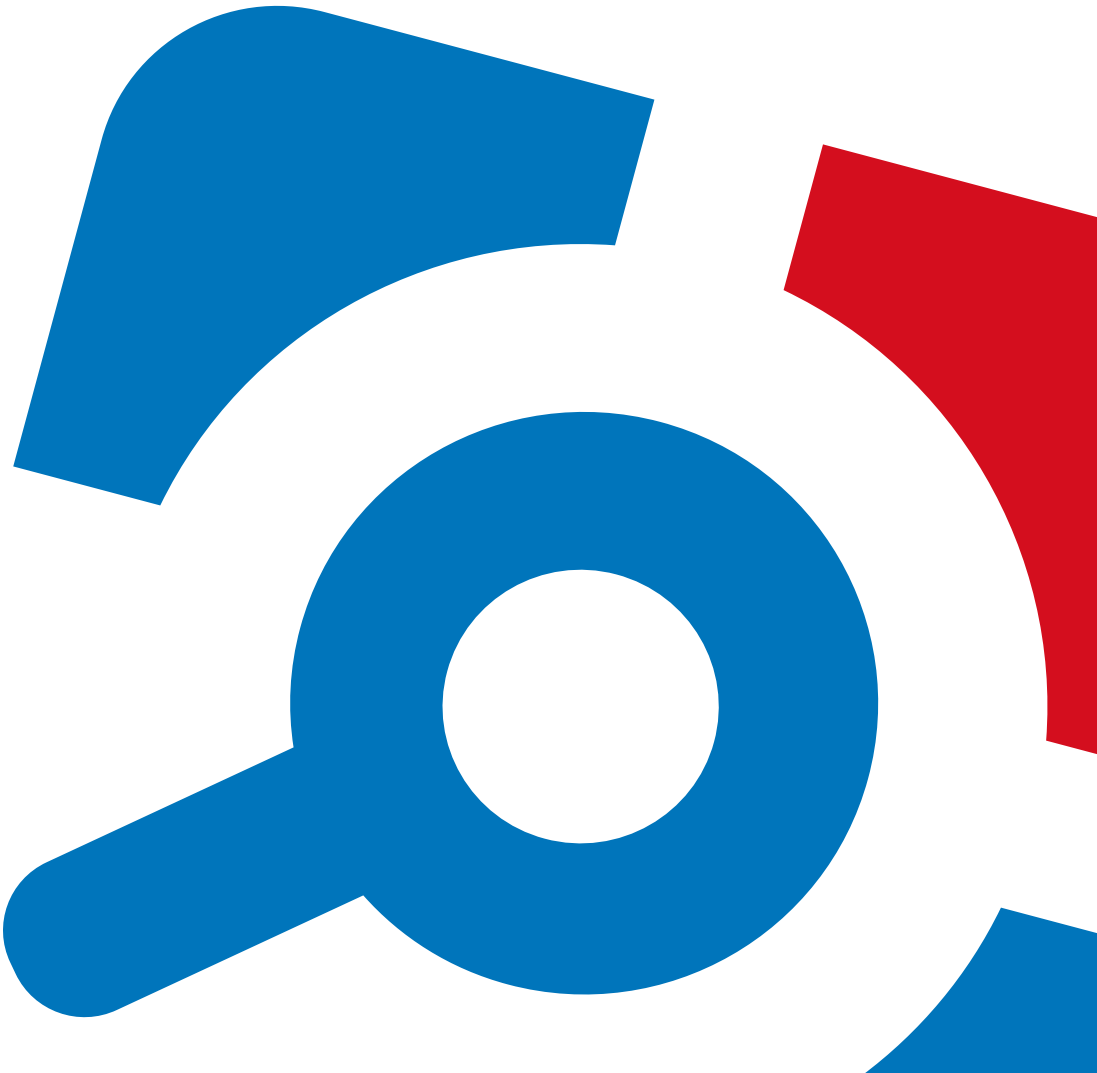
netwrix

Netwrix Auditor

Installation and Configuration Guide

Version: 9.8
10/18/2019



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

Looking for online version? Check out Netwrix Auditor help center.

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 Features and Benefits

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect 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, network devices, SharePoint, Oracle Database, SQL Server, VMware, Windows Server, and User Activity. Empowered with a RESTful API, 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

To learn how Netwrix Auditor can help your achieve your specific business objectives, refer to Netwrix Auditor Best Practices Guide.

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

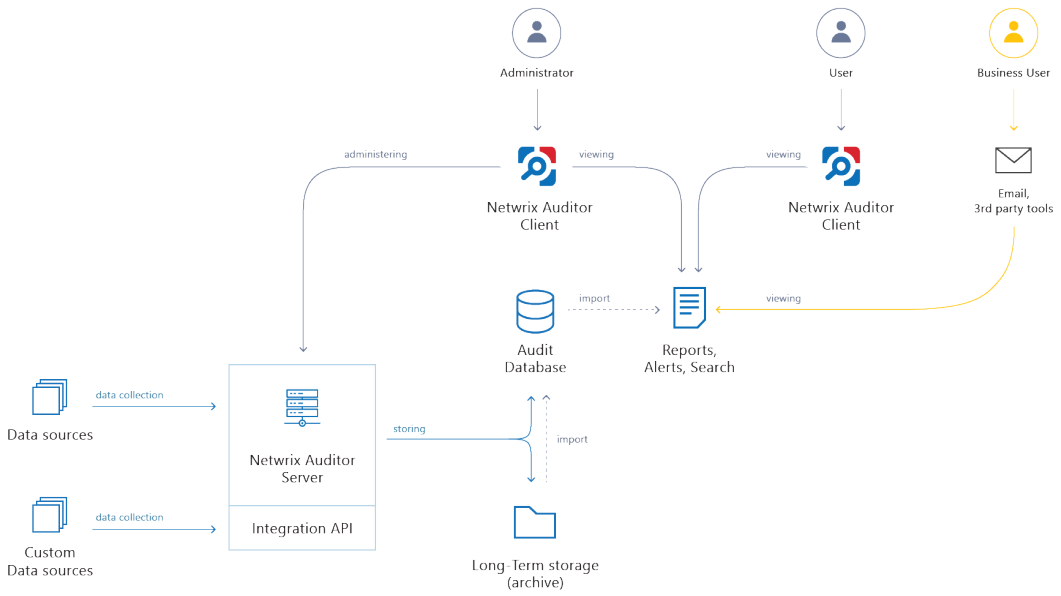
Application	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain 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

Application	Features
	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.
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,

Application	Features
	privileges and security settings, including database objects and directories, user accounts, audit policies, sensitive data, and triggers. 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.
Netwrix Auditor for User Activity	Netwrix Auditor for User Sessions detects and reports on all user actions during a session with the ability to monitor specific users, applications and computers. The product can be configured to capture a video of users' activity on the audited computers.

1.2. How It Works

Netwrix Auditor provides comprehensive auditing of applications, platforms and storage systems. Netwrix Auditor architecture and components interactions are shown in the figure below.



- **Netwrix Auditor Server** — the central component that handles the collection, transfer and processing of audit data from the various data sources (audited systems). Data from the sources not yet supported out of the box is collected using RESTful Integration API.
- **Netwrix Auditor Client** — a component that provides a friendly interface to authorized personnel who can use this console UI to manage Netwrix Auditor settings, examine alerts, reports and search results. Other users can obtain audit data by email or with 3rd party tools — for example, reports can be provided to the management team via the intranet portal.
- **Data sources** — entities that represent the types of audited systems supported by Netwrix Auditor (for example, Active Directory, Exchange Online, NetApp storage system, and so on), or the areas you are interested in (Group Policy, User Activity, and others).
- **Long-Term Archive** — a file-based repository storage keeps the audit data collected from all your data sources or imported using Integration API in a compressed format for a long period of time. Default retention period is 120 months.
- **Audit databases** — these are Microsoft SQL Server databases used as operational storage. This type of data storage allows you to browse recent data, run search queries, generate reports and alerts. Typically, data collected from the certain data source (for example, Exchange Server) is stored to the dedicated Audit database and the long-term archive. So, you can configure as many databases as the data sources you want to process. Default retention period for data stored in the Audit database is 180 days.

1.2.1. Workflow Stages

General workflow stages are as follows:

1. Authorized administrators prepare IT infrastructure and data sources they are going to audit, as recommended in Netwrix Auditor documentation and industry best practices; they use Netwrix Auditor client (management UI) to set up automated data processing.
2. Netwrix Auditor collects audit data from the specified data source (application, server, storage system, and so on).

   To provide a coherent picture of changes that occurred in the audited systems, Netwrix Auditor can consolidate data from multiple independent sources (event logs, configuration snapshots, change history records, etc.). This capability is implemented with Netwrix Auditor Server and Integration API.

   NOTE: For details on custom data source processing workflow, refer to the Integration API documentation.
3. Audit data is stored to the Audit databases and the repository (Long-Term Archive) and preserved there according to the corresponding retention settings.
4. Netwrix Auditor analyzes the incoming audit data and alerts appropriate staff about critical changes, according to the built-in alerts you choose to use and any custom alerts you have created.
   Authorized users use the Netwrix Auditor Client to view pre-built dashboards, run predefined reports, conduct investigations, and create custom reports based on their searches. Other users obtain the data they need via email or third-party tools.
5. To enable historical data analysis, Netwrix Auditor can extract data from the repository and import it to the Audit database, where it becomes available for search queries and report generation.

2. Deployment Planning

This section provides recommendations and considerations for Netwrix Auditor deployment planning. Review these recommendations and choose the most suitable deployment scenario and possible options depending on the IT infrastructure you are going to audit with Netwrix Auditor. Refer to the following sections for detailed information:

- Netwrix Auditor Server and Client
- SQL Server and Audit Database
- File-Based Repository for Long-Term Archive
- Working Folder
- Sample Deployment Scenarios

If you are planning to deploy Data Discovery and Classification edition, refer to this Netwrix Knowledge Base article for recommendations.

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.

2.1. Netwrix Auditor Server and Client

2.1.1. Physical or Virtual?

It is recommended to deploy Netwrix Auditor Server on the virtualized server – to simplify backup, provide scalability for future growth, and facilitate hardware configuration updates. Netwrix Auditor client can be deployed on a physical or virtual workstation, as it only provides the UI.

You can deploy Netwrix Auditor on the VM running on any of the following hypervisors:

- VMware vSphere Hypervisor (ESXi)
- Microsoft Hyper-V
- Nutanix AHV (Acropolis Hypervisor Virtualization) 20180425.199

You can also consider virtual appliance and cloud deployment options provided by Netwrix.

2.1.2. Domains and Trusts

You can deploy Netwrix Auditor on servers or workstations running supported Windows OS version. See system requirements for details.

NOTE: Installation on the domain controller is not supported.

If you plan to have the audited system and Netwrix Auditor Server residing in the workgroups, consider that in such scenario Netwrix Auditor Server cannot be installed on the machine running Windows 7 or Windows Server 2008 R2.

Domain trusts, however, may affect data collection from different data sources. To prevent this, consider the recommendations and restrictions listed below.

If Netwrix Auditor Server and the audit system reside...	Mind the following restrictions...
In the same domain	No restrictions
In two-way 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 Windows Server and 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 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 Windows Server and User Activity, each monitored computer (the computer where Netwrix Auditor User Activity Core Service resides)

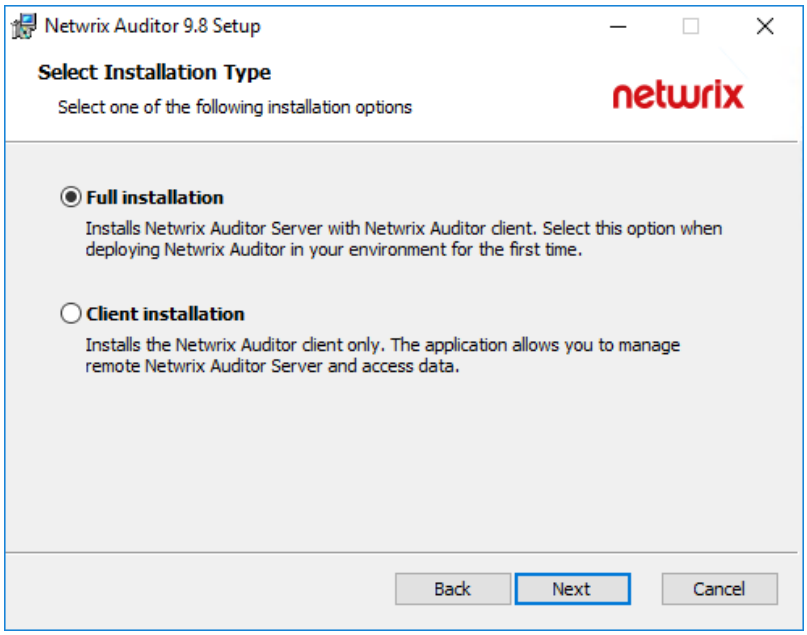
If Netwrix Auditor Server and the audit system reside...	Mind the following restrictions...
	must be able to access the Netwrix Auditor Server host by its DNS or NetBIOS name.

In the next sections you will find some recommendations based on the size of your monitored environment and the number of activity records (ARs) the product is planned to process per day.

NOTE: Activity record stands for one operable chunk of information in Netwrix Auditor workflow.

2.1.3. Simple Deployment

In this scenario, you only deploy Netwrix Auditor Server and default client, selecting **Full installation** option during the product setup.



This scenario can be used for PoC, evaluation, or testing purposes. It can be also suitable for small infrastructures, producing only several thousands of activity records per day.

If you plan to implement this scenario in bigger environments, consider hardware requirements listed in the Netwrix Auditor documentation.

2.1.4. Distributed Deployment (Client-Server)

In this scenario, multiple Netwrix Auditor clients are installed on different machines.

For distributed deployment:

1. First, install Netwrix Auditor Server and default client, selecting **Full installation** during the product setup.
2. Then install as many clients as you need, running the setup on the remote machines and selecting **Client installation** during the setup. Alternatively, you can install Netwrix Auditor client using Group Policy. See Installing Netwrix Auditor Client via Group Policy

NOTE: Default local client will be always installed together with the Netwrix Auditor Server in all scenarios.

2.2. SQL Server and Audit Database

Netwrix Auditor uses SQL Server databases as operational storages that keep audit data for analysis, search and reporting purposes. Supported versions are SQL Server 2008 and later (Reporting Services versions should be 2008 R2 or later).

- You will be prompted to configure the default SQL Server instance when you create the first monitoring plan; also, you can specify it Netwrix Auditor settings.
- You can configure Netwrix Auditor to use an existing instance of SQL Server, or deploy a new instance, as described in the Default SQL Server Instance section.

2.2.1. Sizing

For evaluation and PoC projects you can deploy Microsoft SQL Server 2014 Express Edition with Advanced Services (sufficient for report generation).

For production deployment in bigger environments, it is recommended to use Microsoft SQL Server Standard Edition or higher because of the limited database size and other limitations of Express Edition.

Make your choice based on the size of the environment you are going to monitor, the number of users and other factors. This refers, for example, to Netwrix Auditor for Network Devices: if you need to audit successful logons to these devices, consider that large number of activity records will be produced, so plan for SQL Server Standard or Enterprise edition (Express edition will not fit).

Netwrix Auditor supports automated size calculation for all its databases in total, displaying the result, in particular, in the Database Statistics widget of the **Health Status** dashboard. This feature, however, is supported only for SQL Server 2008 SP3 and later.

2.2.2. Databases

To store data from the data sources included in the monitoring plan, the Monitoring Plan Wizard creates an Audit Database. Default database name is *Netwrix_Auditor_<monitoring_plan_name>*.

NOTE: It is strongly recommended to target each monitoring plan at a separate database.

Also, several dedicated databases are created automatically on the default SQL Server instance. These databases are intended for storing various data, as listed below.

Database name	Description
Netwrix_AlertsDB	Stores alerts.
Netwrix_Auditor_API	Stores activity records collected using Integration API.
Netwrix_Auditor_EventLog	Stores internal event records.
Netwrix_CommonDB	Stores views to provide cross-database reporting.
Netwrix_ImportDB	Stores data imported from Long-Term Archive

These databases do not appear in the UI; if you need their settings to be modified via SQL Server Management Studio, please contact your database administrator. For example, you may need to change logging and recovery model (by default, it is set to ***simple*** for all these databases, as well as for the Audit databases).

See next:

- SQL Server Placement
- SQL Server Reporting Services
- Database Sizing
- Database Settings

2.2.3. SQL Server Placement

When planning for SQL Server that will host Netwrix databases, consider the following:

- Both standalone servers and SQL Server clusters are supported, as well as AlwaysOn Availability Groups.
- For PoC, evaluation scenario or small environment SQL Server can run on the same computer where Netwrix Auditor Server will be installed, or on the remote machine accessible by Netwrix Auditor. Remember to check connection settings and access rights.
- For large and extra-large environments – SQL Server should be installed on a separate server or cluster; installation of Netwrix Auditor and SQL Server on the same server is not recommended in such environments.
- You can configure Netwrix Auditor to use an existing SQL Server instance, or deploy a new instance. If setting up a new instance, you will need to provide the path for storing the SQL databases — it is recommended that you specify the data drive for that purpose (by default, system drive is used).
- You will also need to add the user accounts who will be assigned the **sysadmin** role. Add the following accounts:

a. Configure Data Collecting Account

b. The account currently logged in

c. Local administrator of the machine

- If you plan to have Netwrix Auditor and SQL Server running on different machines, then you should establish fast and reliable connection between them (100 Gbps or higher).
- If you plan to have more than one Netwrix Auditor Servers 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.

See also Requirements for SQL Server to Store Audit Data

2.2.4. SQL Server Reporting Services

Netwrix Auditor utilizes SQL Server Reporting Services (SSRS) engine for report generation.

If you want to generate reports and run search queries against data collected by Netwrix Auditor, you should configure SQL Server Reporting Services (2008 R2 and above required).

Consider that SQL Server and SQL Server Reporting Services can be deployed on the separate machines only in commercial edition. SQL Server Express Edition with Advanced Services does not support such deployment scenario.

If you plan, however, not to use Netwrix Auditor built-in intelligence (search, alerts or reports) but only to receive e-mail notifications on audit data collection results, you may not need to configure SSRS or audit database settings.

2.2.5. Database Sizing

For database sizing, it is recommended to estimate:

1. Size of the environment you are going to monitor
2. Amount of activity records produced by the audited system
3. Retention policy for the audit databases
4. Maximum database size supported by different SQL Server versions

To estimate the number of the activity records produced by your data sources, collected and saved by Netwrix Auditor during the week, you can use the **Activity records by date** widget of the **Health Status** dashboard. See Activity Records Statistics for more information.

Netwrix Auditor supports automated size calculation for all its databases in total, displaying the result, in particular, in the **Database Statistics** widget of the **Health Status** dashboard. To estimate current capacity and daily growth for each database, you can click **View details** and examine information in the table. See Database Statistics for more information.

NOTE: This feature is supported only for SQL Server 2008 SP3 and later.

Remember that database size in SQL Server Express editions may be insufficient. For example, Microsoft SQL Server 2012 SP3 Express Edition has the following limitations which may affect performance:

- Each instance uses only up to 1 GB of RAM
- Each instance uses only up to 4 cores of the first CPU
- Database size cannot exceed 10 GB

2.2.6. Database Settings

Settings of the certain Audit database, including hosting SQL Server, can be specified when you create a monitoring plan and configure data collection for an audited system. Mind the following:

1. To store data from the data sources included in the monitoring plan, you can configure the Audit database on the default SQL Server (recommended), or select another server.
2. By default, database name will be *Netwrix_Auditor_<monitoring_plan_name>*; you can name the database as you need, for example, *Active_Directory_Audit_Data*.

NOTE: To avoid syntax errors, for instance, in the PowerShell cmdlets, it is recommended to use the underscore character (_) instead of space character in the database names.

If not yet existing on the specified SQL server instance, the database will be created there. For this operation to succeed, ensure that Netwrix Auditor service account has sufficient rights on that SQL Server.

Settings of other Netwrix Auditor databases cannot be modified.

2.2.6.0.1. Example

As a database administrator, you can have SQL Server cluster of 2 servers, and 2 Oracle servers. If so, you can create 2 monitoring plans:

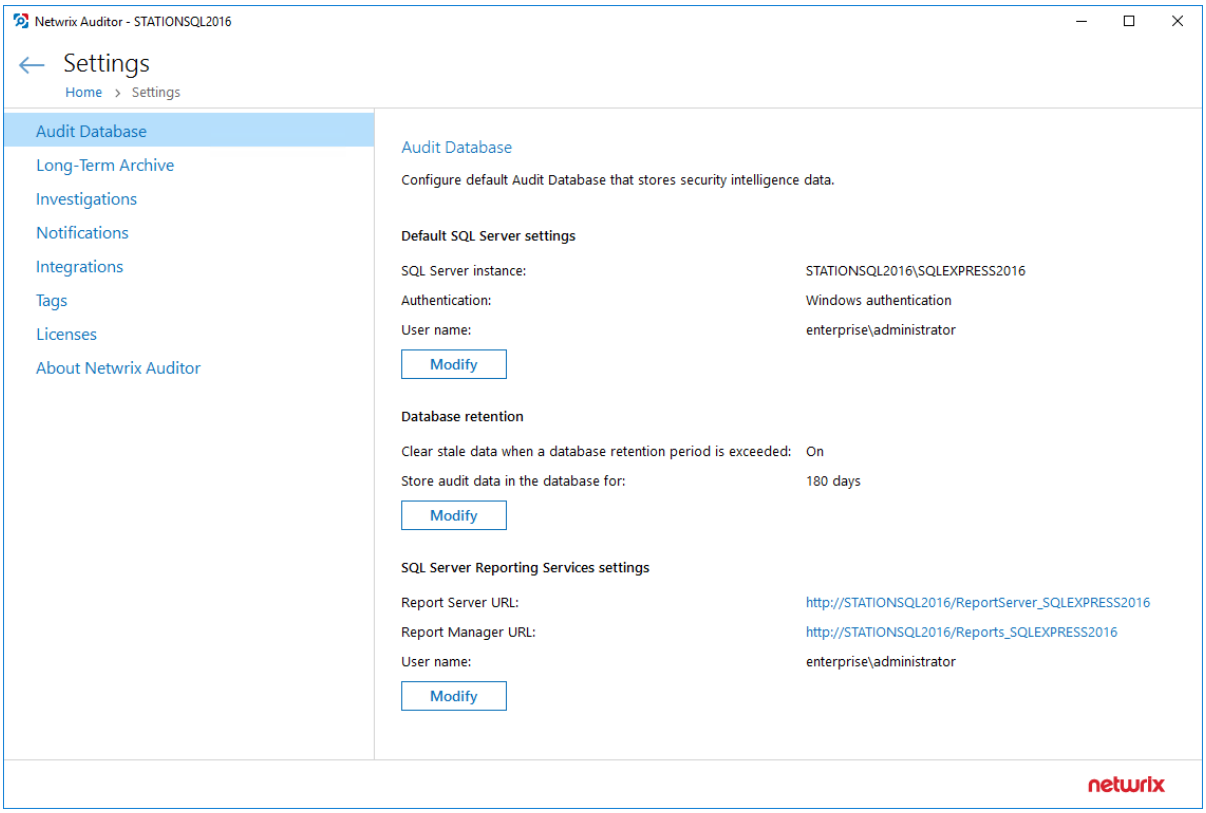
1. First monitoring plan for collecting data from SQL Servers, targeted at *Netwrix_Auditor_SQL_Monitoring* database.
2. Second monitoring plan for collecting data from Oracle servers, targeted at *Netwrix_Auditor_Oracle_Monitoring* database.

2.2.6.1. Database Retention

Consider that retention is a **global** setting, that is, it applies to all Audit databases you configure for your monitoring plans.

To change database retention after the product deployment:

1. In the Netwrix Auditor main screen, select **Settings** → **Audit database**.



2. In the dialog displayed, make sure the **Clear stale data when a database retention period is exceeded:** is set to **ON**, then click **Modify** to specify the required retention period (in days).

NOTE: This setting also applies to the *Netwrix_Auditor_API* database.

2.3. File-Based Repository for Long-Term Archive

Long-Term Archive is a file-based repository for keeping activity records collected by Netwrix Auditor.

2.3.1. Location

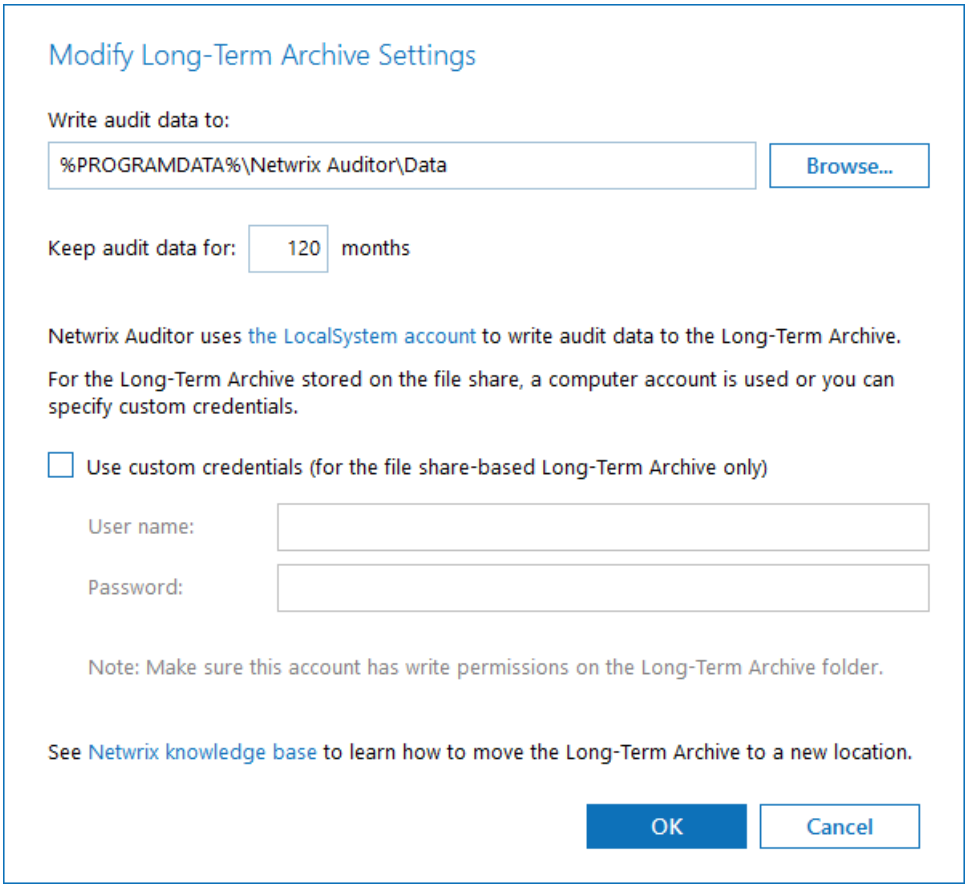
Long-Term Archive can be located on the same computer with Netwrix Auditor Server, or separately - in this case ensure that Netwrix Auditor Server can access the remote machine. By default, the Long-Term Archive (repository) and Netwrix Auditor working folder are stored on the system drive. Default path to the Long-Term Archive is *%ProgramData%\NetwrixAuditor\Data*.

To reduce the impact on the system drive in large and extra-large environments, it is recommended to move Long-Term Archive to another disk. For that, you should estimate the required capacity using recommendations in the next section.

Then you should prepare the new folder for repository, target Netwrix Auditor at that folder, and, if necessary, move repository data from the old to the new location.

To modify Long-Term Archive location and other settings:

1. In Netwrix Auditor client, click **Settings** → **Long-Term Archive**; alternatively, if you are viewing the **Long-Term Archive** widget of the **Health Status** dashboard, click **Open settings**.



2. Click **Modify**, then browse for the required folder.
3. Provide retention settings and access credentials.
4. To move data from the old repository to the new location, take the steps described in this KB article: https://www.netwrix.com/kb/1879.

Netwrix Auditor client will start writing data to the new location right after you complete data moving procedure.

2.3.2. Retention

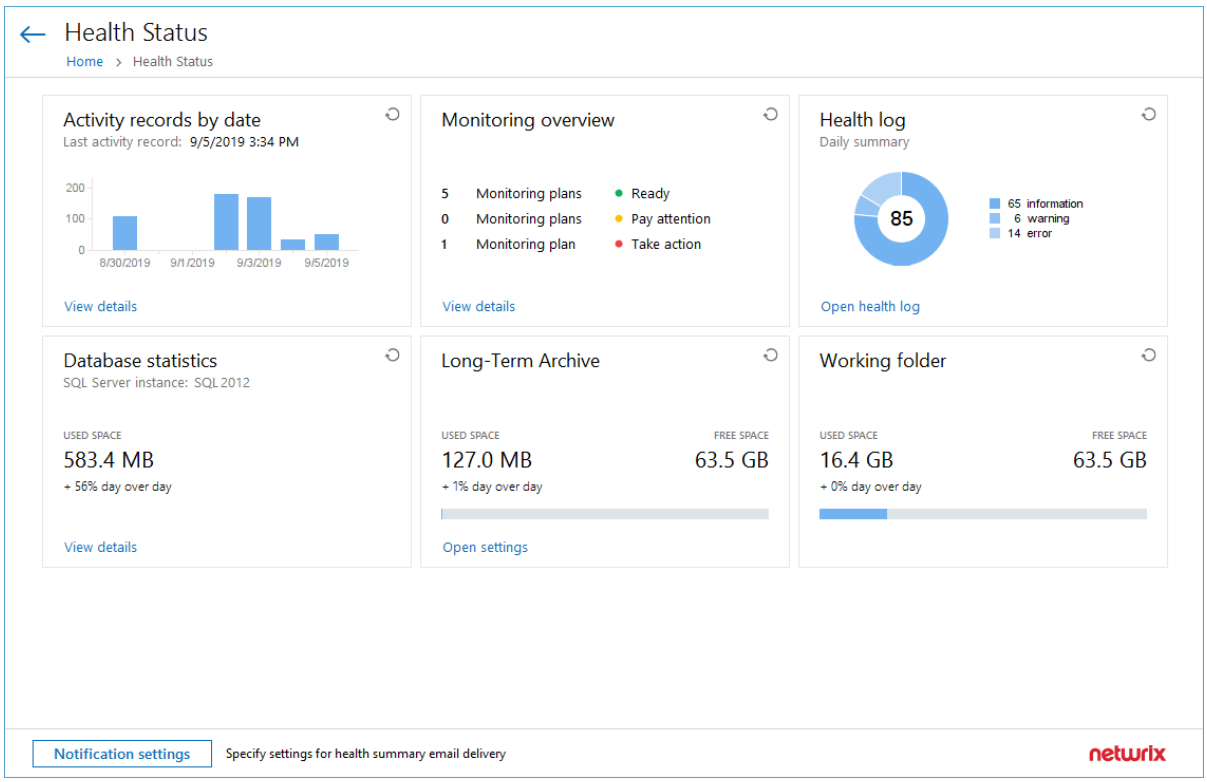
Default retention period for repository data is **120 months**. You can specify the value you need in the Long-Term Archive settings. When retention period is over, data will be deleted automatically.

If the retention period is set to **0**, the following logic will be applied:

- **Audit data for SQL Server, file servers, Windows Server:** only data stored by the last **2** data collection sessions will be preserved.
- **User activity data:** only data stored by the last **7** data collection sessions will be preserved.
- **Other data sources:** only data stored by the last **4** data collection sessions will be preserved.

2.3.3. Capacity

To examine the repository capacity and daily growth, use the Long-Term Archive widget of the **Health Status** dashboard.



To estimate the amount of activity records collected and stored to the repository day by day, use the Activity Records by date widget. Click **View details** to see how many activity records were produced by each data source, collected and saved to the Long-Term Archive and to the database.

Netwrix Auditor will inform you if you are running out of space on a system disk where the repository is stored by default — you will see this information in the **Health Status** dashboard, in the health summary email, and also in the events in the Netwrix Auditor health log.

NOTE: When free disk space is less than **3 GB**, the Netwrix services responsible for audit data collection will be stopped.

2.4. Working Folder

The working folder is a file-based storage that also keeps operational information (configuration files of the product components, log files, and other data). To ensure audit trail continuity, Netwrix Auditor also caches some audit data locally in its working folder for a short period (up to 30 days) prior to storing it to the Long-Term Archive or audit database.

By default, the working folder is located at *C:\ProgramData\Netwrix Auditor\ShortTerm*.

In busy environments and during activity peaks, working folder size may grow significantly and require up to 1 TB, so plan for this file-based storage accordingly. To track the working folder capacity, you can use the **Working Folder** widget of the **Health Status** dashboard. See Netwrix Auditor Administration Guide for more information. See Netwrix Auditor Working Folder for more information.

If you want to change the working folder default location, it is recommended to contact Netwrix technical support for instructions on running the specially designed utility.

2.5. Sample Deployment Scenarios

Recommendations in the sections below refer to deploying the product in the environments of different size:

- Small Environment
- Regular Environment
- Large Environment
- Extra-Large Environment

If you plan to deploy Data Discovery and Classification edition, consider planning for 3 dedicated servers:

- Netwrix Auditor server
- DDC Collector server
- SQL server with 2 instances: for Netwrix Auditor databases and for DDC Collector database

Also, ensure these servers have enough RAM to prevent from performance loss - minimum 12 GB required, 16+ GB recommended.

To learn more, see DDC Edition: How It Works and Deployment Planning for DDC Edition.

When planning for hardware resources, consider that insufficient CPU and RAM may lead to performance bottlenecks. Thus, try to provide not minimal but recommended configuration. Same recommendations refer to planning for storage capacity, especially if you plan to keep historical data for longer periods (e.g., to provide for investigations, compliance audit, etc.) - SSD

2.5.1. Small Environment

Recommendations below refer to deployment in the evaluation lab or small infrastructure (up to 500 users):

1. Prepare a virtual machine meeting the following requirements:

Hardware component	Requirement
Processor	2 cores
RAM	4 GB minimum, 8 GB recommended
Disk space	100 GB on system drive 100 GB on data drive (capacity required for SQL Server and Long-Term Archive)
Screen resolution	Minimum 1280x1024 Recommended 1920x1080 or higher

2. Download and install Netwrix Auditor on that VM, selecting **Full installation** to deploy both server and client components.
3. When prompted to configure the Audit database settings, proceed with installing SQL Server Express Edition with Advanced Services on the same VM. See Install Microsoft SQL Server and Reporting Services for more information.

Alternatively, you can install Netwrix Auditor as a virtual appliance on your VMware vSphere or Hyper-V virtualization server. For more information on this deployment option, refer to the Virtual Appliance page.

2.5.1.1. PoC and Production Infrastructure

- If you are implementing a PoC project, it is strongly recommended that after its completion you create a new Netwrix Auditor server VM dedicated for use in production. Migrating the VM that hosted Netwrix Auditor server during the PoC into production environment is not recommended, as it may lead to performance problems.
- Consider using a dedicated SQL Server for the PoC project. Production database servers are often configured with the features that are not necessary for Netwrix Auditor (like cluster support, frequent backup, and so on). If you have no opportunity to use a dedicated SQL Server, then create an dedicated instance for Netwrix Auditor databases on your existing server.

2.5.2. Regular Environment

Recommendations below refer to the product deployment in a in a regular environment (500 — 1000 users, approximately up to 1 million of activity records generated per day):

1. Prepare a physical or a virtual machine meeting the following requirements:

Hardware component	Requirement
Processor	2-4 cores
RAM	16 - 32 GB
Disk space	200 GB on system drive 0.5 - 1 TB or more on data drive (capacity required for SQL Server and Long-Term Archive)
Screen resolution	Minimum 1280x1024 Recommended 1920x1080 or higher

2. Download and install Netwrix Auditor on that machine. Deploy the required number of Netwrix Auditor clients on the remote Windows machines.

   NOTE: Client-server connection requires user sign-in. You can automate this process, as described Automate Sign-in to Netwrix Auditor Client section.

3. When prompted to configure the Audit database settings, proceed with installing SQL Server Express Edition with Advanced Services. See SQL Server and Audit Database for more information.

Alternatively, you can install Netwrix Auditor as a virtual appliance on your VMware vSphere or Hyper-V virtualization server. For more information on this deployment option, refer to the Virtual Appliance page.

2.5.3. Large Environment

Recommendations below refer to the product deployment in a large environment (up to 20 000 users, approximately 1+ million of activity records generated per day):

1. Prepare a physical or a virtual machine for Netwrix Auditor server, meeting the following requirements:

Hardware component	Requirement
Processor	2 cores minimum, 4 cores recommended
RAM	16 - 32 GB
Disk space	• 200-500 GB on system drive • 0.5 - 1 TB on data drive
Screen resolution	Minimum 1280 x 1024

Hardware component	Requirement
	Recommended 1920 x 1080 or higher

2. Download and install Netwrix Auditor on that machine. Deploy the required number of Netwrix Auditor clients on the remote Windows machines.

   NOTE: Client-server connection requires user sign-in. You can automate this process, as described in the Automate Sign-in to Netwrix Auditor Client section.

3. Prepare Microsoft SQL Server meeting the following requirements:

Hardware component	Requirement
Processor	2-4 cores
RAM	16-32 GB
Disk space	• 100 GB on system drive • 200-400 GB on data drive

Software component	Requirement
Microsoft SQL Server 2008 or later	Standard or Enterprise edition (Express cannot be used due to its database size limitation)
	Dedicated SQL Server instance or cluster is recommended
	SQL Server Reporting Services for reporting

2. When prompted to configure the Audit database settings, proceed using the dedicated SQL Server with Reporting Services.

2.5.4. Extra-Large Environment

Recommendations below refer to the product deployment in an extra-large environment, that is, with more than 20 000 users (10+ million of activity records generated per day):

1. Prepare a physical or a virtual machine for Netwrix Auditor server, meeting the following requirements:

Hardware component	Requirement
Processor	Minimum 4 cores, 8-16 recommended

Hardware component	Requirement
RAM	32 - 64 GB
Disk space	• 300-500 GB on system drive • 1+ TB on data drive
Screen resolution	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher

2. Download and install Netwrix Auditor on that machine. Deploy the required number of Netwrix Auditor clients on the remote Windows machines.

   NOTE: Client-server connection requires user sign-in. You can automate this process, as described in the Automate Sign-in to Netwrix Auditor Client section.

3. Prepare a machine for Microsoft SQL Server meeting the following requirements:

Hardware component	Requirement
Processor	4 cores
RAM	32 - 64 GB
Disk space	• 100 GB on system drive • 1 TB on data drive

Software component	Requirement
Microsoft SQL Server 2008 or later	Standard or Enterprise edition (Express cannot be used due to its database size limitation)
	Dedicated SQL Server instance or cluster is recommended
	SQL Server Reporting Services for reporting

4. As an option, you can install Reporting Services on a dedicated machine. The following hardware configuration is recommended:

Hardware component	Requirement
Processor	4 cores

Hardware component	Requirement
RAM	32 GB
Disk space	• 100 GB on system drive

5. When prompted to configure the Audit database settings, proceed using the dedicated SQL Server and Reporting Services.

2.6. Netwrix Auditor for Network Devices Licensing

Netwrix Auditor for Network Devices tracks the number of active network devices (i.e., sending syslog messages) in its monitoring scope and compares it with the licensed device count. When the licensed amount is exceeded, the application displays a warning.

Consider the following :

- Netwrix Auditor for Network Devices checks audited devices every hour and removes information on inactive ones.
- If Netwrix Auditor does not receive syslog messages from a device for 7 days (by default), the devices is considered to be inactive.
- Information on your network devices will be preserved even if you disable auditing of network devices data source or restart the **Netwrix Auditor for Network Devices Audit Service**.
- License violation occurs when maximum network device limit exceeded.
- Netwrix Auditor for Network Devices includes internal **DeviceCounter** component responsible for calculation procedures.

3. Prerequisites and 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
- Requirements for SQL Server to Store Audit Data

To learn about Netwrix Auditor licenses, refer to the following Netwrix Knowledge Base article: Netwrix Auditor Licensing FAQs. To learn how to install a license, refer to Licenses.

To learn about ports and protocols required for product operation, refer to Protocols and Ports Required for Netwrix Auditor.

To learn about security roles and permissions required for product operation, refer to Configure Netwrix Auditor Service Accounts.

3.1. 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 2019 • Windows Server 2016 • Windows Server 2012/2012 R2 • Windows Server 2008/2008 R2
Azure AD	Azure Active Directory version provided within Microsoft Office 365. **NOTE:** Microsoft Azure *China*, *Germany* and *US Government* regions are not supported. Netwrix Auditor collects data through Office 365 APIs. In order to

Data source	Supported Versions
	access these APIs, you should have an Office 365 business account with global administrator privileges associated with one of suitable Office 365 plans (e.g., Office 365 Enterprise E1). See Assigning Global Administrator Role for Azure AD and Office 365 Auditing for more information.
Exchange	• Microsoft Exchange Server 2016 • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2010 SP1 and above
Exchange Online	Exchange Online version provided within Microsoft Office 365. **NOTE:** Microsoft Azure *China*, *Germany* and *US Government* regions are not supported.

Windows File Servers	• Windows Server OS:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012/2012 R2
	  • Windows Server 2008 R2
	  • Windows Server 2008 SP2 (32 and 64-bit)
	• Windows Desktop OS (32 and 64-bit):
	  • Windows 10
	  • Windows 8.1
	  • Windows 7
	
	NOTE: To collect data from 32-bit operating systems, network traffic compression must be **disabled**.
	
	To collect data from Windows Failover Cluster, network traffic compression must be **enabled**.
	
	See File Servers.

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) • EMC Unity – for recommendations on setting up the auditing, see

Data source	Supported Versions
	this Netwrix Knowledge Base article.
NetApp	• NetApp ONTAP 9.0 – 9.6 (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 Data ONTAP 8 in 7-mode (CIFS configuration only) • NetApp Data ONTAP 7 (CIFS configuration only)
Network Devices	**Cisco devices** • Cisco ASA (Adaptive Security Appliance) 8 and above • Cisco IOS (Internetwork Operating System) 12 and 15 **Fortinet Fortigate** • FortiOS 5, 6 **SonicWall** • SonicWall Web Application Firewall 2.0.x.x • SonicWall NSv 6.5.x.x with SonicOS 6.5.x • SonicWall SMA 11.4.x **Juniper Networks** • vSRX with Junos OS 12.1, Junos OS 18.1 • vMX with Junos OS 17.1 **Palo Alto** • Palo Alto with PAN-OS 8.0.0
Oracle Database	• Oracle Database 11g • Oracle Database 12c On-Premise (all editions) • Oracle Database Cloud Service (Enterprise Edition)
SharePoint	• Microsoft SharePoint Server 2019 • Microsoft SharePoint Server 2016 • Microsoft SharePoint Foundation 2013 and SharePoint Server 2013 • Microsoft SharePoint Foundation 2010 and SharePoint Server 2010
SharePoint Online	SharePoint Online version provided within Microsoft Office 365.

Data source	Supported Versions
	NOTE: Microsoft Azure *China*, *Germany* and *US Government* regions are not supported. Netwrix Auditor collects data through Office 365 APIs. In order to access these APIs, you should have an Office 365 business account with global administrator privileges associated with one of suitable Office 365 plans (e.g., Office 365 Enterprise E1). See Assigning Global Administrator Role for Azure AD and Office 365 Auditing for more information.
SQL Server	• Microsoft SQL Server 2017 • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 **NOTE:** Only stand-alone SQL Servers can be audited. Auditing of Always-On Availability groups is not supported.
VMware	• VMware vSphere (ESX) 6.0 – 6.7 • VMware vSphere Hypervisor (ESXi) 6.0 – 6.7 • VMware vCenter Server 6.0 – 6.7 • **NOTE:** .NET Framework 4.5 or 4.6 on the computer where Netwrix Auditor Server resides required to audit VMware vSphere 6.5 or 6.7.

Event Log	• Windows Server OS:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012/2012 R2
	  • Windows Server 2008 R2
	  • Windows Server 2008 SP2 (32 and 64-bit)
	• Windows Desktop OS (32 and 64-bit):
	  • Windows 10

Data source	Supported Versions
	• Windows 8.1 • Windows 7

Windows Server	• Windows Server OS:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012/2012 R2
	  • Windows Server 2008 R2
	  • Windows Server 2008 SP2 (32 and 64-bit)
	• Windows Desktop OS (32 and 64-bit):
	  • Windows 10
	  • Windows 8.1
	  • Windows 7

DNS	Windows Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 SP2 (32 and 64-bit)
DHCP	Windows Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2
IIS	IIS 7.0 and above
User Activity	• Windows Server OS: • Windows Server 2019

Data source	Supported Versions
	• Windows Server 2016 • Windows Server 2012/2012 R2 • Windows Server 2008 R2 • Windows Server 2008 SP2 (32 and 64-bit) • Windows Desktop OS (32 and 64-bit): • Windows 10 • Windows 8.1 • Windows 7

3.1.1. Technology Integrations

In addition to data sources monitored within product, Netwrix Auditor supports technology integrations leveraging Integration API. Download free add-ons from Netwrix Auditor Add-on Store to enrich your Netwrix Auditor audit trails with activity from the following systems and applications:

Integration	Supported Versions
RADIUS server	• Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016
Amazon Web Services	Version currently provided by Amazon
Cisco devices	• Cisco ASA (Adaptive Security Appliance) 8 and above • Cisco IOS (Internetwork Operating System) 12 and 15
Syslog devices	• Red Hat Enterprise Linux 7 and 6 • SUSE Linux Enterprise Server 12 • openSUSE 42 • Ubuntu 16 • and others devices that support rsyslog messages

For more information about add-ons, refer to Netwrix Auditor Integration API Guide. Also, there are even more add-ons that can export data collected by Netwrix Auditor to other systems (e.g., ArcSight and ServiceNow).

3.2. 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 Planning

3.2.1. Hardware Requirements

This section provides rough estimations of the resources required for Netwrix Auditor PoC or evaluation deployment. Consider that actual hardware requirements will depend on your monitored infrastructure, the number of users in your environment, and activities that occur in the infrastructure per day.

3.2.1.1. Full Installation

The full installation includes both Netwrix Auditor Server and Netwrix Auditor client. This is the initial product installation.

The metrics provided in this section are valid for clean installation on a server without any additional roles or third part applications installed on it. The configuration with SQL Server implies that the instance will be used exclusively by Netwrix Auditor. The use of virtual machine is recommended.

Use the numbers below only for initial estimations and be sure to correct them based on your data collection and monitoring workflow.

You can deploy Netwrix Auditor on a virtual machine running Microsoft Windows guest OS on the corresponding virtualization platform, in particular:

- VMware vSphere
- Microsoft Hyper-V
- Nutanix AHV

Note that Netwrix Auditor supports only Windows OS versions listed in the Software Requirements section.

Hardware component	Starter, evaluation, or small environment	Regular environment (1m ARs/day or less)	Large environment (1-10m ARs/day)	XLarge environment (10m ARs/day or more)
Only Netwrix Auditor Server (SQL Server instance will be deployed on another server)				
Processor	2 cores	4 cores	8 cores	16 cores

Hardware component	Starter, evaluation, or small environment	Regular environment (1m ARs/day or less)	Large environment (1-10m ARs/day)	XLarge environment (10m ARs/day or more)
RAM	4 GB	8 GB	16 GB	64 GB
Disk space	100 GB—System drive 100 GB—Data drive (Long-Term Archive and SQL Server)	100 GB—System drive 400 GB—Data drive	500 GB—System drive* 1.5 TB—Data drive	Up to 1 TB—System drive* Up to several TB per year—Data drive
Screen resolution	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher
Others	—	—	Network capacity 1 Gbit	Network capacity 1 Gbit
Netwrix Auditor Server with SQL Server (SQL Server instance will be deployed on the same server)				
Processor	2 cores	4 cores	**NOTE:** In large and xlarge environments, installation of Netwrix Auditor and SQL Server on the same server is not recommended. To ensure Netwrix Auditor operability, deploy a SQL Server instance on a separate server or cluster. Refer to Microsoft guidelines for SQL Server deployment requirements.	
RAM	4 GB	16 GB		
Disk space	100 GB—System drive 100 GB—Data drive (Long-Term Archive and SQL Server)	100 GB—System drive 1.5 TB—Data drive (Long-Term Archive and SQL Server)		
Screen resolution	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher		

*To ensure audit trail continuity, the product caches some data locally in the Short-Term Archive prior to storing it to the Long-Term Archive. In busy environments and during activity peaks, the cache size may grow significantly and require up to 1 TB. By default, the Long-Term Archive and Short-Term Archive are stored on a system drive. To reduce the impact on the system drive in large and xlarge environments, Netwrix recommends moving your Short-Term Archive and Long-Term Archive to another disk.

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 **Health log** once the free disk space starts approaching the minimum level. When the free disk space is less than 3 GB, the Netwrix services responsible for audit data collection will be stopped.

Review recommendations on how to effectively deploy Netwrix Auditor and its components. See Deployment Planning for more information about deploying Netwrix Auditor components (Long-Term Archive and Audit Database) in a separate location.

3.2.1.2. Client Installation

The client installation includes only Netwrix Auditor client console enables you to connect to the Netwrix Auditor Server installed remotely.

Hardware component	Minimum requirements	Recommended requirements
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

3.2.2. 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 Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2	Windows Server OS: • Windows Server 2019 • Windows

Component	Full installation (both Netwrix Auditor Server and Netwrix Auditor client)	Client installation (only Netwrix Auditor client)
	• Windows Server 2012 • Windows Server 2008 R2 SP1 Windows Desktop OS (64-bit): • Windows 10 • Windows 8.1 • Windows 7 SP1 **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, Windows Server 2016, or Windows Server 2019.	Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 SP1 Windows Desktop OS (32 and 64-bit): • Windows 10 • Windows 8.1 • Windows 7 SP1
.NET Framework	• Any .NET Frameworks that goes with your OS: 3.5 SP1, 4.0, 4.5, or 4.6 **NOTE:** To audit VMware vSphere 6.7 or 6.5, .NET Framework 4.5 or 4.6 is required.	—
Installer	• Windows Installer 3.1 and above	• Windows Installer 3.1 and above

3.2.2.1. Additional Components

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

Data source	Components
• Windows Server (with enabled network traffic compression) • User Activity	*In the monitored environment:* • .NET Framework 3.5 SP1, 4.0, 4.5, or 4.6 depending on the target server

Data source	Components
• SharePoint	*In the monitored 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	Usually, there is no need in any additional components for data collection. **NOTE:** If you get an error message saying some components are missing, please contact Netwrix Technical Support.
• 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. **NOTE:** Netwrix Auditor for Oracle Database incompatible with Oracle Data Access Components for .Net Framework 4.0 and above. Check that the .Net Framework 3.5 feature is enabled. Refer to the following Netwrix Knowledge base article: Netwrix Auditor was unable to process the item: Could not load file or assembly... for more information.
• 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 • 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.

3.3. Requirements for SQL Server to Store Audit Data

If you plan to generate reports, use alerts and run search queries in Netwrix Auditor, consider that your deployment must include Microsoft SQL Server where audit data will be stored. For report generation, Reporting Services (or Advanced Services) are also required. For more information, see SQL Server and Audit Database.

Supported SQL Server versions and editions are listed below:

Version	Edition
SQL Server 2017	• Express Edition with Reporting Services • Standard or Enterprise Edition
SQL Server 2016	• Express Edition with Advanced Services (SP2) • Standard or Enterprise Edition
SQL Server 2014	• Express Edition with Advanced Services • Standard or Enterprise Edition
SQL Server 2012	• Express Edition with Advanced Services • Standard or Enterprise Edition
SQL Server 2008 R2	• Express Edition with Advanced Services • Standard or Enterprise 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 manually install and configure Reporting Services 2008 R2 (or later).

SQL Server AlwaysOn Availability Group can also be used for hosting Netwrix Auditor audit databases. For that, after specifying audit database settings in Netwrix Auditor, you should manually add created database to a properly configured AlwaysOn Availability Group. These steps must be taken each time a new audit database is created in Netwrix Auditor.

See this Microsoft article for details on adding a database to AlwaysOn Availability Group.

You can configure Netwrix Auditor to use an existing SQL Server instance, or deploy a new instance.

NOTE: If your deployment planning reveals that SQL Server Express Edition will be suitable for your production environment, then you can install, for example, SQL Server 2014 Express Edition with

Advanced Services using the **Audit Database Settings** wizard or by manually downloading it from Microsoft web site. See Install Microsoft SQL Server and Reporting Services for more information.

4. 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 to allow inbound connections to local ports on the target and outbound connections to remote ports on the source.

Tip for reading the table: For example, on the computer where Netwrix Auditor client is installed (**source**), allow **outbound** connections to **remote** 135 TCP port. On the computer where Netwrix Auditor Server resides (**target**), allow **inbound** connections to **local** 135 TCP port.

Port	Protocol	Source	Target	Purpose
135	TCP	Computer where Netwrix Auditor client is installed	Netwrix Auditor Server	Netwrix Auditor remote client console
9004	TCP	Monitored computers	Netwrix Auditor Server	Core services responsible for user activity monitoring
9011	TCP	Computers where Netwrix Auditor for Windows Server Compression Services reside	Netwrix Auditor Server	Network traffic compression and interaction with hubs and services
9699	TCP	Script / query host	Netwrix Auditor Server	Netwrix Auditor Integration API
Dynamic: 1024 -65535	TCP	Computers where Netwrix Auditor Server and Netwrix Auditor client are installed	Netwrix Auditor Server	Netwrix Auditor internal components interaction. Allow **C:\Program Files (x86)\Netwrix Auditor\Audit Core\NwCoreSvc.exe** to use the port.
For Managed Service Providers: 443	TCP	Netwrix Auditor Server	Netwrix Partner Portal	Reporting on active MSP licenses

In most environments, the rules are created automatically and you do not need to open more ports to ensure successful data collection.

In rare cases, for example if your security policies require you to provide a justification for opening each particular port, you might need a more detailed overview. Check out Netwrix Auditor online help center to learn more about ports used by the product.

5. 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:

- Installing Netwrix Auditor
- Installing Core Services to Audit User Activity and SharePoint (Optional)

It also includes advanced scenarios such as:

- Installing Netwrix Auditor Client via Group Policy
- Install Netwrix Auditor in Silent Mode

5.1. Installing Netwrix Auditor

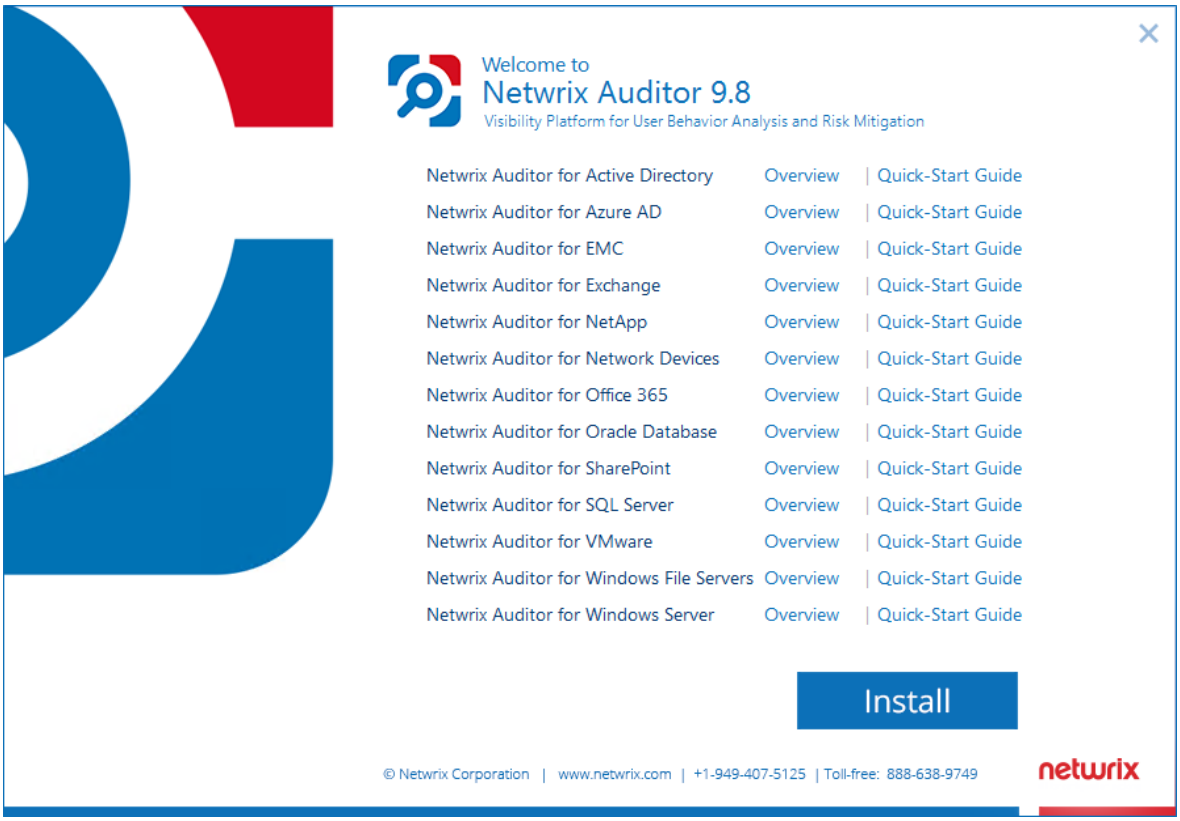
NOTE: For instructions on upgrade procedures, refer to Upgrade to the Latest Version.

To install Netwrix Auditor

1. Download Netwrix Auditor 9.8 from 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.

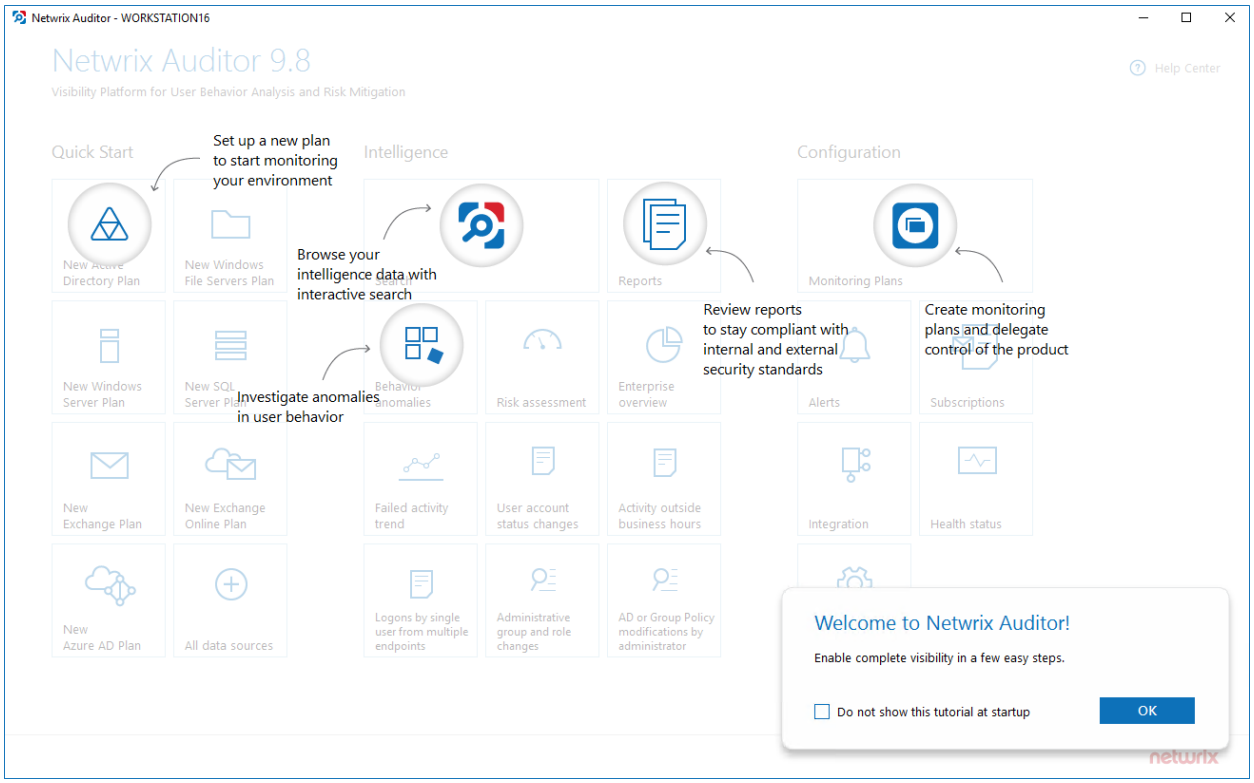
2. Unpack the installation package. The following window will be displayed on successful operation completion:



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 server and client on the same machine. In this case the main component called Netwrix Auditor Server and the Netwrix Auditor client will be installed.
   - **Client installation**—Select if you want to install a UI client to provide access to configuration and audit data.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are invited to take part in the Netwrix Customer Experience Program. It is optional on your part to help Netwrix improve the quality, reliability, and performance of Netwrix products and services. If you accept, Netwrix collects statistical information on how the Licensee uses the product in accordance with applicable law. Select **Skip** if you do not want to participate in the program.

   NOTE: You can always opt-out of the Netwrix Customer Experience Program later.
7. 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.

5.2. Installing Core Services to Audit User Activity and SharePoint (Optional)

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

5.2.1. Install Netwrix Auditor for SharePoint Core Service

This section contains instructions on how to install Netwrix Auditor for SharePoint Core Service.

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

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 Monitoring 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 Assigning 'SharePoint_Shell_Access' Role for more information.

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.

5.2.2. 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.

5.3. Installing Netwrix Auditor Client via Group Policy

The Netwrix Auditor client can be deployed on multiple computers via 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.

5.3.1. 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**.

5.3.2. Create and Distribute Installation Package

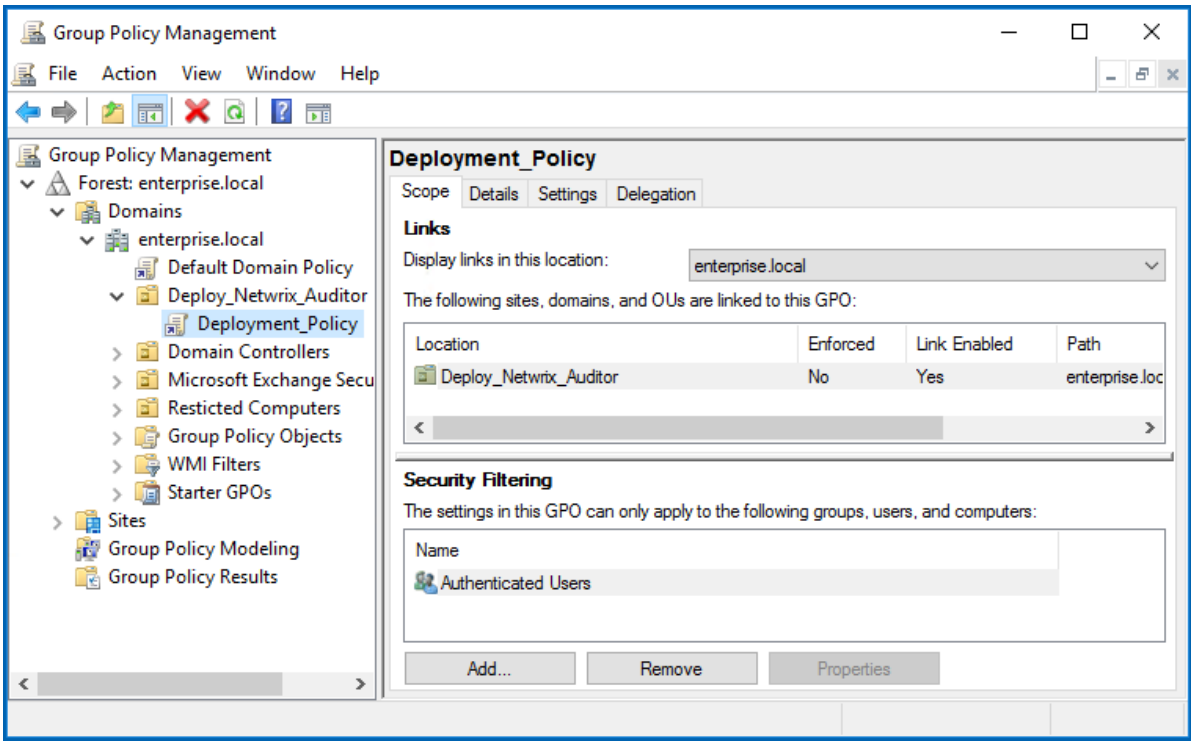
1. Create a shared folder that will be used for distributing the installation package.

   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.

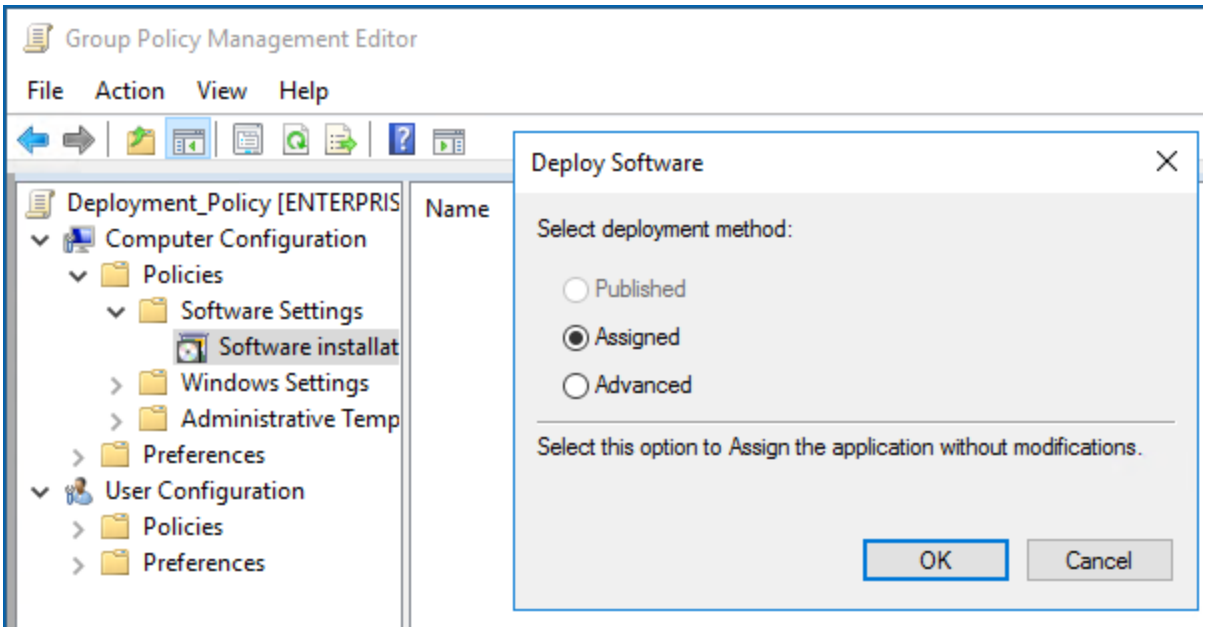
5.3.3. Create a Group Policy to Deploy Netwrix Auditor

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**.

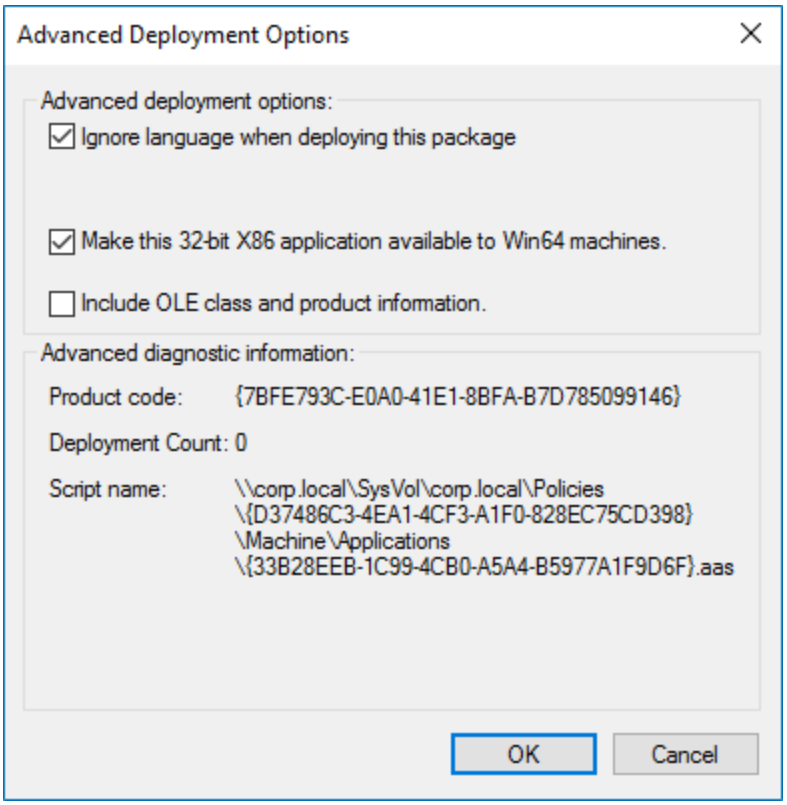


3. Right-click the newly created GPO and select **Edit** from the pop-up menu.
4. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies → Software Settings → Software installation.**
5. In the right page, right-click and select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

5.4. 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

6. Upgrade to the Latest Version

Netwrix recommends that you upgrade from the older versions of Netwrix Auditor to the latest version available in order to take advantage of the new features.

Seamless upgrade to Netwrix Auditor 9.8 is supported for versions **9.6** and **9.7**.

If you need to upgrade from an earlier version, please contact technical support.

See next:

- Before Starting the Upgrade
- Upgrade Procedure

6.1. Before Starting the Upgrade

6.1.1. Take Preparatory Steps

Before you start the upgrade, it is strongly recommended to take the following steps:

1. Check that the account under which you plan to run the setup has **local Administrator** rights.
2. Back up Netwrix databases – these are all Audit databases, Integration API database, and others (their default names start with *Netwrix*). For that:
    a. Start **Microsoft SQL Server Management Studio** and connect to SQL Server instance hosting these databases.
    b. In **Object Explorer**, right-click each Netwrix database and select **Tasks → Back Up**.
    c. Wait for the process to complete.
3. Back up the Long-Term Archive folder, by default located at *C:\ProgramData\Netwrix Auditor\Data*. You can, for example, copy and archive this folder manually, or use your preferred backup routine.
4. Finally, close Netwrix Auditor console.

6.1.2. General Considerations and Known Issues (Upgrade from 9.7 and 9.6)

During the seamless upgrade from previous versions, Netwrix Auditor preserves its configuration, so you will be able to continue auditing right after finishing the upgrade. However, there are some considerations you should examine - they refer to the upgrade process and post-upgrade product operation. The issues listed below applicable to both: upgrade from 9.7 and 9.6.

1. After the upgrade you may receive temporary data collection errors – they occur when the program tries to upload collected data to the Audit Database before the database upgrade is finished.
2. Shortly after the upgrade, Netwrix Auditor may display incorrect monitoring statuses for the items included in the monitoring plan. With the next scheduled data collection, statuses will be updated and displayed normally.
3. Consider the following upgrade notes related to IT Risk Assessment metrics:

    a. After upgrade, risk values displayed having *"No data"* until the product stores a historical snapshot of your system configuration. This refers to IT risk listed below:

    Permissions:

    - **Site collections with the "Get a link" feature enabled**
    - **Sites with the "Anonymous access" feature enabled**

    Data:

    - **Documents and List Items Accessible by Everyone and Authenticated Users**

    Infrastructure:

    - **Servers with inappropriate operating systems**
    - **Servers with under-governed Windows Update configurations**
    - **Servers with unathorized antivirus software**

4. After the upgrade Netwrix Auditor will take some time to synchronize data and make it available for state-in-time reporting, so you will have to wait for this process to complete before reports are filled in with data. This refers to reports listed below:

    Active Directory - State-in-Time reports:

    - **Account Permissions in Active Directory**
    - **Active Directory Account Permissions Details**
    - **Object Permissions in Active Directory**
    - **Active Directory Object Permissions Details**
    - **Effective Group Membership**
    - **Users and Computers - Effective Group Membership**

    Windows Server - State-in-Time reports:

    - **Domain Accounts Running Scheduled Tasks and Services**
    - **Windows Update Configuration**

5. Check your **Network Devices** subscriptions and alerts created in Netwrix Auditor 9.7. Some activity records were refreshed and probably do not match filters, so you should set it up anew.

6. Subscription to the **Administrative Group Members** and **Effective Group Membership** reports may become inoperable, so you should set it up anew.
7. If you were auditing Azure AD, remember to review your Data Collecting Account settings after the upgrade, because this account must be assigned *Azure Active Directory Premium Plan 1* or *Azure Active Directory Premium Plan 2* license. See Configure Data Collecting Account for more information.

6.1.2.1. Upgrade from Netwrix Auditor 9.6 Known Issues

Starting with 9.7, Netwrix Auditor introduces new IT Risk Assessment dashboard that replaces the corresponding reports. After upgrade from 9.6, each subscription to IT Risk Assessment Reports is superseded with subscription to Risk Assessment Dashboard filtered to fully match original. Consider the following notes:

1. IT Risk Assessment dashboard subscriptions delivery is scheduled to 7.00 am daily instead of 8.00 am for report subscriptions.
2. The first daily subscription is empty if the product did not store a historical snapshot until 0.00 am of the current upgrade day. The next day the subscription will contain accurate data. It is subject to the following IT Risk Assessment reports subscriptions in Netwrix Auditor 9.6:
   - **Files and folders accessible by everyone**
   - **File and folder names containing sensitive data**
   - **Potentially harmful files on file shares**
   - **Direct permissions on files and folders**

6.2. Upgrade Procedure

You can upgrade Netwrix Auditor 9.6 and 9.7 to 9.8 by running the installation package.

To perform the upgrade

1. Make sure you have completed the preparatory steps described in the Before Starting the Upgrade section.
2. Run the setup on the computer where Netwrix Auditor Server resides. Refer to Installing Netwrix Auditor section for detailed instructions.
3. If you have a client-server deployment, then after upgrading the server run the setup on all remote machines where Netwrix Auditor Client resides.

NOTE: If you were auditing User Activity or SharePoint server / farm, and the corresponding Core Services were installed automatically according to the monitoring plan settings, then they will be upgraded automatically during the initial data collection.

7. 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	For Azure AD auditing, no special settings are required. However, remember to do the following: 1. Configure data collecting account, as described in Configure Data Collecting Account. 2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Azure AD.

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 network traffic compression when tracking mailbox access on Exchange 2007 and 2010.

Data source	Required configuration

	• 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
	
	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.
	
	Remember to do the following:
	1. Check that Data Collection Account meets the requirements specified in Configure Data Collecting Account for Exchange Online. You may need to take the steps described in Assigning 'Audit Logs', 'Mail Recipients' and 'View-Only Configuration' Admin Roles to Office 365 Account
	2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Office 365

Windows 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"*

Data source	Required configuration

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).

- The following **Advanced audit policy** settings must be configured:
  - The **Audit: Force audit policy subcategory settings (Windows 7 or later)** security option must be enabled.
  - Depending on your OS version, configure the categories as follows:

Windows Server 2008	
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"*

Data source	Required configuration

Audit Handle Manipulation	*"Success"* and *"Failure"*
Audit Detailed file share	*"Failure"*
Audit Removable Storage	*"Success"* and *"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"*
Audit Handle Manipulation	*"Success"*
Audit File Share	*"Success"*
Policy Change	
Audit Audit Policy Change	*"Success"*

- 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)

Data source	Required configuration
	• 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. **NOTE:** If you plan to audit Windows Server 2019 or Windows 10 Update 1803 without network compression service, make sure the following inbound connection rules are enabled: • Remote Scheduled Tasks Management (RPC) • Remote Scheduled Tasks Management (RPC-EMAP) ***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 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

Data source	Required configuration
	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
	  ◦ 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**:

Data source	Required configuration

- 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`.

    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

Data source	Required configuration
	• 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.
Network Devices	***In the audited environment:*** **For Cisco ASA**: • The **global configuration** mode is selected. • The `logging enable` option is selected on the Cisco ASA device. • The `logging host` parameter is set to the host address of the audited CiscoASA device. And UDP port (for, example 514) is used for sending messages. **NOTE:** Do not select the **EMBLEM format logging** for the syslog server option. • The `logging timestamp` option enabled. • The `logging trap` option is selected from 1 to 6 inclusive. **For Cisco IOS**: • The **global configuration** mode is selected. • The `logging timestamp` option enabled. • The `logging trap` option is selected from 1 to 6 inclusive. • The `logging host` parameter is set to the host address where the service is going to be installed. And UDP port (for, example 514) is used for sending messages. **For Fortinet Fortigate**: The target Fortinet Fortigate device must be configured via **Command Line Interface** (CLI) as described in the Configure Fortinet FortiGate Devices section. **For PaloAlto**:

Data source	Required configuration
	Create a Syslog Server profile and syslog forwarding for the target PaloAlto device via Web Interface as described in the Configure PaloAlto Devices section. **For Juniper**: The target Juniper device must be configured via **JunOS Command Line Interface** (CLI) as described in the Configure Juniper Devices section. **For SonicWall**: Configure log settings, depending on your device type. See Configure Network Devices for Monitoring for more information.

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

Data source	Required configuration
	• 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
SQL Server	No configuration required. **NOTE:** If you plan to audit an SQL Server for data changes and browse the results using 'Before' and 'After' filter values, make sure that the audited SQL database tables have a primary key (or a unique column). Otherwise, 'Before' and 'After' values will not be reported.
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 7 or later)** security option must be enabled.
	  • For **Windows Server 2008**—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"*.

Data source	Required configuration

- 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 **Enable Persistent Time Stamp** local group policy must be enabled.
- The **Application, Security**, and **System** event log maximum size must be set to 4 GB. The retention method must be set to *"Overwrite events as needed"*.
- For auditing scheduled tasks, the **Microsoft-Windows-TaskScheduler/Operational** event 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 DHCP, the **Microsoft-Windows-Dhcp-Server/Operational** event 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 DNS, the **Microsoft-Windows-DNS-Server/Audit** event 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"*.
- 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)
  - 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

Data source	Required configuration
	opened. See Protocols and Ports Required for Monitoring Windows Server for details. • For auditing removable storage media, two **Event Trace Session** objects must be created. **NOTE:** If you want to use Network traffic compression, make sure that the Netwrix Auditor Server is accessible by its FQDN name.
Event Log (including Cisco)	***In the audited environment:*** • For Windows-based platforms: the **Remote Registry** service must be running and its **Startup Type** must be set to *"Automatic"*. • For Syslog-based platforms: the Syslog daemon must be configured to redirect events.
IIS	***In the audited environment:*** • The **Remote Registry** service must be running and its **Startup Type** must be set to *"Automatic"*. • The **Microsoft-IIS-Configuration/Operational log** must be enabled and its **maximum size** must be set to 4 GB. The retention method of the log must be set to *"Overwrite events as needed"*.

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

Data source	Required configuration
	• 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 Monitoring Active Directory
- Configure Infrastructure for Monitoring Exchange
- Configure Infrastructure for Monitoring Exchange Online
- Configure Windows File Servers for Monitoring
- Configure EMC Isilon for Monitoring
- Configure EMC VNX/VNXe for Monitoring
- Configure NetApp Filer for Monitoring
- Configure Network Devices for Monitoring
- Configure Oracle Database for Monitoring
- Configure SharePoint Farm for Monitoring
- Configure Windows Server for Monitoring
- Configure Infrastructure for Monitoring Windows Event Logs
- Configure Domain for Monitoring Group Policy
- Configure Infrastructure for Monitoring IIS

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

7.1. Configure Domain for Monitoring Active Directory

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

- Automatically when creating a monitoring plan

  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.

  NOTE: 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.

- Manually.

To configure your domain for monitoring manually, make sure you have the following tools installed:

1. Install Group Policy Management Console
2. Install ADSI Edit

Also, 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
- Adjusting Security Event Log Size and Retention Settings
- Adjust Active Directory Tombstone Lifetime
- Enable Secondary Logon Service

For AD auditing, also remember to do the following:

1. Configure Data Collecting Account, as described in Configure Data Collecting Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Active Directory, Exchange, and Group Policy

NOTE: If you have an on-premises Exchange server 2010, 2013 or 2016 in your Active Directory domain, consider that some changes can be made via that Exchange server. To be able to audit and report who made those changes, you should configure the Exchange Administrator Audit Logging (AAL) settings, as described Configure Exchange Administrator Audit Logging Settings.

Also, the account used for data collection must belong to the **Organization Management** or **Records Management** group

-OR-

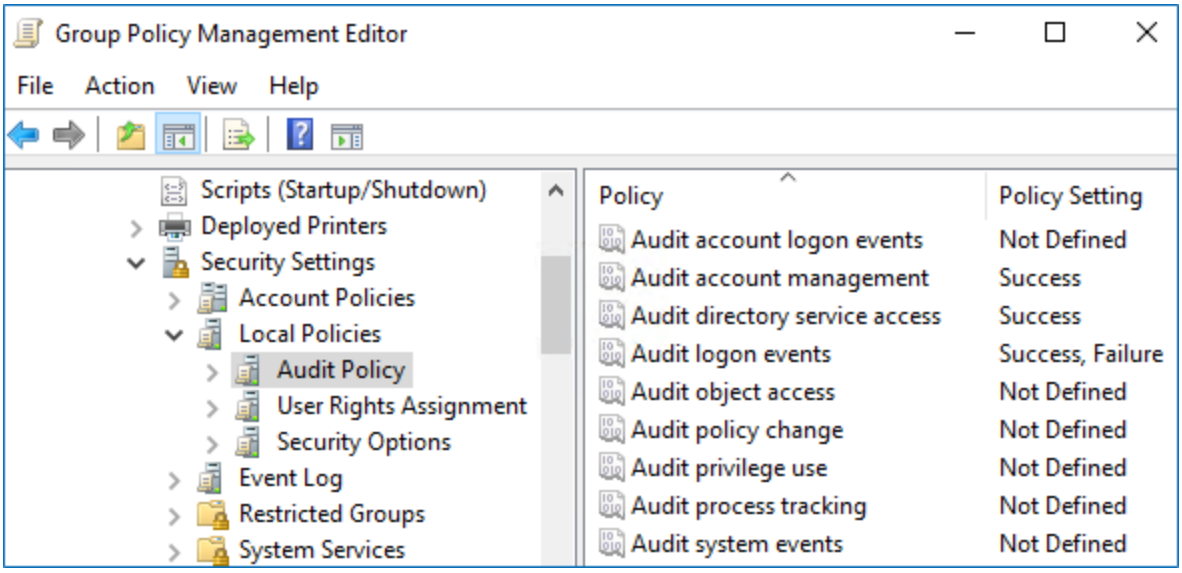
be assigned the Audit Logs management role. See Assigning 'Audit Logs' Role for more information.

7.1.1. 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.

7.1.2. 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:

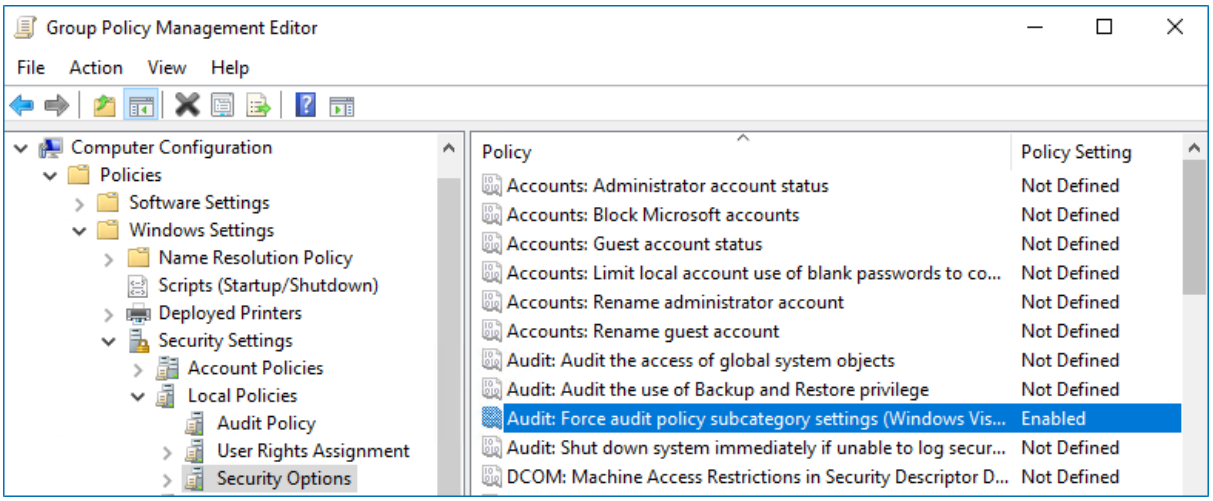
- To configure security options
- To configure advanced audit policies

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



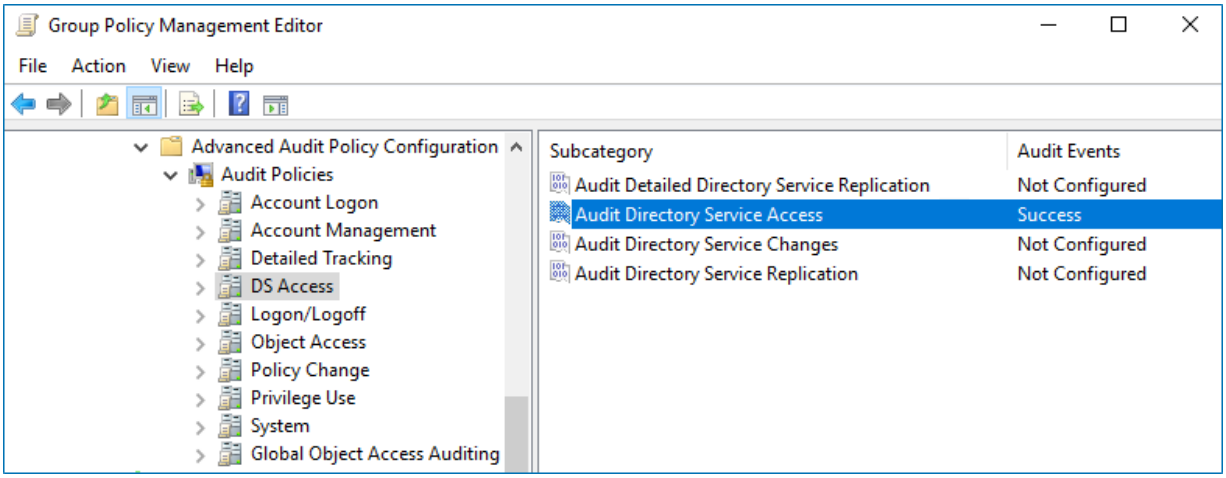
5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

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	*"Success"*

Policy Subnode	Policy Name	Audit Events
	NOTE: These policies are only required to collect the information on the originating workstation, i.e., the computer from which a change was made.	



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

7.1.3. 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.

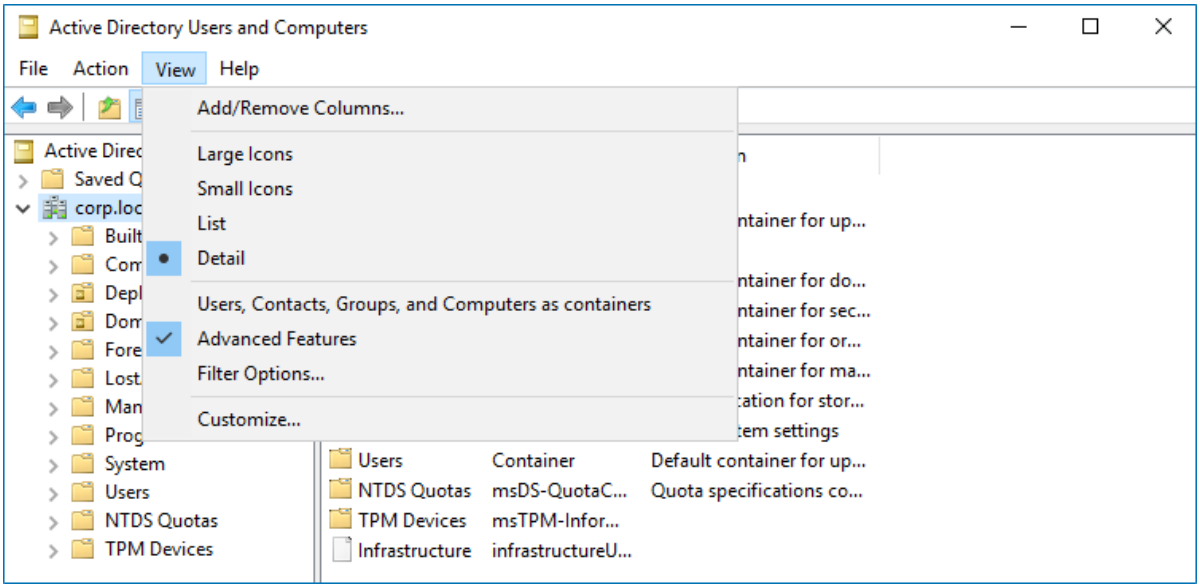
Perform the following procedures to configure object-level auditing for the Domain, Configuration and Schema partitions:

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

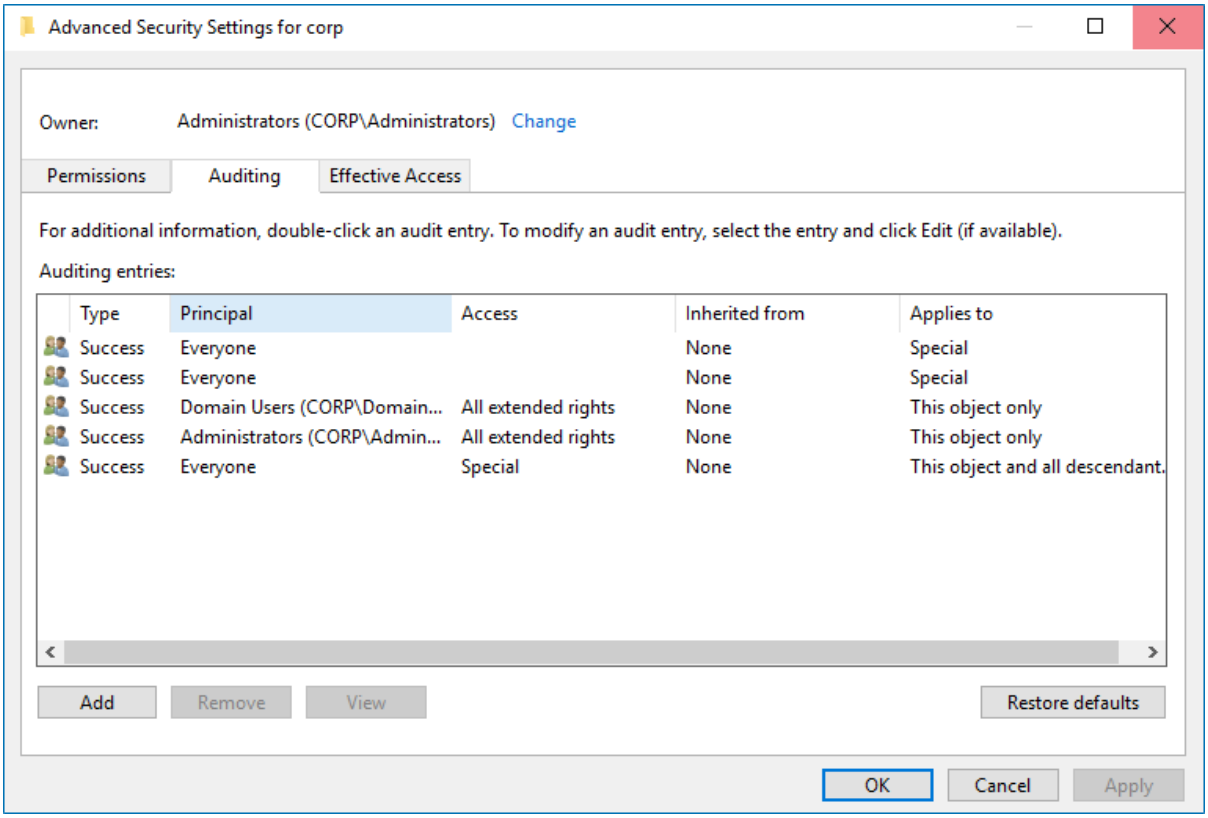
To configure object-level auditing for the Domain partition

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.

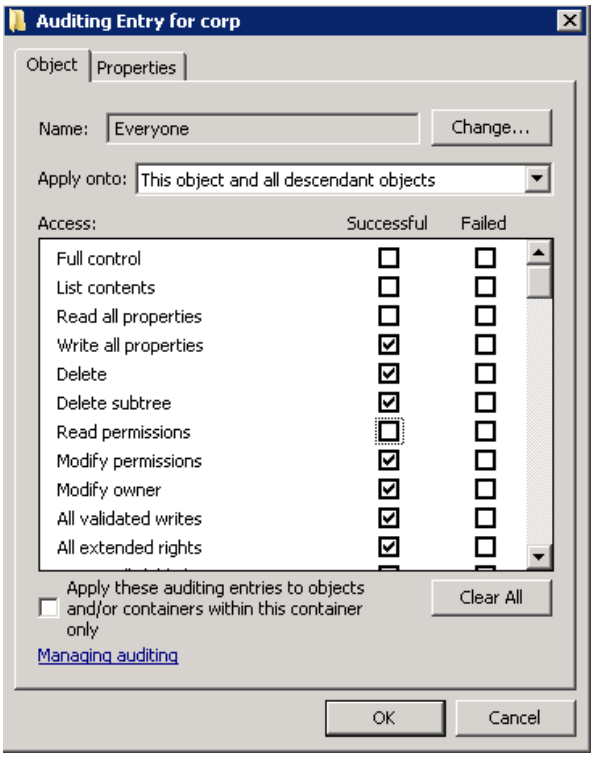


3. Right-click the **<domain_name>** node and select **Properties.** Select the **Security** tab and click **Advanced**. In the **Advanced Security Settings for <domain_name>** dialog, select the **Auditing** tab.



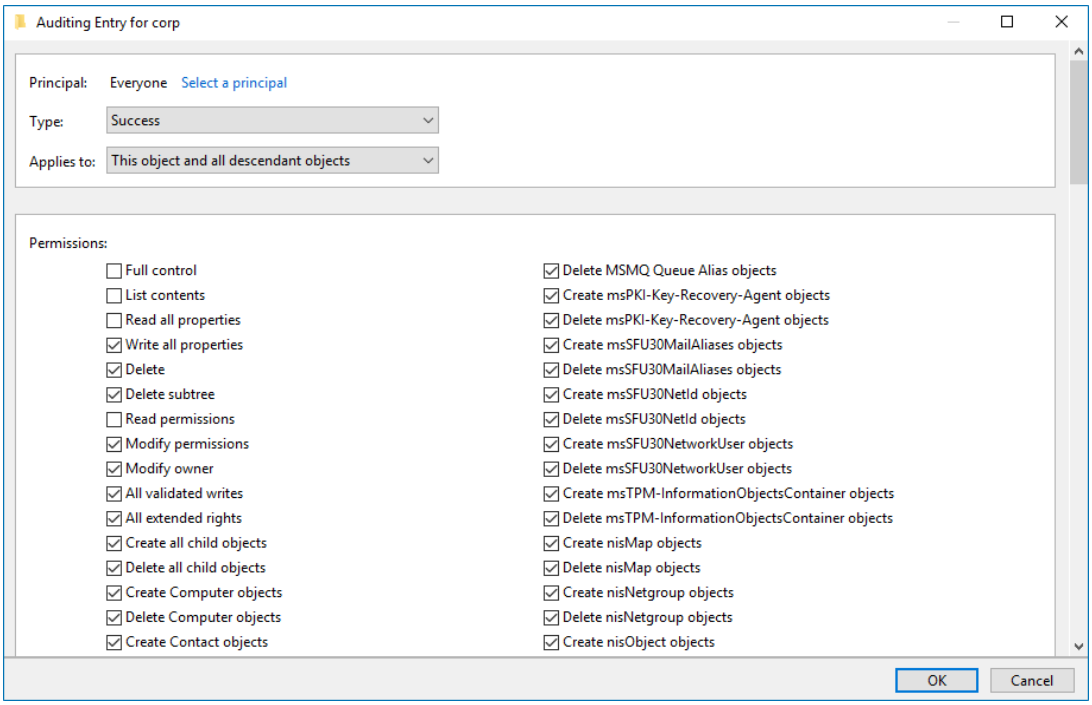
4. Do one of the following depending on the OS:

- 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"*.

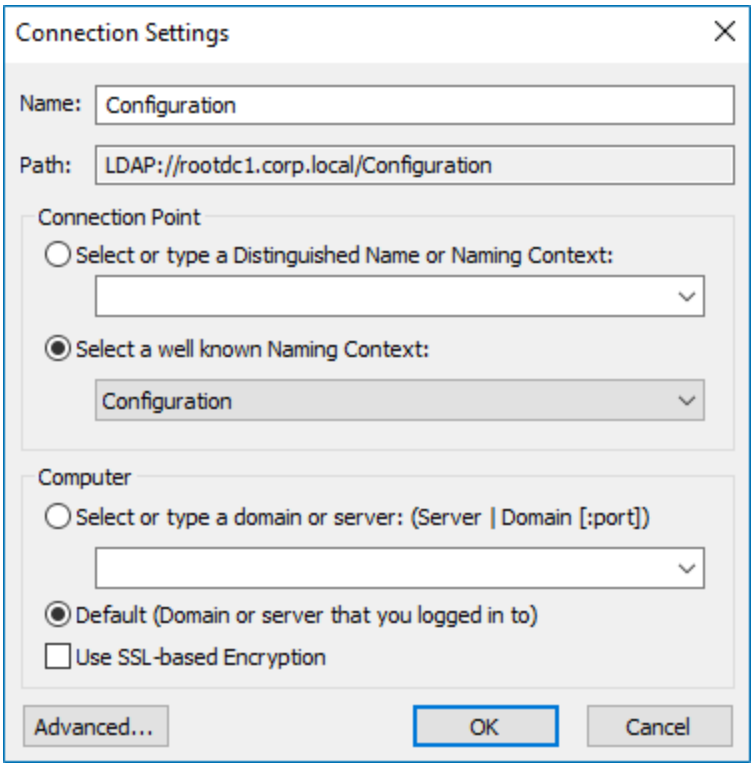
- On Windows Server 2012 and above
  a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.
  b. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.
  c. Set **Type** to *"Success"* 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.



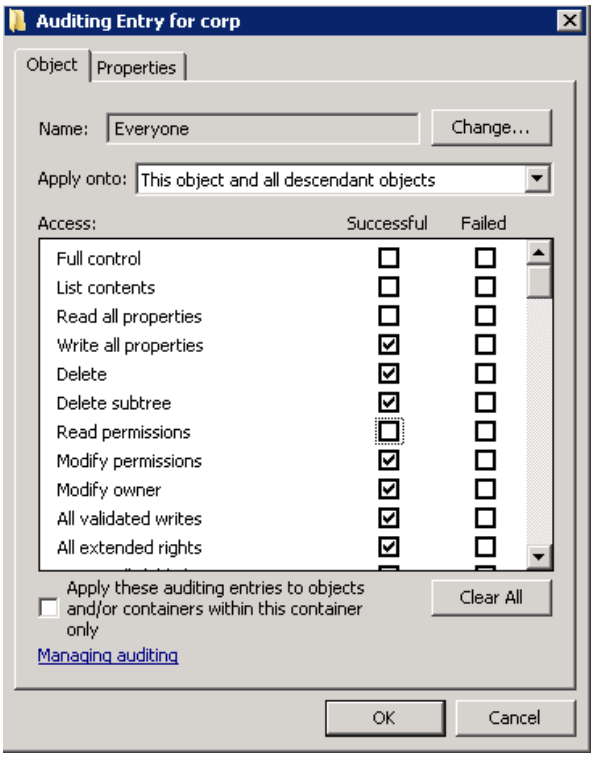
To enable object-level auditing for the Configuration and Schema partitions

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

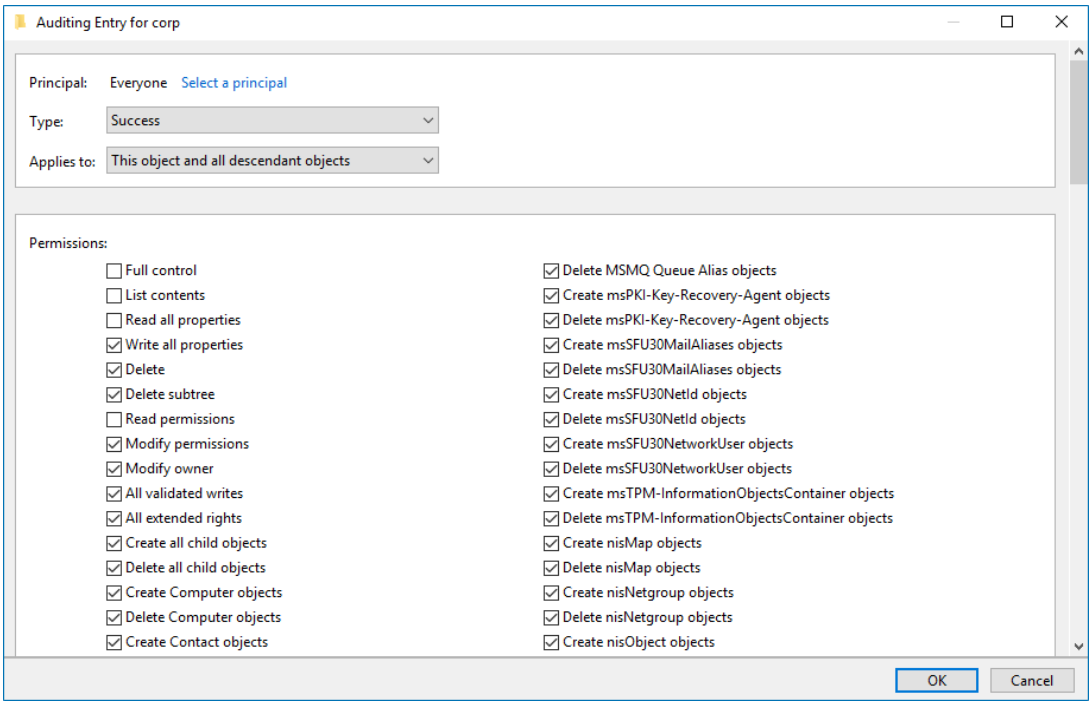
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

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.

7.1.4. Adjusting Security Event Log Size and Retention Settings

Defining the Security event log size is essential for change auditing. If the log size is insufficient, overwrites may occur before data is written to the Long-Term Archive and the Audit Database, and some audit data may be lost.

To prevent overwrites, you can increase the maximum size of the Security event log and set retention method for this log to "*Overwrite events as needed*".

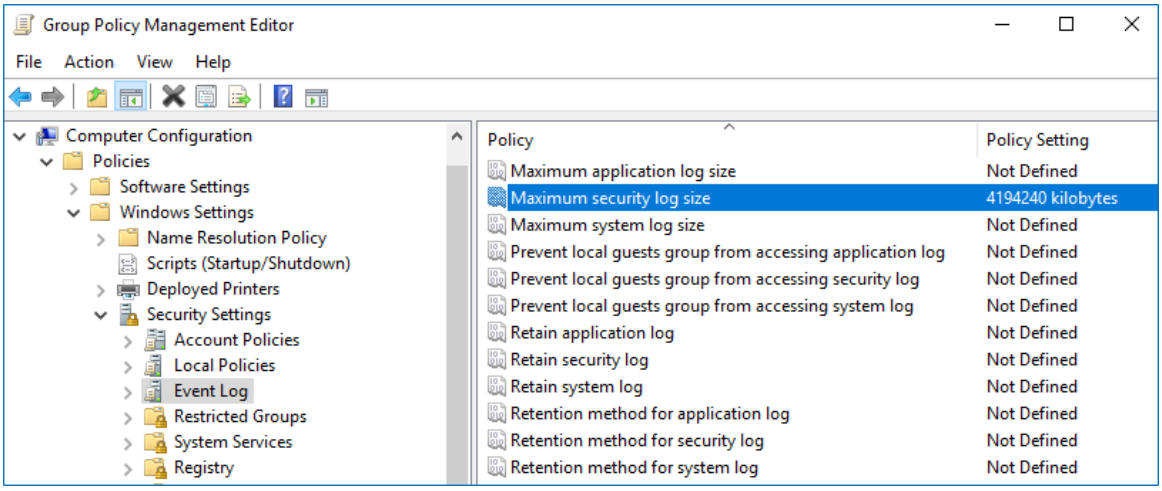
To adjust your Security event log size and retention method, follow the procedure described below.

NOTE: To read about event log settings recommended by Microsoft, refer to this article.

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.

7.1.4.1. Auto-archiving Security Log (optional)

If "Overwrite" option is not enough to meet your data retention requirements, you can use auto-archiving option for Security event log to preserve historical event data in the archive files. This option can be enabled centrally for all domain controllers, using the procedure described below. In such scenario, the logs will be automatically archived when necessary (no events will be overwritten).

To enable Security log auto archiving centrally for 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"*

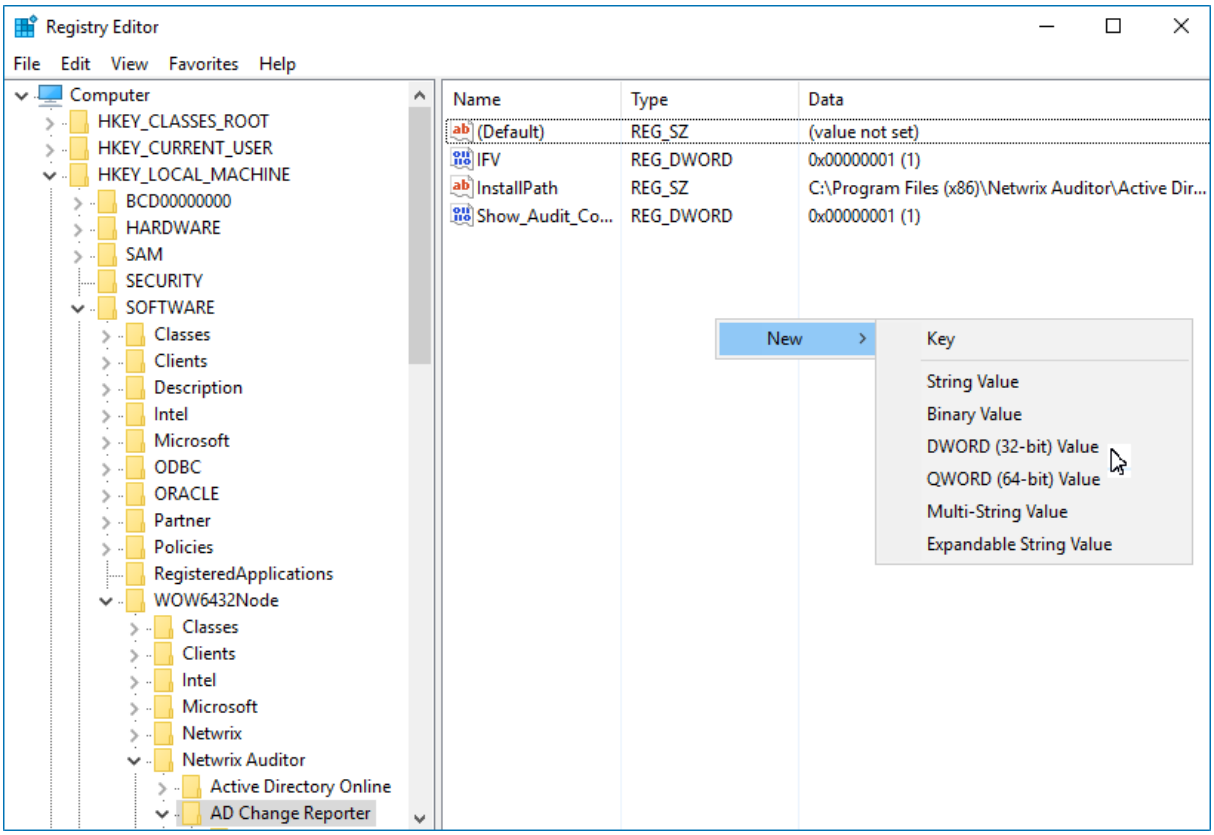
6. Navigate to **Start → Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

With the automatic log backup enabled, you may want to adjust the retention settings for log archives (backups). Default retention period for these files is **50** hours; when it expires, log archives are deleted. To adjust this setting, follow this procedure described below.

To configure the retention period for the backup logs

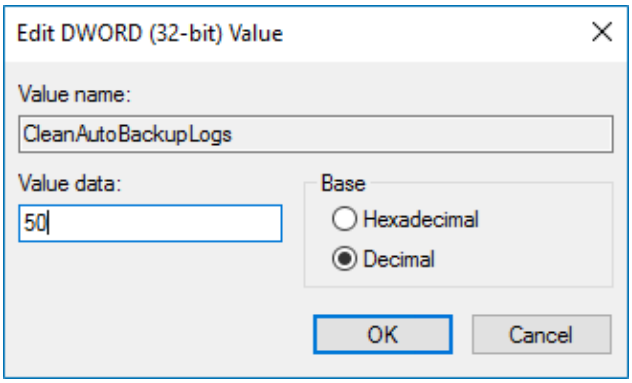
1. On the computer where Netwrix Auditor Server is installed, open **Registry Editor**: navigate to **Start→ Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE → SOFTWARE → Wow6432Node → Netwrix Auditor → AD Change Reporter**.
3. In the right-pane, right-click and select **New → DWORD (32-bit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

7.1.5. 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

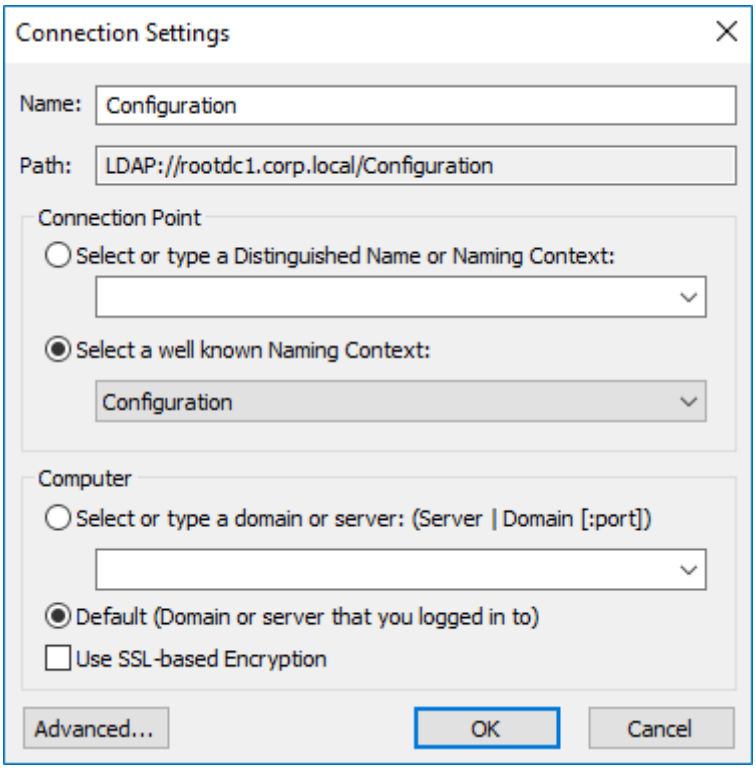
objects in the product snapshots (this data is stored in the Long-Term Archive, a local file-based storage of audit data) and AD tombstones.

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

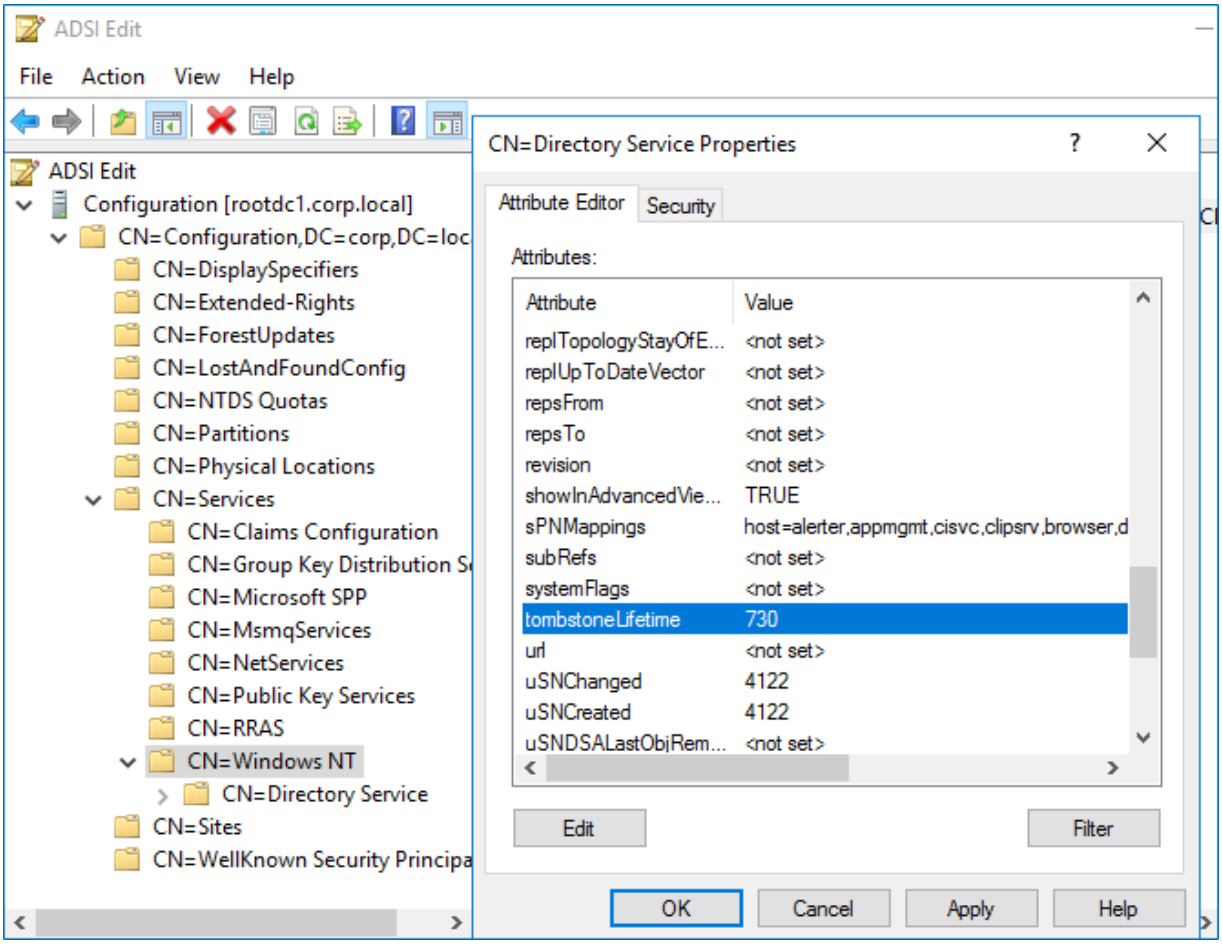
NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2008 and above, this component is installed together with the AD DS role, or it can be downloaded and installed along with Remote Server Administration Tools. Refer to Install ADSI Edit for detailed instructions on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

7.1.6. 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.

7.2. Configure Infrastructure for Monitoring Exchange

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

- Automatically when creating a monitoring plan

  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.

  NOTE: 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.

- Manually. You need to adjust the same audit settings as those required for monitoring Active Directory. See Configure Domain for Monitoring 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 track non-owner access, configure mailbox monitoring. See Configure Exchange for Monitoring Mailbox Access for more information.

For Exchange auditing, also remember to do the following:

1. Configure Data Collecting Account, as described in Configure Data Collecting Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Active Directory, Exchange, and Group Policy

7.2.1. 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 monitored Exchange server 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.

7.2.2. Configure Exchange for Monitoring Mailbox Access

Netwrix Auditor allows tracking non-owner mailbox access in your Exchange organization. Review the following procedures:

- To configure mailbox access tracking for 2010 manually
- To configure mailbox access tracking for Exchange 2013 and 2016 manually

To configure mailbox access tracking for 2010 manually

NOTE: Perform the procedure below only if you do not want to enable network traffic compression option when setting up Exchange monitoring in Netwrix Auditor.

1. On the computer where the monitored Exchange server 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 tracking for Exchange 2013 and 2016 manually

NOTE: Perform the procedures below only if you do not want to enable the automatic audit configuration option when setting up monitoring in Netwrix Auditor.

You can configure auditing for:

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

Track...	Steps...
All mailboxes	1. On the computer where the monitored Exchange server is installed, navigate to **Start → Programs → Exchange Management Shell**. 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,`

Track...	Steps...
	`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 monitored Exchange server 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"` • `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.

7.3. Configure Infrastructure for Monitoring Exchange Online

You can configure your Exchange Online for monitoring 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 settings will be checked on each data collection and adjusted if necessary.

- Manually. Special manual configuration steps only required if you are going to track 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.

Track...	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"` • `Domain\User. Example: enterprise.local\MJones` • `Email address. Example: analyst@enterprise.onmicrosoft.com` • `GUID. Example: {c43a7694-ba06-46d2-ac9b-205f25dfb32d}` • `LegacyExchangeDN. Example: /o=EnterpriseDev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=97da560450c942aba 81b2da46c60858a-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`

Track...	Steps...

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

7.4. Configure Windows File Servers for Monitoring

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 monitor an entire file server, consider the following:

- If you specify a single computer name, Netwrix Auditor will monitor 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 monitoring 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 monitoring 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.

For Windows File Server, also remember to do the following:

1. Configure Data Collecting Account, as described in Configure Data Collecting Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring File Servers

7.4.1. 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.

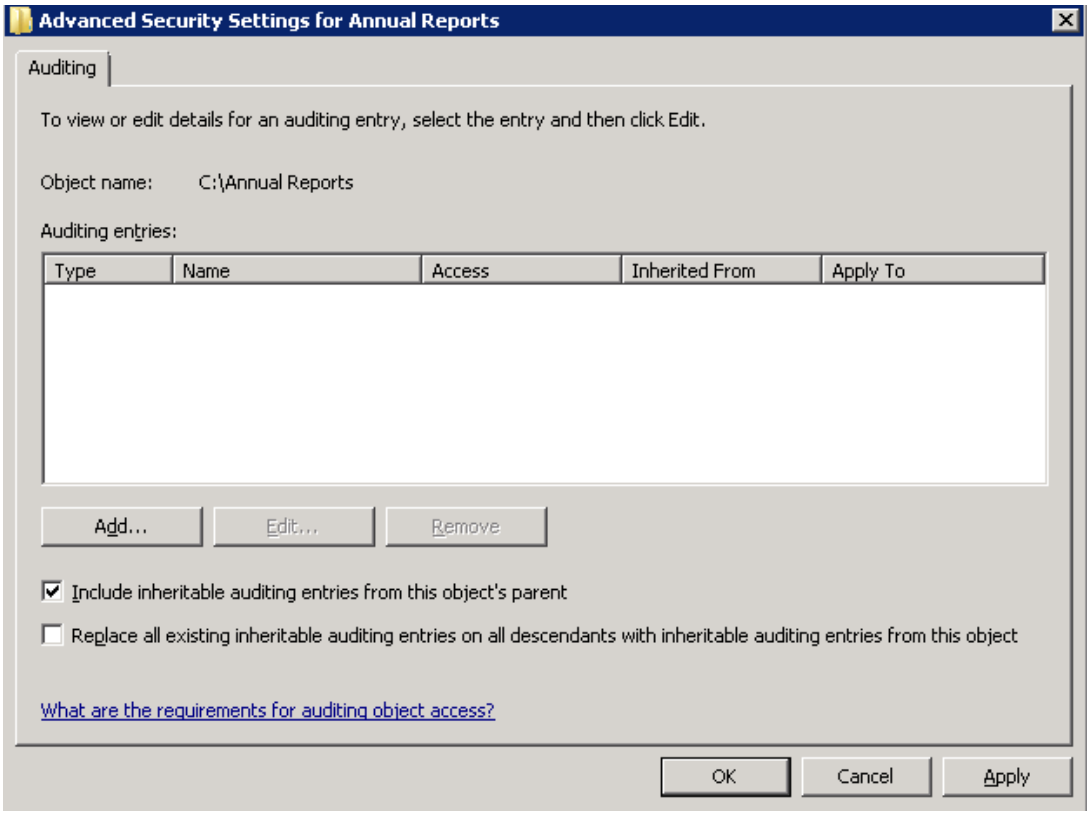
Perform one of the following procedures depending on the OS:

- 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.

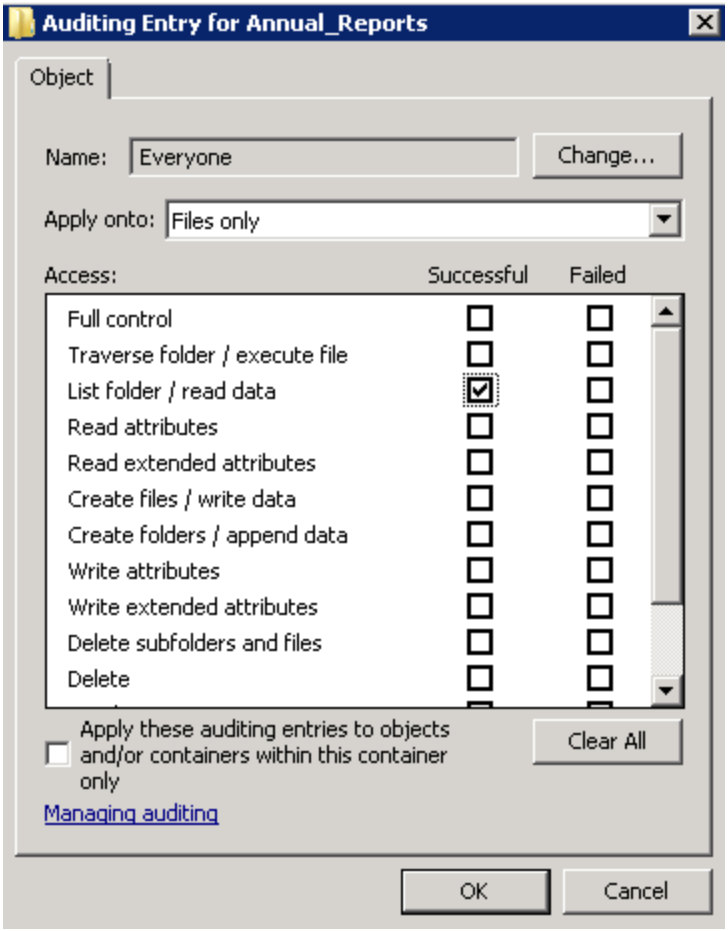
5. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads and changes as well as failed read and change attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain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

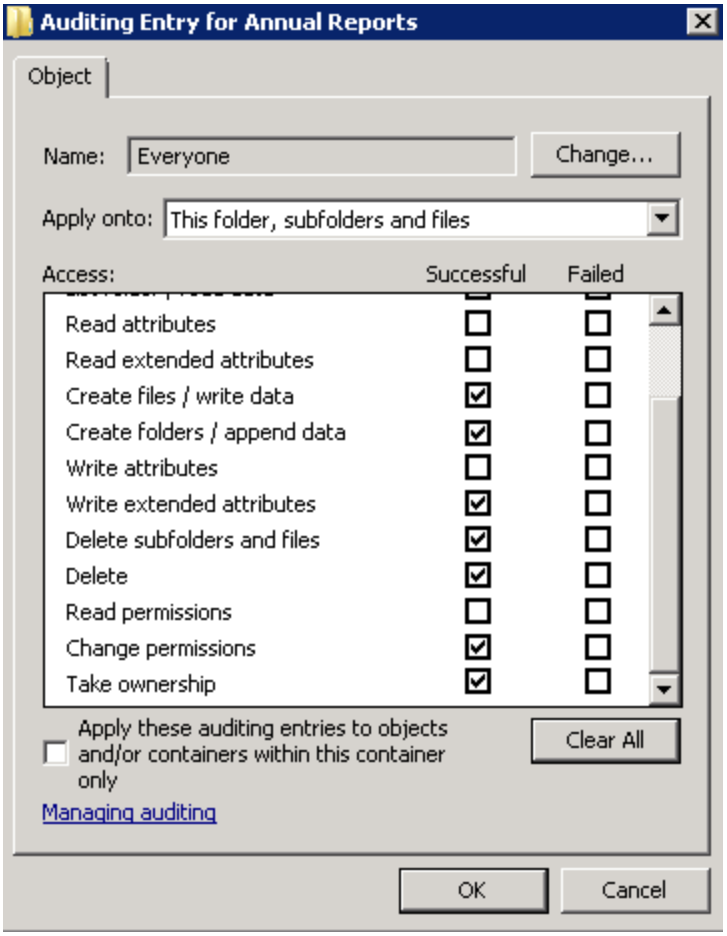


- Apply onto—Select *"Files only"*.
- Check *"Successful"* and *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful changes

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

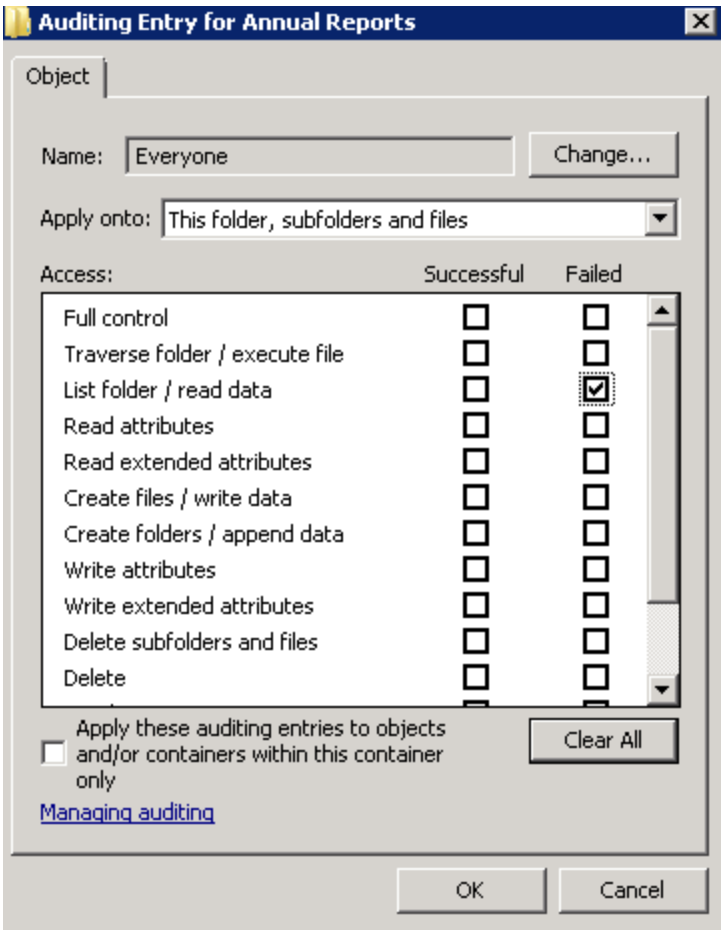
Auditing Entry



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

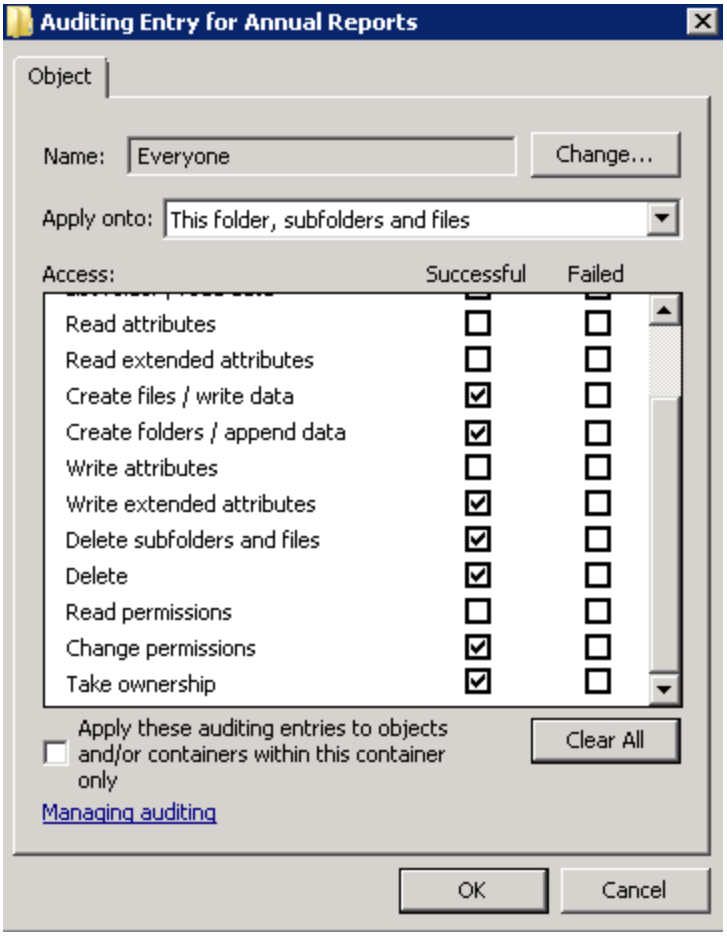


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed change attempts

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

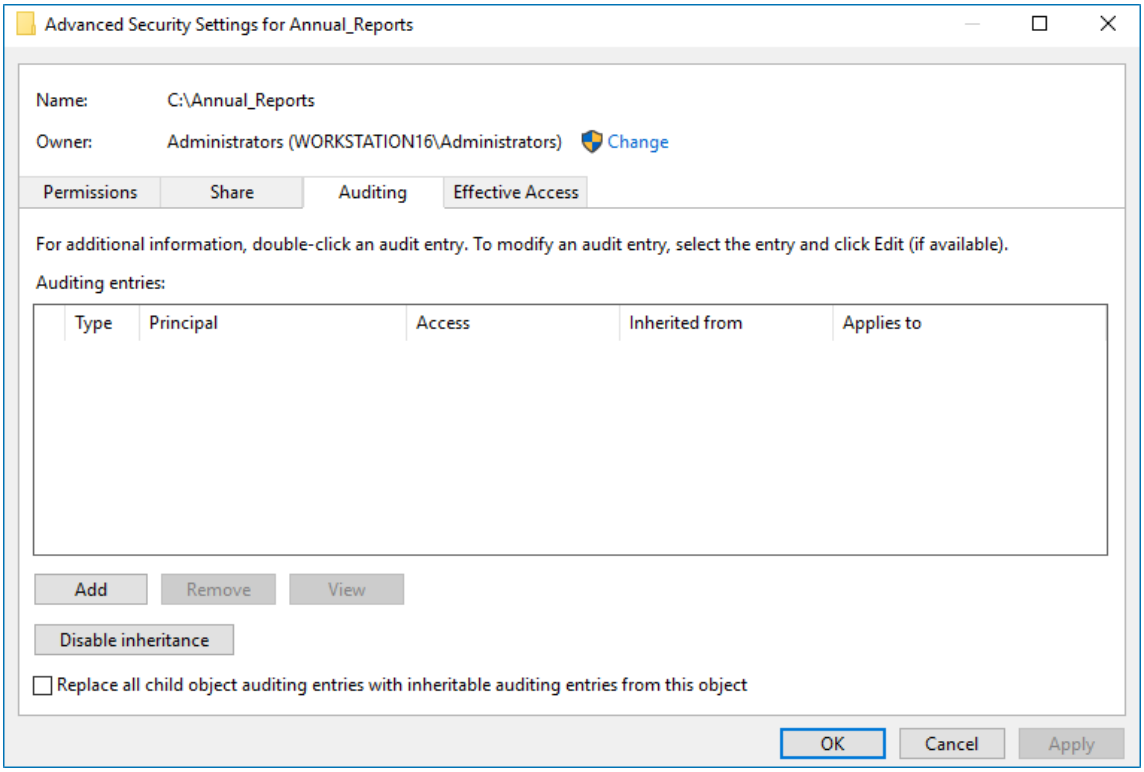
Auditing Entry



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

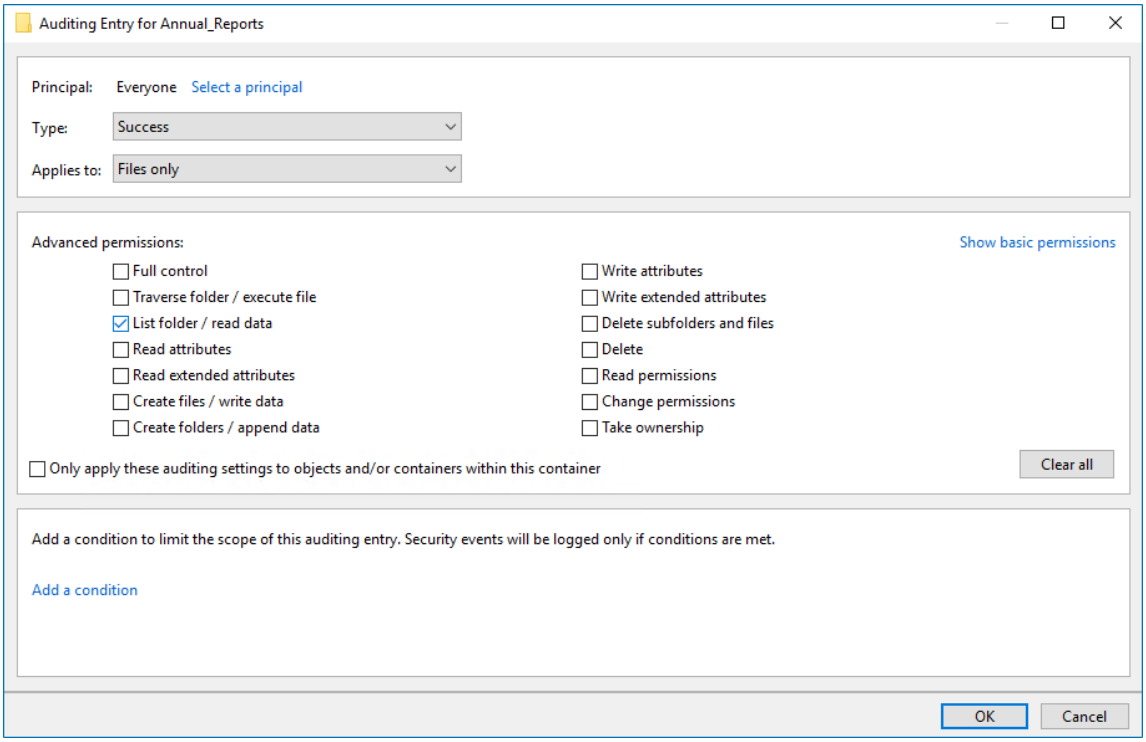
6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will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

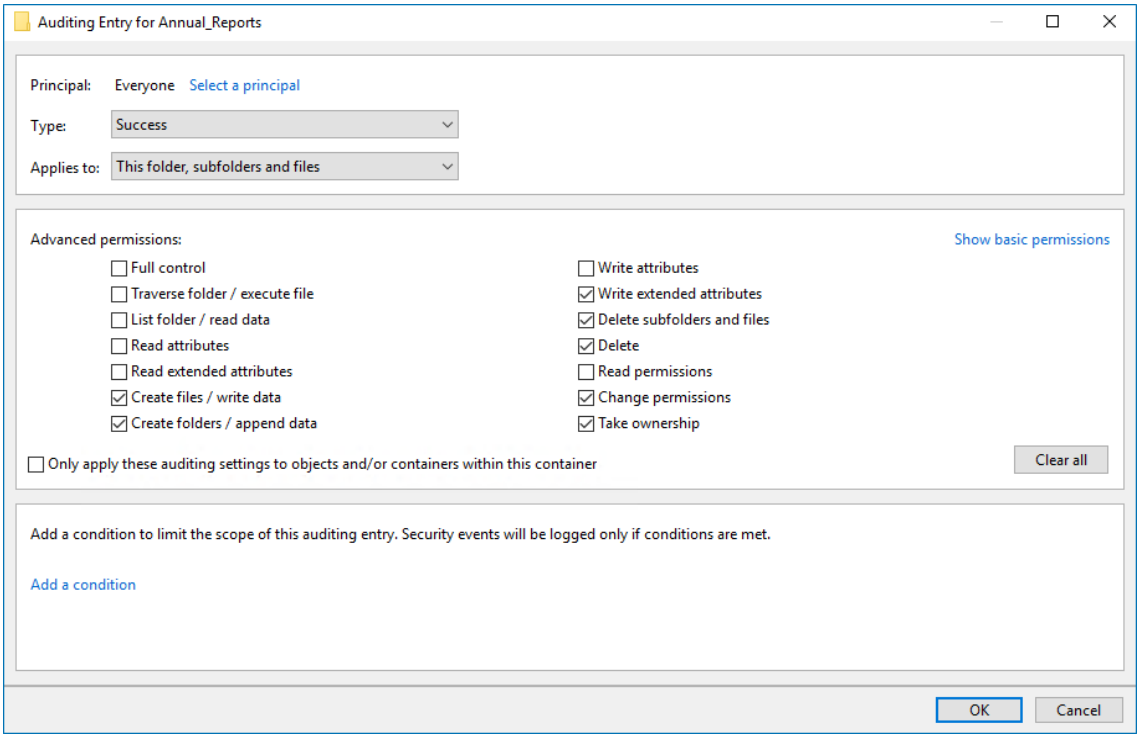


- Type—Set to *"Success"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful changes

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

Auditing Entry

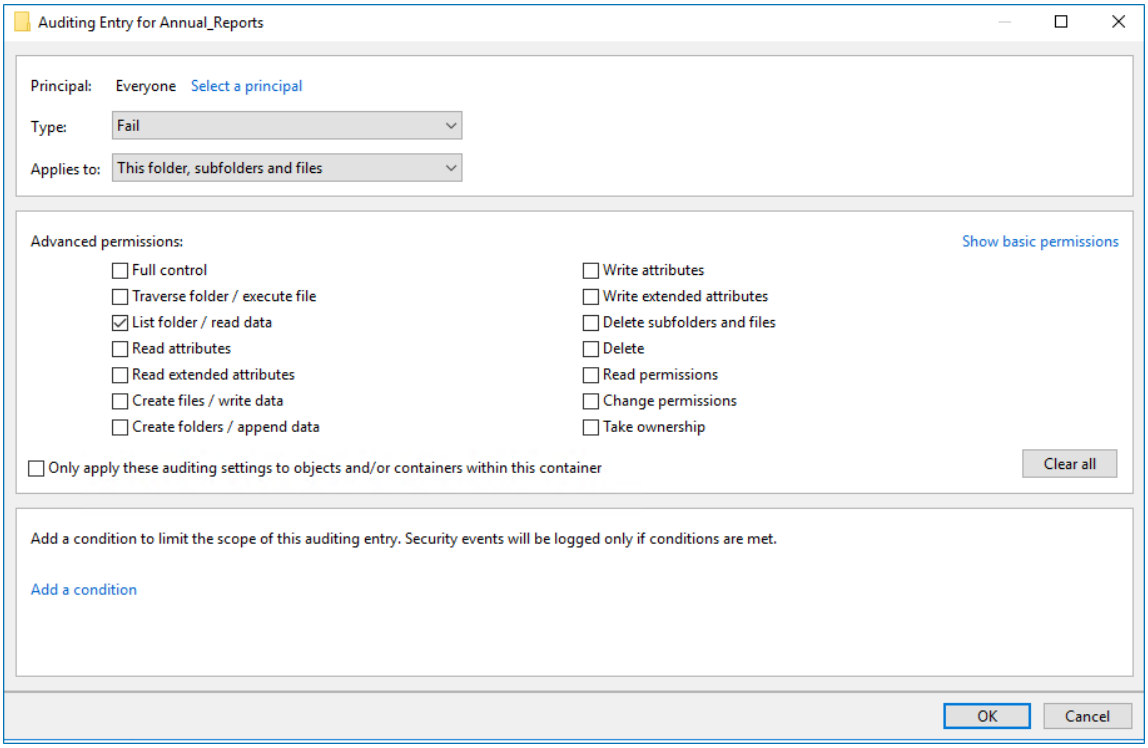


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that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

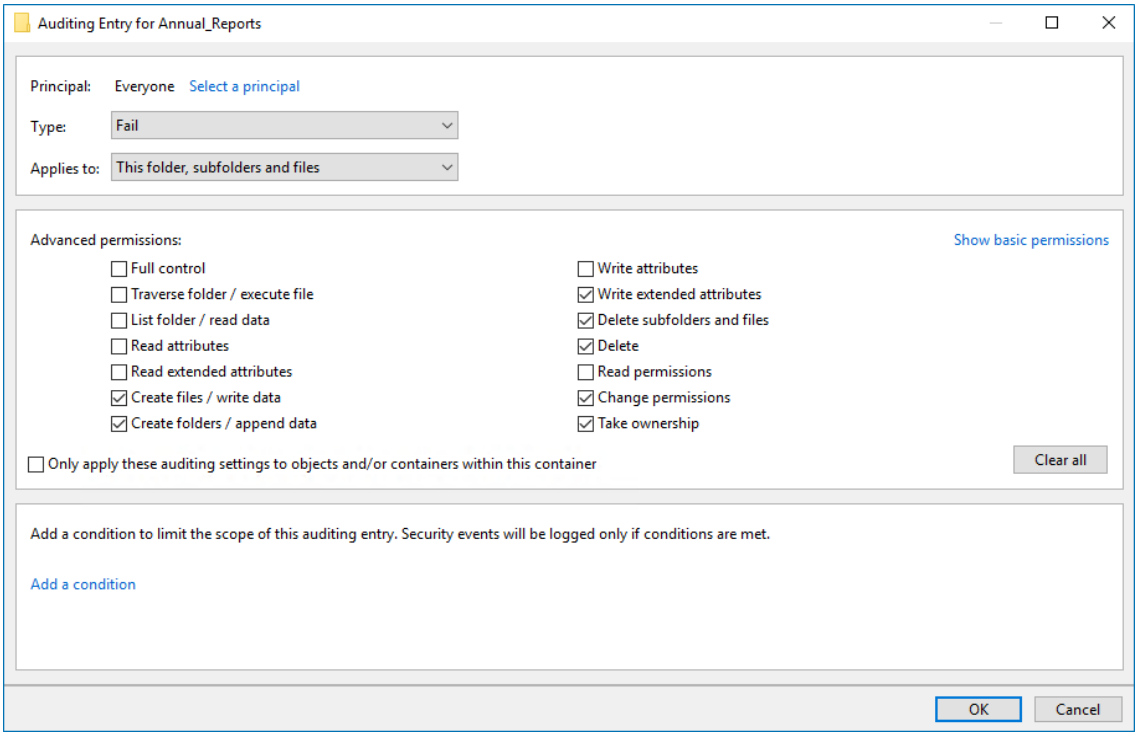


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed change attempts

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

Auditing Entry



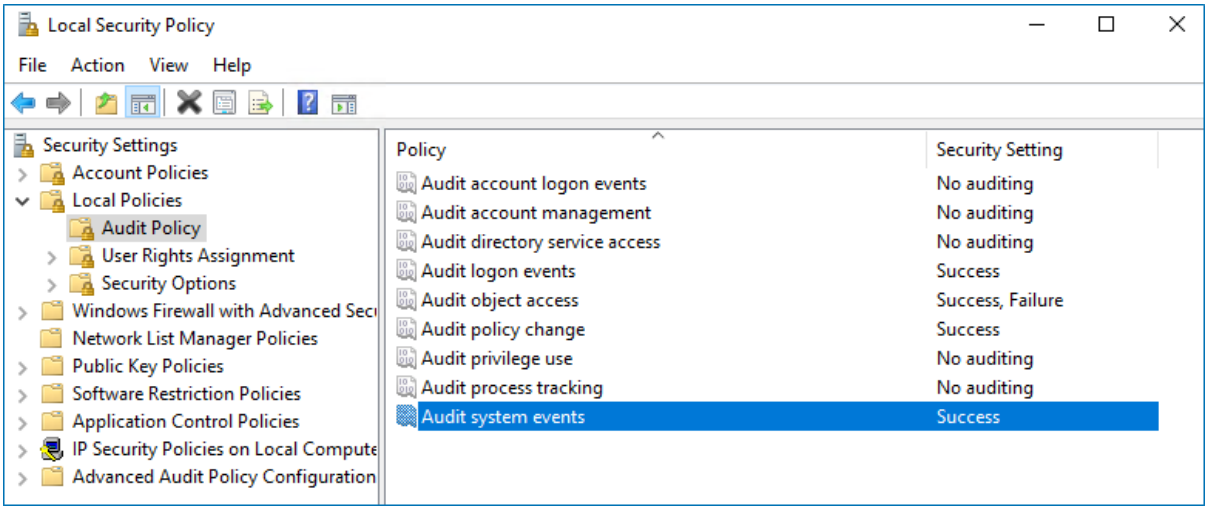
- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that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

7.4.2. 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"*



7.4.3. 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
- To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

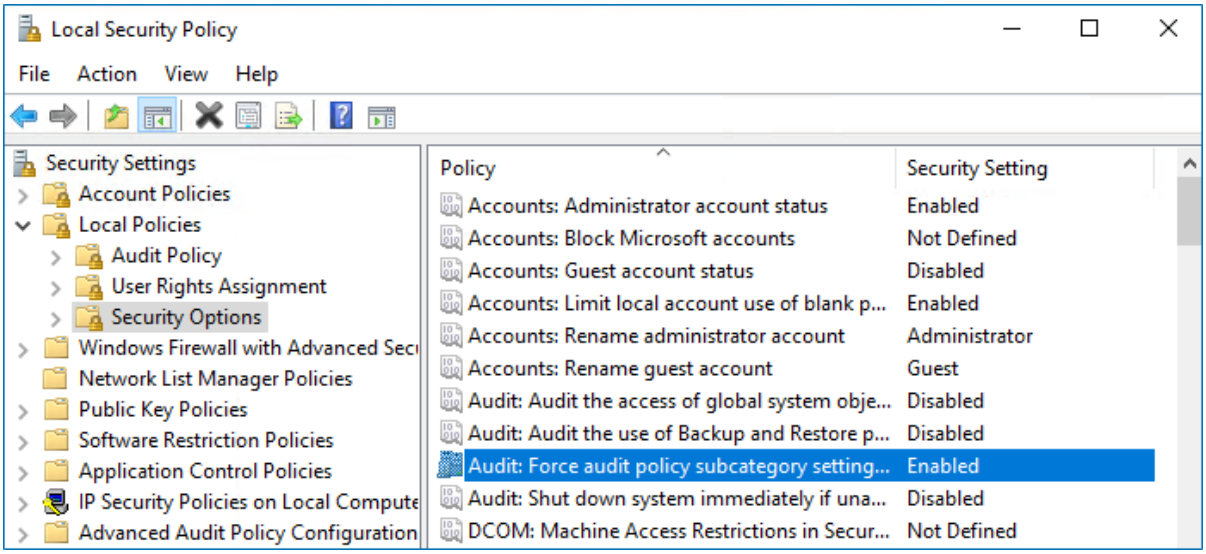
To configure security options

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 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** policy.



3. Double-click the policy and enable it.

To configure advanced audit policy on Windows Server 2008

In Windows Server 2008 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 Create System Startup / Shutdown and User Logon / Logoff Scripts Microsoft article 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"`.

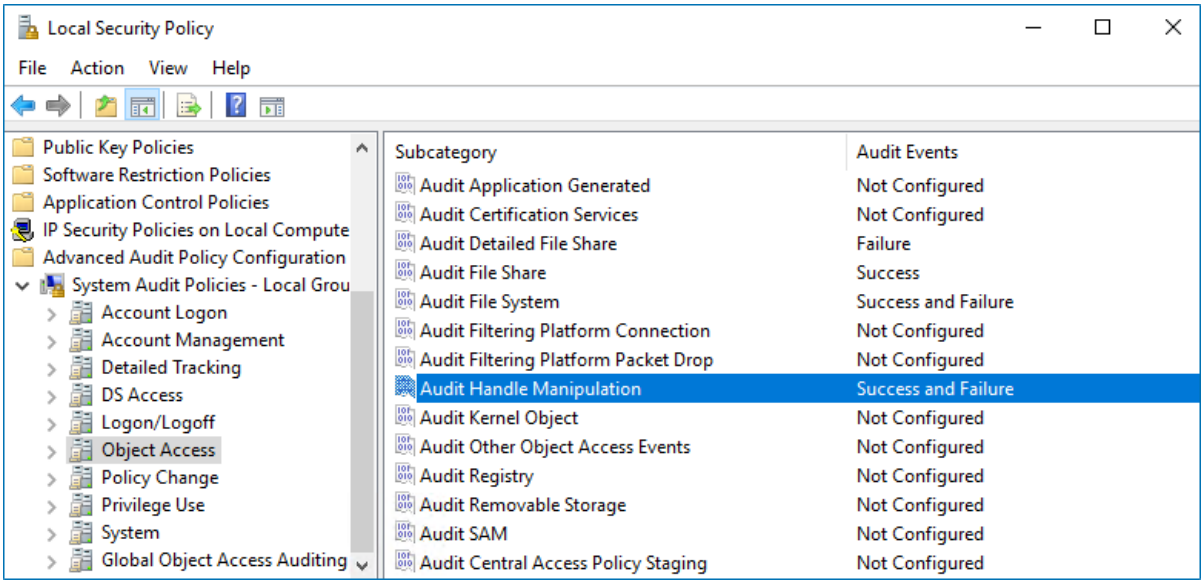
To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

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"*
	• Audit Removable Storage	*"Success"* and/or *"Failure"* depending on the type of events you want to track.
Policy Change	• Audit Audit Policy Change	*"Success"*
Logon/Logoff	• Logon	*"Success"*
	• Logoff	*"Success"*
System	• Security State Change	*"Success"*

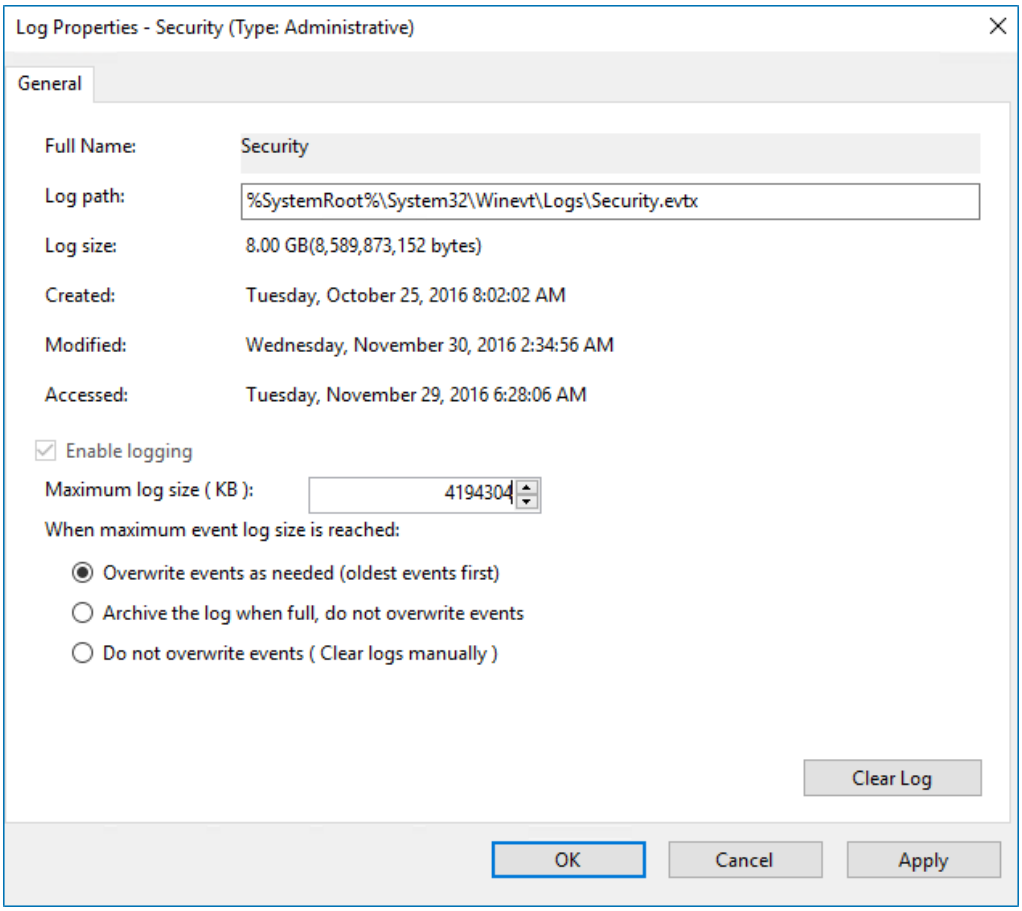


7.4.4. Configure Event Log Size and Retention Settings

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**.

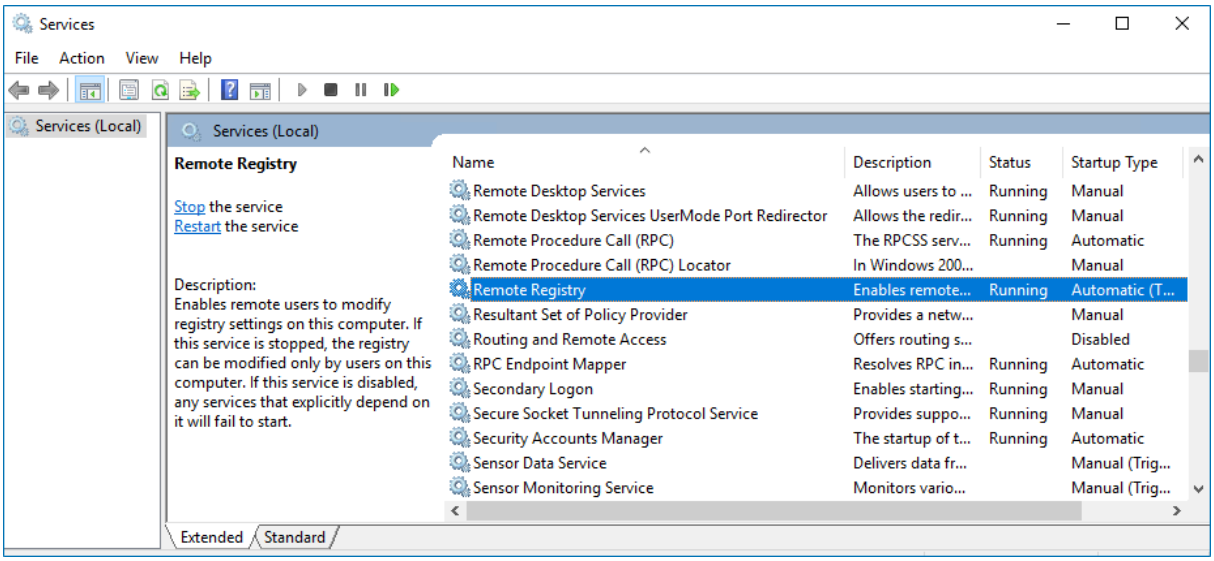


3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field, specify the size—4GB.
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

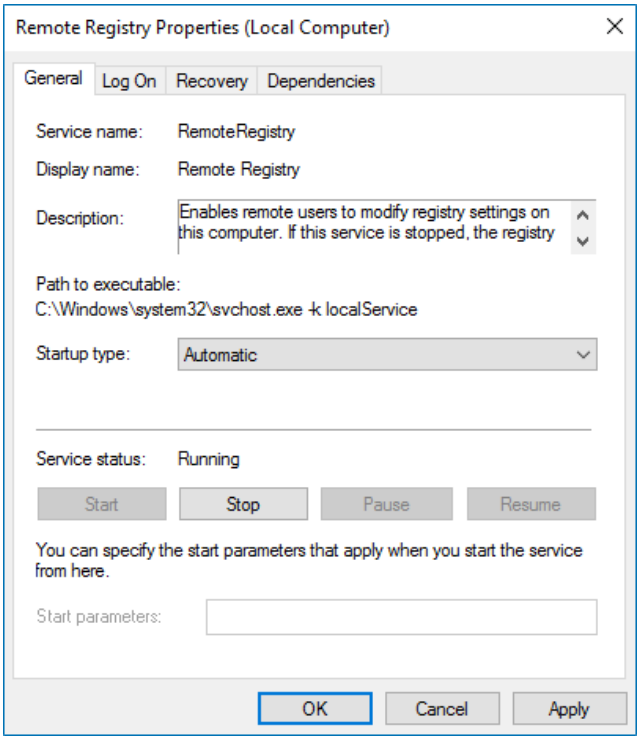
NOTE: Make sure the **Maximum security log size** group policy does not overwrite your log settings. To check this, start the **Group Policy Management** console, proceed to the GPO that affects your server, and navigate to **Computer Configuration → Policies → Windows Settings → Security Settings →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

7.4.5. Enable 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**.

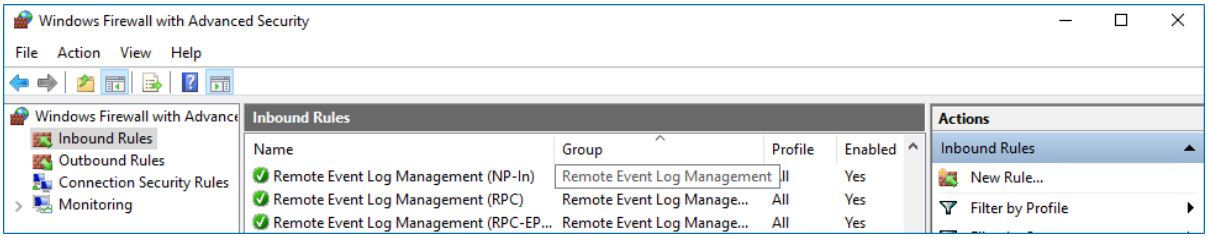


4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.

7.4.6. 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)**

7.4.7. 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 7 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.

7.5. Configure EMC VNX/VNXe for Monitoring

You can configure your file shares for monitoring 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.

To configure EMC Unity storage system audit, take the steps described in this Netwrix Knowledge Base article.

7.5.1. 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.

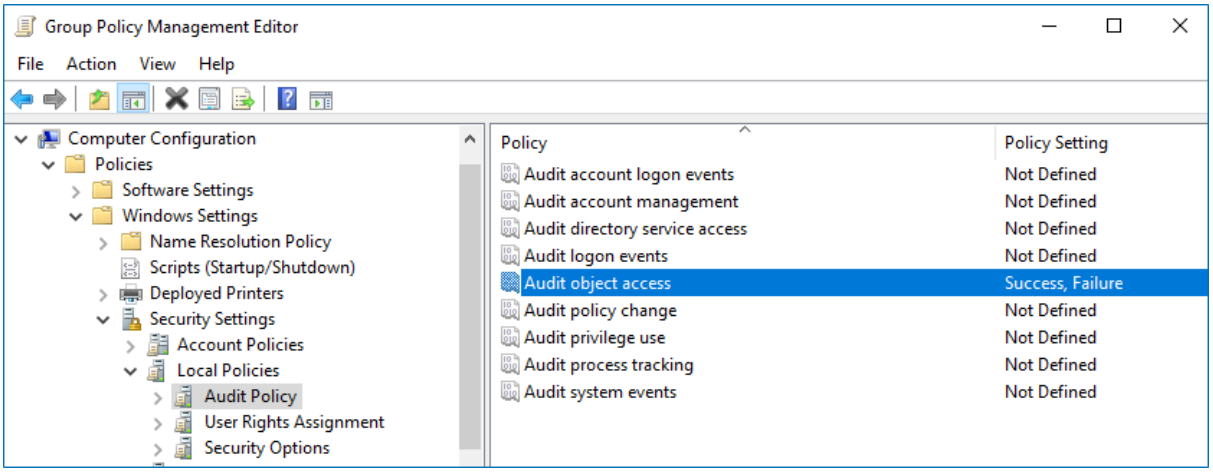
6. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security** and set the **File** value to *"C:\events\security.evt"*.
7. Set the **MaxSize** value to *"4 000 000 000 (decimal)"*.
8. Restart the corresponding Data Mover for the changes to take effect.

7.5.2. 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.

7.5.3. 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.

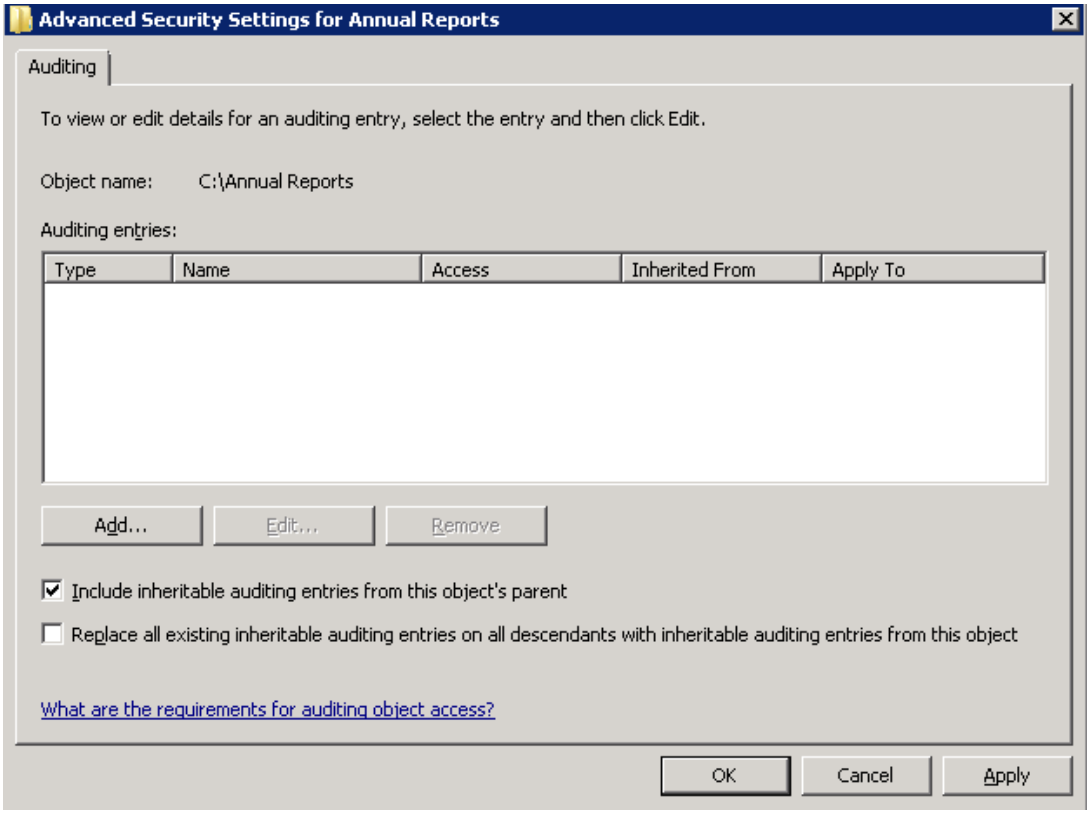
To configure audit settings for the CIFS file shares, perform the following procedure on the audited file share:

- 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:

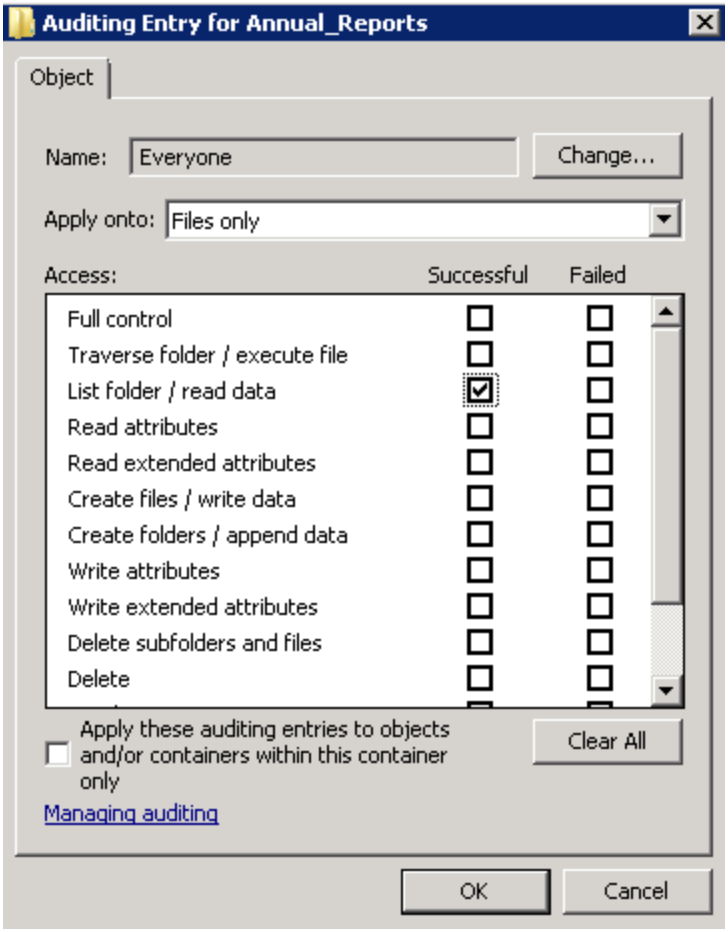
   - Successful reads
   - Successful changes

- Failed read attempts
- Failed change attempts

Auditing Entry

Successful reads

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

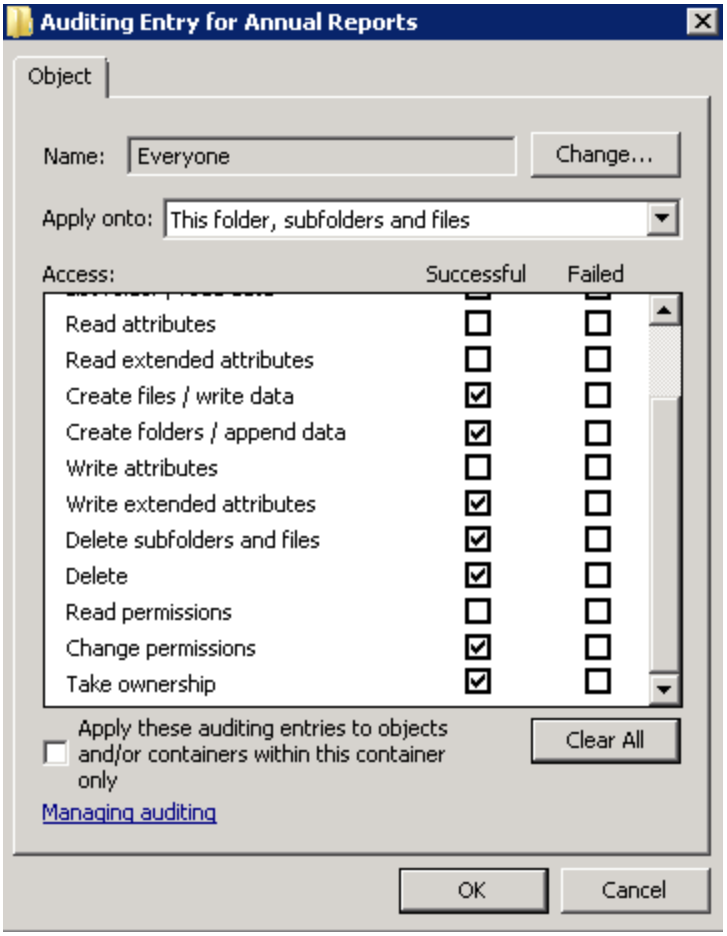


- Apply onto—Select *"Files only"*.
- Check *"Successful"* and *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful changes

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

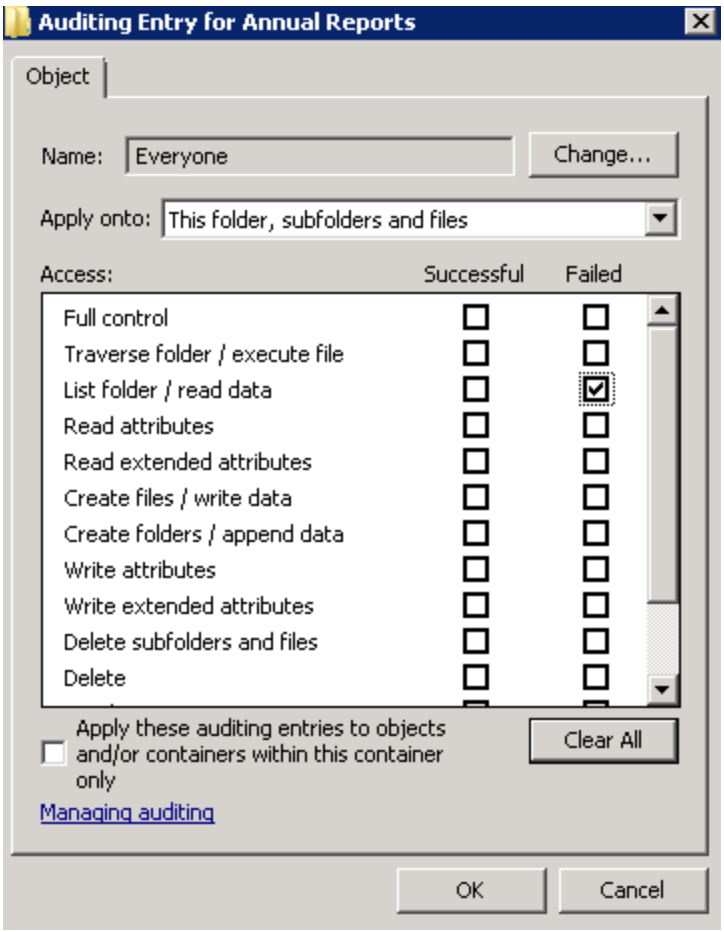
Auditing Entry



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

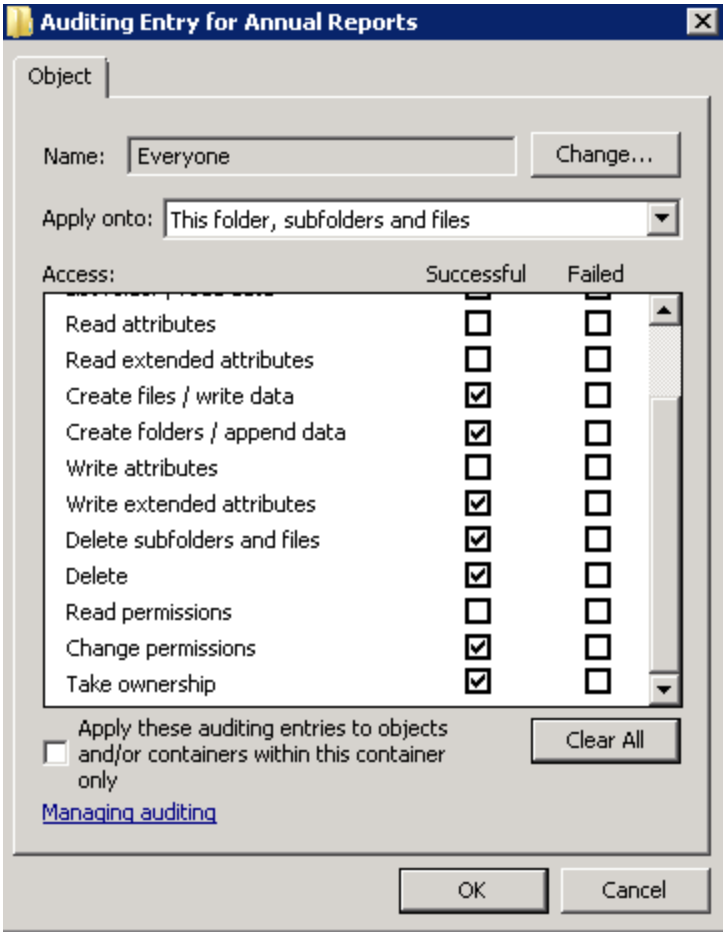


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed change attempts

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

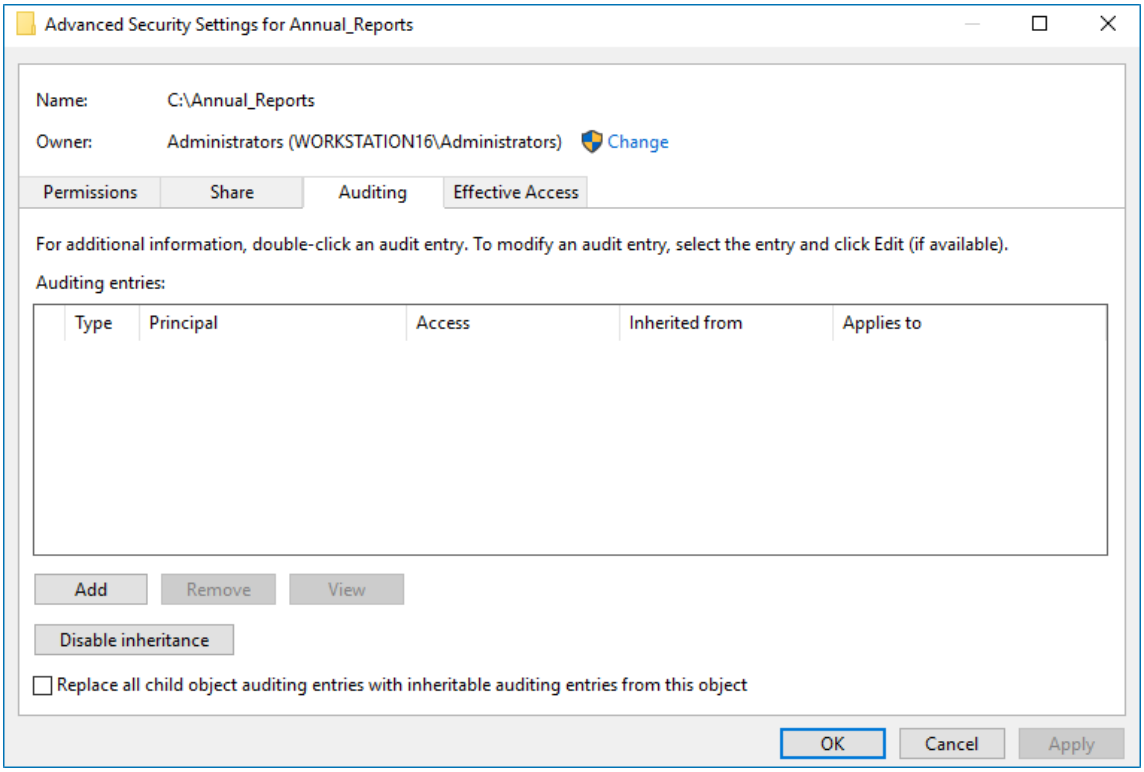
Auditing Entry



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

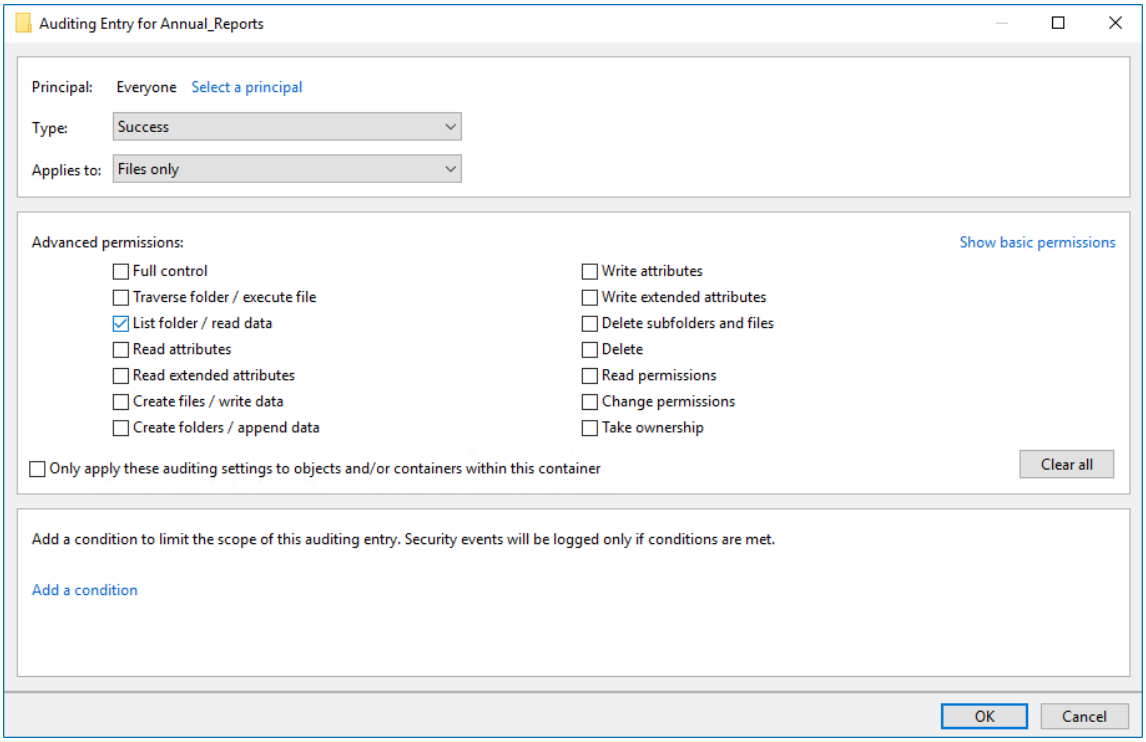
6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will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

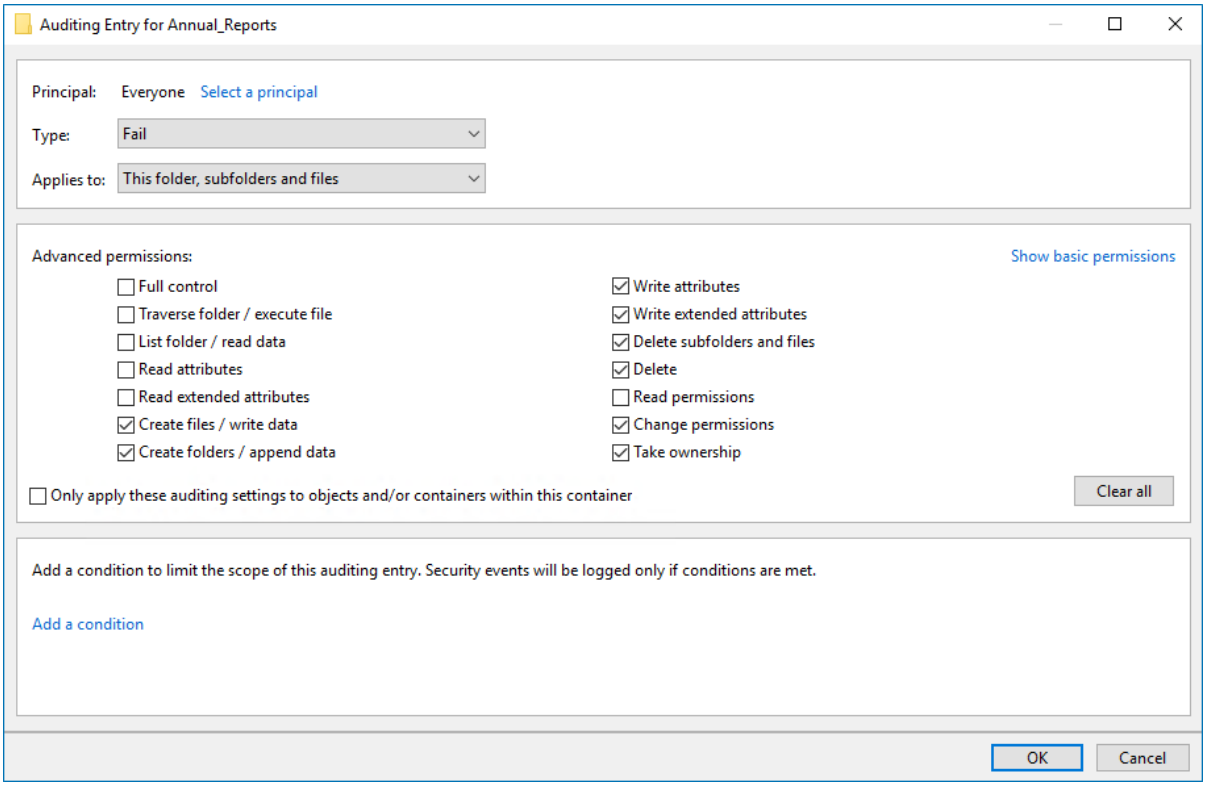


- Type—Set to *"Success"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful changes

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

Auditing Entry

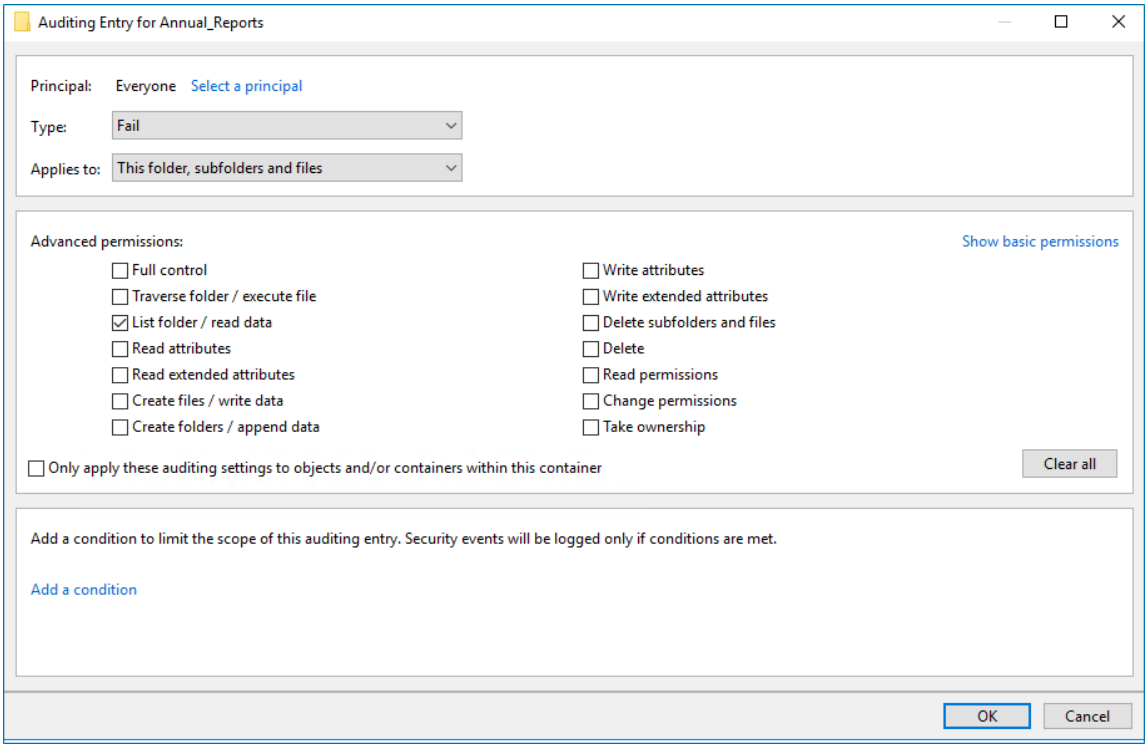


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write attributes
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership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

Failed read attempts

Auditing Entry

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

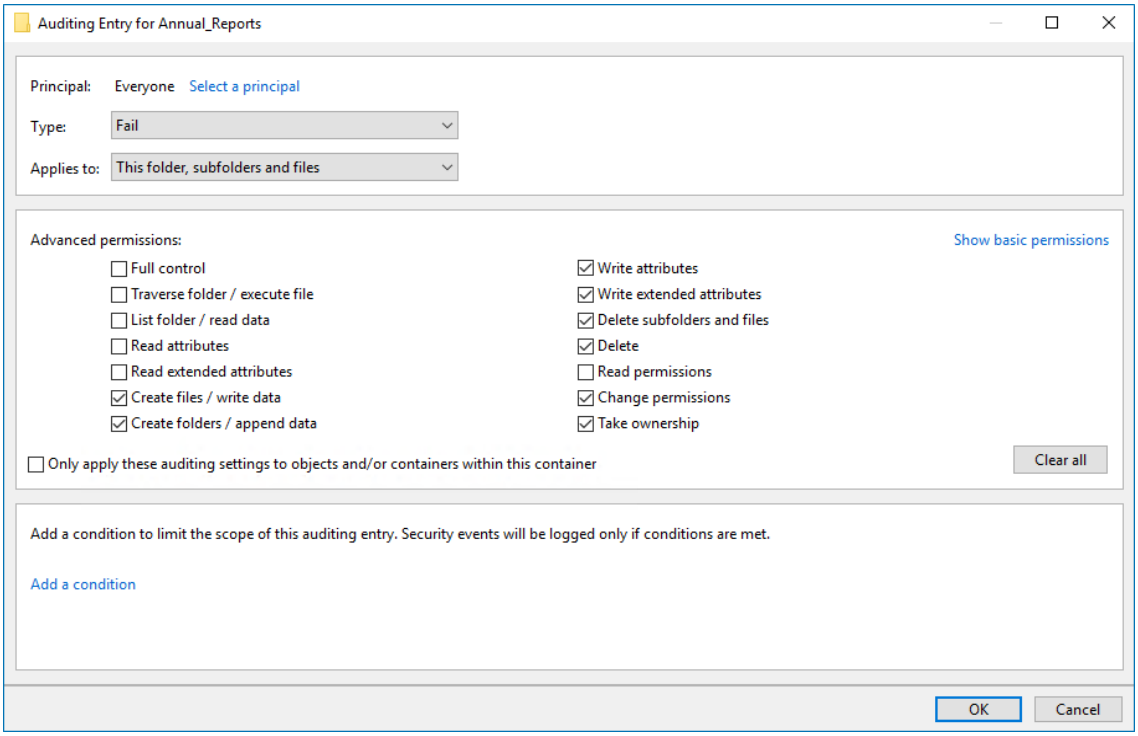


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

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.

7.6. Configure EMC Isilon for Monitoring

To configure your EMC Isilon appliance for monitoring 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.

7.6.1. Configure EMC Isilon in Normal and Enterprise Modes

You can configure your cluster for monitoring 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	
`isi zone zones modify zone1 --audit- failure=create,write,delete,set_`	`isi audit settings modify --zone= zone1 --audit-failure= create,write,delete,set_`

EMC Isilon 7.x	EMC Isilon 8.x
`security,rename`	`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"
```

7.6.2. Configure EMC Isilon in Compliance Mode

You can configure your cluster for monitoring 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"
```

7.7. Configure NetApp Filer for Monitoring

You can configure your file shares for monitoring 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 monitoring, perform the following procedures:
  - Configure NetApp Data ONTAP 7 and 8 in 7-mode for Monitoring or Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring
  - 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.

7.7.1. Configure NetApp Data ONTAP 7 and 8 in 7-mode for Monitoring

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

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

7.7.1.1. 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>
  ```

7.7.1.2. 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>
```

7.7.1.3. 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>
```

7.7.1.4. 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

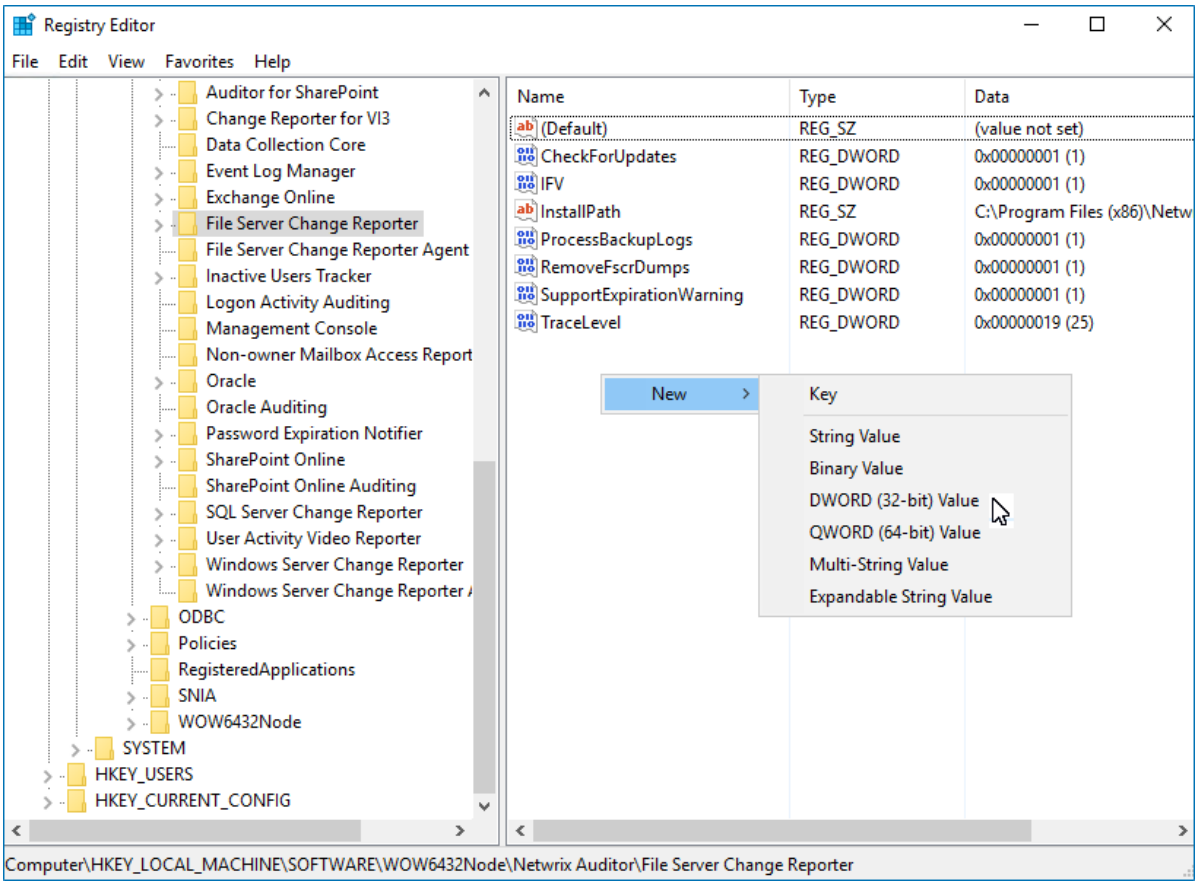
1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. In order to avoid overwriting of the security logs, set the following values:
   - `cifs.audit.logsize 300 000 000 (300 MB)`
   - `cifs.audit.autosave.onsize.enable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

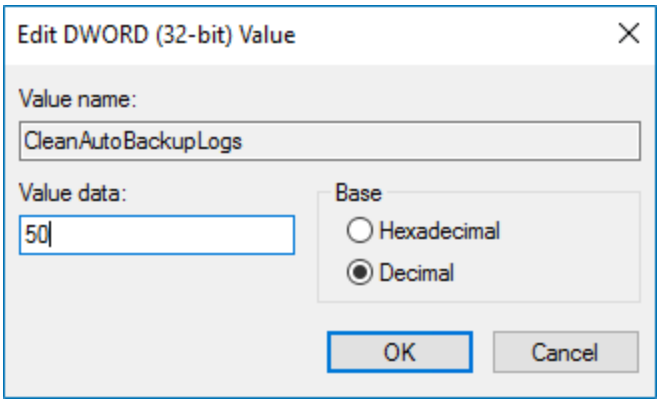
To configure logs retention period

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.

7.7.2. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring

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

- Prerequisites
- Configure ONTAPI Web Access

- Configure Firewall Policy
- Configure Event Categories and Log

7.7.2.1. 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 - 9.6	• 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.

7.7.2.2. 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.
```

7.7.2.3. 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 - 9.5
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 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
   ```

7.7.2.4. 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>` 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

To...	Execute...
	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
```

For ONTAPI 9.0 or later 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, file-share, audit-policy-
                                    change, 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

Option	Setting
	NOTE: Only required if you use Clustered Data ONTAP 8.3, ONTAP 9.0, ONTAP 9.1 or later. You cannot select event categories if you use Clustered Data ONTAP 8.2. For ONTAP 9.0 and later, also check the following options: `file-ops, file-share, audit-policychange`. For ONTAP 8.3, just check `file-ops`.
`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. 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
```

NOTE: For ONTAP 9.0 and later, also check the following settings: `file-ops, file-share, audit-policychange`.

For ONTAP 8.3, just check `file-ops`.

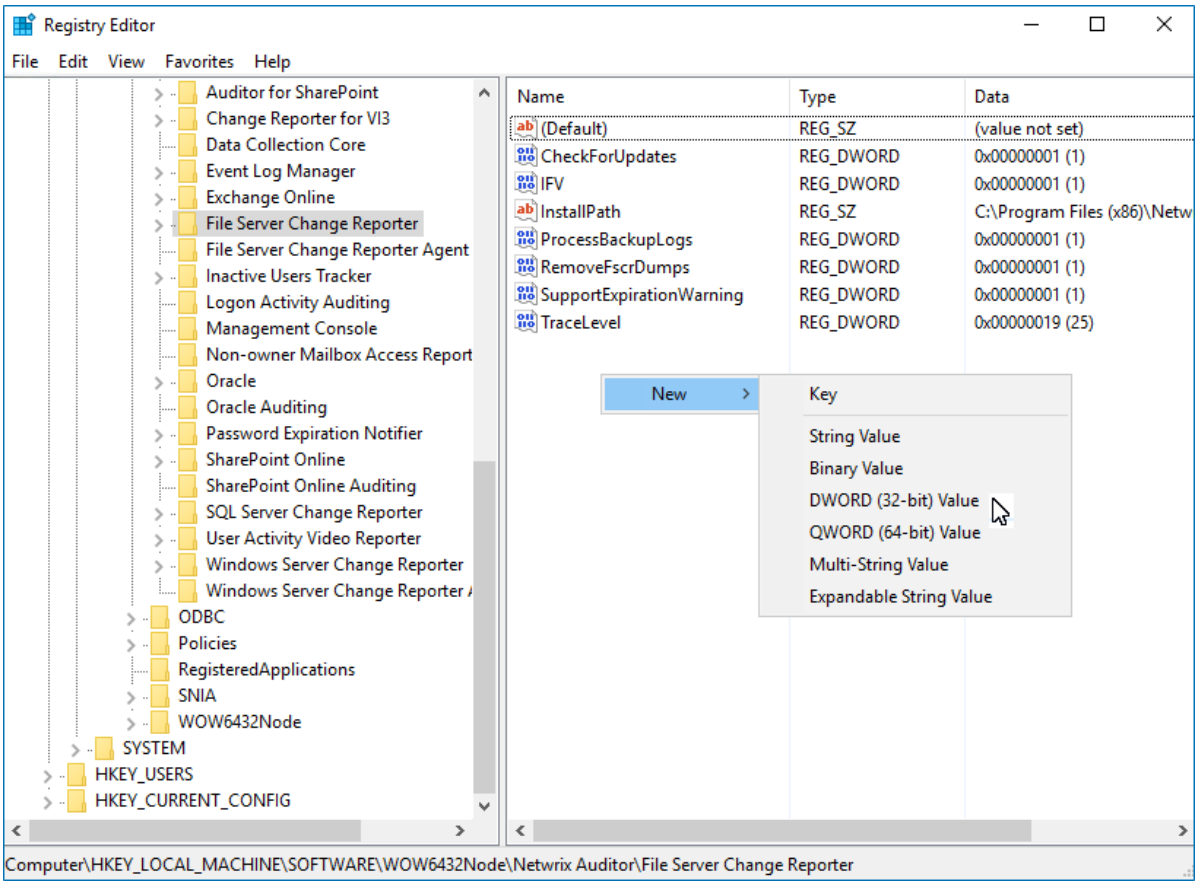
To configure logs retention period

1. On the computer where Netwrix Auditor Server resides, open **Registry Editor**: navigate to **Start** →

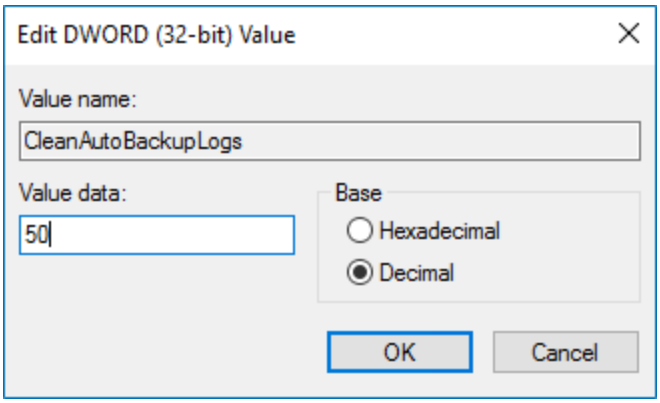
Run and type *"regedit"*.

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.

7.7.3. 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.

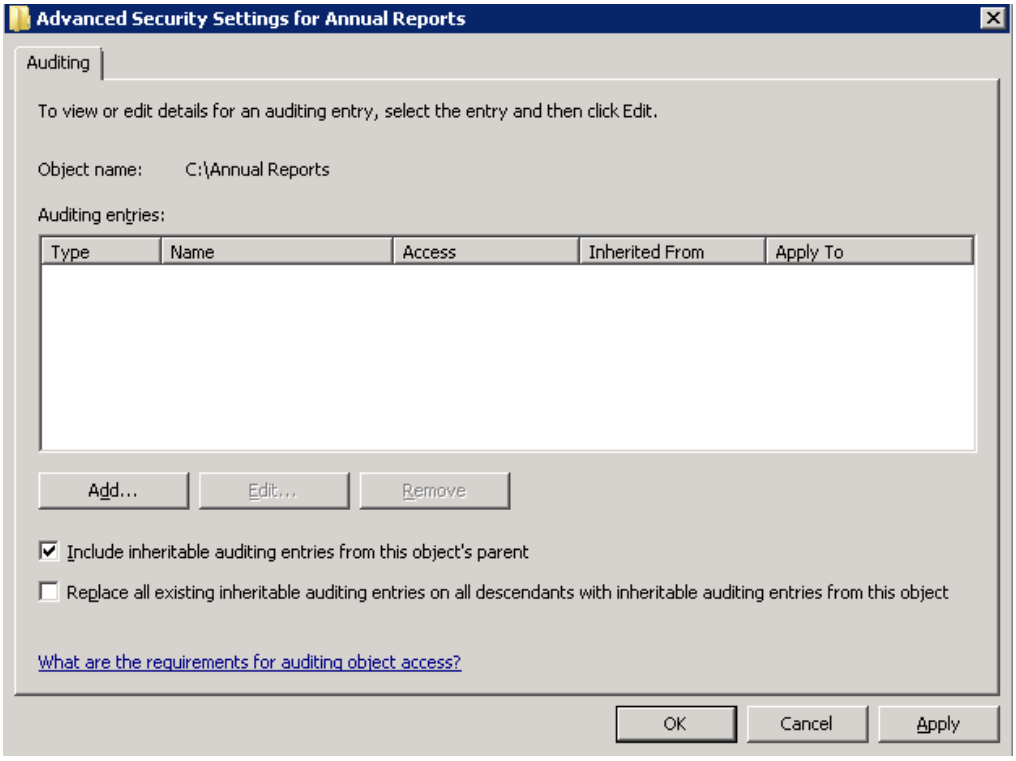
Do one of the following depending on the OS:

- 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**.

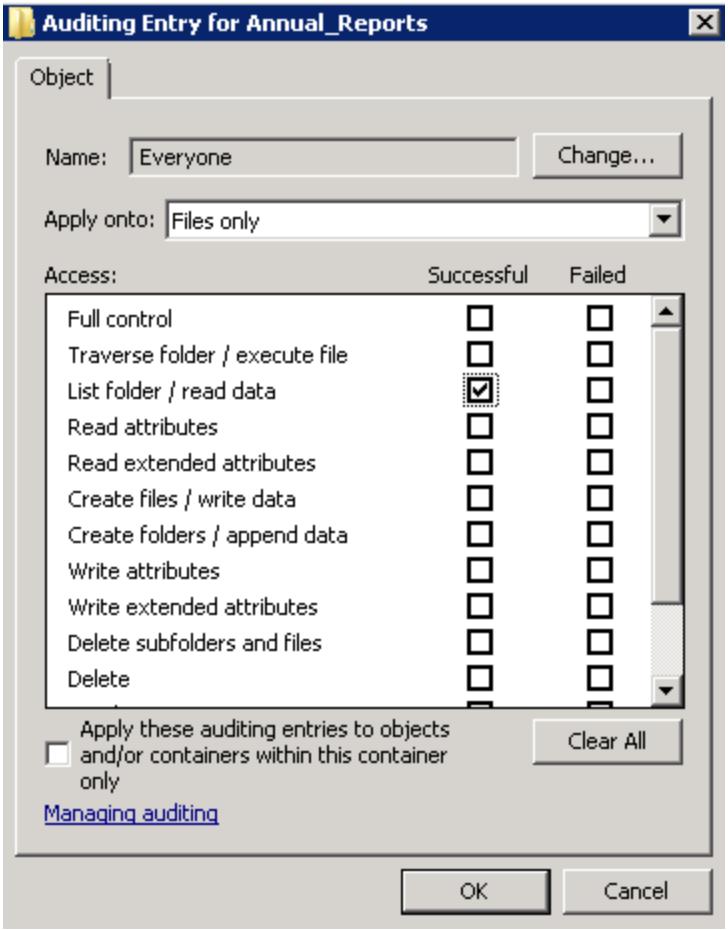
NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the Reports functionality and the product will only audit user accounts that belong to the selected group.

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:

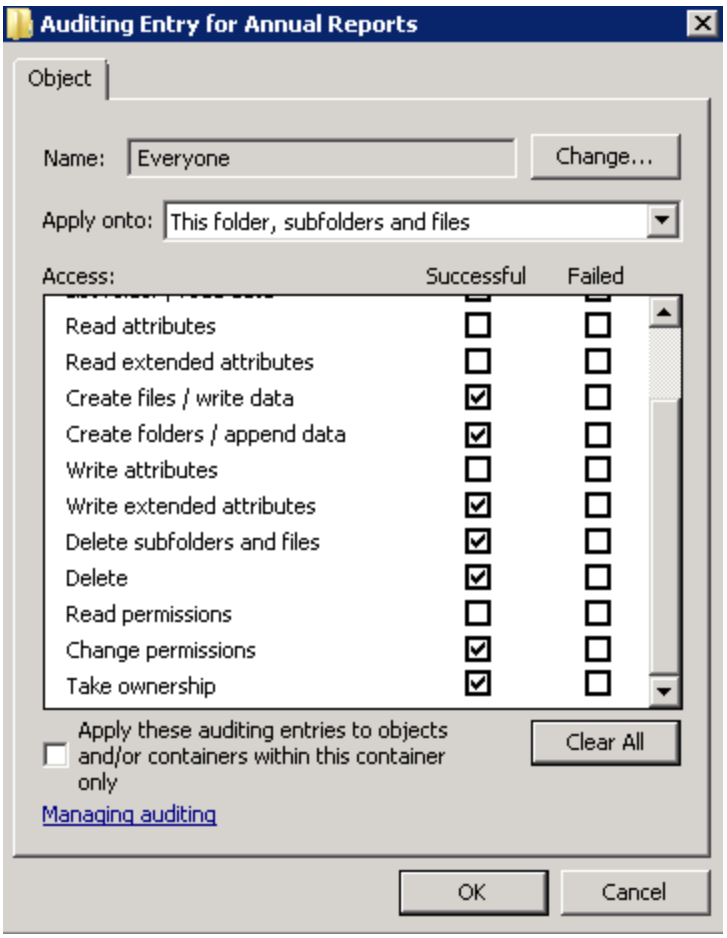


Auditing Entry

- 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 extended attributes
  - Delete subfolders and files

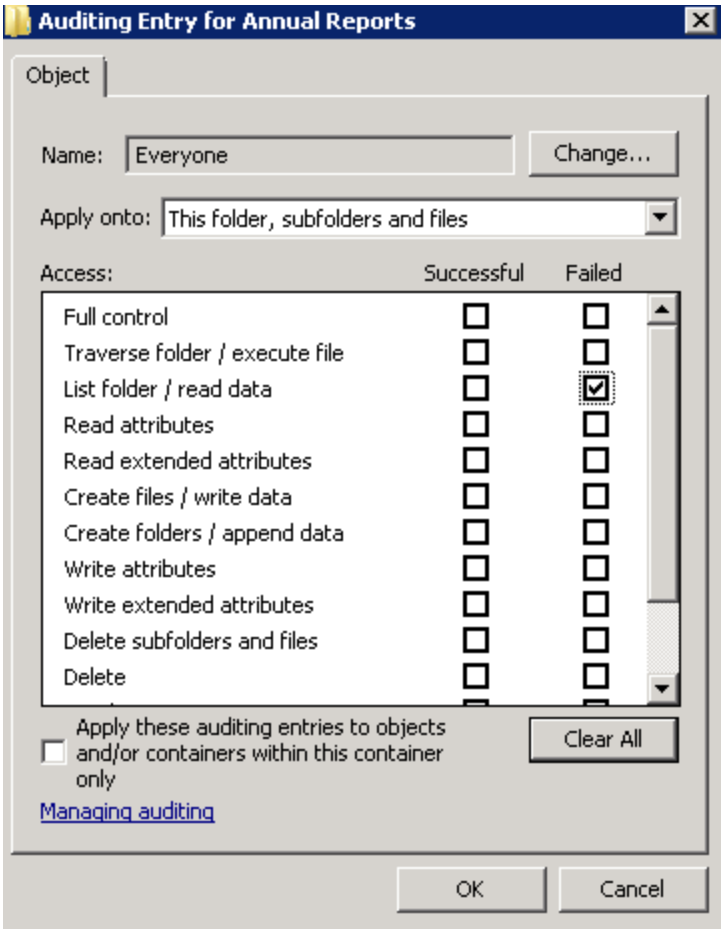
Auditing Entry

- 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.

Failed read attempts

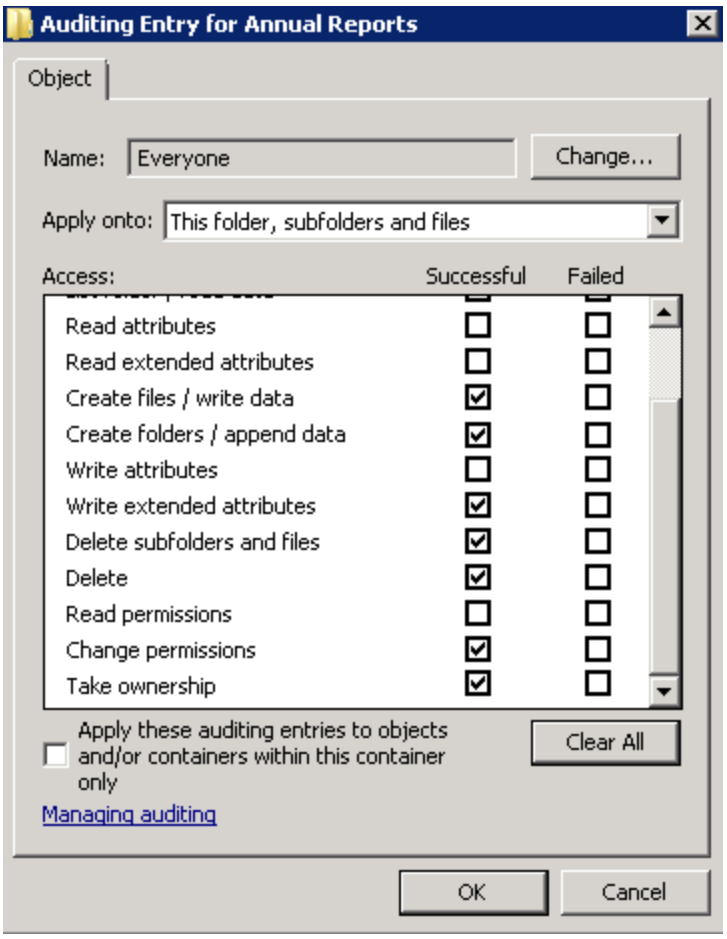
The Auditing Entry below shows Advanced Permissions for auditing failed read attempts only:



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

Auditing Entry
Failed 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 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

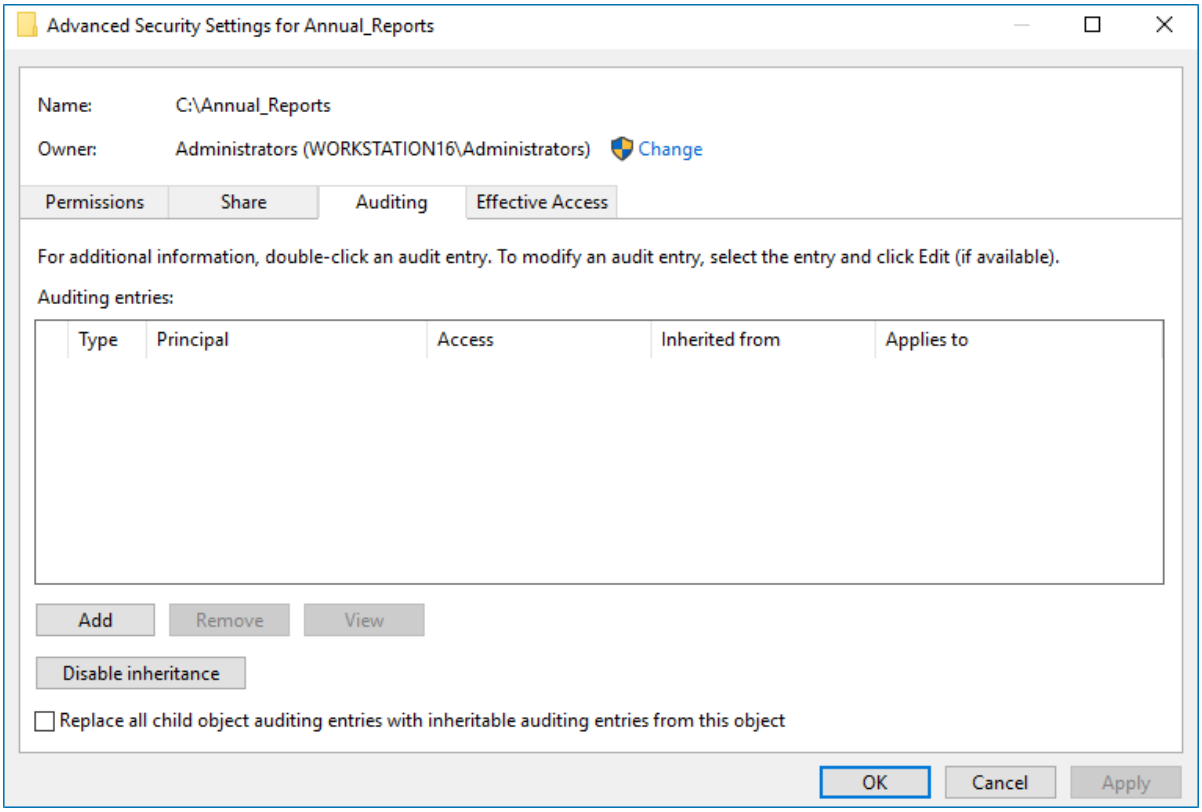
container only checkbox is cleared.

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**.

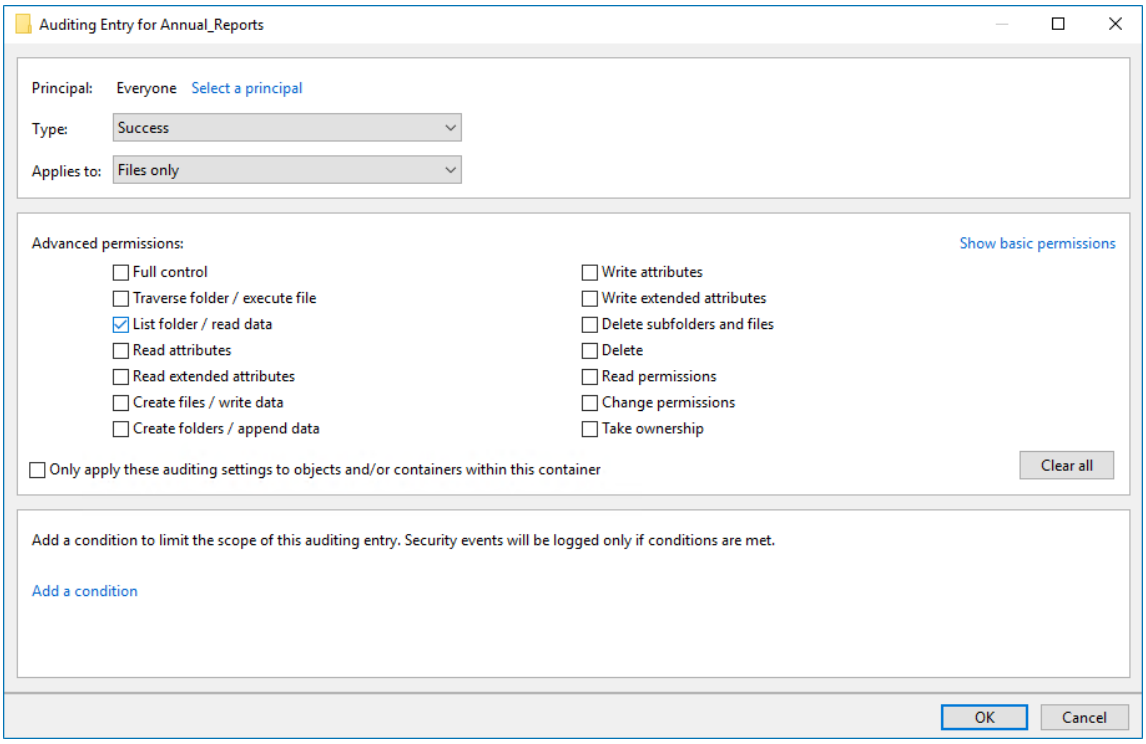
NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. In this case, the product will only monitor user accounts that belong to the selected group.

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:

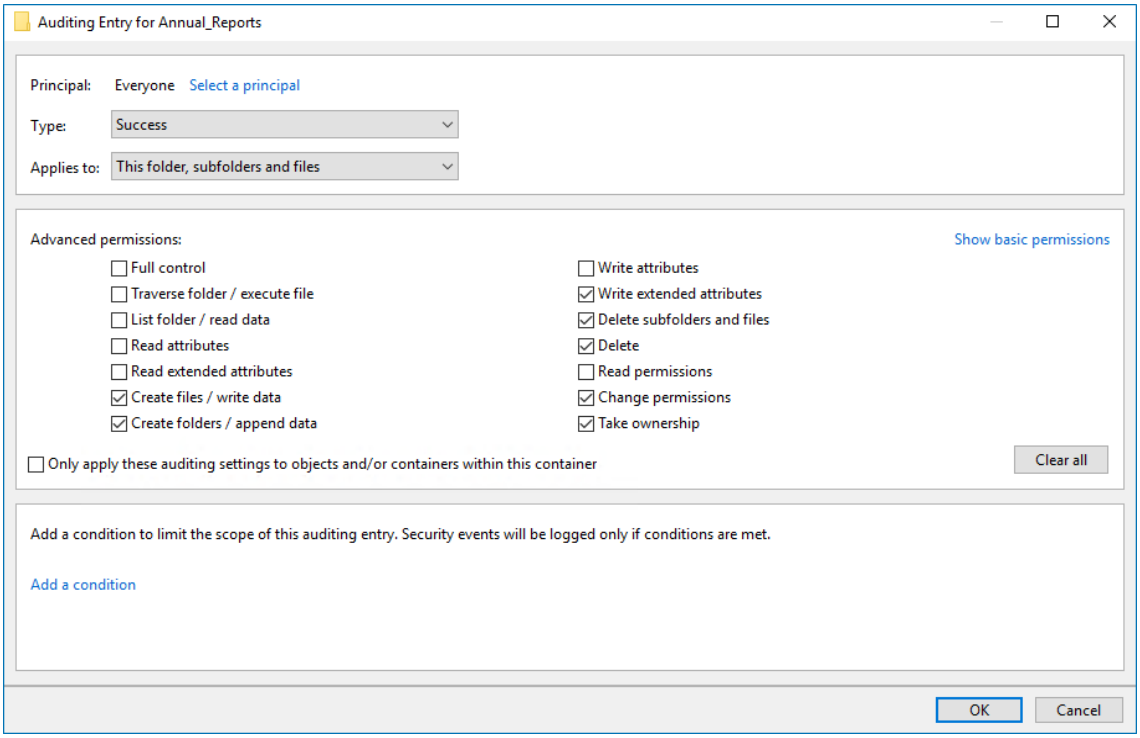


- Type—Set to*"Success"*.
- Applies to—Set to*"Files only"*.
- Advanced permissions—Select**List folder / read data**.
- Make sure that the**Only apply these auditing settings to objects and/or containers**

Auditing Entry
within this containercheckbox is cleared.

Successful changes

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

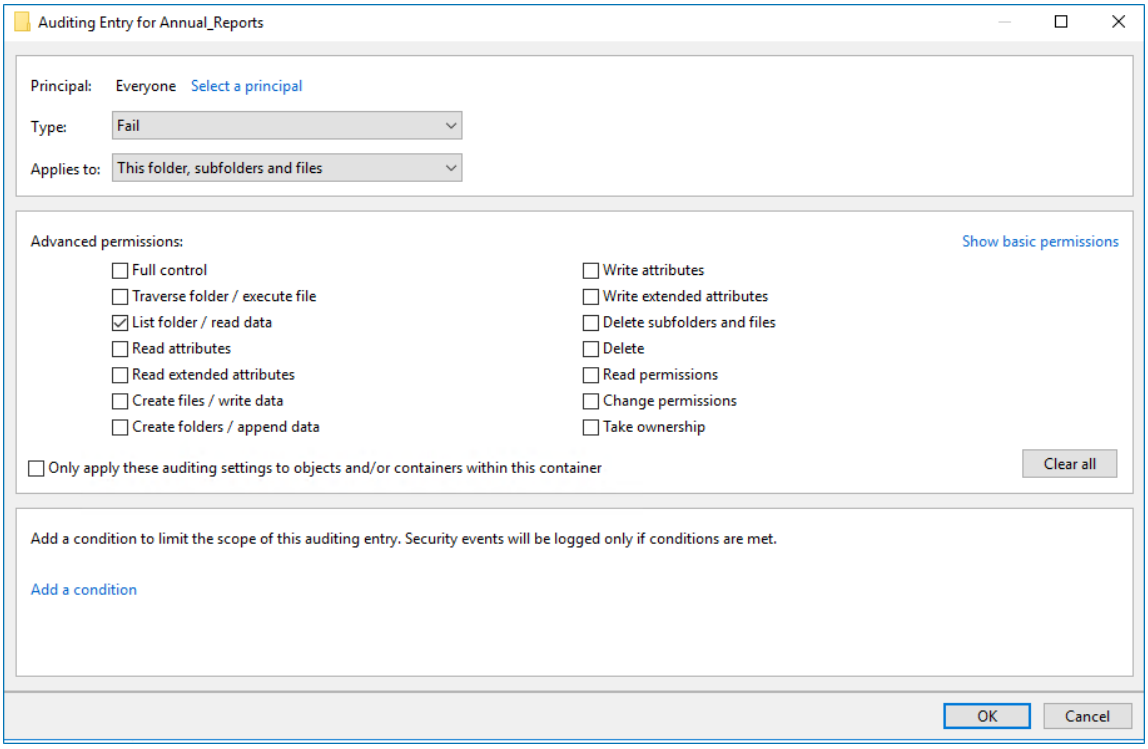


- Type—Set to*"Success"*.
- Applies to—Set to*"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that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

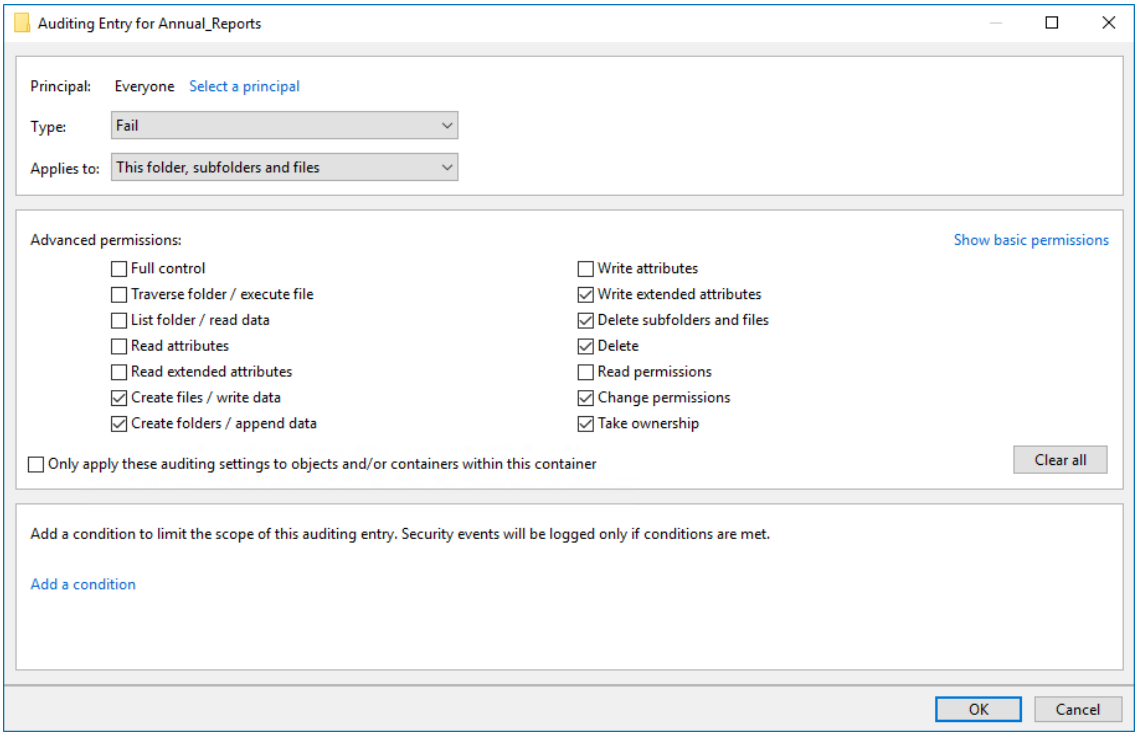


- Type—Set to*"Fail"*.
- Applies to—Set to*"This folder, subfolders and files"*.
- Advanced permissions—Select**List folder / read data**.
- Make sure that the**Only apply these auditing settings to objects and/or containers within this container**checkbox is cleared.

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 extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

NOTE: To audit successful changes on NetApp 8.x or earlier, also select **Write Attributes** in the **Advanced permissions** list in the auditing entry settings.

7.8. Configure Network Devices for Monitoring

To configure your network devices for monitoring perform the following procedures, depending on your device:

- Configure Cisco ASA Devices
- Configure Cisco IOS
- Configure Fortinet FortiGate Devices
- Configure PaloAlto Devices
- Configure Juniper Devices
- Configure SonicWall Devices

7.8.1. Configure Cisco ASA Devices

To configure your Cisco ASA devices, do the following:

1. Navigate to your Cisco ASA device terminal through the SSH/Telnet connection (for example, use PuTTY Telnet client).
2. Access the **global configuration** mode. For example:

   ```
   hostname# configure terminal
   hostname(config)#
   ```

3. Enable logging. For example:

   ```
   hostname(config)# logging enable
   ```

4. Set the IP address of the computer that hosts Netwrix Auditor Server as the `logging host` parameter. And make sure that the UDP port is used for sending syslog messages (e.g., 514 UDP port). For example:

   ```
   hostname(config)# logging host <Netwrix Auditor server IP address>
   ```

   NOTE: Do not select the **EMBLEM format logging** for the syslog server option.

5. Enable the `logging timestamp` option. For example:

   ```
   hostname(config)# logging timestamp
   ```

6. Set the `logging trap` option from 1 to 6 inclusive. For example:

   ```
   hostname(config)# logging trap 5
   ```

7.8.2. Configure Cisco IOS

To configure your Cisco IOS devices, do the following:

1. Navigate to your Cisco IOS device terminal through the SSH/Telnet connection (for example, use PuTTY Telnet client).
2. Access the **global configuration** mode. For example:

   ```
   Router# configure terminal
   ```

3. Enable time stamps in syslog messages:

   ```
   Router# service timestamps log datetime localtime show-timezone
   ```

4. Set the `logging trap` option from 1 to 6 inclusive. For example:

   ```
   Router# logging trap 5
   ```

5. Set the IP address of the Netwrix Auditor Server as the `logging host` parameter. And make sure that the UDP port is used for sending syslog messages (e.g., 514 UDP port). For example:

   ```
   Router# 192.168.1.5 514
   ```

7.8.3. Configure Fortinet FortiGate Devices

To configure your Fortinet FortiGate devices, enable logging to multiple Syslog servers and configure FortiOS to send log messages to remote syslog servers in **CEF** format. Do one of the following:

- To configure Fortinet FortiGate devices via Command Line Interface
- To configure Fortinet FortiGate devices through the Fortigate Management Console

To configure Fortinet FortiGate devices via Command Line Interface

1. Log in to the Command Line Interface (CLI).
2. Enter the following commands:

   ```
   config log syslogd setting
   set format cef
   ```

   NOTE: To enable CEF format in some previous FortiOS versions, enter the `set csv disable` command.

   ```
   set csv disable
   set facility <facility_name>
   set port 514
   set reliable disable
   set server <ip_address_of_Receiver>
   set status enable
   end
   ```

To configure Fortinet FortiGate devices through the Fortigate Management Console

1. Open **Fortigate Management Console** and navigate to **Log&Report** → **Log Config** → **Log Setting**.
2. Select the **Syslog** checkbox.
3. Expand the **Options** section and complete the following fields:

Option	Description
Name/IP	Enter the address of your Netwrix Auditor Server.
Port	Set to *"514"*.
Level	Select desired logging level.
Facility	Netwrix recommends using default values.
Data format	Select **CEF**. **NOTE:** To enable CEF format in some previous FortiOS versions, unselect the **Enable CSV** checkbox.

4. Click **Apply**.

7.8.4. Configure PaloAlto Devices

To configure your PaloAlto devices, create a Syslog server profile and assign it to the log settings for each log type.

To configure a Syslog server profile

1. Connect to your PaloAlto device: launch an Internet browser and enter the IP address of the firewall in the URL field (https://<IP address>).
2. In the **Web Interface**, navigate to **Device** → **Server Profiles** → **Syslog**.
3. Click **Add** and specify profile name, for example, *"SyslogProf1"*.
4. Specify syslog server parameters:

Parameter	Description
Name	Specify unique name for a syslog server.
Syslog Server	Provide a server name by entering its FQDN or IPv4 address.

Parameter	Description
Transport	Select **UDP**.
Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).
Format	Select **IETF**.
Facility	Netwrix recommends using default values.

To configure syslog forwarding

1. In the **Web Interface**, navigate to **Device** → **Log Settings**.
2. For **System**, **Config** and **User-ID** logs, click **Add** and enter unique name of your syslog server.
3. On the **syslog** panel, click **Add** and select the syslog profile you created above.
4. Click **Commit** and review the logs on the syslog server.

7.8.5. Configure SonicWall Devices

To configure your SonicWall devices, do the following, depending on your device type:

- To configure SonicWall Web Application Firewall
- To configure SonicWall SMA
- To configure SonicWall NSv series

To configure SonicWall Web Application Firewall

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:84443*, where **IP address** is the IP of the device and **84443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate to **Log** → **Settings** and configure the following:

Parameter	Description
• Log Level • Alert Level • Syslog Level	Set to "Info".
• Enable Audit Log	Select these checkboxes.

Parameter	Description
• Send to Syslog Server in Audit Log Settings • Send to Syslog Server in Access Log Settings	
Primary Syslog Server	Enter the address of your Netwrix Auditor Server.
Primary Syslog Server Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).

4. Click **Accept**.
5. Navigate to **Log** → **Categories**.
6. Select the following checkboxes:
   - **Authentication**
   - **Authorization & Access**
   - **System**
   - **Web Application Firewall**
   - **Geo IP & Botnet Filter In Log Categories (Standard)**
7. Click **Accept**.

To configure SonicWall SMA

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:8443*, where **IP address** is the IP of the device and **8443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate **Log** → **Settings** and configure the following:

Parameter	Description
• Log Level • Alert Level • Syslog Level	Set to "Info".
• Enable Audit Log • Send to Syslog Server in Audit Log Settings	Select these checkboxes.

Parameter	Description
• Send to Syslog Server in Access Log Settings	
Primary Syslog Server	Enter the address of your Netwrix Auditor Server.
Primary Syslog Server Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).

4. Click **Accept**.
5. Navigate to **Log** → **Categories**.
6. Select the following checkboxes:
   - **Authentication**
   - **Authorization & Access**
   - **System**
   - **Web Application Firewall**
   - **Geo IP & Botnet Filter In Log Categories (Standard)**
7. Click **Accept**.

To configure SonicWall NSv series

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:443*, where **IP address** is the IP of the device and **443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate to **Manage** → **Log Settings** → **Base Setup**.
4. Select all checkboxes in the **Syslog** column.
5. Click **Accept**.
6. Navigate to **Manage** → **Log Settings** → **Syslog**.
7. Set the **Syslog Format** to **Default**.
8. Click **Add**.
9. In the dialog appears, select **Create new address object** option in the **Name or IP Address** combo box.
10. Provide name and IP address of the new object.
11. Click **OK**.

12. In the **Add Syslog Server** dialog, find the IP address you specified on the step 10 in the **Name or IP Address** list.
13. Click **OK**.
14. Click **Save**.

7.8.6. Configure Juniper Devices

To configure you Juniper devices, do the following:

1. Launch the JunOS Command Line Interface (CLI).
2. Execute the following commands:

   ```
   # configure
   # set system syslog host <host address> any info
   ```

   where `<host address>` is the IP address of the computer where Netwrix Auditor Server is installed.

   ```
   # set system syslog host <host address> port <port name>
   ```

   where

   `<host address>` is the IP address of the computer where Netwrix Auditor Server is installed

   AND

   `<port number>` is the name of the UDP port used to listen to network devices (514 port used by default). See Network Devices for more information.

   ```
   # set system syslog time-format <current year>
   # commit
   ```

7.9. Configure Oracle Database for Monitoring

Before you start monitoring 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

Also, remember to do the following:

1. Configure Data Collecting Account, as described in Grant 'Create Session' and 'Select' Privileges to Access Oracle Database
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Oracle Database

7.9.1. 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 monitor...	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.

7.9.2. 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 monitor...	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, Oracle`	• 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 monitor...	Execute the command...
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.

7.9.3. 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.

7.9.4. 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 Enterprise Edition (Fine Grained Auditing)	`SELECT POLICY_NAME, ENABLED from DBA_AUDIT_POLICIES;`

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.

7.10. Configure SharePoint Farm for Monitoring

You can configure your SharePoint farm for monitoring 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.

  NOTE: In this case, Netwrix Auditor will enable automatic audit log trimming for all monitored site collections; log retention period will be set to 7 days. Also, consider that after a site collection is processed, Netwrix Auditor will automatically delete the events older than 1 day from its audit log.

- 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.

  For SharePoint auditing, also remember to do the following:

  1. Configure Data Collecting Account, as described in Configure Data Collecting Account
  2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring SharePoint

7.10.1. 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.

7.10.2. 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**.
   - SharePoint 2019 — In the upper-right corner, click **Settings** (gear).
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.

Consider that if you are using SharePoint 2019, then to enable this option you will have to adjust audit settings automatically with Netwrix Auditor (as described in the New Monitoring Plan section), or use some scripting.

7.10.3. 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.

7.11. Configure Windows Server for Monitoring

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

- Automatically when creating a monitoring plan

  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.

  NOTE: 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.

- Manually.
  This method can be used, for example, in small and medium-sized environment. 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
  - Adjusting Event Log Size and Retention Settings
  - Configure Windows Firewall Inbound Connection Rules
  - Adjusting DHCP Server Operational Log Settings
  - Configure Removable Storage Media for Monitoring
  - Configure Enable Persistent Time Stamp Policy
- Using Group Policy Objects.
  In particular, the following procedures can be performed using GPO:
  - Configure Local Audit Policies
  - Adjusting Event Log Size and Retention Settings
  - Configure Enable Persistent Time Stamp Policy

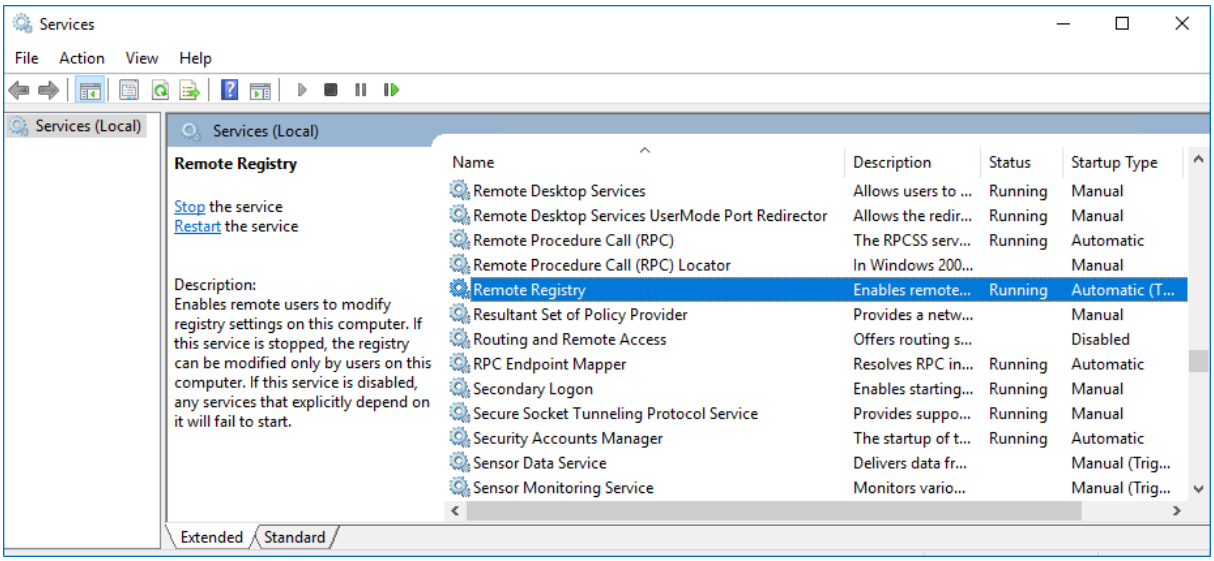
NOTE: You can configure other settings manually, as described in the corresponding sections.

For Windows Server auditing, also remember to do the following:

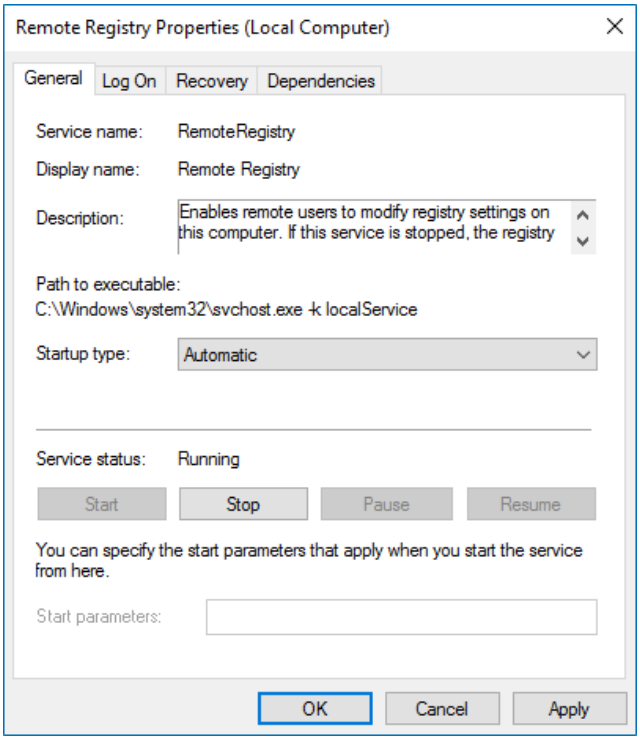
1. Configure Data Collecting Account, as described in Configure Data Collecting Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Windows Server

7.11.1. 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.

7.11.2. Configure Windows Registry Audit Settings

Windows Registry audit permissions must be configured on each Windows server you want to audit so that the "Who" and "When" values are reported correctly for each change. For test environment, PoC or evaluation you can use automatic audit configuration. 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:

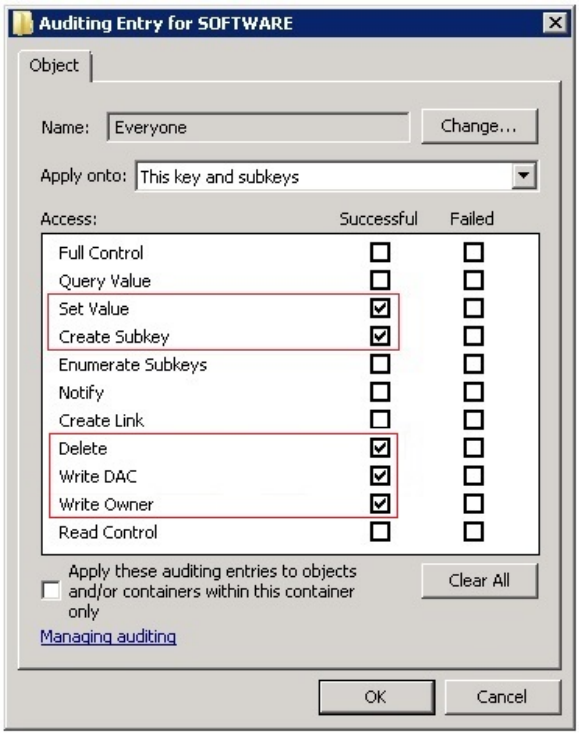
- Set Value
- Create Subkey
- Delete
- Write DAC
- Write Owner

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

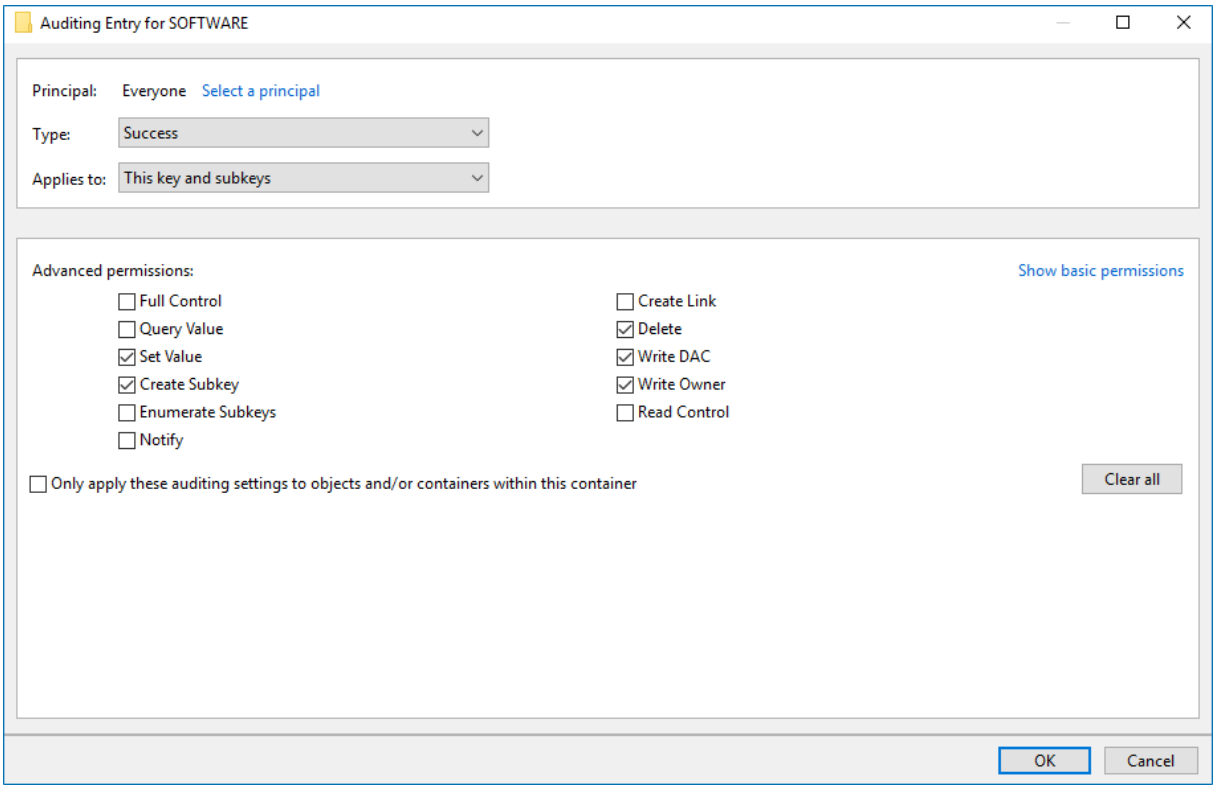
1. On your target server, open **Registry Editor**: navigate to **Start → Run** and type *"regedit"*.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click **Advanced**.
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.

NOTE: Using Group Policy for configuring registry audit is not recommended, as registry DACL settings may be lost.

7.11.3. 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.

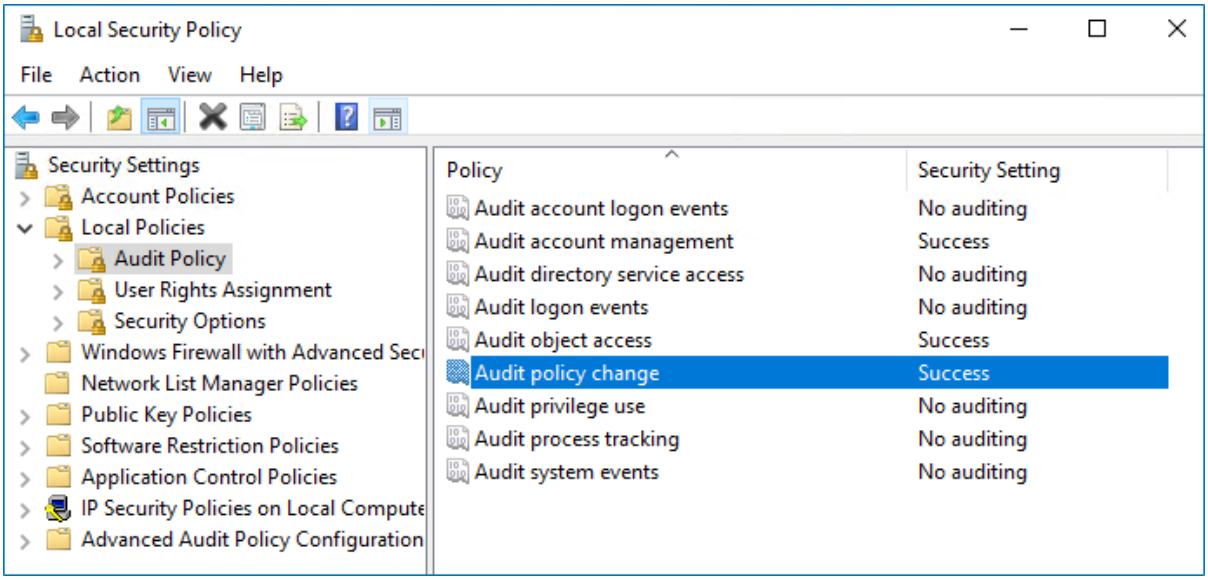
7.11.3.1. Manual Configuration

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"*



7.11.3.2. Configuration via Group Policy

Personnel with administrative rights can use Group Policy Objects to apply configuration settings to multiple servers in bulk.

To configure audit policies (Windows Server 2008 R2 and later)

1. Open the Group Policy Management console on the domain controller, browse to **Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies**.
2. Configure the following audit policies:

Policy Sub-node	Policy Name	Audit Events
Account Management	Audit Computer Account Management	*"Success"*
	Audit Security Group Management	*"Success"*
	Audit User Account Management	*"Success"*
Object Access	Audit Handle Manipulation	*"Success"*
	Audit Other Object Access Events	*"Success"*
	Audit Registry	*"Success"*
	Audit File Share	*"Success"*
Policy Change	Audit Audit Policy Change	*"Success"*

When finished, run the `gpupdate /force` command to force group policy update.

7.11.4. 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:

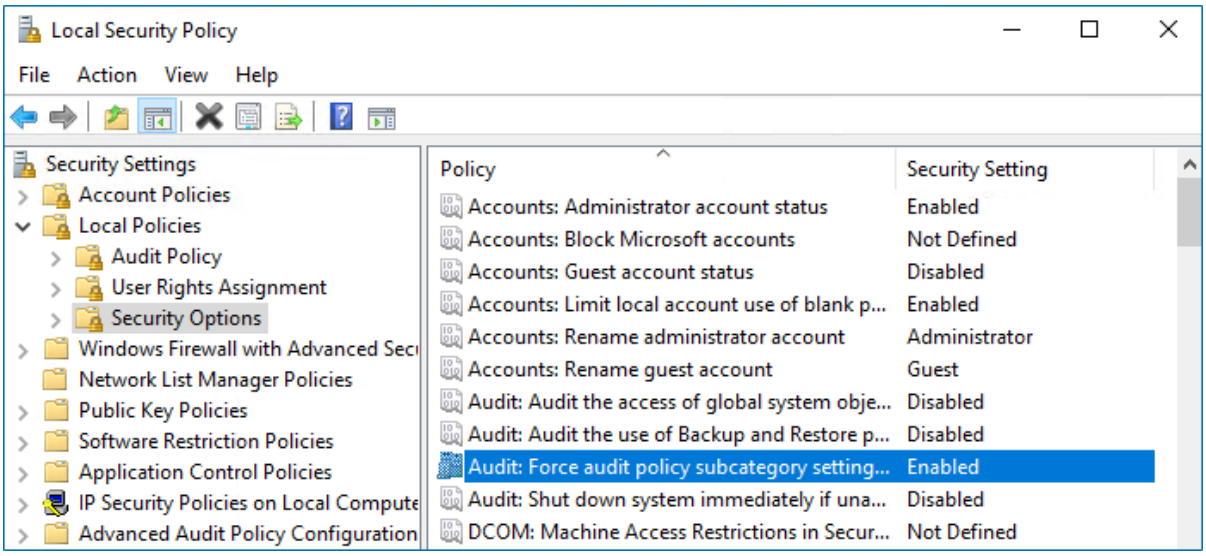
- To configure security options
- To configure advanced audit policy on Windows Server 2008
- To configure advanced audit policies on Windows Server 2008 R2 / Windows 7 and above

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 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** policy.



3. Double-click the policy and enable it.

To configure advanced audit policy on Windows Server 2008

In Windows Server 2008 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 Create System Startup / Shutdown and User Logon / Logoff Scripts Microsoft article 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

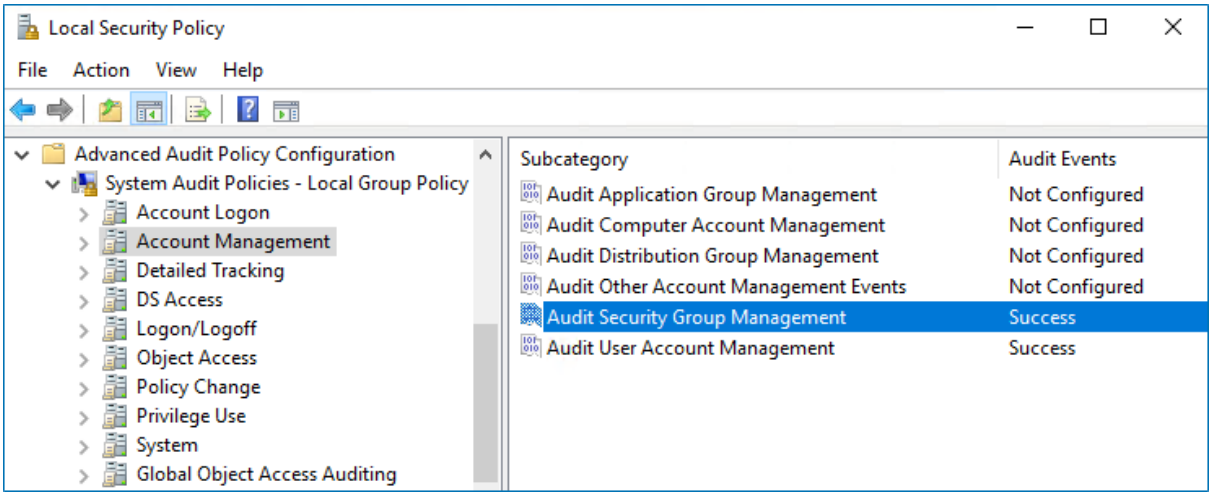
In Windows Server 2008 R2 and Windows 7 and above, Advanced audit policies are integrated with Group Policies, so they can be applied via Group Policy Object or Local Security Policies. The procedure below describes how to apply Advanced policies via Local Security Policy console.

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"*



7.11.5. Adjusting Event Log Size and Retention Settings

Consider that if the event log size is insufficient, overwrites may occur before data is written to the Long-Term Archive and the Audit Database, and some audit data may be lost.

To prevent overwrites, you can increase the maximum size of the event logs and set retention method for these logs to "*Overwrite events as needed*". This refers to the following event logs:

- Application
- Security
- System

- Microsoft-Windows-TaskScheduler/Operational
- Microsoft-Windows-DNS-Server/Audit (only for DCs running Windows Server 2012 R2 and above)

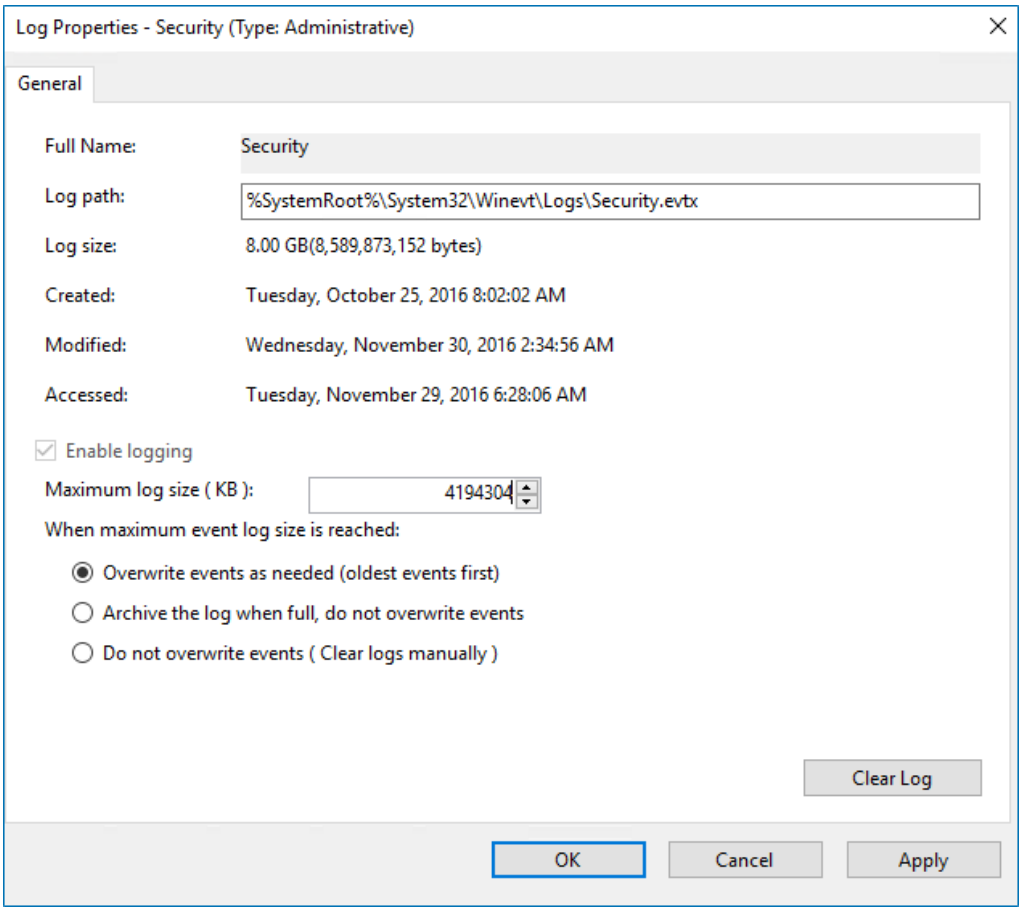
NOTE: To read about event log settings recommended by Microsoft, refer to this article.

The procedure below provides a possible way to specify the event log settings manually. However, if you have multiple target computers, consider configuring these settings via Group Policy as also described in this section

7.11.5.1. Manually

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**

     NOTE: Configure setting for TaskScheduler/Operational log only if you want to monitor scheduled tasks.
   - **Applications and Services Logs → Microsoft → Windows → DNS-Server → Audit**

     NOTE: Configure setting for DNS log only if you want to monitor DNS changes. 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.

7.11.5.2. Using Group Policy

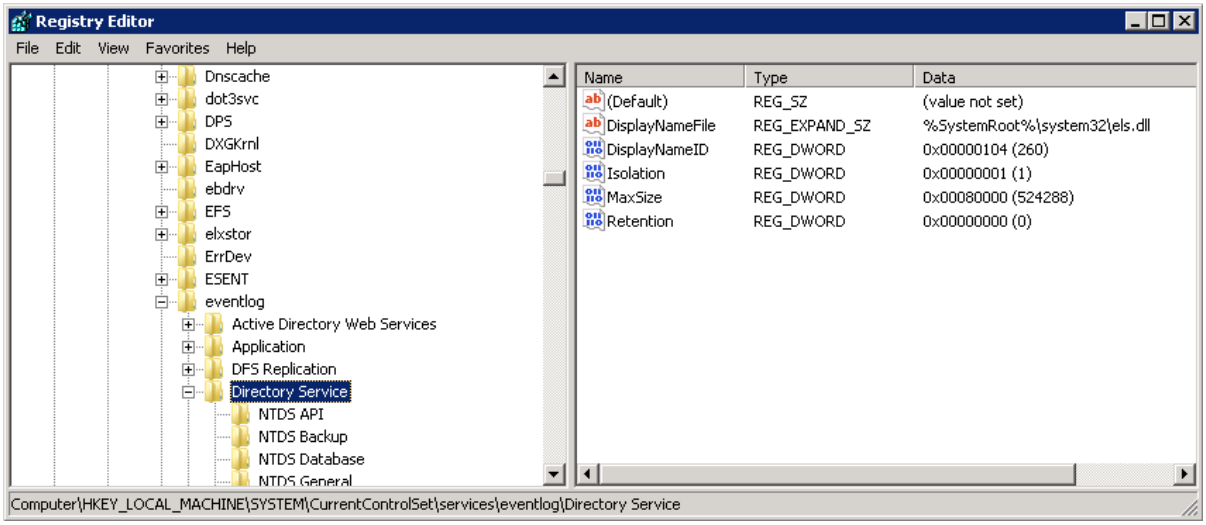
Personnel with administrative rights can use Group Policy Objects to apply configuration settings to multiple servers in bulk.

To configure settings for Application, System and Security event logs

1. Open the Group Policy Management Editor on the domain controller, browse to **Computer Configuration → Policies → Administrative Templates → Windows Components → Event Log Service**.
2. Select the log you need.
3. Edit **Specify the maximum log file size** setting - its value is usually set to *4194240 KB*.
4. Specify retention settings for the log – usually **Overwrite as needed**.

To configure settings for other logs

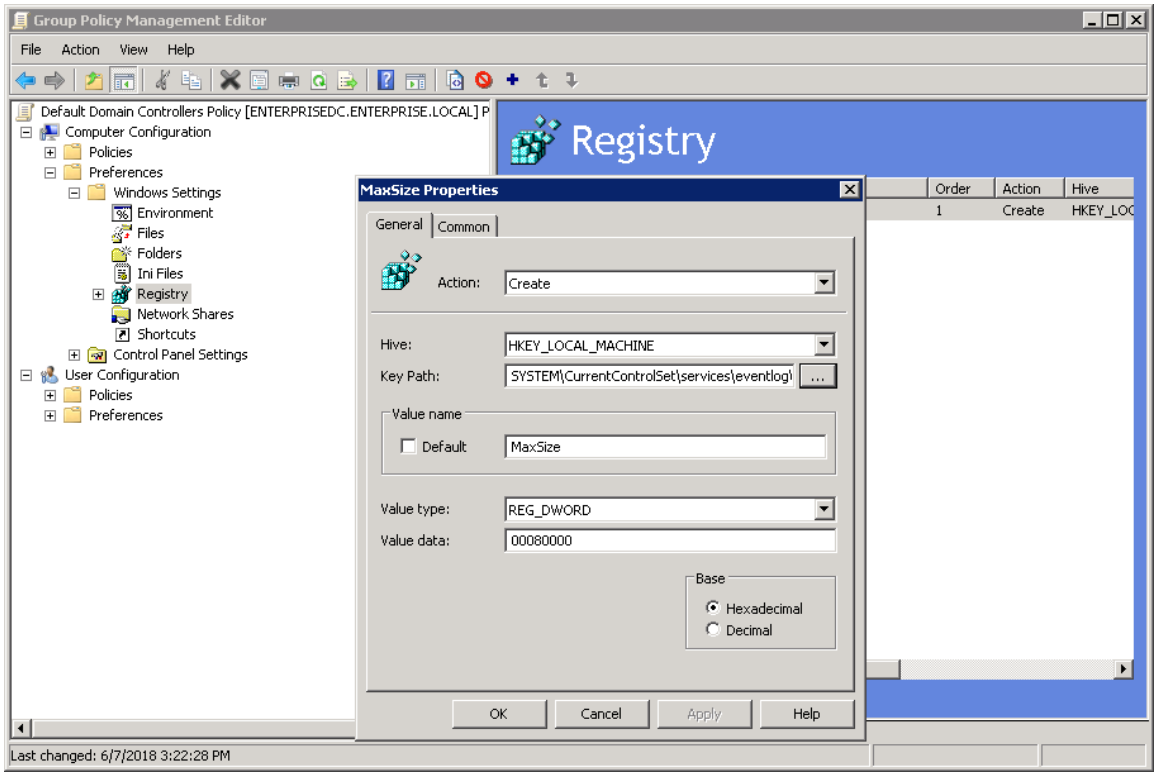
1. Open the registry editor and go to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\<log_name>**. For example: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Directory Service**
2. Set the **MaxSize** to the required decimal value (in bytes).



You can configure Group Policy Preferences to push registry changes to the target domain computers. For the example above (Directory Service Log), do the following:

1. In Group Policy Management Console on the domain controller browse to **Computer → Preferences → Windows Settings → Registry**.
2. Right-click **Registry** and select **New → Registry Item**.
3. In the **Properties** window on the **General** tab select:
   - **Action → Create**
   - **Hive → HKEY_LOCAL_MACHINE**

- **Key Path** – browse to **MaxSize** value at **SYSTEM\CurrentControlSet\Services\EventLog\Directory Service**



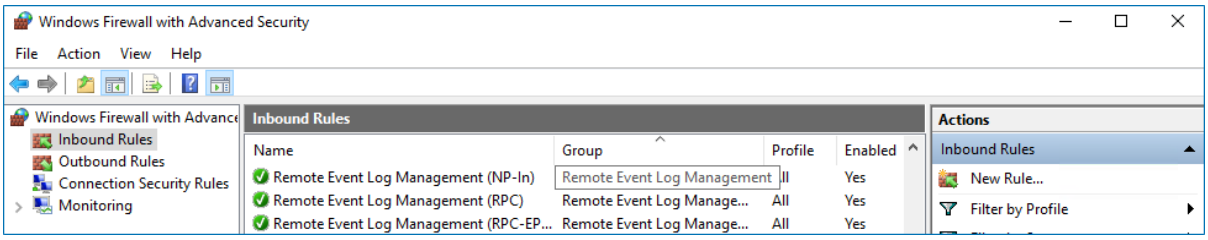
4. Change the **MaxSize REG_DWORD** to the required decimal value (in bytes).
5. Save the preferences and link them to the necessary servers (OUs).

When finished, run the `gpupdate /force` command to force group policy update.

7.11.6. 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)**

If you plan to audit Windows Server 2019 or Windows 10 Update 1803 without network compression service, make sure the following inbound connection rules are enabled:

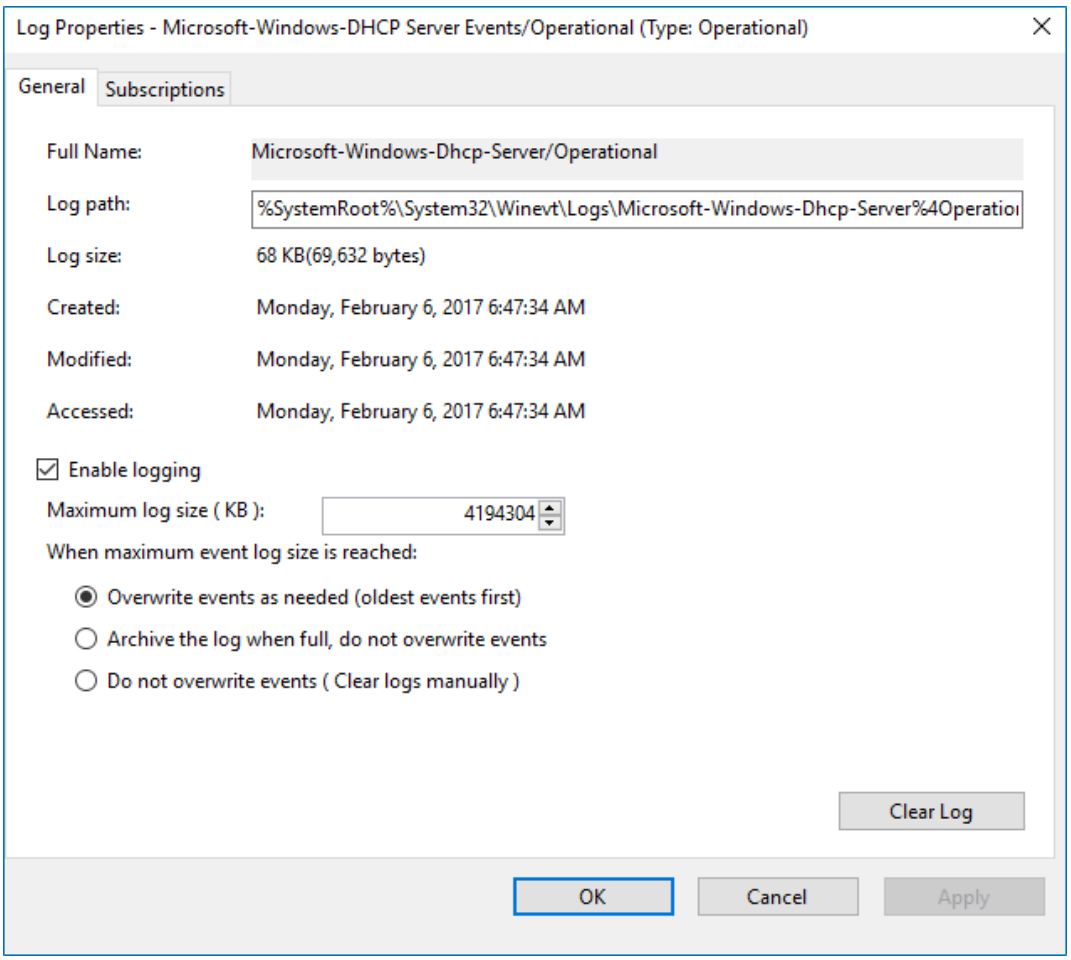
- **Remote Scheduled Tasks Management (RPC)**
- **Remote Scheduled Tasks Management (RPC-EMAP)**

7.11.7. Adjusting DHCP Server Operational Log Settings

If you plan to monitor DHCP changes, you may need to adjust your DHCP Server Operational log settings (size and retention method). For that, take the steps described below.

1. On the DHCP server, navigate to **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 the **Enable logging** option is selected.
5. Set **Maximum log size** to **4 GB**.
6. Set the retention method to **Overwrite events as needed (oldest events first)**. Click **OK** to save the settings and close the dialog.

7.11.8. Configure Removable Storage Media for Monitoring

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

Review the following for additional information:

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

To configure removable storage media monitoring 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 monitoring 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\EventTraceSessionTemplate.xml"*.
     - `<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.

Option	Description
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.

7.11.9. Configure Enable Persistent Time Stamp Policy

The **Enable Persistent Time Stamp** policy must be enabled on the target servers to track the shutdowns.

7.11.9.1. Manual Configuation

This section explains how to configure policies locally with the **Local Group Policy Editor** snap-in.

To enable the policy

1. On the audited server, open the **Local Group Policy Editor** snap-in: navigate to **Start → Run** and type *"gpedit.msc"*.
2. Navigate to **Computer Configuration → Administrative Templates → System** and locate the policy.

Policy Name	State
Enable Persistent Time Stamp	*"Enabled"*

7.11.9.2. Configuration via Group Policy

To apply settings to the whole domain, you can use Group Policy. Remember to consider the possible impact on your environment.

To enable the policy

1. Open the Group Policy Management console on the domain controller, browse to **Computer Configuration → Policies → Administrative Templates → System**.
2. Locate the **Enable Persistent Time Stamp** policy in the right pane, right-click it and select **Edit**.
3. Switch policy state to **Enabled**.

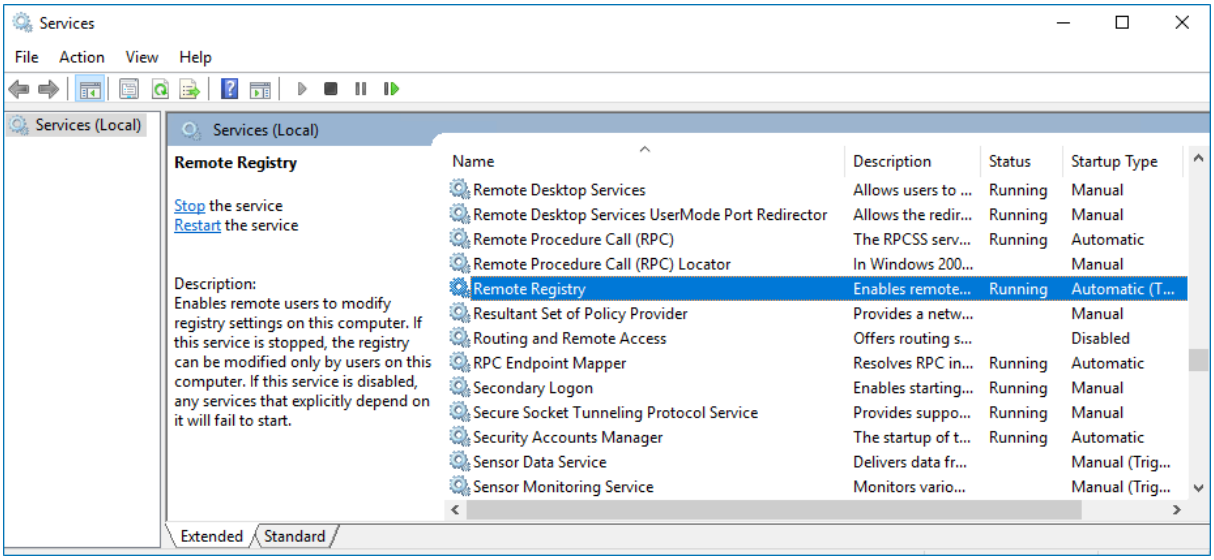
When finished, run the `gpupdate /force` command to force group policy update

7.12. Configure Infrastructure for Monitoring Windows Event Logs

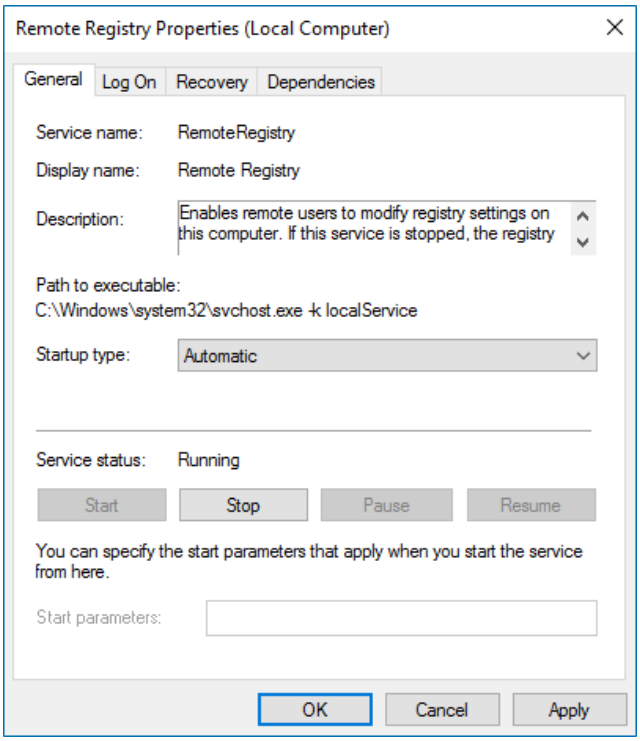
The **Remote Registry** service must be enabled on the target computers.

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.

7.13. Configure Domain for Monitoring Group Policy

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

- Automatically when creating a monitoring plan

  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.

  NOTE: 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.

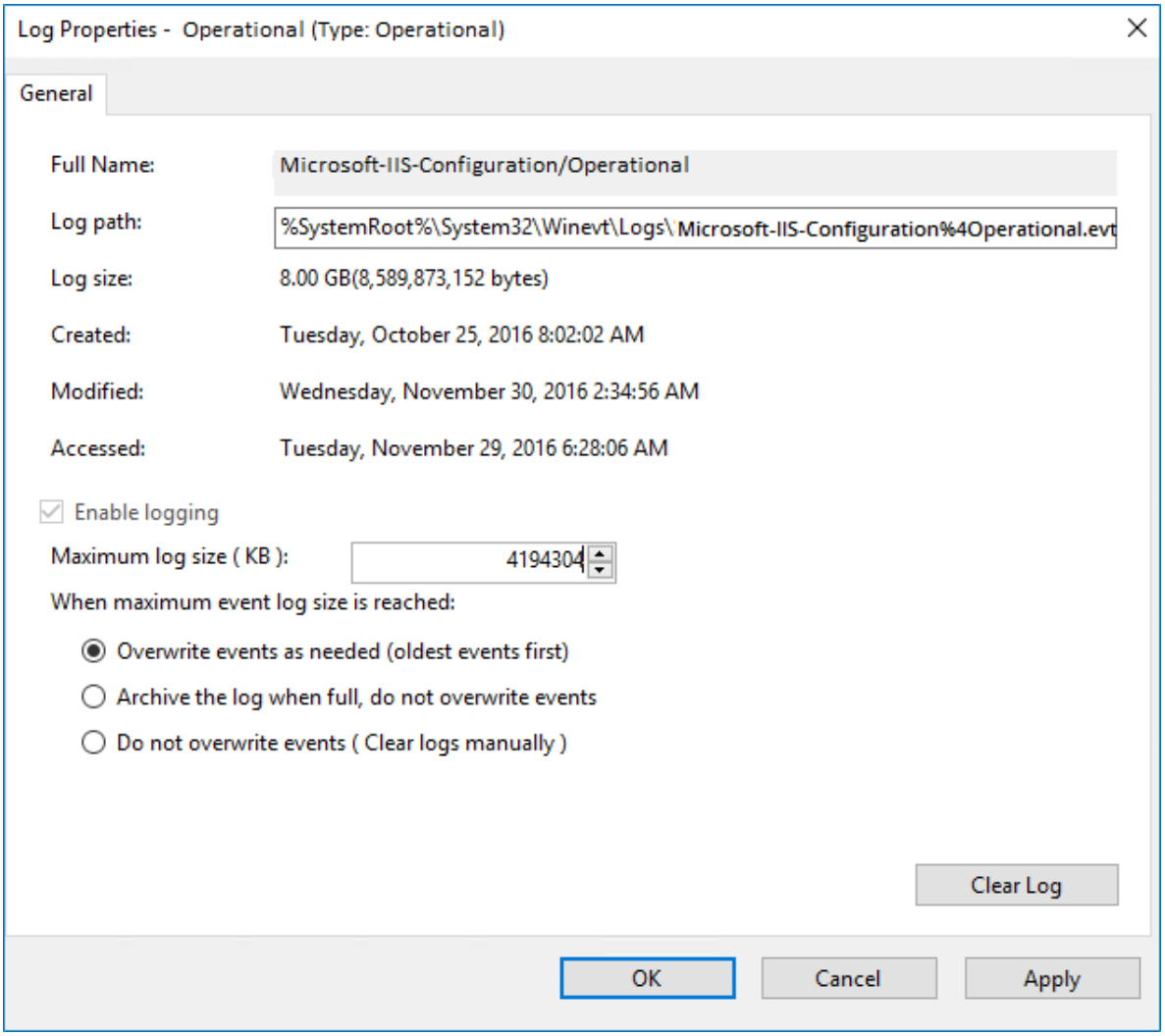
- Manually. You need to adjust the same audit settings as those required for monitoring Active Directory. See Configure Domain for Monitoring Active Directory for more information.

7.14. Configure Infrastructure for Monitoring 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 Monitoring 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)**.

7.15. Configure Infrastructure for Monitoring Logon Activity

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

- Automatically when creating a monitoring plan

  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.

  NOTE: 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.

- Manually. To configure your domain manually for monitoring 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

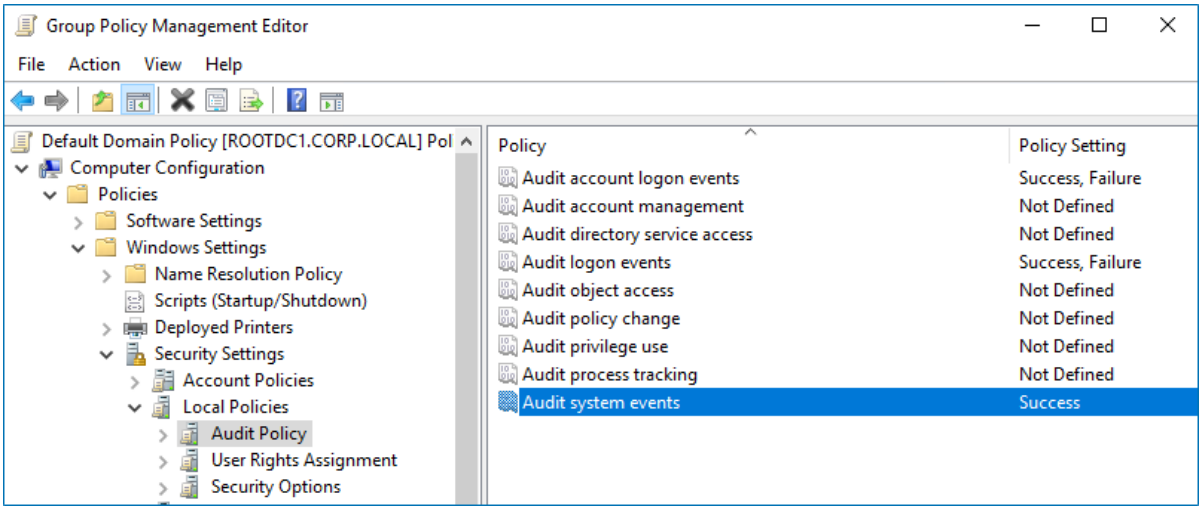
7.15.1. Configure Basic Domain Audit Policies

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"*

Policy	Audit Events
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.

7.15.2. 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

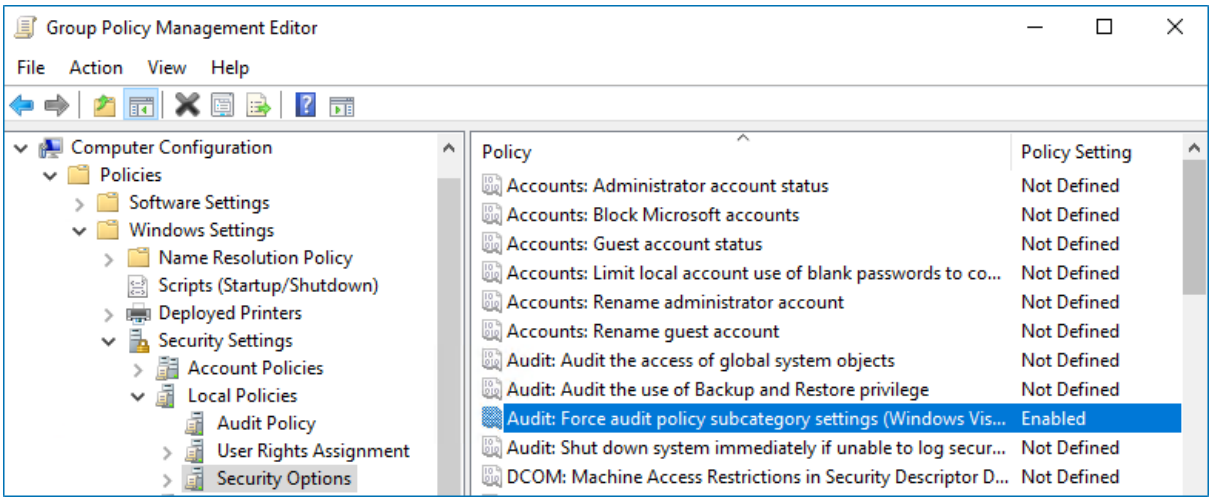
NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings to override audit policy category settings** option.

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



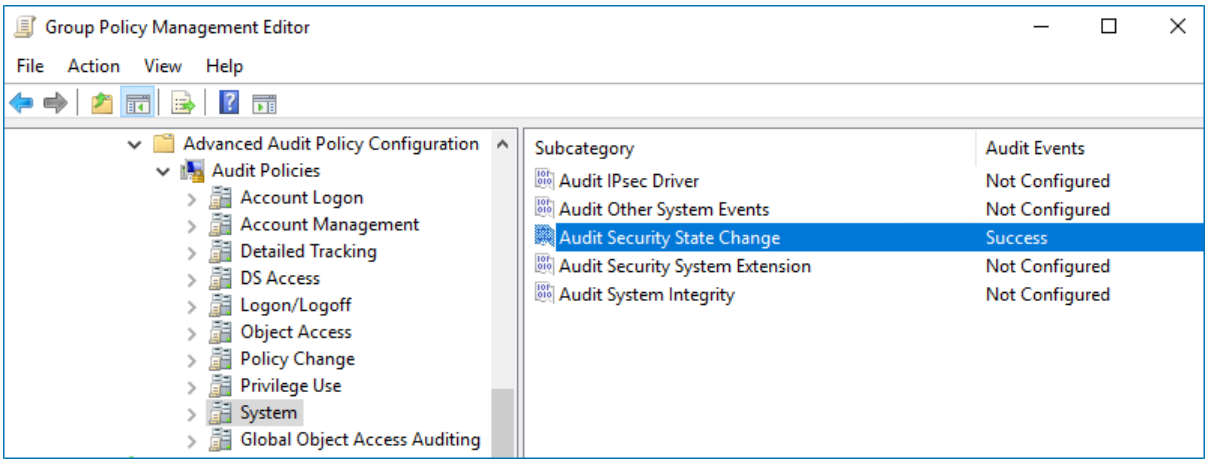
5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

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	*"Success"* and *"Failure"*

Policy Subnode	Policy Name	Audit Events
	• Audit Credential Validation	
	• 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"*

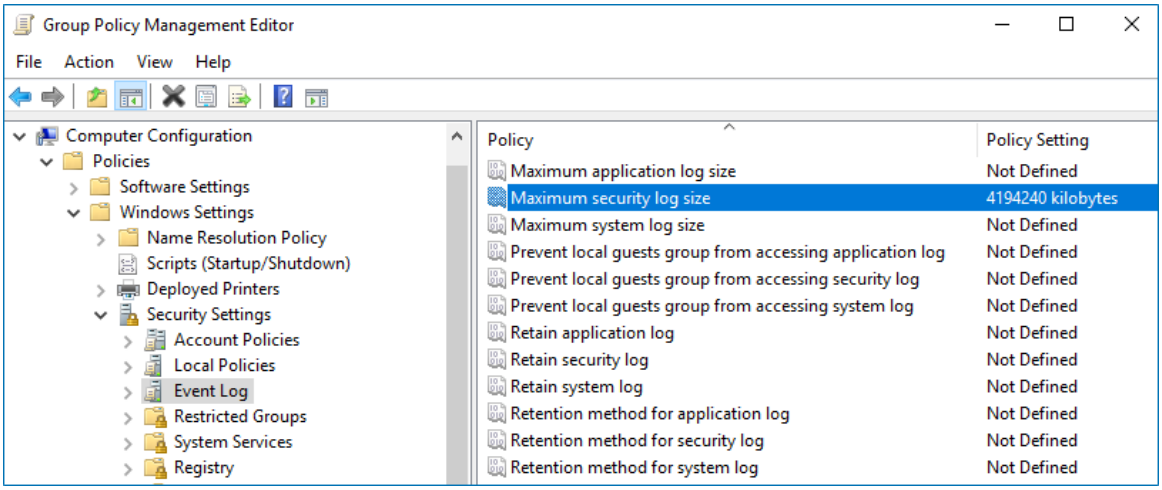


5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

7.15.3. 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.

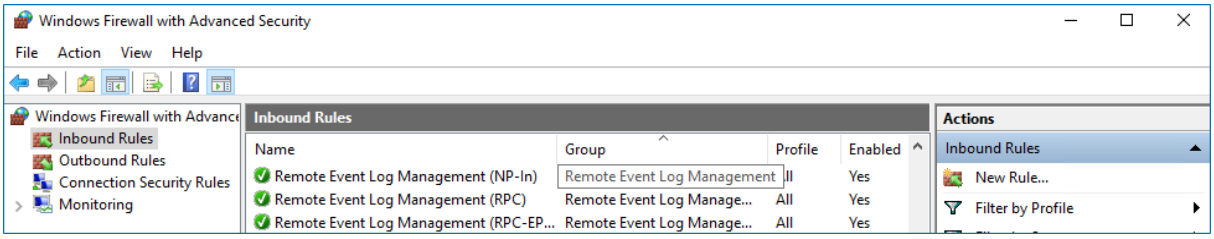


4. In the **Maximum security log size Properties** dialog, select **Define this policy setting** and set maximum security log size to *"4194240"* kilobytes (4GB).
5. Select the **Retention method for security log** policy. In the **Retention method for security log Properties** dialog, check **Define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

7.15.4. 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)**

7.16. Configure Computers for Monitoring User Activity

Perform the following procedures to configure computers for monitoring 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 monitored computers. See Install Netwrix Auditor User Activity Core Service for more information.

7.16.1. 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 9004 for inbound connections

1. On the computer where Netwrix Auditor is installed, 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:
   - On the **Rule Type** step, select **Program**.
   - On the **Program** step, specify the path: *%Netwrix Auditor installation folder%/Netwrix Auditor/User Activity Video Recording/UAVRServer.exe*.
   - On the **Action** step, select the **Allow the connection** action.
   - On the **Profile** step, make sure that the rule applies to **Domain**.
   - On the **Name** step, specify the rule's name, for example **UA Server 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 *"9004"*.

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"*.

7.16.2. Configure Video Recordings Playback Settings

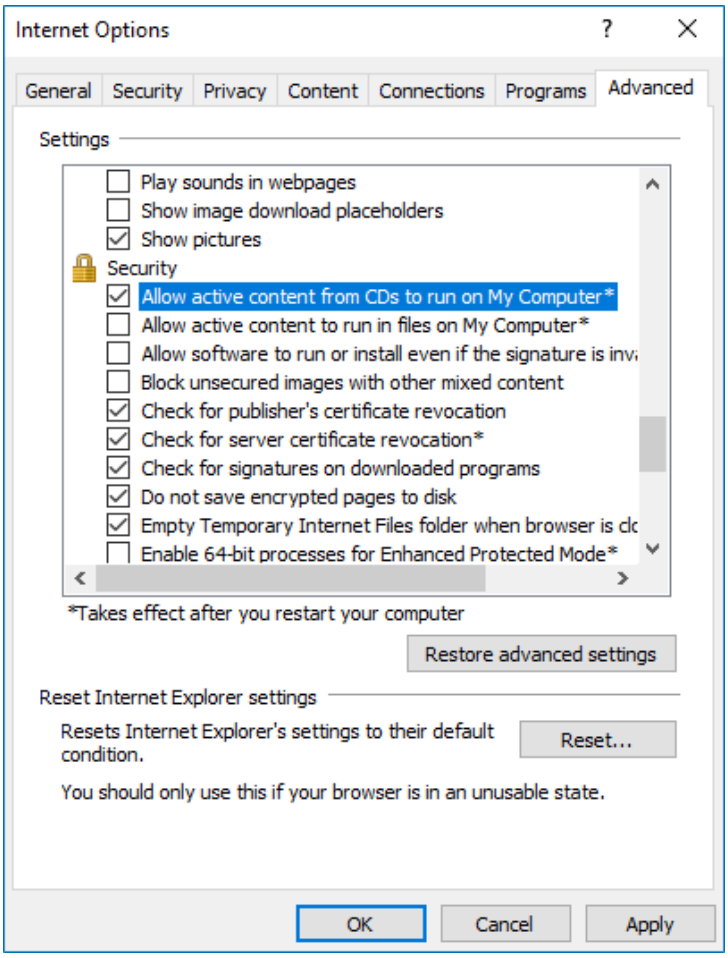
Video recordings of users' activity can be watched in any Netwrix Auditor client. Also, recordings are available as links in web-based reports and email-based Activity Summaries.

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.

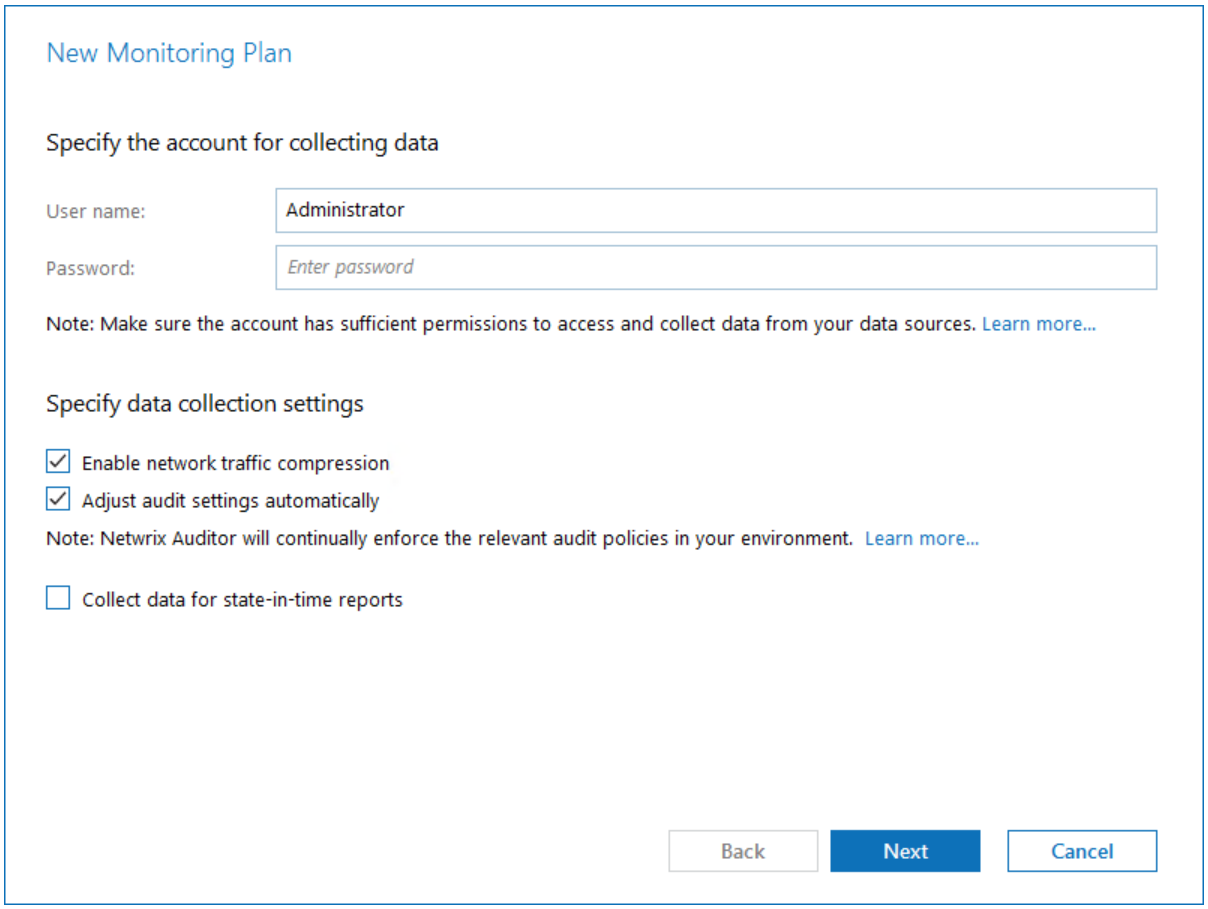
8. Configure Netwrix Auditor Service Accounts

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.

8.1. Configure Data Collecting Account

This service account is used to collect audit data from the data source items; it is specified during the monitoring plan creation:



Netwrix recommends creating a special service account for that purpose. Depending on the data source your monitoring plan will process, the account must meet the corresponding requirements.

Data source	Required rights and permissions:
Active Directory	***On the computer where Netwrix Auditor Server is installed:*** • Membership in the local **Administrators** group (for auditing local or trusted domain) ***In the target domain*** 1. Depending on the network traffic compression setting you need to use, one of the following is required: • If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group **NOTE:** If you need granular rights to be assigned instead, please contact Netwrix Technical support. • If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the

Data source	Required rights and permissions:

Manage auditing and security log policy must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy for more information.

2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

   NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group

3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required:

   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.

   b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**

   c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.

Azure AD

In the Cloud:

Initial data collection

- When first configuring a monitoring plan for auditing an Azure AD domain, the account must be assigned the **Global Administrator** role in Azure AD (**Company Administrator** in Azure AD PowerShell terms). See Assigning Global Administrator Role for Azure AD and Office 365 Auditingfor more information.

After the initial data collection

- The **Global Administrator** role can be removed from the collection account. (Ongoing audit data collection leverages granted Office 365 Management APIs access permission, and therefore requires no tenant-level or site-level permissions.)
- If the **Global Administrator** role was removed from the account, and you plan to audit *Successful* and/or *Failed Logons*, assign one of the following roles to the

Data source	Required rights and permissions:
	account: • **Security Reader** • **Security Administrator** • Also, to audit *Successful* and/or *Failed Logons*, the account must be assigned **Azure Active Directory Premium Plan 1** or **Azure Active Directory Premium Plan 2** license. **NOTE:** Accounts with multi-factor authentication are not supported. The account needs to be created as a Cloud-Only account.
Exchange	***On the computer where Netwrix Auditor Server is installed:*** • Membership in the local **Administrators** group (for auditing local or trusted domain) ***In the target domain*** 1. Depending on the network traffic compression setting you need to use, one of the following is required: • If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group **NOTE:** If you need granular rights to be assigned instead, please contact Netwrix Technical support. • If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy for more information. 2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information. **NOTE:** Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group 3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required: a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key

Data source	Required rights and permissions:
	on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information. b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators** c. **Read/Write** share permission and **Full control** security permission on the logs backup folder **NOTE:** Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group. Also, if the AD domain has an Exchange organization running Exchange 2010, 2013, or 2016, then: • the account must belong to the **Organization Management** or **Records Management group**(see Adding Account to 'Organization Management' Group for more information). -OR- • the **Audit Logs management** role must be assigned to this account (see .Assigning 'Audit Logs' Role for more information).
Exchange Online	***In the Cloud:*** • To connect to Exchange Online, the account must be assigned the following Exchange admin roles: • **Audit logs** • **Mail Recipients** • **View-Only Configuration** See Assigning 'Audit Logs', 'Mail Recipients' and 'View-Only Configuration' Admin Roles to Office 365 Account for more information **NOTE:** Accounts with multi-factor authentication are not supported. The account needs to be created as a Cloud-Only account.
Windows File Servers	***On the target server:*** 1. The account must be a member of the local **Administrators** group. 2. The **Manage auditing and security log** and **Backup files and directories** policies must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy and Configuring 'Back up Files and Directories' Policy for more

Data source	Required rights and permissions:
	information. 3. The account requires **Read** share permission on the audited shared folders. 4. The account requires **Read** NTFS permission on all objects in the audited folders. 5. To audit *Domain-Named DFS NameSpace*, the account must be a member of the **Built-in Server Operators** group on the domain controllers of 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. 1. The account must be a member of the local **Administrators** group. 2. The account requires **Read** permissions on the audited shared folders. 3. The account requires **Read** permissions on the folder where audit events are logged (*/ifs/.ifsvar/audit/*) 4. To connect to **EMC Isilon**, an account must be assigned a custom role (e.g., netwrix_audit) that has the following privileges: Platform API (ISI_PRIV_LOGIN_PAPI) readonly Auth (ISI_PRIV_AUTH) readonly Audit (ISI_PRIV_AUDIT) readonly Backup (ISI_PRIV_IFS_BACKUP) readonly See Configuring Your EMC Isilon Cluster for Auditing for more information. **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

Data source	Required rights and permissions:

	• 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 all
	  • vserver audit rotate-log all
	  • vserver cifs readonly
	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.
	Review the following for additional information:
	• Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access

Network Devices	No special configuration required. While creating a monitoring plan, you need to specify the account used to collect data from network devices. Feel free to use any account (not necessarily credentials to connect to the device)— these credentials do not affect Netwrix Auditor and monitored IT infrastructure.
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:

Data source	Required rights and permissions:
	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` For Oracle Database 12c Release 2, also grant the `SELECT` privilege on the following object: `audsys.aud$unified` **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. Review the following for additional information: • Grant 'Create Session' and 'Select' Privileges to Access Oracle Database
SharePoint	***On the target server:*** • 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 Review the following for additional information:

Data source	Required rights and permissions:
	• Assigning 'SharePoint_Shell_Access' Role **NOTE:** For settings required to collect **state-in-time data** from a SharePoint farm, see Object Types and Attributes Monitored on SharePoint.
SharePoint Online (including OneDrive for Business)	***In the Cloud:*** **Initial data collection** • 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. **After the initial data collection** • The **Global Administrator** role can be removed from the collection account. Ongoing audit data collection leverages granted Office 365 Management APIs access permission and therefore requires no tenant-level or site-level permissions. **NOTE:** Accounts with multi-factor authentication are not supported. The account needs to be created as a Cloud-Only account. Review the following for additional information: • Assigning Global Administrator Role for Azure AD and Office 365 Auditing
SQL Server	***On the target server:*** • To access target SQL Server, data collection account should be a Windows account, specified in the *domain\user* format. SQL Server logins and authentication method are not supported. • The account must be assigned the **System Administrator** role on the target SQL Server Review the following for additional information: • Assigning 'System Administrator' Role
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 Review the following for additional information:

Data source	Required rights and permissions:
	• Configuring 'Manage Auditing and Security Log' Policy
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:* • Membership in the local **Administrators** group (for auditing local or trusted domain) *In the target domain* 1. Depending on the network traffic compression setting you need to use, one of the following is required: • If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group **NOTE:** If you need granular rights to be assigned instead, please contact Netwrix Technical support. • If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy for more information. 2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information. **NOTE:** Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group 3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required: a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information. b. Membership in one of the following groups: **Administrators**, **Print**

Data source	Required rights and permissions:
	Operators, **Server Operators** c. **Read/Write** share permission and **Full control** security permission on the logs backup folder **NOTE:** Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.
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 is enabled: the account must belong to the **Domain Admins** group OR If network traffic compression is disabled: the **Manage auditing and security log** policy must be defined for this account • The account must belong to one of the following domain groups: **Backup Operators** (only if the account is not a member of the **Domain Admins** group). • The **Read** permissions to the following registry key on each DC in the target domain: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* • The **Read** permissions to the following registry key on each DC in the target domain: *HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv*
Password Expiration in Active Directory—collected with Password Expiration Notifier	***In the target domain:*** • A member of the **Domain Users** group

Data source	Required rights and permissions:
User Activity	*On the target server:* • A member of the local **Administrators** group

8.1.1. For Active Directory Auditing

Before you start creating a monitoring plan to audit your Active Directory, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On Netwrix Auditor server:

- Membership in the local **Administrators** group (for auditing local or trusted domain)

In the target domain:

1. Depending on the network traffic compression setting you need to use, one of the following is required:
   - If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group

     NOTE: If you need granular rights to be assigned instead, please contact Netwrix Technical support.

   - If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account.
     See Configuring 'Manage Auditing and Security Log' Policy for more information.
2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

   NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group
3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required:
   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.
   b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**
   c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.

8.1.1.1. Configuring '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.

8.1.1.2. Granting Permissions for '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.

8.1.1.3. Assigning Permission To Read the Registry Key

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

This permission should be assigned on each domain controller in the audited domain, so if your domain contains multiple domain controllers, you may prefer 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.

NOTE: For auditing Logon Activity, you also need to assign the **Read** permission to the *HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv* registry key.

8.1.2. For Windows File Server Auditing

Before you start creating a monitoring plan to audit your Windows file servers, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The **Manage auditing and security log** and **Backup files and directories** policies must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy and Configuring 'Back up Files and Directories' Policy for more information.
3. The account requires **Read** share permission on the audited shared folders.

4. The account requires **Read** NTFS permission on all objects in the audited folders.
5. To audit *Domain-Named DFS NameSpace*, the account must be a member of the **Built-in Server Operators** group on the domain controllers of the domain where the file server belongs to.

8.1.2.1. Configuring '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.

8.1.3. For Windows Server Auditing

Before you start creating a monitoring plan to audit your Windows servers (including DNS and DHCP servers), plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target servers:

1. The **Manage auditing and security log** policy must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy
2. This account must be a member of the local **Administrators** group.

8.1.4. For Exchange Auditing

Before you start creating a monitoring plan to audit your Exchange server, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

1. Depending on the network traffic compression setting you need to use, one of the following is required:
   - If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group

     NOTE: If you need granular rights to be assigned instead, please contact Netwrix Technical support.

   - If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log**

policy must be defined for this account.
See Configuring 'Manage Auditing and Security Log' Policy for more information.

2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

   NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group

3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required:

   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.

   b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**

   c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.

Also, if the AD domain has an Exchange organization running Exchange 2010, 2013, or 2016, then:

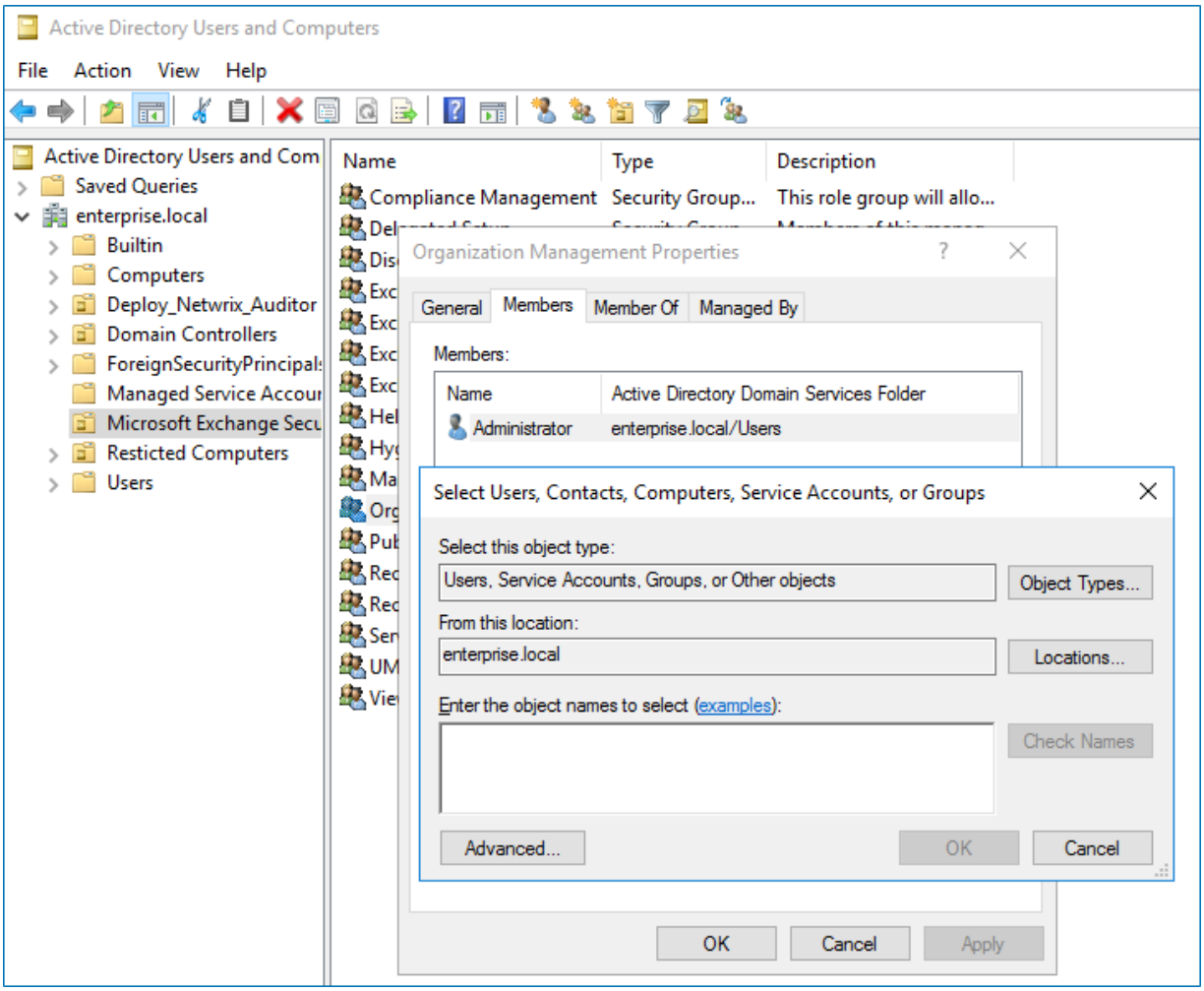
- the account must belong to the **Organization Management** or **Records Management group** (see Adding Account to 'Organization Management' Group for more information)

  -OR-

- the **Audit Logs management** role must be assigned to this account (see .Assigning 'Audit Logs' Role for more information)

8.1.4.1. Adding 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.

8.1.4.2. Assigning 'Audit Logs' Role

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.

8.1.5. For Azure AD Auditing

Before you start creating a monitoring plan to audit your Azure AD, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

In the Cloud:

The account needs to be created as a Cloud-Only account.

Initial data collection

- When first configuring a monitoring plan for auditing an Azure AD domain, the account must be assigned the **Global Administrator** role in Azure AD (**Company Administrator** in Azure AD PowerShell terms). See Assigning Global Administrator Role for Azure AD and Office 365 Auditingfor more information.

After the initial data collection

- The **Global Administrator** role can be removed from the collection account. (Ongoing audit data collection leverages granted Office 365 Management APIs access permission, and therefore requires no tenant-level or site-level permissions.)
- If the **Global Administrator** role was removed from the account, and you plan to audit *Successful* and/or *Failed Logons*, assign one of the following roles to the account:
  - **Security Reader**
  - **Security Administrator**

  See Assigning 'Security Administrator' or 'Security Reader' Role
- Also, to audit *Successful* and/or *Failed Logons*, the account must be assigned **Azure Active Directory Premium Plan 1** or **Azure Active Directory Premium Plan 2** license.

NOTE: Accounts with multi-factor authentication are not supported.

8.1.5.1. Assigning Global Administrator Role for Azure AD and Office 365 Auditing

When first creating a monitoring plan for Azure AD or Office 365 auditing, you need to specify the account assigned the **Global Administrator** role. This role is required to create a dedicated application in your Azure AD domain.

NOTE: Accounts with multi-factor authentication are not supported in both scenarios.

Depending on your company's security policies, select one of the following options:

1. Assign the **Global Administrator** role to an account for initial data collection and then remove the role. In this case, you need to assign additional roles to this account (**Security Reader** / **Security Administrator**) to audit Successful and / or Failed Logons. Netwrix recommends selecting this option to comply with your organization's security policies.

   Review the following for additional information:

   - To run initial data collection with the Global Administrator account
   - Assigning 'Security Administrator' or 'Security Reader' Role

2. Use the account assigned to be the **Global Administrator** on a regular basis. Any additional role assignments not required. When choosing this option, contact your security administrator to avoid violation of security policy in your organization.

To run initial data collection with the Global Administrator account

1. Sign in to Azure AD portal using your Microsoft account.
2. Select **Azure Active Directory** on the left.
3. Select an account that you want to use as Data Collecting Account for Azure AD or create a new user.
4. Make sure you disabled multi-factor authentication for this account.
5. Expand the **Directory role** and select **Global administrator**.

   NOTE: In Microsoft Graph API, Azure AD Graph API, and Azure AD PowerShell, this role is identified as **Company Administrator**.

6. Click **Ok**.
7. In Netwrix Auditor, create a monitoring plan for auditing Azure AD and specify this account on the **Specify the account for collecting data** step. See Netwrix Auditor Administration Guide for detailed instructions on how to create a monitoring plan.
8. Wait until initial data collection completes.
9. Open Azure AD portal and remove the **Global administrator** role from the account.

8.1.5.2. Assigning 'Security Administrator' or 'Security Reader' Role

To audit *Successful* and/or *Failed Logons* in Azure AD, the **Security Administrator** or **Security Reader** role is required. To assign the role you need, do the following:

1. Sign in to Azure AD portal using your Microsoft account.
2. Select **Azure Active Directory** on the left.
3. Navigate to **Roles and administrators**.

4. Click the **Security administrator** or **Security Reader** role.
5. Click **Add member** and select the account that you want to assign the role to.

For more information on the Administrator role permissions, refer to the following Microsoft article: Administrator role permissions in Azure Active Directory.

8.1.6. For Exchange Online Auditing

Before you start creating a monitoring plan to audit your Exchange Online organization, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

In the Cloud:

- The account needs to be created as a Cloud-Only account.
- To connect to Exchange Online, the account must be assigned the following Exchange admin roles:
  - **Audit logs**
  - **Mail Recipients**
  - **View-Only Configuration**

See Assigning 'Audit Logs', 'Mail Recipients' and 'View-Only Configuration' Admin Roles to Office 365 Account for more information.

NOTE: Accounts with multi-factor authentication are not supported.

8.1.6.1. Assigning '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.

Option	Description
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.

8.1.7. For EMC Isilon Auditing

Before you start creating a monitoring plan to audit your EMC Isilon file storage system, plan for the account that will be used for data collection. The following scenarios are possible:

- Automatic configuration: you can use a special shell script for configuring an audited EMC Isilon cluster and granting necessary privileges to the account used to collect audit data.
- Manual configuration: you can grant all the necessary permissions to data collecting account manually. For that, ensure the account meets the requirements listed below.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The account requires **Read** permissions on the audited shared folders.
3. The account requires **Read** permissions on the folder where audit events are logged (*/ifs/.ifsvar/audit/*)
4. To connect to **EMC Isilon** storage cluster, an account must be assigned a custom role (e.g., *netwrix_audit*) that has the following privileges:

Platform API (ISI_PRIV_LOGIN_PAPI)	readonly
Auth (ISI_PRIV_AUTH)	readonly
Audit (ISI_PRIV_AUDIT)	readonly
Backup (ISI_PRIV_IFS_BACKUP)	readonly

See Configuring Your EMC Isilon Cluster for Auditing for more information.

NOTE: If you plan to connect to a cluster that works in the compliance mode, the account must meet additional requirements.

8.1.7.1. Configuring Your EMC Isilon Cluster for Auditing

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

8.1.8. For EMC VNX/VNXe Auditing

Before you start creating a monitoring plan to audit your EMC VNX/VNXe file storage system, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The account requires **Read** permissions on the audited shared folders.

8.1.9. For NetApp Auditing

Before you start creating a monitoring plan to audit your NetApp file storage system, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

NOTE: If you want to authenticate with AD user account, you must enable it to access SVM through ONTAPI. See Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access for more information.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The account requires **Read** permissions (resultant set) on the audited shared folders.
3. The account requires:
   - **Read** permissions (resultant set) on the audit logs folder and its contents
   - **Delete** permissions (resultant set) on the contents of this folder
4. 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
5. 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 all
- vserver audit rotate-log all
- vserver cifs readonly

See Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access

NOTE: You can also assign the built-in **vsadmin** role.

8.1.9.1. Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling 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:

Capability	Related command (example)
• version	readonly
• volume	readonly
• vserver audit	all
• vserver audit rotate-log	all
• vserver cifs	readonly

NOTE: The capabilities must be assigned one by one.

To review currently applied capabilities, you can use the following command:

```
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.

4. To be able to add event policy for NetApp, the role you set up for working with ONTAPI must have the following attributes:

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

NOTE: This relates to NetApp 8.3.2 and later

8.1.10. For Oracle Database Auditing

Before you start creating a monitoring plan to audit your Oracle Database, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

1. The `CREATE SESSION` system privilege must be granted to the account used to connect to Oracle Database for data collection.
2. Depending on your Oracle Database version, the `SELECT` privilege on the following objects must be granted to that account:

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_$unified_audit_trail • all_unified_audit_actions • audit_unified_policies • audit_unified_enabled_policies For Oracle Database 12c Release 2, also grant the SELECT privilege on the following object: audsys.aud$unified

NOTE: To learn how to grant system privileges to the account, see Grant 'Create Session' and 'Select' Privileges to Access Oracle Database. Alternatively, you can grant the default administrator role to the account.

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

8.1.10.1. Grant 'Create Session' and 'Select' Privileges to Access Oracle Database

When creating a monitoring plan for your Oracle Database, you should specify the account that has sufficient privileges to collect data from the database. At least, the following privileges are required:

- 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 assign the default administrator role to that account.

You can grant the required privileges to the existing account, or create a new one. Follow the procedure described below.

To grant CREATE SESSION and SELECT privileges to the account:

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. Decide on the account that will be used to access this database for audit data collection. You can:
   - Use the account that already exists

     - OR -
   - Create a new account – for that, execute:
     `CREATE USER <account_name> IDENTIFIED BY PASSWORD;`
4. Grant `CREATE SESSION` system privilege to that account. For that, execute:
   `GRANT CREATE SESSION TO <account_name>;`
5. Depending on your Oracle Database version, grant `SELECT` privilege on the objects listed in the table below:

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_$parameter TO <account_name>;` • `GRANT SELECT ON dba_audit_mgmt_clean_events TO <account_name>;` • `GRANT SELECT ON dba_obj_audit_opts TO <account_name>;` • `GRANT SELECT ON dba_audit_policies TO <account_name>;` • `GRANT SELECT ON fga_log$ 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`

For...	Execute...
	<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>; For Oracle Database 12c Release 2, also grant the SELECT privilege on the following object: GRANT SELECT ON audsys.aud$unified 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 are using Oracle Database Enterprise Edition.

Alternatively, you can grant the default administrator role to that account. For that, execute:

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

8.1.11. For SQL Server Auditing

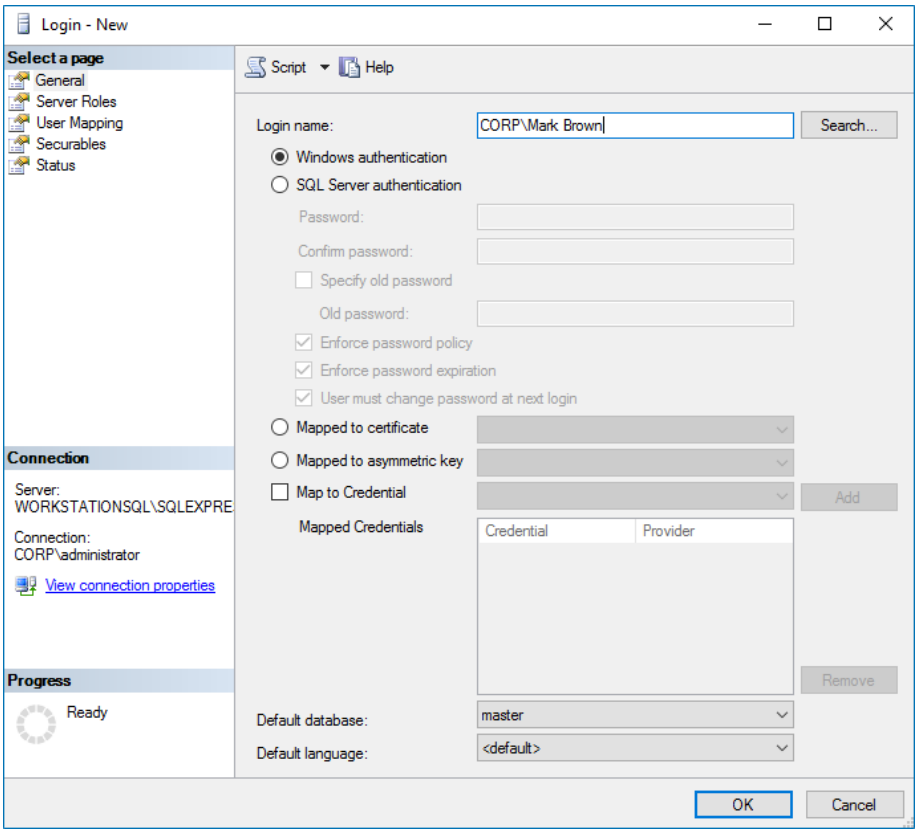
Before you start creating a monitoring plan to audit your SQL Server, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target SQL Server:

- To access SQL Server, Windows authentication will be used, so data collection account should be a Windows account specified in the *domain\user* format.
  SQL Server logins and authentication method are not supported.
- The account must be assigned the **System Administrator** server role for this SQL Server. See Assigning 'System Administrator' Role for more information.

8.1.11.1. Assigning '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 SQL Server instance.
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.

8.1.12. For SharePoint Auditing

Before you start creating a monitoring plan to audit your SharePoint farm, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target SharePoint farm:

1. On the SharePoint server where the Netwrix Auditor Core Service will be deployed: the account must be a member of the local **Administrators** group.
   To learn more about Netwrix Auditor Core Services, refer to Installing Core Services to Audit User Activity and SharePoint (Optional).
2. On the SQL Server hosting SharePoint database: the **SharePoint_Shell_Access** role.
   See Assigning 'SharePoint_Shell_Access' Role
3. If you plan to collect **state-in-time data** from a SharePoint farm, the account will also meet the requirements below:

- for site collection processing – lock status must differ from *No access*
- for web application processing – the following permissions must be assigned to this account:
  - *Open items*
  - *View items*
  - *Browse directories*
  - *View pages*
  - *Browse user information*
  - *Open*
  - *Enumerate permissions*

8.1.12.1. Assigning '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>
   ```

8.1.13. For SharePoint Online Auditing

Before you start creating a monitoring plan to audit your SharePoint Online farm, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

In the Cloud:

Initial data collection

- 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.

After the initial data collection

- The **Global Administrator** role can be removed from the collection account. Ongoing audit data collection leverages granted Office 365 Management APIs access permission and therefore requires no tenant-level or site-level permissions.

NOTE: Accounts with multi-factor authentication are not supported.

The account needs to be created as a Cloud-Only account.

8.1.14. For VMware Server Auditing

Before you start creating a monitoring plan to audit your VMware hosts, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target VMware hosts:

The account must have at least **Read-only** role on the audited hosts.

8.1.15. For Network Devices Auditing

You can use any account to audit your network devices (not necessarily the credentials used to connect to the device itself), as long as these credentials do not affect Netwrix Auditor or monitored IT infrastructure.

Provide this account in the monitoring plan wizard.

8.1.16. For Group Policy Auditing

Before you start creating a monitoring plan to audit the group policy in the domain, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On Netwrix Auditor Server:

- Membership in the local **Administrators** group (for auditing local or trusted domain)

On the target server:

1. Depending on the network traffic compression setting you need to use, one of the following is required:
   - If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group

     NOTE: If you need granular rights to be assigned instead, please contact Netwrix Technical support.

   - If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account.
     See Configuring 'Manage Auditing and Security Log' Policy for more information.
2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group

3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required:

   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.

   b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**

   c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.

8.1.17. For Logon Activity Auditing

Before you start creating a monitoring plan to audit the logon activity in your domain, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

In the target domain:

1. Depending on the network traffic compression setting you need to use, one of the following is required:

   - If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group
   - If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account.
     See Configuring 'Manage Auditing and Security Log' Policy for more information.

2. Membership in the **Backup Operators** group (if the account you plan to use for data collection is not a member of the Domain Admins group).
3. **Read** permission to access the following registry keys on the domain controllers in the target domain:

   - *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security*
   - *HKEY_LOCAL_MACHINE\Security\Policy\PolAdtEv*

   See Assigning Permission To Read the Registry Key for more information.

8.1.18. For Event Log Auditing

Before you start creating a monitoring plan to audit the event logs of your servers (including IIS), plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target server:

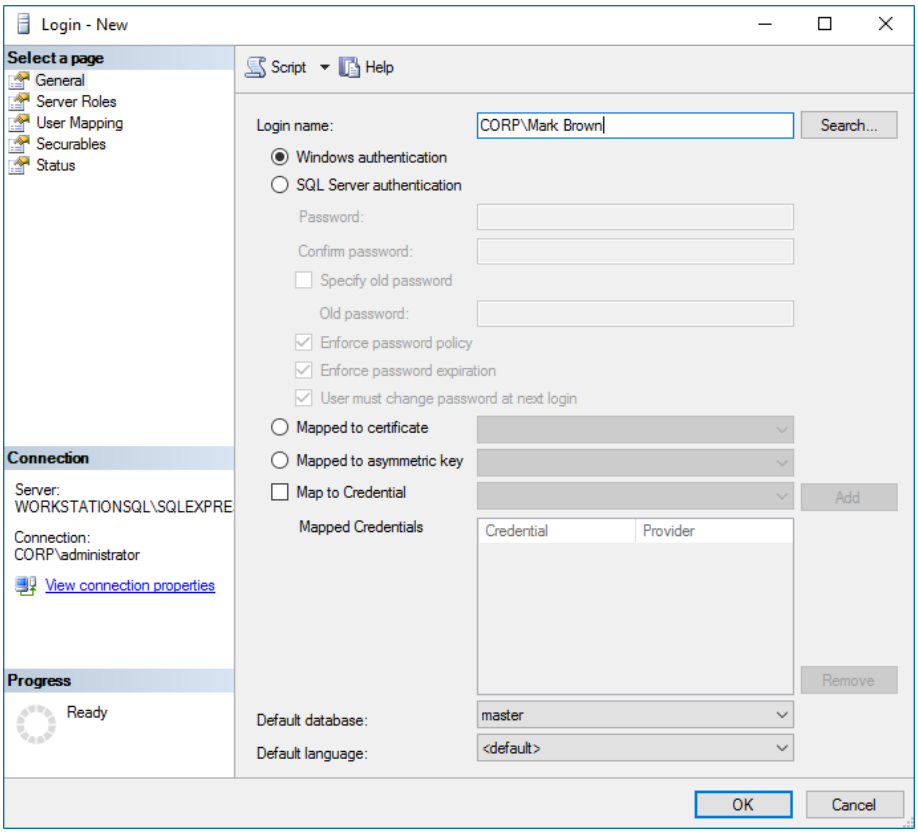
The account must have be a member of the local **Administrators** group.

8.2. 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.

8.3. 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**.

8.3.1. 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**.

8.4. 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:

- Advanced permissions on the folder where the Long-Term Archive is stored:
  - **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**
- On the file shares where report subscriptions are saved:
  - **Change** share permission
  - **Create files / write data** folder permission

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.

9. Uninstall Netwrix Auditor

9.1. 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**.

9.2. 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.

10. 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 and Reporting Services

10.1. 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**.

10.2. 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.

10.3. Install Microsoft SQL Server and Reporting Services

Netwrix Auditor uses Microsoft SQL Server database as short-term data storage and utilizes SQL Server Reporting Services engine for report generation. You can either use your existing SQL Server for these purposes, or deploy a new server instance. System requirements for SQL Server are listed in the corresponding section of this guide.

Consider the following:

1. Supported versions are 2008 and later. Note that SQL Server Reporting Services 2008 is not supported; for this version you should install and configure Reporting Services 2008 R2 or later.
2. Supported editions are Enterprise, Standard and Express with Advanced Services (it includes Reporting Services).
3. If downloading SQL Server Express Edition with Advanced Services from Microsoft site, make sure you download the file whose name contains **SQLEXPRADV**. Otherwise, Reporting Services will not be deployed, and you will not be able to analyze and report on collected data.

By the way of example, this section provides instructions on how to:

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

For detailed information on installing other versions/editions, refer to Microsoft website.

NOTE: Maximum database size provided in SQL Server Express editions may be insufficient for storing data in bigger infrastructures. Thus, when planning for SQL Server, consider maximum database capacity in different editions, considering the size of the audited environment.

10.3.1. Install Microsoft SQL Server 2014 Express

Do the following:

1. Download SQL Server 2014 Express with Advanced Services from Microsoft website. When choosing the required download, make sure you selected the file whose name contains **SQLEXPRADV** - for example, **SQLEXPRADV_x64_ENU.exe**.
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.

10.3.2. Verify Reporting Services Installation

As a rule, Netwrix Auditor can use Reporting Services 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. Navigate to **Start → All Apps → SQL ServerReporting 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)
   - **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 necessary, 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

U

V

W